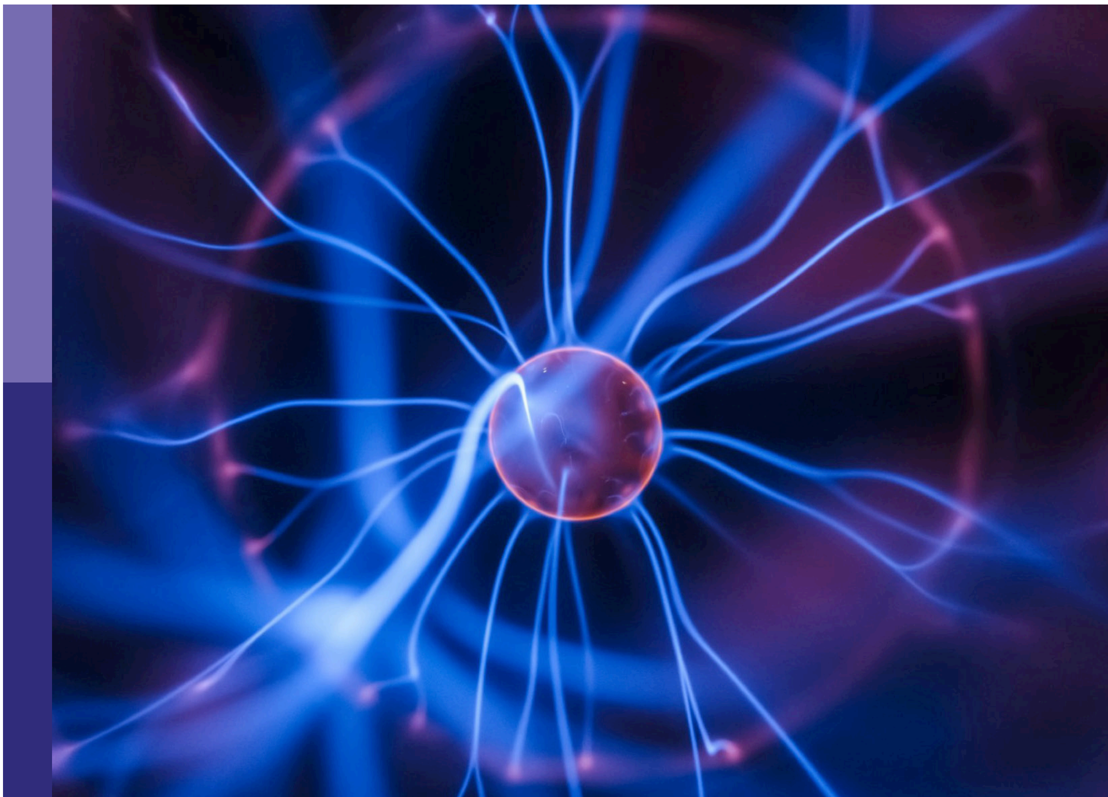
frontiers | Research Topics

Multiparty secure quantum and semiquantum computations

Edited by
Tianyu Ye, Nanrun Zhou, Mingxing Luo,
Amiya Nayak and Xiubo Chen

Published in
Frontiers in Physics



ISSN 1664-8714
ISBN 978-2-8325-3850-0
DOI 10.3389/978-2-8325-3850-0

About Frontiers

Frontiers is more than just an open access publisher of scholarly articles: it is a pioneering approach to the world of academia, radically improving the way scholarly research is managed. The grand vision of Frontiers is a world where all people have an equal opportunity to seek, share and generate knowledge. Frontiers provides immediate and permanent online open access to all its publications, but this alone is not enough to realize our grand goals.

Frontiers journal series

The Frontiers journal series is a multi-tier and interdisciplinary set of open-access, online journals, promising a paradigm shift from the current review, selection and dissemination processes in academic publishing. All Frontiers journals are driven by researchers for researchers; therefore, they constitute a service to the scholarly community. At the same time, the *Frontiers journal series* operates on a revolutionary invention, the tiered publishing system, initially addressing specific communities of scholars, and gradually climbing up to broader public understanding, thus serving the interests of the lay society, too.

Dedication to quality

Each Frontiers article is a landmark of the highest quality, thanks to genuinely collaborative interactions between authors and review editors, who include some of the world's best academicians. Research must be certified by peers before entering a stream of knowledge that may eventually reach the public - and shape society; therefore, Frontiers only applies the most rigorous and unbiased reviews. Frontiers revolutionizes research publishing by freely delivering the most outstanding research, evaluated with no bias from both the academic and social point of view. By applying the most advanced information technologies, Frontiers is catapulting scholarly publishing into a new generation.

What are Frontiers Research Topics?

Frontiers Research Topics are very popular trademarks of the *Frontiers journals series*: they are collections of at least ten articles, all centered on a particular subject. With their unique mix of varied contributions from Original Research to Review Articles, Frontiers Research Topics unify the most influential researchers, the latest key findings and historical advances in a hot research area.

Find out more on how to host your own Frontiers Research Topic or contribute to one as an author by contacting the Frontiers editorial office: frontiersin.org/about/contact

Multiparty secure quantum and semiquantum computations

Topic editors
Tianyu Ye — Zhejiang Gongshang University, China
Nanrun Zhou — Shanghai University of Engineering Sciences, China
Mingxing Luo — Southwest Jiaotong University, China
Amiya Nayak — University of Ottawa, Canada
Xiubo Chen — Beijing University of Posts and Telecommunications (BUPT), China

Citation
Ye, T., Zhou, N., Luo, M., Nayak, A., Chen, X., eds. (2023). *Multiparty Secure quantum and semiquantum computations*. Lausanne: Frontiers Media SA.
doi: 10.3389/978-2-8325-3850-0

Table of contents

TYPE Editorial
PUBLISHED 28 February 2023
DOI 10.3389/fphy.2023.1139505

Editorial: Multiparty secure quantum and semiquantum computations

Tianyu Ye*

Zhejiang Gongshang University, Hangzhou, China

KEYWORDS

multi-party secure quantum and semiquantum computation, multiparty quantum key agreement, multi-party quantum and semiquantum private comparison, multi-party quantum secret sharing, quantum voting, multi-party semiquantum key distribution

Editorial on the Research Topic
Multiparty secure quantum and semiquantum computations

OPEN ACCESS

EDITED BY
Omar Magana-Loaiza,
Louisiana State University, United States

REVIEWED BY
H. Z. Shen,
Northeast Normal University, China

*CORRESPONDENCE
Tianyu Ye,
✉ yetianyu@mail.zjgsu.edu.cn

SPECIALTY SECTION
This article was submitted to Quantum Engineering and Technology,
a section of the journal
Frontiers in Physics

RECEIVED 07 January 2023
ACCEPTED 20 February 2023
PUBLISHED 28 February 2023

CITATION
Ye T (2023), Editorial: Multiparty secure quantum and semiquantum computations.
Front. Phys. 11:1139505.
doi: 10.3389/fphy.2023.1139505

During recent 2 decades, multi-party secure quantum computation and multi-party secure semiquantum computation have successfully attracted the attentions of researchers and have been greatly developed, whose security is decided by the fundamental laws of quantum mechanics, such as the uncertainty principle, the non-orthogonal state indistinguishable theorem, the quantum non-cloning theorem et al. However, there are still important and difficult Research Topic on them need to be solved. This Research Topic aims to show the recent achievements and the future challenges in *Multiparty secure quantum and semiquantum computations*. Research Topic of interest includes: multiparty secure quantum computation, containing multiparty quantum key agreement, multiparty quantum summation, multiparty quantum multiplication, multiparty quantum private comparison, multiparty quantum sealed-bid auction, multiparty quantum voting, multiparty quantum ranking, etc., multiparty secure semiquantum computation, containing multiparty semiquantum key agreement, multiparty semiquantum summation, multiparty semiquantum private comparison, multiparty semiquantum sealed-bid auction, multiparty semiquantum voting, etc., and quantum network and quantum Internet.

There are 18 papers published totally in this Research Topic. In order to solve the problem of generating temporary session key for secure communication in optical-ring quantum networks, an authenticated multiparty quantum key agreement method for optical-ring quantum communication networks was proposed by Gao et al. A novel multi-party quantum private comparison protocol with d-dimensional Bell states was proposed, where a semi-honest quantum third party can determine the size relationship of all participants' privacies without knowing the private information (Wang et al.). A new non-entangled quantum secret sharing protocol among different nodes based on locally indistinguishable orthogonal product states was designed, which promotes the development of quantum secure communication in the future (Fu et al.). In order to solve the problem that most of the quantum voting protocols are impractical due to the currently limited quantum storage capabilities, based on the interference principle of light, a new quantum voting protocol without quantum memory was constructed (Xu et al.). An original multi-party semiquantum key distribution protocol based on hyperentangled Bell states simultaneously in polarization and spatial degrees of freedom was put forward, which enhances the channel capacity (Tian et al.). A semiquantum key distribution protocol which allows one quantum user to distribute two different private secret keys to two classical users respectively at the same time was proposed (Wu et al.). Two joint photon-number splitting attacks against a single-state semiquantum key distribution system were put forward, with which Eve can obtain key information without being detected by Alice or Bob (Mi et al.). A multi-party semiquantum private comparison protocol based on the maximally entangled GHZ-type state was designed, which can compare the equality of *n* parties within one execution of the protocol (Wu et al.). We hope that these research achievements can help promote the developments of multi-party secure quantum computation and multi-party secure semiquantum computation.

Author contributions

This Editorial is written by T Y Ye.

Conflict of interest

The author declares that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Publisher's note

All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers. Any product that may be evaluated in this article, or claim that may be made by its manufacturer, is not guaranteed or endorsed by the publisher.

ORIGINAL RESEARCH
published: 13 July 2022
doi: 10.3389/fphy.2022.962781

Authenticated Multiparty Quantum Key Agreement for Optical-Ring Quantum Communication Networks

Li-Zhen Gao[1], Xin Zhang[2]*, Song Lin[3]*, Ning Wang[2] and Gong-De Guo[2]*

[1]College of Computer Science and Information Engineering, Xiamen Institute of Technology, Xiamen, China, [2]College of Computer and Cyber Security, Fujian Normal University, Fuzhou, China, [3]Digital Fujian Internet-of-Things Laboratory of Environmental Monitoring, Fujian Normal University, Fuzhou, China

Quantum communication networks are connected by various devices to achieve communication or distributed computing for users in remote locations. In order to solve the problem of generating temporary session key for secure communication in optical-ring quantum networks, a quantum key agreement protocol is proposed. In the key agreement protocols, an attacker can impersonate a legal user to participate in the negotiation process and eavesdrop the agreement key easily. This is often overlooked in most quantum key agreement protocols, which makes them insecure in practical implementation. Considering this problem, the function of authenticating the user's identity is added in the proposed protocol. Combining classical hash function with identity information, we design the authentication operation conforming to the characteristics of quantum search algorithm. In the security analysis of the proposed protocol, quantum state discrimination is utilized to show that the protocol is secure against common attacks and impersonation attack. In addition, only single photons need to be prepared and measured, which makes our protocol feasible with existing technology.

Keywords: quantum communication, quantum key agreement, identity authentication, quantum search algorithm, unambiguous state discrimination

OPEN ACCESS

Edited by:
Tianyu Ye,
Zhejiang Gongshang University, China

Reviewed by:
Ma Hongyang,
Qingdao University of Technology,
China
Xiaoping Lou,
Hunan Normal University, China

***Correspondence:**
Xin Zhang
xiao_xin_09@163.com
Song Lin
lins95@gmail.com
Gong-De Guo
ggd@fjnu.edu.cn

Specialty section:
This article was submitted to
Quantum Engineering and
Technology,
a section of the journal
Frontiers in Physics

Received: 06 June 2022
Accepted: 22 June 2022
Published: 13 July 2022

Citation:
Gao L-Z, Zhang X, Lin S, Wang N and
Guo G-D (2022) Authenticated
Multiparty Quantum Key Agreement
for Optical-Ring Quantum
Communication Networks.
Front. Phys. 10:962781.
doi: 10.3389/fphy.2022.962781

1 INTRODUCTION

Communication is the exchange and transmission of information between people in a certain way. With the development of communication technology, people pay more attention to the privacy and security of data. In the present communication networks, RSA public key scheme is widely used for secure communication since it depends on the mathematical problem of large integer decomposition. However, the famous quantum factorization algorithm proposed by Shor [1] shows that this scheme is no longer safe. To ensure the security of communication, the research of quantum cryptography attracts people's attention. In contrast to the security of classical cryptography that are based on the assumption of computational complexity, the security of quantum cryptography relies on quantum-mechanics principles, which makes it unconditionally secure in theory. Since the first quantum key distribution protocol (BB84 protocol) was proposed [2], people try to solve some secure communication tasks with quantum cryptography, including quantum key distribution(QKD) [2–4], and quantum secure direct communication (QSDC) [5–7].

In addition to key distribution, key agreement (KA) is another major method of key establishment and plays a key role in the field of cryptography. In a key agreement protocol, two or more users in communication networks can agree on temporary session keys to achieve secure communication. As a significant cryptographic primitive, key agreement is flexibly used in multiparty secure computing, access control, electronic auctions, and so on. However, as the concept of quantum computer was put forward, classical key agreement was found to be as vulnerable to quantum computation as classical key distribution. Therefore, quantum key agreement (QKA) has been naturally proposed and has recently become a new research hotspot.

In 2004, [8] proposed the first two-party QKA protocol, which was designed based on the correlation of measurement results of EPR pairs. Unfortunately, this protocol is insecure, as shown in Ref. [9]. That same year, [10] proposed a fair and secure two-party QKA protocol based on BB84. Afterwards, researchers expands the number of negotiators from two to multiple parties to fit the actual scenarios. [11] proposed the first multi-party QKA (MQKA) protocol with Bell states and entanglement exchange in 2013. But in the same year, [12] pointed out that the protocol was unfair, then proposed a new MQKA protocol with single photons. Later [13] introduced two unitary operations and proposed the circle-type MQKA to improve the execution efficiency. Since then, many scholars have used various properties of quantum mechanics to design a few subtle MQKA protocols [14,15].

Actually, these protocols are only theoretically secure. Once they are used in practice, they will inevitably encounter the same problem as classical key agreement, namely, the impersonation attack. That is, an attacker may impersonate a legal user to participant in the protocol. Moreover, in classical key agreement protocols [16–19], the authentication of users is usually considered to protect against this particular attack. However, this is often overlooked in QKA. Although in some MQKA protocols, authentication of classical channels has been required to prevent classical messages from being tampered, message authentication is different from identity authentication. Therefore, in designing a secure QKA protocol, the authentication of users should be considered as in other authenticated quantum cryptographic protocols [20–24].

In this paper, an authenticated MQKA protocol for optical-ring quantum networks is proposed. The result shows that when all users perform the protocol honestly, they can get the correct negotiation key simultaneously. According to our analysis, the protocol in the network is secure against both common attacks and impersonation attacks.

2 PRELIMINARIES

2.1 Review of Communication Network

Let us start with a brief review of quantum communication networks. A communication network is a data link in which isolated individuals share resources and communicate through physical connections of various devices. The classical communication networks mainly consists of three parts: transmission, switching and terminal. According to the topological structure, it can be divided into bus, star, tree, ring and mesh types. Evidently, different types of networks are flexibly applied to different scenarios. This also provides the foundation for the study of quantum communication networks.

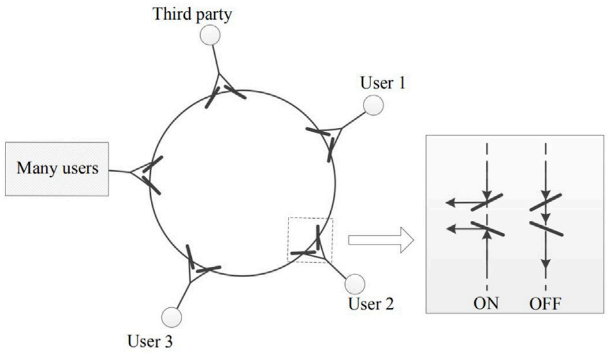


FIGURE 1 | An optical-ring quantum communication network. The third party and users of the network are linked with their loop by the coupled fibers. By the "space optical switch", the photons can be received by the right users.

Similar to classical communication networks, quantum communication networks can be classified into four types in terms of topology, which are: a passive-star network, an optical-ring network, a wavelength-routed network, and a wavelength-addressed bus network [25–27]. Among them, since the optical-ring topology is lower cost in the construction of the network, it is more conducive to promotion and studied by more people. In 2002, [28] have proposed an efficient multiuser quantum communication network, which can realize the QKD between arbitrary two users in the cascaded loop local networks. Inspired by them, we propose a multiparty quantum key agreement protocol in an optical-ring network.

Unlike the scheme of [28], the communication network in this paper only considers one loop, not a cascade. As shown in **Figure 1**, the network consist of three parts. 1) A third party. The third party is to facilitate communication between users on the network. 2) Users. Linked via coupled fibers and distributed in the communication network. 3) Switch. At each node, there is a "space optical switch", which is usually closed. Whenever a session key is required to be established, the photons are transmitted through the optical fiber among all users.

2.2 Review of Quantum Search Algorithm

Let us introduce Grover's search algorithm [29], which is used in the protocol. Suppose that we want to search a target $|\varphi_{mn}\rangle = |mn\rangle$, $m, n \in \{0, 1\}$, in the database of a set of two-qubit states, i.e.,

$$|\tilde{\varphi}_{xy}\rangle = \frac{1}{2}(|0\rangle + (-1)^y|1\rangle)(|0\rangle + (-1)^x|1\rangle), \tag{1}$$

where $x, y \in \{0, 1\}$. In order to search the target, two specific unitary operations need to be performed on $|\tilde{\varphi}_{xy}\rangle$. Namely, the phase reversal operation $U_{mn} = I - 2|\varphi_{mn}\rangle\langle\varphi_{mn}|$ and the amplitude amplification operation $V_{xy} = 2|\tilde{\varphi}_{xy}\rangle\langle\tilde{\varphi}_{xy}| - I$. After executing these two unitary operations, we get

$$V_{xy}U_{mn}|\tilde{\varphi}_{xy}\rangle = |\varphi_{mn}\rangle. \tag{2}$$

In this paper, since the global phase has no effect on results, it can be ignored.

In addition, the unitary operation U_{mn} has two good properties, which have been used to design some quantum cryptographic protocols [30,31]. We suppose that a total of r operations of U_{mn} are performed on a two-qubit state. On the one hand, when the number of r is odd, there is

$$U_{m_r n_r} \cdots U_{m_2 n_2} U_{m_1 n_1} = U_{mn}, \tag{3}$$

where $m = m_1 \oplus m_2 \oplus \cdots \oplus m_r$ and $n = n_1 \oplus n_2 \oplus \cdots \oplus n_r$, the symble $\oplus$ indicates bitwise Exclusive OR. In combination with **Eq. 2**, we know that the deterministic measurements can be obtained by single-particle measurement with basis $MB_Z = \{|0\rangle, |1\rangle\}$ at last. When the number of executions is even, there is

$$U_{m_r n_r} \cdots U_{m_2 n_2} U_{m_1 n_1} |\tilde{\varphi}_{xy}\rangle = |\tilde{\varphi}_{mn}\rangle, \tag{4}$$

where $m = x \oplus m_1 \oplus m_2 \oplus \cdots \oplus m_r$ and $n = y \oplus n_1 \oplus n_2 \oplus \cdots \oplus n_r$. Then, the measurements can be obtained by single-particle measurement with basis $MB_X = \{|+\rangle, |-\rangle\}$.

In our protocol, the user encodes his private input by unitary operation U_{mn}. In addition, to assure that the protocol satisfies the characteristics of Grover's algorithm after identity encoding, we design the identity encoding operations as U_{00} and $U_{01}U_{10}$ respectively. In the protocol, the user always encodes his identity information after private input encoding, that is, the encoded quantum state is $U_{00}U_{mn}|\tilde{\varphi}_{xy}\rangle$ or $U_{01}U_{10}U_{mn}|\tilde{\varphi}_{xy}\rangle$. Furthermore, there exists $U_{m_1 n_1}U_{m_2 n_2} = X_{m_1 \oplus m_2, n_1 \oplus n_2}$. So when the identity encode is U_{00}, the private input stays the same. Otherwise, on the basis of **Eq. 3**, $U_{01}U_{10}U_{mn} = U_{\bar{m}\bar{n}}$, where $\bar{m} = m \oplus 1, \bar{n} = n \oplus 1$, which means the private input is flipped once.

3 QUANTUM KEY AGREEMENT PROTOCOL WITH IDENTITY AUTHENTICATION

Now, let us describe the proposed quantum key agreement protocol for optical-ring quantum communication networks, which can realize the key negotiation between arbitrary N users in the networks. In this network, a third party P_0 is semi-trusted, who can perform the operation U_{mn}. Suppose there are M users in the network and any N of them perform the quantum key agreement. That is, the switches for N users are turned on at the proper time, while the switches for the remaining $M - N$ users are constantly off.

Without loss of generality, assume that the first N users participant in the negotiation, denoted as $P_1, P_2, \ldots, P_N$. They can not only perform the operations U_{mn} and V_{xy}, but also have the ability to prepare and measure single particles. They want to negotiate a session key K with the help of P_0, where $K = S_1 \oplus S_2 \oplus \cdots \oplus S_N$, and S_i is P_i's private input with length of $2n$. Furthermore, each user has an identity information ID_i of length l. In order to ensure the legitimacy of these users' identity, it is necessary for $P_i (i = 1, 2, \ldots, N)$ to complete the identity authentication with P_0, who shares master key $\bar{k}_i$ with P_i.

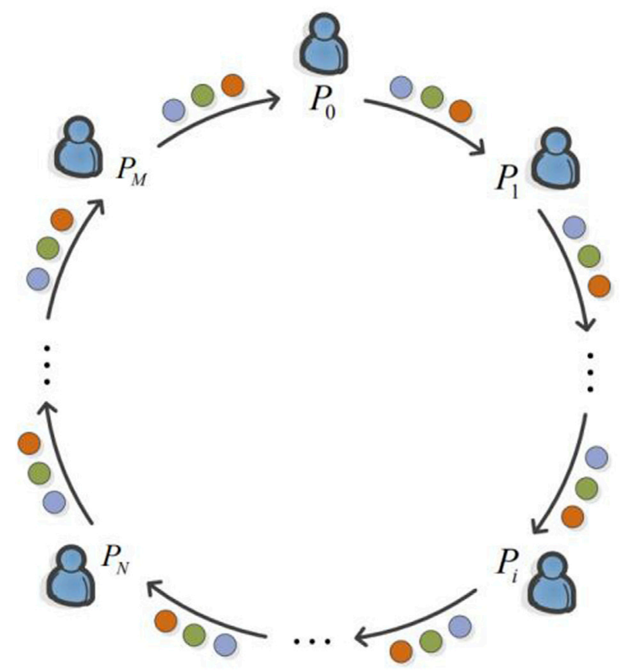


FIGURE 2 | (Color online) The detailed performance of the proposed protocol, in which different colored circles represent the particles prepared by different users.

It should be noted that the switches for $P_N, \ldots, P_M$ are always closed, i.e., photons can be transmitted directly from P_N to P_0. The general process of this protocol is shown in **Figure 2**.

In this quantum communication network, multi parties are connected by a quantum channel and a classical public channel. The quantum channel consists usually of an optical fiber. The classical channel, however, can be any communication link. Users and the third party can send classical messages via the classical channel, and these messages cannot be tampered with by anyone. That is, this transmitted classical message is required to be authenticated. Typically, the public classical channel can be achieved by broadcasting. However, it is worth noting that message authentication is different from identity authentication. So, we still need to verify the identity of each user. In the following, a description of the procedure for the protocol is given.

Step 1: P_0 and $P_i (i = 1, 2, \ldots, N)$ generate a random sequence r_0 and r_i respectively and declare them through the classical channel. Then P_0 selects a hash function f: $2^* \rightarrow 2^n$ and declares it. P_0 and each user calculate their authenticated message $h_i = f_{\bar{k}_i}(ID_i \parallel r_i \parallel r_0)$, where $\parallel$ denotes string concatenation.

Step 2: Each user $P_i (i = 1, 2, \ldots, N)$ generates a random bit sequence $L_i = (l_{i,1}, l_{i,2}, \ldots, l_{i,2n})$ and $B_i = (b_{i,1}, b_{i,2}, \ldots, b_{i,2n})$ with length of $2n$. In the process with P_i as an initiator, an ordered sequence T_i of n two-qubit states is prepared by P_i according to L_i:

$$T_i = \left(|\tilde{\varphi}_{l_{i,1},l_{i,2}}\rangle, |\tilde{\varphi}_{l_{i,3},l_{i,4}}\rangle, \ldots, |\tilde{\varphi}_{l_{i,2n-1},l_{i,2n}}\rangle\right), \tag{5}$$

where, the tth quantum state is $|\tilde{\varphi}_{l_{i,2t-1},l_{i,2t}}\rangle \in \{|\tilde{\varphi}_{00}\rangle, |\tilde{\varphi}_{01}\rangle, |\tilde{\varphi}_{10}\rangle, |\tilde{\varphi}_{11}\rangle\}$.

Step 3: P_i performs the identity encoding operation on the tth quantum state of the sequence T_i according to the values of $h_{i,t}$ and $b_{i,2t-1}$. Concretely, when $h_{i,t} \oplus b_{i,2t-1} = 0$, P_i performs U_{00}; otherwise, he performs $U_{01}U_{10}$. Then the encoded sequence is denoted as $\tilde{T}_{i,i\boxplus 1}$, which is sent to the next user $P_{i\boxplus 1}$ over the quantum channel, where $\boxplus$ ($\boxminus$) represents addition (subtraction) module $N + 1$.

Step 4: At this point, $P_{i\boxplus 1}$ opens his switch to receive the photons emitted by P_i. When $P_{i\boxplus 1}$ receives the sequence $\tilde{T}_{i,i\boxplus 1}$, he will perform corresponding operation to encode his own private input $s_{i\boxplus 1,2t-1}$, $s_{i\boxplus 1,2t}$. Namely, $P_{i\boxplus 1}$ performs the unitary operation $U_{s_{i\boxplus 1,2t-1},s_{i\boxplus 1,2t}}$ on the tth quantum state. After that, $P_{i\boxplus 1}$ performs his identity encoding similar to Step 3, and sends the encoded particle string $\tilde{T}_{i,i\boxplus 2}$ to the user $P_{i\boxplus 2}$.

Step (*g* + 3) (*g* = 2, 3, . . ., *N*): Similar to Steps 4 and 3, $P_{i\boxplus g}$ encodes his private input and identity information. After that, he sends the encoded sequence $\tilde{T}_{i,i\boxplus(g+1)}$ to $P_{i\boxplus(g+1)}$. Notice that P_0 knows the hash values of all users. When the sequence of particles is transmitted to P_0, he calculate $h_{0,t} = \oplus_{i=1}^{N} h_{i,t}$. Based on the result, P_0 performs his identity encoding on the sequence. That is, if $h_{0,t}$ is 0, he performs U_{00}; Otherwise, he performs $U_{01}U_{10}$.

Step (*N* + 4): When all users $P_i(i = 1, 2, \ldots, N)$ receive the sequence $\tilde{T}_{i,i}$ from $P_{i\boxminus 1}$, they publish the random bit string B_i in random order. Then, P_i calculates $B^{2t-1} = \oplus_{i=1}^{N} b_{i,2t-1}\ (t = 1, 2, \ldots, n)$ and performs different operations as shown in follows.

1) When B^{2t-1} is 0, P_i measures the single photon with basis MB_X directly to get the measurement result $|\tilde{\varphi}_{w_{i,2t-1},w_{i,2t}}\rangle$, then he can extract the session key:

$$k_{i,2t-1}k_{i,2t} = s_{i,2t-1}s_{i,2t} \oplus w_{i,2t-1}w_{i,2t} \oplus l_{i,2t-1}l_{i,2t}. \tag{6}$$

2) When B^{2t-1} is 1, according to the classical bit sequence L_i, the unitary operation $V_{l_{i,2t-1},l_{i,2t}}$ is performed on the tth two-qubit state in the quantum sequence, then the particles are measured with basis MB_Z to obtained the result $|\varphi_{w_{i,2t-1},w_{i,2t}}\rangle$. The agreement key is extracted as

$$k_{i,2t-1}k_{i,2t} = s_{i,2t-1}s_{i,2t} \oplus w_{i,2t-1}w_{i,2t} \oplus 11. \tag{7}$$

Obviously, each user P_i can obtain the agreement keys $K_i = (k_{i,1}, k_{i,2}, k_{i,3}, k_{i,4}, \ldots, k_{i,2N-1}, k_{i,2N})$.

Step (*N* + 5): The eavesdropping detection process is executed. Namely, all users choose δn samples to detect whether malicious or forged users exist. Specifically, each user P_i randomly selects $\lfloor \frac{\delta n}{N} \rfloor$ samples from K_i, and declares these samples' positions. Then, he requires the other users $P_j(j \neq i)$ to announce the corresponding part of K_j. Since only legitimate users know the correct hash values and make the hash values satisfy $h_0 \oplus (\oplus_{i=1}^{N} h_{i,t}) = 0$, the users can get a consistent negotiation key by step (N + 4). Afterwards, P_i calculates the error rate according to his $k_{i,m}$ and the other users' $k_{j,m}$. That is, the number of inconsistencies in the sample as a proportion of the total sample size. If the error rate exceeds a certain threshold, the protocol is abandoned. Otherwise, the other users $P_j(j \neq i)$ perform similar actions. It should be noted that there are no common elements in the samples selected by all users. Finally, the remaining particles form their session key.

TABLE 1 | The classical sequences of the example.

	P_1	P_2	P_3
ID_i	010,110	001,101	100,011
r_i	1,100	1,111	0,010
h_i	0,111	1,010	0,101
S_i	01,101,011	01,000,100	10,110,001
L_i	10,001,101	00,110,110	01,101,100
B_i	00,100,100	10,110,010	11,011,110
$B_{i,2t-1} \oplus h_{i,t}$	0,011	0,111	1,110

To illustrate the negotiation process more clearly, we give an example with ($N = 3$, $M = 5$). Similarly, we assume that P_1, P_2 and P_3 are involved in key negotiation and the switches for P_4 and P_5 are always off. In this case, P_1, P_2 and P_3 respectively hold secret inputs with length of 8 (i.e. n = 4), S_1 = 01,101,011, S_2 = 01,000,100, and S_3 = 10,110,001 and identity information with length of 6, ID_1 = 010,110, ID_2 = 001,101, ID_3 = 100,011. By the following steps, they can agree on a session key, $K = S_1 \oplus S_2 \oplus S_3$.

In Step 1, each user $P_i(i = 1, 2, 3)$ gets the random string r_i. In addition, P_0 generates r_0. Then, they can obtain the hash values h_i according to the selected hash function. In the next step, P_1(P_2, P_3) generates two random 8-bit strings L_1 and B_1 (L_2 and B_2, L_3 and B_3). From L_1(L_2, L_3), P_1(P_2, P_3) prepares the single photons to obtain the two-particle sequence T_1(T_2, T_3). The concrete values of these classical bit sequences are listed in **Table 1**.

After that, they proceed to the encoding phase of the protocol. The process with P_1 as the initiator is described in detail, where the sequence T_1 is back to P_1 after being encoded by all users. Concretely, in Step 3, P_1 performs the unitary operations $U_{00} \otimes U_{00} \otimes U_{01}U_{10} \otimes U_{01}U_{10}$ to encode his identity information. Afterwards, P_1 transmits the encoded sequence $\tilde{T}_{1,2}$ to P_2. When P_2 receives the sequence from P_1, he encodes his private input and identity information by performing unitary operations in Step 4, and sends to P_3. Similarly, P_3 also performs encoding operations. It is worth noting that the sequence $\tilde{T}_{1,0}$ sent from P_3 to P_0 passes through P_4 and P_5. When P_0 receives the sequence, he calculates h_0 = 1,000, which means his operations are $U_{01}U_{10} \otimes U_{00} \otimes U_{00} \otimes U_{00}$. After that, P_0 sends the encoded sequence to P_1. Obviously, the transmission process of particle sequences, which are prepared by P_2 and P_3, is similar to the above process. The variations of quantum states in three sequences are shown in **Table 2**. In Step 7, when all users receive the travelling particles $\tilde{T}_{1,1}, \tilde{T}_{2,2}, \tilde{T}_{3,3}$, they make the random strings B_i public in random order. P_1 (P_2, P_3) calculates B^{2t-1} = 0,010. Therefore, P_1 (P_2, P_3) performs $I \otimes I \otimes V_{11} \otimes I$ ($I \otimes I \otimes V_{01} \otimes I, I \otimes I \otimes V_{11} \otimes I$). After that, they measure with appropriate measurement basis. By corresponding calculation, they get K_1, K_2, K_3 respectively. Apparently, if there is no eavesdropping, $K_1 = K_2 = K_3$ = 10,011,110.

4 ANALYSIS OF THE PROTOCOL

For a quantum key agreement protocol, it is generally required to satisfy correctness and security, regardless of the structure of the communication network. That is, all users can get the correct

TABLE 2 | Change of the particle sequences during the encoding phase of the three-user protocol.

	P_1	P_2	P_3
T_i	$\lvert\tilde{\varphi}_{10}\rangle\otimes\lvert\tilde{\varphi}_{00}\rangle\otimes\lvert\tilde{\varphi}_{11}\rangle\otimes\lvert\tilde{\varphi}_{01}\rangle$	$\lvert\tilde{\varphi}_{00}\rangle\otimes\lvert\tilde{\varphi}_{11}\rangle\otimes\lvert\tilde{\varphi}_{01}\rangle\otimes\lvert\tilde{\varphi}_{10}\rangle$	$\lvert\tilde{\varphi}_{01}\rangle\otimes\lvert\tilde{\varphi}_{10}\rangle\otimes\lvert\tilde{\varphi}_{11}\rangle\otimes\lvert\tilde{\varphi}_{00}\rangle$
$\tilde{T}_{i,i\boxplus 1}$	$U_{00}\lvert\tilde{\varphi}_{10}\rangle\otimes U_{00}\lvert\tilde{\varphi}_{00}\rangle\otimes\lvert\tilde{\varphi}_{00}\rangle\otimes\lvert\tilde{\varphi}_{10}\rangle$	$U_{00}\lvert\tilde{\varphi}_{00}\rangle\otimes\lvert\tilde{\varphi}_{00}\rangle\otimes\lvert\tilde{\varphi}_{10}\rangle\otimes\lvert\tilde{\varphi}_{01}\rangle$	$\lvert\tilde{\varphi}_{10}\rangle\otimes\lvert\tilde{\varphi}_{01}\rangle\otimes\lvert\tilde{\varphi}_{00}\rangle\otimes U_{00}\lvert\tilde{\varphi}_{00}\rangle$
$\tilde{T}_{i,i\boxplus 2}$	$U_{01}\lvert\tilde{\varphi}_{10}\rangle\otimes\lvert\tilde{\varphi}_{11}\rangle\otimes U_{10}\lvert\tilde{\varphi}_{00}\rangle\otimes U_{11}\lvert\tilde{\varphi}_{10}\rangle$	$\lvert\tilde{\varphi}_{01}\rangle\otimes U_{00}\lvert\tilde{\varphi}_{00}\rangle\otimes U_{11}\lvert\tilde{\varphi}_{10}\rangle\otimes\lvert\tilde{\varphi}_{00}\rangle$	$\lvert\tilde{\varphi}_{01}\rangle\otimes U_{00}\lvert\tilde{\varphi}_{01}\rangle\otimes U_{00}\lvert\tilde{\varphi}_{00}\rangle\otimes\lvert\tilde{\varphi}_{00}\rangle$
$\tilde{T}_{i,i\boxplus 3}$	$\lvert\tilde{\varphi}_{10}\rangle\otimes U_{00}\lvert\tilde{\varphi}_{11}\rangle\otimes\lvert\tilde{\varphi}_{01}\rangle\otimes U_{10}\lvert\tilde{\varphi}_{10}\rangle$	$\lvert\tilde{\varphi}_{10}\rangle\otimes\lvert\tilde{\varphi}_{00}\rangle\otimes\lvert\tilde{\varphi}_{01}\rangle\otimes U_{00}\lvert\tilde{\varphi}_{00}\rangle$	$\lvert\tilde{\varphi}_{00}\rangle\otimes U_{10}\lvert\tilde{\varphi}_{01}\rangle\otimes\lvert\tilde{\varphi}_{01}\rangle\otimes U_{00}\lvert\tilde{\varphi}_{00}\rangle$
$\tilde{T}_{i,i}$	$\lvert\tilde{\varphi}_{01}\rangle\otimes\lvert\tilde{\varphi}_{11}\rangle\otimes U_{00}\lvert\tilde{\varphi}_{01}\rangle\otimes\lvert\tilde{\varphi}_{00}\rangle$	$\lvert\tilde{\varphi}_{11}\rangle\otimes\lvert\tilde{\varphi}_{10}\rangle\otimes U_{01}\lvert\tilde{\varphi}_{01}\rangle\otimes\lvert\tilde{\varphi}_{00}\rangle$	$\lvert\tilde{\varphi}_{01}\rangle\otimes\lvert\tilde{\varphi}_{00}\rangle\otimes U_{10}\lvert\tilde{\varphi}_{01}\rangle\otimes\lvert\tilde{\varphi}_{11}\rangle$

session key by executing the protocol. Security, on the other hand, implies that no attacker can obtain any information about the session key without being detected. Analysis shows that it can resist not only common external and internal attacks, but also impersonation attack.

4.1 Correctness

Obviously, with the example of three users in previous section, we can easily know that the session keys obtained by all users are equal. In this section, we will give a more rigorous proof to give a more convincing conclusion.

Without loss of generality, the session key derived from the tth quantum state is taken as an example. That is, we discuss whether or not the following equation holds:

$$k_{1,2t-1}k_{1,2t} = k_{2,2t-1}k_{2,2t} = \cdots = k_{N,2t-1}k_{N,2t}. \tag{8}$$

In the protocol, in order to obtain $k_{1,2t-1}k_{1,2t}$, P_1 prepares the initial quantum state $|\tilde{\varphi}_{l_{1,2t-1},l_{1,2t}}\rangle$ in Step 2. After that, P_1 and the other users perform their encoding operations on that quantum state in turn. For the sake of simplicity, let the identity of P_i be $O_{i,t}$, where, $O_{i,t} = h_{i,t} \oplus b_{i,2t-1}$ when $i \neq 0$; $O_{0,t} = h_{0,t} = \oplus_{j=1}^{N} h_{j,t}$ when $i = 0$. Thus, in step $(N + 4)$, the quantum state received by P_1 is in:

$$U_{O_{0,t}}U_{O_{N,t}}U_{s_{N,2t-1},s_{N,2t}}\cdots U_{O_{3,t}}U_{s_{3,2t-1},s_{3,2t}}U_{O_{2,t}}U_{s_{2,2t-1},s_{2,2t}}U_{O_{1,t}}|\tilde{\varphi}_{l_{1,2t-1},l_{1,2t}}\rangle. \tag{9}$$

In the protocol, when $O_{i,t} = 0$, $U_{O_{0,t}} = U_{00}$; when $U_{O_{i,t}} = 1$, $U_{O_{i,t}} = U_{01}U_{10}$. Then, the parity times of the unitary operations U_{xy} performed by the users are

$$C = O_{1,t} \oplus O_{2,t} \oplus\cdots\oplus O_{N,t} \oplus O_{0,t}. \tag{10}$$

By calculation, we get

$$C = \oplus_{i=1}^{N} b_{i,2t-1}. \tag{11}$$

Obviously, $C = B^{2t-1}$. So, in the protocol, the users can get the number of operations performed on the quantum state by calculating B^{2t-1}. Where, when $C = 0$, the unitary operation is executed an even number of times; otherwise, it is executed an odd number of times.

Due to the good reciprocity of the unitary operation U_{xy}, **Eq. 9** can be rewritten as:

$$U_{O_{0,t}}U_{O_{N,t}}\cdots U_{O_{3,t}}U_{O_{2,t}}U_{O_{1,t}}U_{s_{N,2t-1},s_{N,2t}}\cdots U_{s_{3,2t-1},s_{3,2t}}U_{s_{2,2t-1},s_{2,2t}}|\tilde{\varphi}_{l_{1,2t-1},l_{1,2t}}\rangle. \tag{12}$$

In addition, since $U_{xy}U_{xy} = I$, the identity encoding operation $U_{O_{0,t}}U_{O_{N,t}}\cdots U_{O_{3,t}}U_{O_{2,t}}U_{O_{1,t}}$ has the following conclusion. When $C = 0$, there are

$$U_{O_{0,t}}U_{O_{N,t}}\cdots U_{O_{3,t}}U_{O_{2,t}}U_{O_{1,t}} = I. \tag{13}$$

When $C = 1$, we get:

$$U_{O_{0,t}}U_{O_{N,t}}\cdots U_{O_{3,t}}U_{O_{2,t}}U_{O_{1,t}} = U_{11} \textit{ or } U_{01}U_{10}. \tag{14}$$

So, **Eq. 12** is equivalent to

$$U_{s_{N,2t-1},s_{N,2t}}\cdots U_{s_{2,2t-1},s_{2,2t}}|\tilde{\varphi}_{l_{1,2t-1},l_{1,2t}}\rangle, \tag{15}$$

and

$$U_{11}U_{s_{N,2t-1},s_{N,2t}}\cdots U_{s_{2,2t-1},s_{2,2t}}|\tilde{\varphi}_{l_{1,2t-1},l_{1,2t}}\rangle, \tag{16}$$

or

$$U_{01}U_{10}U_{s_{N,2t-1},s_{N,2t}}\cdots U_{s_{2,2t-1},s_{2,2t}}|\tilde{\varphi}_{l_{1,2t-1},l_{1,2t}}\rangle. \tag{17}$$

Therefore, the user P_1 can perform different operations to extract the session key depending on the number of unitary operations.

As mentioned in Step $(N + 4)$ of the protocol, when the number of unitary operations is even, according to **Eq. 4**, P_1 directly measures the quantum state as in **Eq. 15** with MB_X to obtain $|\tilde{\varphi}_{w_{1,2t-1},w_{1,2t}}\rangle$. From **Eq. 6**, we can obtain

$$\begin{aligned} k_{1,2t-1}k_{1,2t} &= s_{1,2t-1}s_{1,2t} \oplus w_{1,2t-1}w_{1,2t} \oplus l_{1,2t-1}l_{1,2t} \\ &= s_{1,2t-1}s_{1,2t} \oplus s_{2,2t-1}s_{2,2t} \oplus\cdots\oplus s_{N,2t-1}s_{N,2t}. \end{aligned} \tag{18}$$

When the number of unitary operations is odd, according to **Eqs. 2** and **3**, P_1 needs to perform the unitary operation $V_{l_{1,2t-1},l_{1,2t}}$ on the quantum state of **Eq. 16** or **Eq. 17**, and then use MB_Z to obtain the result $|\varphi_{w_{1,2t-1},w_{1,2t}}\rangle$. In terms of **Eq. 7**, the agreement key is extracted as follows.

$$\begin{aligned} k_{1,2t-1}k_{1,2t} &= s_{1,2t-1}s_{1,2t} \oplus w_{1,2t-1}w_{1,2t} \oplus 11 \\ &= s_{1,2t-1}s_{1,2t} \oplus s_{2,2t-1}s_{2,2t} \oplus\cdots\oplus s_{N,2t-1}s_{N,2t}. \end{aligned} \tag{19}$$

Apparently, the agreement key is the sum of the private inputs of all users regardless of whether the number of operations is odd or even. Similarly, the quantum state $|\tilde{\varphi}_{l_{i,2t-1},l_{i,2t}}\rangle$ prepared by user P_i is obtained after being encoded by other users as

$$U_{O_{i\boxminus 1,t}}U_{s_{i\boxminus 1,2t-1},s_{i\boxminus 1,2t}}U_{O_{0,t}}U_{O_{N,t}}U_{s_{N,2t-1},s_{N,2t}}\cdots U_{O_{i\boxplus 1,t}}U_{s_{i\boxplus 1,2t-1},s_{i\boxplus 1,2t}}U_{O_{i,t}}|\tilde{\varphi}_{l_{i,2t-1},l_{i,2t}}\rangle. \tag{20}$$

In the same way, the user P_i can obtain

$$\begin{aligned} k_{i,2t-1}k_{i,2t} &= s_{i,2t-1}s_{i,2t} \oplus w_{i,2t-1}w_{i,2t} \oplus l_{i,2t-1}l_{i,2t} \\ &= s_{1,2t-1}s_{1,2t} \oplus s_{2,2t-1}s_{2,2t} \oplus\cdots\oplus s_{N,2t-1}s_{N,2t}. \end{aligned} \tag{21}$$

or

$$\begin{aligned} k_{i,2t-1}k_{i,2t} &= s_{i,2t-1}s_{i,2t} \oplus w_{i,2t-1}w_{i,2t} \oplus 11 \\ &= s_{1,2t-1}s_{1,2t} \oplus s_{2,2t-1}s_{2,2t} \oplus \cdots \oplus s_{N,2t-1}s_{N,2t}. \end{aligned} \tag{22}$$

From **Eqs. 18** and **21** or **Eqs. 19** and **22**, it is shown that all users receive the same agreement key, i.e., **Eq. 8** holds. Therefore, the proposed protocol is correct.

4.2 Security

In this section, we analyze the security of the proposed protocol in the optical-ring quantum communication network. It not only proves that the protocol is secure against common external attacks and internal attacks, but also proves that impersonation attacks are also ineffective for this protocol.

4.2.1 External Attacks

Assuming Eve is an external attacker, who may try her best to eavesdrop on the private input S_i, the session key K or the master key $\bar{k}_i$ without being detected. Next, we will discuss these three cases.

Case 1: Eavesdropping user's private input.

In the proposed protocol, each user has a private input. Since the private input constitutes the final session key, it is evident that it should be kept secret from others. Subsequently, we discuss that how Eve eavesdrops on the secret input of users.

During the process of the protocol, each user performs three operations: particle preparation, encoding private input and identity information, and single-particle measurement. Obviously, the disclosure of users' private inputs only occurs after the encoding operations. So, Eve's attacks mainly take place in the transmission of the particle sequence. In the following, we will consider two common attacks: intercept-resend attack and entangle-measure attack.

Intercept-resend attack. Eve firstly intercepts the particle sequence sent from P_j, and measures it. Based on the measurements, Eve re-prepares the sequence to send to $P_{j\boxplus 1}$. In this way, Eve hopes to obtain the private input without being detected. However, this is impossible. In the protocol, the carrier particles after different encoding operation numbers belong to two sets of non-orthogonal states, which are in

$$\{|++\rangle, |+-\rangle, |-+\rangle, |--\rangle\}, \tag{23}$$

or

$$\left\{\frac{1}{2}(|00\rangle - |01\rangle - |10\rangle - |11\rangle), \frac{1}{2}(|00\rangle - |01\rangle + |10\rangle + |11\rangle), \frac{1}{2}(|00\rangle + |01\rangle - |10\rangle + |11\rangle), \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle - |11\rangle)\right\}, \tag{24}$$

where, the second set can be converted into $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$ after the unitary operation V_{xy}. The identity encoding of user is determined by both hash values h_j and random numbers B_j. Until step $(N+4)$ of the protocol, Eve does not know the value of B_j. Therefore, she can only perform random operations to obtain the information. That is, she randomly chooses the measurement base. Evidently, the probability that Eve selects a right measurement basis is approximately 50%. Then, a fake particle string is prepared and sent to $P_{j\boxplus 1}$ based on the measurement results. In this case, Eve introduces an error with a probability of $(\frac{1}{2}*\frac{3}{4}) = \frac{3}{8}$. Hence, this attack can be easily detected in step $(N+5)$. In a word, Eve cannot get user's private input without being detected in this way.

Entangle-measure attack. Assuming that Eve wants to perform the entangle-measure attack, she can intercept the travelling sequence prepared by $P_{j\boxminus 1}$, and apply entangling operation U_E between her own ancillary particles and the intercepted particles. At last, she transmits the particles to P_j. P_j just encodes his private input and identity information directly in the particles. Afterwards, the encoding sequence is transmitted to $P_{j\boxplus 1}$, at which point Eve intercepts again. Then, she measures the ancillary particles to infer the private input S_j.

Without loss of generality, the effect of Eve's unitary operation U_E can be shown as

$$U_E|\alpha\rangle|E\rangle = |00\rangle|e_{00}\rangle + |01\rangle|e_{01}\rangle + |10\rangle|e_{10}\rangle + |11\rangle|e_{11}\rangle, \tag{25}$$

where, $|e_{00}\rangle$, $|e_{01}\rangle$, $|e_{10}\rangle$, $|e_{11}\rangle$ are pure states determined by U_E. The quantum state in the sequence intercepted by Eve again is shown in **Table 3**.

By simply calculating, we get the correlation between these eight states

$$\begin{aligned} |\alpha_7\rangle &= |\alpha_0\rangle + |\alpha_4\rangle - |\alpha_3\rangle \\ &= |\alpha_1\rangle + |\alpha_5\rangle - |\alpha_3\rangle \\ &= |\alpha_2\rangle + |\alpha_6\rangle - |\alpha_3\rangle. \end{aligned} \tag{26}$$

Obviously, there is a linear correlation between the quantum states after different coding operations. As Chefles and Barnett [32] said, the necessary and sufficient condition for distinguishing the quantum states is linear independence. Therefore, these linearly correlated quantum states cannot be unambiguous discriminated, which means Eve cannot obtain the private input S_j through the entangle-measure attack.

Case 2: Eavesdropping the session key.

Here, we discuss whether Eve is able to eavesdrop on the session key K. Since $K = S_1 \oplus S_2 \oplus \cdots \oplus S_N$, Eve can generally use two methods to obtain the value of K. One is that Eve tries to eavesdrop each value of S_i to infer the agreement key. However, from the analysis of Case 1, we know that Eve cannot succeed. The other method involves directly eavesdropping on the value of K. According to the analysis above, we know that Eve is unable to distinguish between two linearly correlated sets of quantum states. So, Eve will always be detected if the number of encoding operations is unknown. Then, what if she was directly involved in the protocol? Namely, she might execute the impersonation attack.

In this protocol, a semi-trusted third party, P_0, is introduced to help these parties accomplish this task. So, Eve may impersonates P_0 (called $\hat{P}_0$) to attack the protocol. In **Section 4.2.2**, we prove that a genuine P_0 cannot attain the session key. So, we could deduce directly that $\hat{P}_0$ is also unable to eavesdrop successfully. Hence, in this section, we focus on the second case. Namely, Eve wants to disguise herself as one user to execute the protocol with

TABLE 3 | Quantum states after different encoding operations on the entangling state.

	xy* ⊕ *mn	**Encoded Quantum State**
Odd times encoding $U_{xy}\|\tilde{\varphi}_{mn}\rangle$	00	$\|\alpha_0\rangle = \frac{1}{2}(\|00\rangle\|e_{00}\rangle - \|01\rangle\|e_{01}\rangle - \|10\rangle\|e_{10}\rangle - \|11\rangle\|e_{11}\rangle)$
	01	$\|\alpha_1\rangle = \frac{1}{2}(\|00\rangle\|e_{00}\rangle - \|01\rangle\|e_{01}\rangle + \|10\rangle\|e_{10}\rangle + \|11\rangle\|e_{11}\rangle)$
	10	$\|\alpha_2\rangle = \frac{1}{2}(\|00\rangle\|e_{00}\rangle + \|01\rangle\|e_{01}\rangle - \|10\rangle\|e_{10}\rangle + \|11\rangle\|e_{11}\rangle)$
	11	$\|\alpha_3\rangle = \frac{1}{2}(\|00\rangle\|e_{00}\rangle + \|01\rangle\|e_{01}\rangle + \|10\rangle\|e_{10}\rangle - \|11\rangle\|e_{11}\rangle)$
Even times encoding $X_{xy}\|\tilde{\varphi}_{mn}\rangle$	00	$\|\alpha_4\rangle = \frac{1}{2}(\|00\rangle\|e_{00}\rangle + \|01\rangle\|e_{01}\rangle + \|10\rangle\|e_{10}\rangle + \|11\rangle\|e_{11}\rangle)$
	01	$\|\alpha_5\rangle = \frac{1}{2}(\|00\rangle\|e_{00}\rangle + \|01\rangle\|e_{01}\rangle - \|10\rangle\|e_{10}\rangle - \|11\rangle\|e_{11}\rangle)$
	10	$\|\alpha_6\rangle = \frac{1}{2}(\|00\rangle\|e_{00}\rangle - \|01\rangle\|e_{01}\rangle + \|10\rangle\|e_{10}\rangle - \|11\rangle\|e_{11}\rangle)$
	11	$\|\alpha_7\rangle = \frac{1}{2}(\|00\rangle\|e_{00}\rangle - \|01\rangle\|e_{01}\rangle - \|10\rangle\|e_{10}\rangle + \|11\rangle\|e_{11}\rangle)$

others. Suppose Eve impersonates P_j (called $\hat{P}_j$). $\hat{P}_j$ prepares the quantum carriers, and hopes attain the K_{-P_j}, that is, the negotiation key of other users except P_j. In fact, this action can be detected by the authentication in step $(N + 5)$. As $\bar{k}_j$ is only known to the valid user P_j and P_0, $\hat{P}_j$ cannot calculate correct hash value h_j. Because of the special relationship between hash values, $h_0 = \oplus_{i=1}^{N} h_i$, as long as any one h_j is error, this relationship is broken. Consequently, the quantum states will be changed, and the measurement using the measurement basis determined by B^{2t-1} will result in random results. In other words, her impersonation was discovered. Therefore, the proposed protocol is secure against such attack.

Case 3: Eavesdropping the master key.

We discuss whether it is possible for Eve to eavesdrop on the master key $\bar{k}_i$. $\bar{k}_i$ is shared only by users P_i and P_0 and is related to the hash value h_i. In the proposed protocol, the public information is identity ID_i, random string r_i, and hash function f. Evidently, Eve cannot infer $\bar{k}_i$ from these public information. So, she wants to infer $\bar{k}_i$ from h_i. However, P_i does not disclose h_i. In the protocol, users decide the identity operation with h_i and B_i. Even if the user announces the random string in step $(N + 4)$, Eve does not have access to any information about $\bar{k}_i$ for $B^{2t-1} = \oplus_{i=1}^{N-1} b_{i,2t-1}$, independent of h_i.

4.2.2 Internal Attacks

Compared with external attackers, internal parties have greater capacity since they are involved in the execution of the protocol. In the following, we will discuss some attacks of users.

Case 1: Dishonest users' collusion attacks.

In the case of a single dishonest user, even if he participates in the protocol, he cannot obtain the hash values of other parties from the information he knows. Therefore, he can be detected in step $(N + 5)$ just like an external attacker. It is important to note that there is more than one dishonest user in a protocol, and the most serious case is only one honest user. Obviously, in this case, all dishonest users want to conspire to eavesdrop the private input of the only honest party and determine the final key K. If the protocol is secure in the extreme case, it is secure in others. Next, we will discuss this situation.

Since P_0 is semi-trusted in the protocol, he cannot conspire with others. When P_j is the only honest one, other dishonest users will attack P_0 and P_j. For simplicity, let us take the example of three users ($N = 3$, $M = 3$). The users P_1 and P_3 in particular position are assumed to be dishonest, denoted as P_1^* and P_3^*. The running process of the example is shown in **Figure 3**. The attack will be performed in the following ways.

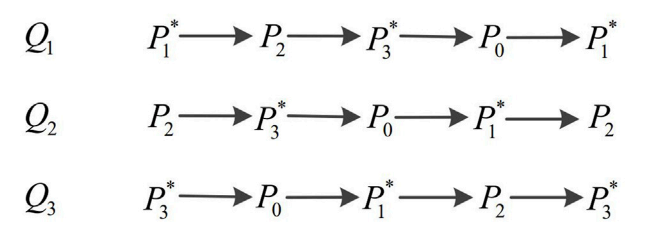

Q_1 $P_1^* \rightarrow P_2 \rightarrow P_3^* \rightarrow P_0 \rightarrow P_1^*$
Q_2 $P_2 \rightarrow P_3^* \rightarrow P_0 \rightarrow P_1^* \rightarrow P_2$
Q_3 $P_3^* \rightarrow P_0 \rightarrow P_1^* \rightarrow P_2 \rightarrow P_3^*$

FIGURE 3 | Running process of the example, Q_i represents the process in which the initiator is P_i.

For one thing, we discuss the attack on P_0, where the dishonest users wish to obtain the hash value h_0. Through the above protocol, we know $h_0 = h_1 \oplus h_2 \oplus h_3$, which means it is determined by hash values of other users. In this case, since P_1^* and P_3^* conspired, they could know both h_1 and h_3. In spite of this, they could only know $h_1 \oplus h_3 = h_0 \oplus h_2$, but unable to determine the specific h_0 and h_2. Eventually, they have to obtain the information through the negotiation process. However, even P_1^* and P_3^* conspired, no matter what kind of attack they use, the deterministic information about h_0 could not be obtained. Because the encoded quantum states are nonorthogonal, they cannot be perfectly distinguished.

For another, we discuss the attack on P_2, in which the dishonest users wish to obtain the identity information h_2, the private input S_2, or determine the final key. Since P_1^* and P_3^* failed to attack P_0, it is impossible to determine whether the specific h_2 is 0 or 1. Next, we discuss attacks during the protocol process. Evidently, there is no information about S_2 is disclosed during Q_2 in **Figure 3**. In the encoding process Q_3, P_2 encodes his own information in the last stage of transmission. Since these three transmission processes are actually synchronized, it is obvious that P_1^* and P_3^* cannot encode the pre-negotiated message in Q_3 to determine the final key. So the most likely attack to obtain S_2 and determine the final key occurs in Q_1. In the transmission process of Q_1, P_1^* prepares and encodes n two-qubit particles, represented as $\tilde{T}_{1,2}$. Then, he sends them to P_2 and shares all his information with P_3^*. Since P_3^* does not know whether $h_2 \oplus b_2$ is 0 or 1, he does not know whether the particles should be measured with basis MB_X directly or basis MB_Z after the operation V. Therefore, he

TABLE 4 | Comparison of several multi-party QKA protocols.

	Communication Network Type	Identity Authentication	Decoy Particles	Quantum Source	Particle Efficiency
[31]	Optical-ring	No	Yes	Single photon	$\eta = \frac{1}{(\delta N+1)N}$
[15]	Optical-ring	No	No	Entangled particles	$\eta = \frac{1}{2N^2}$
The proposed protocol	Optical-ring	Yes	No	Single photon	$\eta = \frac{2-\delta}{3N}$

can only get random results like an external attacker. To sum up, the proposed protocol is immune to this attack.

Case 2: A semi-trusted third party's attack.

Here, P_0 is semi-trusted. That is, he cannot conspire with others, but misbehave on his own. For clarity, we represent the dishonest third party as P_0^*. P_0^* wishes to obtain P_j's private input S_j or the session key K. Apparently, he has the advantage of knowing h_j. However, in this protocol, the user decides what kind of identity operation to perform through the value $h_j \oplus b_j$. Even if P_0^* knows each person's hash value, he would not be able to get the correct operation information before step $(N+4)$. In addition, due to the non-cloning theorem, it is impossible for P_0^* to preserve the quantum state without knowing about it. Therefore, this protocol is secure against the attack by a semi-trusted third party.

Case 3: A dishonest user's impersonation attack.

Users may also carry out impersonation attack in addition to the attacks described above. His purpose is to determine the agreement key by himself, and succeed in cheating others to accept this fake key. Even if P_i is part of the protocol, he cannot perform correct identity encoding operation without knowing P_j's hash value. Because the master key $\bar{k}_j$ is only shared by P_j and P_0. Just like the impersonation attack by external attacker, the measurement result is random, which is difficult to pass the detection in step $(N+5)$. Therefore, a forged user cannot participate in the protocol and determine the session key without being detected.

Based on the above analysis, we prove that the protocol in the context of quantum networks is secure.

4.3 Efficiency

In this section, we will discuss the particle efficiency of the proposed protocol. According to [33], the particle efficiency is defined as

$$\eta = \frac{c}{q+b}, \tag{27}$$

where, c is the length of the final shared key string, q is the number of qubits transmitted in the quantum channel, and b is the number of classical bits transmitted for decoding. In our scheme, the length of the final shared key is $(2-\delta)n$, the number of transmitted qubits is n^*N, and the number of transmitted classical bits is $2n^*N$. Therefore, the particle efficiency of the proposed protocol is

$$\eta = \frac{2-\delta}{3N}. \tag{28}$$

Without considering the detection of particles, the particle efficiency of the example presented in this paper is $\eta = \frac{2}{3^*3} = 22.2\%$.

Compared with [31] and [15], although they both perform multi-user quantum key agreement in an optical-ring communication network, there are differences in the specific negotiation process. **Table 4** shows that our protocol is preferable as its readily accessible quantum resource, good security and high efficiency.

5 CONCLUSION

Before presenting our conclusion, we briefly discuss the hash function used in the protocol. In the protocol, we use the hash value to complete the authentication of the user. Only the legitimate user knows the correct hash value. In the absence of an impersonation attack, the hash values satisfy $h_0 = \oplus_{i=1}^{N} h_i$. So the selection criteria of the measurement basis is correct. Moreover, the hash values are not public. No one can obtain valid information from known information. Therefore, the introduction of classical hash function does not reduce the security of the protocol. Even if the classical hash function is corrupted by quantum computation, each user's master key is still secure. Since the master key is only shared by the third party and users through QKD, it can achieve absolute security. In addition, the security analysis shows that no matter what kind of attacks are used, the master key cannot be obtained by attackers. In this way, the shared master key can be reused and the user's identity can be authenticated, which greatly improves the practicability of the protocol.

In this paper, we study an authenticated quantum key agreement protocol, which is another main key establishment method in addition to quantum key distribution. This scheme enables key negotiation for any N users in optical-ring quantum networks. Each user in the protocol has his own identity information and shares a master key with a semi-trusted third party. With the help of the third party, they can simultaneously obtain the negotiated key. Security analysis shows that the protocol is secure against common attacks and impersonation attack. Furthermore, the implementation of the protocol only requires preparing and measuring single particles, which can be easily implemented with current technology. And, our method can be easily applied to other MQKA protocols with authentication in quantum networks, so that they can resist impersonation attack in practical. Since the implementation of the protocol is inevitably affected by noise, the threshold value for the error rate should be provided before implementing it. As mentioned in [34], the exact value of the threshold is determined by a variety of practical elements, such as the desired level of security, the noise level of channels, etc. Therefore, choosing an appropriate threshold is complex, which is also the case for many multi-party quantum cryptographic protocols. Combined with quantum state discrimination, we will study this issue in the future.

DATA AVAILABILITY STATEMENT

The original contributions presented in the study are included in the article/supplementary material, further inquiries can be directed to the corresponding authors.

AUTHOR CONTRIBUTIONS

All authors listed have made a substantial, direct, and intellectual contribution to the work and approved it for publication.

REFERENCES

1. Shor PW. Polynomial-time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. *SIAM J Comput* (1997) 26:1484–509. doi:10.1137/S0097539795293172
2. Bennett CH, Brassard G. Quantum Cryptography: Public Key Distribution and coin Tossing. In: Proc IEEE Int Conf Comput, Syst and Signal Process. Manhattan, New York: IEEE (1984). p. 175–9.
3. Gisin N, Ribordy G, Tittel W, Zbinden H. Quantum Cryptography. *Rev Mod Phys* (2002) 74:145–95. doi:10.1103/RevModPhys.74.145
4. Schwonnek R, Goh KT, Primaatmaja IW, Tan EYZ, Wolf R, Scarani V, et al. Device-independent Quantum Key Distribution with Random Key Basis. *Nat Commun* (2021) 12:1–8. doi:10.1038/s41467-021-23147-3
5. Long GL, Liu XS. Theoretically Efficient High-Capacity Quantum-Key-Distribution Scheme. *Phys Rev A* (2002) 65:032302. doi:10.1103/PhysRevA.65.032302
6. Sun Z, Song L, Huang Q, Yin L, Long G, Lu J, et al. Toward Practical Quantum Secure Direct Communication: A Quantum-memory-free Protocol and Code Design. *IEEE Trans Commun* (2020) 68:5778–92. doi:10.1109/TCOMM.2020.3006201
7. Zhang H, Sun Z, Qi R, Yin L, Long G-L, Lu J. Realization of Quantum Secure Direct Communication over 100 Km Fiber with Time-Bin and Phase Quantum States. *Light Sci Appl* (2022) 11:1–9. doi:10.1038/s41377-022-00769-w
8. Zhou N, Zeng G, Xiong J. Quantum Key Agreement Protocol. *Electron Lett* (2004) 40:1149–50. doi:10.1049/el:20045183
9. Tsai CW, Chong SK, Hwang T. Comment on "quantum Key Agreement Protocol with Maximally Entangled States". *Proc 20th Crypt Info Secur Conf* (2010) 2010:47–9.
10. Chong SK, Hwang T. Quantum Key Agreement Protocol Based on Bb84. *Opt Commun* (2010) 283:1192–5. doi:10.1016/j.optcom.2009.11.007
11. Shi RH, Zhong H. Multi-party Quantum Key Agreement with Bell States and Bell Measurements. *Quan Inf Process* (2013) 12:921–32. doi:10.1007/s11128-012-0443-2
12. Liu B, Gao F, Huang W, Wen QY. Multiparty Quantum Key Agreement with Single Particles. *Quan Inf Process* (2013) 12:1797–805. doi:10.1007/s11128-012-0492-6
13. Sun ZW, Zhang C, Wang BH, Li Q, Long DY. Improvements on "multiparty Quantum Key Agreement with Single Particles". *Quan Inf Process* (2013) 12: 3411–20. doi:10.1007/s11128-013-0608-7
14. Sun Z, Yu J, Wang P. Efficient Multi-Party Quantum Key Agreement by Cluster States. *Quan Inf Process* (2016) 15:373–84. doi:10.1007/s11128-015-1155-1
15. Lin S, Zhang X, Guo GD, Wang LL, Liu XF. Multiparty Quantum Key Agreement. *Phys Rev A* (2021) 104:042421. doi:10.1103/PhysRevA.104.042421
16. Ateniese G, Steiner M, Tsudik G. Authenticated Group Key Agreement and Friends. In: Proceedings of the 5th ACM Conference on Computer and Communications Security (1998). p. 17–26. doi:10.1145/288090.288097
17. Teng J, Wu C, Tang C. An Id-Based Authenticated Dynamic Group Key Agreement with Optimal Round. *Sci China Inf Sci* (2012) 55:2542–54. doi:10.1007/s11432-011-4381-x
18. Zhang L, Wu Q, Qin B, Domingo-Ferrer J. Identity-based Authenticated Asymmetric Group Key Agreement Protocol. In: *Int Comput Combinatorics Conf.* Berlin, Heidelberg: Springer (2010). p. 510–9. doi:10.1007/978-3-642-14031-0_54
19. Chen Q, Wu T, Hu C, Chen A, Zheng Q. An Identity-based Cross-Domain Authenticated Asymmetric Group Key Agreement. *Information* (2021) 12: 112–2489. doi:10.3390/info12030112
20. Zeng G, Zhang W. Identity Verification in Quantum Key Distribution. *Phys Rev A* (2000) 61:022303. doi:10.1103/PhysRevA.61.022303
21. Shi BS, Li J, Liu JM, Fan XF, Guo GC. Quantum Key Distribution and Quantum Authentication Based on Entangled State. *Phys Lett A* (2001) 281:83–7. doi:10.1016/S0375-9601(01)00129-3
22. Mihara T. Quantum Identification Schemes with Entanglements. *Phys Rev A* (2002) 65:052326. doi:10.1103/PhysRevA.65.052326
23. Wang Y, Lou X, Fan Z, Wang S, Huang G. Verifiable Multi-Dimensional (T,n) Threshold Quantum Secret Sharing Based on Quantum Walk. *Int J Theor Phys* (2022) 61:1–17. doi:10.1007/s10773-022-05009-w
24. Lou X, Wang S, Ren S, Zan H, Xu X. Quantum Identity Authentication Scheme Based on Quantum Walks on Graphs with Ibm Quantum Cloud Platform. *Int J Theor Phys* (2022) 61:1–15. doi:10.1007/s10773-022-04986-2
25. Kumavor PD, Beal AC, Yelin S, Donkor E, Wang BC. Comparison of Four Multi-User Quantum Key Distribution Schemes over Passive Optical Networks. *J Lightwave Technol* (2005) 23:268.
26. Elkouss D, Martinez-Mateo J, Ciurana A, Martin V. Secure Optical Networks Based on Quantum Key Distribution and Weakly Trusted Repeaters. *J Opt Commun Netw* (2013) 5:316–28. doi:10.1364/JOCN.5.000316
27. Fröhlich B, Dynes JF, Lucamarini M, Sharpe AW, Yuan Z, Shields AJ. A Quantum Access Network. *Nature* (2013) 501:69–72. doi:10.1038/nature12493
28. Xue P, Li CF, Guo GC. Conditional Efficient Multiuser Quantum Cryptography Network. *Phys Rev A* (2002) 65:022317. doi:10.1103/PhysRevA.65.022317
29. Grover LK. Quantum Mechanics Helps in Searching for a Needle in a Haystack. *Phys Rev Lett* (1997) 79:325–8. doi:10.1103/PhysRevLett.79.325
30. Hsu LY. Quantum Secret-Sharing Protocol Based on Grover's Algorithm. *Phys Rev A* (2003) 68:022306. doi:10.1103/PhysRevA.68.022306
31. Cao H, Ma W. Multiparty Quantum Key Agreement Based on Quantum Search Algorithm. *Sci Rep* (2017) 7:45046. doi:10.1038/srep45046
32. Chefles A, Barnett SM. Optimum Unambiguous Discrimination between Linearly Independent Symmetric States. *Phys Lett A* (1998) 250:223–9. doi:10.1016/S0375-9601(98)00827-5
33. Cabello A. Quantum Key Distribution in the Holevo Limit. *Phys Rev Lett* (2000) 85:5635–8. doi:10.1103/PhysRevLett.85.5635
34. Scarani V, Bechmann-Pasquinucci H, Cerf NJ, Dušek M, Lütkenhaus N, Peev M. The Security of Practical Quantum Key Distribution. *Rev Mod Phys* (2009) 81:1301–50. doi:10.1103/RevModPhys.81.1301

FUNDING

This work was supported by the National Natural Science Foundation of China (Grants Nos. 61,772,134, 61,976,053 and 62,171,131), Fujian Province Natural Science Foundation (Grant No. 2022J01186), the research innovation team of Embedded Artificial Intelligence Computing and Application at Xiamen Institute of Technology (KYTD202003), and the research innovation team of Intelligent Image Processing and Application at Xiamen Institute of Technology (KYTD202101).

Conflict of Interest: The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Publisher's Note: All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers. Any product that may be evaluated in this article, or claim that may be made by its manufacturer, is not guaranteed or endorsed by the publisher.

frontiers | Frontiers in Physics

TYPE Original Research
PUBLISHED 15 August 2022
DOI 10.3389/fphy.2022.981225

Check for updates

OPEN ACCESS

EDITED BY
Tianyu Ye,
Zhejiang Gongshang University, China

REVIEWED BY
Tingting Song,
Jinan University, China
Hao Cao,
Anhui Science and Technology University, China
Liyun Hu,
Jiangxi Normal University, China

*CORRESPONDENCE
Hong-Yang Ma,
hongyang_ma@aliyun.com

SPECIALTY SECTION
This article was submitted to Quantum Engineering and Technology, a section of the journal Frontiers in Physics

RECEIVED 29 June 2022
ACCEPTED 06 July 2022
PUBLISHED 15 August 2022

CITATION
Wang H-W, Cao Q, Xue Y-J, Ding L, Liu H-Y, Dong Y-M and Ma H-Y (2022), Determining quantum topological semion code decoder performance and error correction effectiveness with reinforcement learning.
Front. Phys. 10:981225.
doi: 10.3389/fphy.2022.981225

Determining quantum topological semion code decoder performance and error correction effectiveness with reinforcement learning

Hao-Wen Wang [1], Qian Cao [1], Yun-Jia Xue [1], Li Ding [1], Han-Yang Liu [1], Yu-Min Dong [2] and Hong-Yang Ma [3]*

[1]School of Information and Control Engineering, Qingdao University of Technology, Qingdao, China,
[2]School of Computer and Information Science, Chongqing Normal University, Chongqing, China,
[3]School of Sciences, Qingdao University of Technology, Qingdao, China

Quantum error correction technology is a vital method to eliminate noise during the operation of quantum computers. To solve the problem caused by noise, in this paper, reinforcement learning is used to encode defects of Semion codes, and the experience replay technique is used to realize the design of decoder. Semion codes are quantum topological error correction codes with the same symmetry group $\mathbb{Z}_2$ as Kitaev toric codes, we used the topological characteristics of error correction codes to map qubits to multi-dimensional space, and error correction accuracy of the decoder is calculated to be 77.5%. Calculate the threshold of topological quantum Semion code, depending on the code distance, resulting in different thresholds, $p_{threshold}$ = 0.081574 when the code distance is d = 3, 5, 7 and threshold $p_{threshold}$ = 0.09542 when the code distance is d = 5, 7, 9. And we design the $\mathbb{Q}$-network to optimize the cost of quantum circuit gates and compare the size of the cost reduction under different thresholds. Reinforcement learning is an important method for designing Semion code decoders and optimizing numerical values, providing more general error models and error correction codes for future machine engineering decoders.

KEYWORDS

quantum error correction technology, topological quantum semion code, reinforcement learning, decoder performance, qubit overhead

1 Introduction

Quantum computing and quantum information have made tremendous progress over the years, and technologies based on quantum communication and quantum error correction (QEC) are developing rapidly [1–4]. The robustness of quantum memory to outer noise and noise removal is an extremely significant resource for quantum fault tolerance [5–9]. Among quantum memories, Among quantum memories, Kitaev toric code [10] is the first proposed topological torus code, which is a simple two-dimensional lattice gauge theory with the $\mathbb{Z}_2$ gauge group. A double-Semion model is a model with the same gauge group theory as Kiteav but with not the same topological properties [11,12]. Although the double Semion model and Kitaev have the same standard set, there are some differences. Double Semion codes weave two elementary quasiparticle excitations that will give ± i phase, showing the statistic of anyons, while Kitaev toric codes only give a ±1 phase factor. The topological order provides a wide range of new topological codes with non-Pauli stabilizers, such as error correction codes: Semion code, which is topologically ordered, respect the stabilizer formalism, but due to Pauli X and Pauli Z existing in the square operator, it is not Pauli's code, it can not be represented as a tensor product of Pauli matrices, so it is not Calderbank-Shor-Steane (CSS) code [13].

Threshold is an effective means of characterizing fault tolerance performance. Specifically, when the physical error rate of qubits is lower than a certain threshold, quantum error correction can be applied to perform effective quantum computing, and the logical error rate can be suppressed to an arbitrarily low level. Due to the fragile nature of quantum information, future universal quantum computers could diagnose syndromes based on the logic qubits of stabilizers. To prevent error propagation and logical failures, a decoder needs to be designed that provides a set of recovery operations to correct errors given a specific syndrome, must include the corresponding error statistics [13] for any given syndrome, and must account for the defects of the syndrome due to measurement errors of the stabilizer, requiring QEC. At present, there are many decoders designed based on topological codes, not only toric codes [14,15], but also color codes [16,17]. The logical qubit is composed of a large number of entangled physical qubits. It can prevent local disturbance caused by errors such as bit flips when the logic operation requires global changes.

Reinforcement learning (RL) combined with deep learning has achieved great success in many fields [18–20]. Techniques from machine learning have begun to find applications in various fields of quantum physics and to fast solve decoding problems [21–23], decoders of many kinds of neural networks have been proposed, although such methods have obvious advantages, it promises extremely fast decoding times, flexibility relative to underlying code and noise models, and the ability to scale to large code distances, there is room for improvement and application. At present, there are many decoders designed based on toric codes and color codes [24,25], but few decoders based on Semion code are involved. Although the performance of our proposed decoder is not better than the current decoder, its value lies in the show that it is feasible to implement the design of Semion code using RL. The paper studies a decoder to find the optimal error correction strategy for quantum topological Semion codes. In the field of quantum computing, it is necessary to try to measure the logical errors generated by the decoder given the syndrome, and to detect the logical errors generated by the decoder through intelligent algorithms. We apply deep learning to quantum computing, decoding for future universal self-training devices provides ideas.

The following contents are arranged as follows. In Section 2, a brief background on quantum topological Semion codes and RL. In Section 3, an algorithm was designed for quantum topological Semion codes. In Section 4, analysis of error correction performance, and conclude in Section 5.

2 Background

2.1 Quantum topological semion code

The double Semion model plays a principal role in the fields of gapped systems and new topological orders [26], and the Semion code is an error correction code that needs to be studied in depth in topological codes. Semion code is a QEC code with the characteristics of the double Semion model. The Semion code has a topological protection effect on quantum information and will not affect the global error due to local errors. Semion code is a non-CSS and non-Pauli topological code described as a hexagonal lattice Λ. We map the qubits in three-dimensional space and use the topology of the code to convert qubits into qubits in multi-dimensional space. The edges represent physical qubits and the vertices represent stabilizer operators. The vertex operator is represented by V_Q, and vertex Q is represented as shown in Figure 1(1), and the Pauli Z operator is represented as:

$$V_Q = Z_i Z_j Z_k \tag{1}$$

Plaquette operator is represented by P_G, and apply the Pauli X operator on the sides of the hexagon:

$$P_G = \prod_{k\in\partial G} X_k \sum_{\vec{j}} p_G(\vec{j})|\vec{j}\rangle\langle\vec{j}| \tag{2}$$

$\vec{j}$ in the above formula represents the bit string of a state on the basis of calculation, ∂G belongs to the edge of the plaquette boundary, the value of $p_G(\vec{j})$ is $\{\pm1, \pm i\}$. The diagonal operator $\sum_{\vec{j}} p_G(\vec{j})|\vec{j}\rangle\langle\vec{j}|$ acts on the twelve qubits in Figure 1(2).

2.2 Reinforcement learning

RL problems consider an agent that interacts with the environment [27]. The agent can manipulate and observe parts and perform a sequence of actions to accomplish a particular problem. Through RL, we can find the optimal policy of the action subject in the system. The optimal policy is the policy that proxies the best return in the process of interacting with the system. Discrete problems are usually considered. At each time step t, the environment can be represented by a state $s_t \in S$, where S is the state space. Given

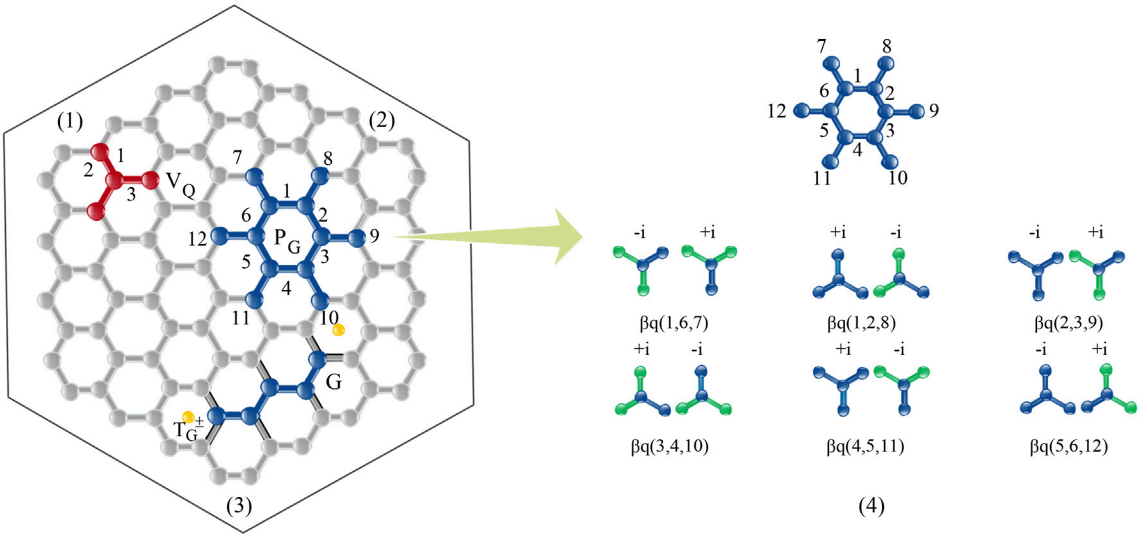


FIGURE 1
Hexagonal lattice diagram, the outermost hexagonal frame is only for aesthetics and does not represent a bounded hexagonal diagram. (1) Vertex operator V_Q. (2)Plaquette operator P_G, the plaquette operator not only includes the blue hexagon, but also the outputting legs connecting the hexagon. (3)The path G of the positive or negative chirality string operator $T_G^{\pm}$ is represented by the blue path, the connecting line represents the $T_G^{\pm}$ support $Conn(G)$, and the yellow dots represent a pair of vertex excitations generated at the endpoints of the path G. (4)Phase factor diagram expanded from (2).

a state, the agent can choose to perform an action $a_t \in A$, where A is the action space. According to the result after the agent selects the action, the state is updated accordingly, entering a new state s_{t+1}, and providing the agent with feedback on the action selection in the form of reward r_{t+1}, starting from time t, the return $R_t = r_{t+1} + \lambda r_{t+1} + \lambda^2 r_{t+1} + \cdots$, where $\lambda \leq 1$ is the discount factor that quantifies how one wants to value immediate and subsequent returns [28]. There will be a constant return $r = 1$ for each step. To formalize the agent's decision-making process, we define the agent's policy as π, and $\pi(a, s)$ is the probability that the agent chooses $a_t = a$ when the state is in $s_t = s$. By using a measure of discounted cumulative reward, the value of any given state depends not only on immediate rewards from that state following a particular policy but also on expected rewards in the future.

3 Algorithmic process

3.1 Explore semion code

As shown in Figure 1(4), the subscript q runs over the vertices belonging to the plaquette G. β_q can be represented by twelve qubits as

$$\begin{aligned}\Sigma_{q\in G}\beta_q &= i^{n_7^+}\left(n_1^+n_6^- - n_1^-n_6^+\right) i^{n_8^-}\left(n_1^-n_2^- - n_1^+n_2^+\right)\\ &= i^{n_9^-}\left(n_2^+n_3^+ - n_2^-n_3^-\right) i^{n_{10}^+}\left(n_3^-n_4^+ - n_3^+n_4^-\right)\\ &= i^{n_{11}^-}\left(n_4^-n_5^- - n_4^+n_5^+\right) i^{n_{12}^-}\left(n_5^+n_6^+ - n_5^-n_6^-\right)\end{aligned} \tag{3}$$

and

$$n_i^{\pm} = \frac{1}{2}(1 \pm Z_i) \tag{4}$$

According to the above analysis, $p_G(\vec{j})$ can be clearly defined as

$$\sum_j p_G(\vec{j})|\vec{j}\rangle\langle\vec{j}| = \prod_{k\in\partial G}(-1)^{n_{k-1}^- n_k^+}\prod_{q\in G}\beta_q \tag{5}$$

Therefore, according to the above reasoning, we add β_q to P'_G on each vertex, and we can obtain a P'_G expression that conforms to the entire Hilbert space.

$$P'_G = \prod_{k\in\partial G} X_k \prod_{k\in\partial G}(-1)^{n_{k-1}^- n_k^+} \tag{6}$$

P'_G satisfies the commutate [29] principle of the operator, and the plaquette operator allows the definition based on stability topological error-correcting code in agent form.

The same as the string operator in Kitaev toric code, T^Z in Semion code is expressed as a string operator that generates grid excitation [30], that is, T^Z is a string of Z operators. Each stabilizer commutes with these operators except the grid operator at the end of the string, and the string X produces the string operator of the vertex excitation, as shown in Figure 1(3). We commute the characters on the path G. The string is marked as T_G^+ and is supported by coon. T_G^+ can only act on the coon set of qubits non-trivially. According to the constraints: (1)The square of the string operator is 1. (2)It must be determined by exchanging with the stabilizer. The system of linear equations can be withdrawn from $F(\vec{j})$,

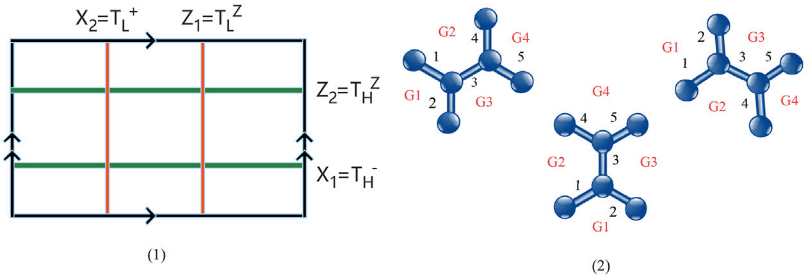


FIGURE 2
(1)Uncomplicated example of two sets of logical operators on a torus, with arrows denoting the identified boundaries. (2)The three possible edge orientations on the X operator can be applied. The qubit marked 3 is influenced in any case, in addition to this, it may leave flux excitations on the four surrounding plaquettes labeled by *G1*, *G2*, *G3*, *G4*.

$$F(\vec{j}) = F(\vec{j} \oplus \vec{i}) \tag{7}$$

the qubit of $F(\vec{j})$ in $Coon(G)$ [11] is 0, and the ⊕ sign represents the sum of the remainder of the bit string to Z. The value of $F(\vec{j})$ is $\{\pm 1, \pm i\}$. So the string T_G^+ is:

$$T_G^+ = \prod_{k \in G} X_k \sum_j F(\vec{j}) |\vec{j}\rangle\langle\vec{j}| \tag{8}$$

The quasiparticle vertex excitation behavior generated by T_G^+ is the same as that of anyons.

The positive chirality string is defined as T^+, the negative chirality string is T^-, and the negative chirality string can be got by calculating the T^Z string operator, that is, $T^- = T^Z T^+$. The operator commutes with the Z operator, and the Z operator and $T^\pm$ do not commute. In conclusion, the commutation principle to be followed is:

$$[T^\pm, T^\pm] = 0, [T^\mp, T^\pm] = 0, [T^Z, T^\pm] = 0 \tag{9}$$

The Hamiltonian is used as the coding space, Semion codes are alike to Kitaev toric codes, with vertex and plaquette operators. Embedding the Semion code in Kitaev toric code results in two quantum memories with logical qubits. The logical operator consists of T_L^+ and T_H^+, $H(L)$ is any homogeneous non-trivial path in the horizontal (vertical) direction, and the other pair logical operator is T_L^- and T_H^-, which are non-self-intersecting or overlapping the composition of each path is shown in Figure 2(1). Two logical qubits of the code require two pairs of logical operators, which are defined as X_1 and X_2:

$$X_1 = T_H^-, Z_1 = T_L^Z, X_2 = T_L^+, Z_2 = T_H^Z \tag{10}$$

The set of these operators satisfies the inverse relationship. The hexagonal lattice makes the distance of the X operator twice that of the Z operator, which can better avoid errors. To perform error correction, the stabilizers have to be measured periodically, and the excitations have to be annihilated by bringing them together using the string operators.

3.2 Build noise models

The error-correcting ability [31] of QEC codes depends on the type and strength of qubit manager errors [32–34]. In the context of topological codes, two error models have been extensively studied, namely depolarizing noise and independent bit-flip and phase errors. In the depolarizing noise model, each qubit has an error according to the following probability $(1-p_{error})$ for no error, and $\frac{p_{error}}{3}$ for X, Y, and Z errors. p_{error} is a parameter between 0 and 1. The model is symmetric between X, Y, Z.

In the independent bit-flip and phase errors, each qubit will be affected by the error, we record the probability of X error, Y error, and Z error as p_{XYZ}, so the probability of error is $p_{error} = 2p_{XYZ} - p_{XYZ}^2$. As shown in Table 1.

Assuming that the X operator is applied to a qubit, for three possible edge orientations, the probability of a syndrome error can be obtained, with the "+" sign indicating the excitation on a given plaquette. Table 2 shows the probabilities of calculating a given flux pattern, corresponding to Figure 2(2).

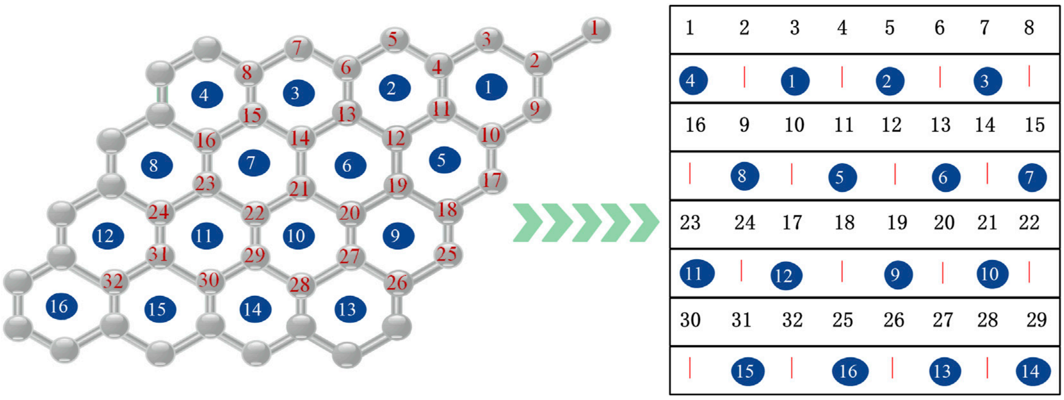
Consider that the error operator of the n-qubit Pauli operator is E. In the stabilizer, errors are detected by measuring the stabilizer generator. If no errors occur, these measurements will output +1 eigenvalues. If an error E occurs, the same as The stabilizer generator against E commutation will output −1, and the output of the stabilizer measurement is the error syndrome. To correct the error, the inverse operator of the error is applied, and in the case of the self-inverse Pauli error, the same operator can be applied [35,36]. The main task of error correction is to determine the correction operator to apply to a given syndrome. The decoder is designed to give an error model and output a correction operator after analyzing the probabilities of all possible errors consistent with the observed syndrome. The optimal decoder is to choose the most suitable correction chain, and this choice will depend heavily on the specific error model.

TABLE 1 Error model.

Noise model	X error	Y error	Z error
Depolarizing noise	$\frac{p_{error}}{3}$	$\frac{p_{error}}{3}$	$\frac{p_{error}}{3}$
Independent bit-flip and phase errors	$2p_{XYZ} - p_{XYZ}^2$	$2p_{XYZ} - p_{XYZ}^2$	$2p_{XYZ} - p_{XYZ}^2$

TABLE 2 Different probabilities of plaquette excitation.

T (*G*1, *G*2, *G*3, *G*4)	Orientation (a)	Orientation (b)	Orientation (c)
(+ + ++)	$\frac{1}{16}$	$\frac{1}{16}$	$\frac{1}{16}$
(− − ++)	$\frac{1}{16}$	$\frac{1}{16}$	$\frac{1}{16}$
(− + −+)	$\frac{1}{16}$	$\frac{1}{16}$	$\frac{1}{16}$
(+ −−+)	$\frac{1}{16}$	$\frac{9}{16}$	$\frac{1}{16}$
(− + +−)	$\frac{1}{16}$	$\frac{1}{16}$	$\frac{1}{16}$
(+ − +−)	$\frac{1}{16}$	$\frac{1}{16}$	$\frac{1}{16}$
(+ + −−)	$\frac{1}{16}$	$\frac{1}{16}$	$\frac{1}{16}$
(− −−−)	$\frac{9}{16}$	$\frac{1}{16}$	$\frac{9}{16}$



1	2	3	4	5	6	7	8
4	|	1	|	2	|	3	|
16	9	10	11	12	13	14	15
|	8	|	5	|	6	|	7
23	24	17	18	19	20	21	22
11	|	12	|	9	|	10	|
30	31	32	25	26	27	28	29
|	15	|	16	|	13	|	14

FIGURE 3
Lattice transformation square diagram. The left picture is a schematic diagram of a hexagonal lattice. The numbers with blue circles represent half calculations. There are 16 symbols in total, the red numbers are vertex operators, and there are 32 in total. The figure on the right is a converted square lattice. The numbers with blue circles represent plaquette operators, and red "|" represents the spatial structure. Extra values do not have any meaning, other numbers are vertices. In the previous figure, letters were used to represent vertices and plaquette operators. Due to the large number here, we use numbers to represent.

3.3 Convert to square form

Embed the Semion code into the torus. We improved it and used the Ref. [37] programming framework to map the hexagonal lattice of Semion code to square, Ref. [11] provided an idea for our conversion process. As shown in Figure 3, the left picture is a schematic diagram of a hexagonal lattice, the numbers with blue circles represent half calculations, there are sixteen symbols in total, the red numbers are vertex operators, and there are thirty-two in total. The data outside of the square is the period filling used, which shows the periodic boundary condition of the Semion code. The figure on the right is a converted square lattice, and the numbers with blue circles represent plaquette operators. The "|" in the figure is to ensure hexagonal space structure. Its value is always recorded as zero and does not correspond to any element measured by the stabilizer. The numbers in the blue circles represent companion calculations. Letters were used to represent vertices and plaquette operators, when the code distance is d, there are $2d^2$ vertices and d^2 plaquettes, so there are $3d^2$ stabilizers in total. Map the Semion code into a square and choose $d = 4$, so a square image of 8×8 is obtained. We assume that vertex and plaquette operators are marked from right to left and top to bottom. The syndrome of vertex s corresponds to the $W_{k,m}$ of an image element, where k and m are expressed as follows:

$$k = 2 \times \left\lfloor \frac{q-1}{2d} \right\rfloor + 1 \tag{11}$$

$$m = mod\left(q - 1 + (1 - 2d)\left\lfloor \frac{q-1}{2d} \right\rfloor, 2d\right) + 1 \tag{12}$$

The syndrome of plaquette G corresponds to the $W_{k,m}$ of the image element, where k and m are expressed as follows:

$$k = 2 \times \left\lfloor \frac{G-1}{2d} \right\rfloor + 2 \tag{13}$$

$$m = mod\left(2G + (1 - 4d)\left\lfloor \frac{G-1}{d} \right\rfloor, 2d\right) + 1 \tag{14}$$

3.4 Emulate semion codes decoder

Quantum computers are affected by the noise of the external environment, which makes the operations perform defects. Therefore, an error correction mechanism is needed to improve the defects. The decoding algorithm needs to count the homology of each particle to restore topological information [6,38]. Stabilizer code allows errors to be detected by measuring stable code operators without changing the encoding information and correcting errors by performing recovery operations [39]. If the encoding task has a specific structure, the decoding task can be easier to handle, and an efficient decoder with better performance can be obtained. The topological code stabilizer is geometrically local, and the abnormal return value indicates that some qubits have errors [40]. Local errors can be detected and corrected by encoding quantum information in a non-local manner. Error syndromes consist of measurements of non-trivial stabilizer operators, and syndrome analysis can infer what errors have occurred and how to correct them.

Using the $\mathbb{Q}$ function to represent the action-value function of a set of actions and the cumulative reward of the corresponding transition, update the estimate of $\mathbb{Q}$ using the formula:

$$\mathbb{Q}(s,a) + \delta\left[\left(r + \lambda max_{a'}\mathbb{Q}(s',a')\right) - \mathbb{Q}(s,a)\right] \rightarrow \mathbb{Q}(s,a) \tag{15}$$

where $\delta < 1$ is the learning rate. The action-value function $\mathbb{Q}(s,a)$ represents the payoff of taking action a in state s and following a certain strategy at π. In the next step of $\mathbb{Q}$-learning, $\mathbb{Q}(s,a) = r + \lambda max_{a'}\mathbb{Q}(s',a')$ is used to quantify $\mathbb{Q}$, $s \rightarrow s'$ is the optimal policy to follow for the current estimate of $\mathbb{Q}$. The policy is given by $\max_a \mathbb{Q}(s,a)$ taking action a will eventually converge to the optimal policy, and it is quite useful to follow the ε-greedy policy, which takes the optimal action for the estimate of $\mathbb{Q}(s,a)$ with probability $(1 - \varepsilon)$, but take a random action with probability ε. For a large state-action space, it is impossible to store a complete action-value function. In deep $\mathbb{Q}$-learning, a deep neural network is used to represent the action-value function. The input layer is the representation of a certain state, and the output layer is possible the value of the action, using $\mathbb{Q}(s,a,\theta)$ to denote the parameterization of the $\mathbb{Q}$-function by the neural network, and θ to denote the network's complete set of weights and biases.

The RL decoder used is the evaluation of the capability of generated action by an agent through reinforcement information provided by the environment, without telling the agent how to generate corrective action. Since the outer environment offers a little piece of information, an agent must learn through experience. It learns a mapping from the environment state to the behavior so that the selected behavior can get the maximum reward of the environment, and the system dynamically adjusts the parameters. To achieve the maximum enhancement signal. In a larger state-action space, it is impossible to save a complete action-value function, using depth $\mathbb{Q}$-learning, a deep neural network represents the action-value function, and the input layer represents a specific state. The output layer is the value of some earthly actions. This simulation part uses a neural network-based decoder [41,42], uses RL methods to optimize the observation of Semion code syndrome, and gradually proposes the recovery chain of a syndrome.

Training of decoder adopts deep $\mathbb{Q}$-network algorithm, which uses experience playback technology to store experience gained by an agent in the form of a conversion tuple in-memory buffer. A specific process is to first send syndrome to an agent in the action part, according to the defect of $\mathbb{Q}$-network, select action store results in a buffer in the form of a tuple, and then enter the learning process, and use stochastic gradient descent algorithm to reduce $\mathbb{Q}$-network prediction for a gap between target and sample target, according to the requirements of the target network, network parameters are optimized, and then a new training sequence is started, the weight of $\mathbb{Q}$-network is synchronized with the weight of target network. In terms of sample selection, the samples are divided into three independent parts, namely the training set, validation set, and test set. The training set is used to estimate the model, the validation set is used to determine the network structure or parameters that control the complexity of the model, and the test set tests the performance of the final selected optimal model. 50% of the sample is the training set, 25% of the sample is the validation and test sets, and all three parts are randomly selected from the sample.

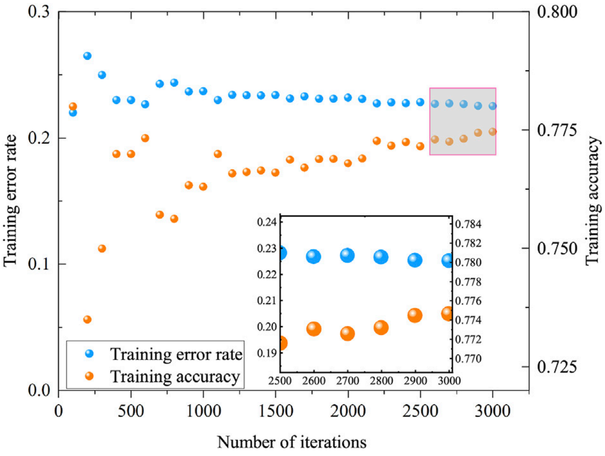


FIGURE 4
The number of training times corresponds to the function of training error rate and training accuracy. The horizontal axis represents the number of training times, and the vertical axis represents the training error rate and accuracy rate. Training error and accuracy are marked in blue and orange, respectively. For accurate viewing, zoom plots are set to make it easier to observe the data.

4 Error correction performance analysis

4.1 Error correction performance

Taking depolarization noise as an example, through the training of the decoder, the data map shown in Figure 4 is obtained. It is found that the performance of the decoder is better, and the accuracy of error correction can reach 77.5%. The decoder in this paper is to calculate the threshold of the Semion code. The logical error rate is drawn in the range of the physical error rate for different code distances, and the threshold is generally determined as the physical error rate value at the intersection of the two. For physical error rates below the intersection of the two, the logical error rate will decrease as the code distance increases. For each physical error rate, the logical error rate is calculated as the average of multiple independent instances, and for experimental certainty, it must be determined that a certain number of logical errors are observed each time in an actual experiment. For the code distance d, the logical error rate $p_{logical}$ should have the following correspondence:

$$p_{logical} = \left(p_{error} - p_{threshold}\right) \times d^{\frac{1}{v_o}} \tag{16}$$

where p_{error} is the physical error rate, $p_{threshold}$ is the threshold, v_o is the scaling exponent. Based on the above formula, this paper obtains the data graph as shown in Figure 5. It can be observed in Figure 5(1) that when the logical error rate $p_{logical} = 0.31257$, the threshold $p_{threshold} = 0.081574$. Figure 5(2) can be observed, but when the logical error rate $p_{logical} = 0.2642$, the threshold $p_{threshold} = 0.09542$. Thresholds vary due to code distances and qubits. It is considered to compare the outcome of this paper with a series of previous estimates of thresholds, some small difference between estimates is reasonable due to not the same execution of decoding algorithms and numerical simulations. As can be seen from the two graphs in Figure 5, when the physical error rate is below the threshold, the greater the code distance the more errors can be corrected, so the logical error rate will be lower. When the physical error rate is above the threshold, although a larger code distance can correct more errors, the logical error rate will be greater as the code itself has more quantum bits and more errors will occur.

Our threshold is significantly lower than that of other papers, this difference seems to be related to the definition of logical error rate, some papers define logical error rate $p_{logical}$ as the error rate measured per round [43–45], according to the analysis of Ref. [46], with the d increase, the p_{error} of continuous curve intersection will decrease, and this definition will lead to an overestimation of the threshold. This is roughly the same as the data of some articles. Therefore, it is difficult for this paper to make a conclusive statement on the difference in the results. Nonetheless, this paper achieves the feasibility of implementing $\mathbb{Q}$-networks for Semion code decoders.

4.2 Quantum circuit performance

RL has a good effect on optimization problems. It can extract non-local laws from noise and perform transfer learning in various tasks. Applying this advantage to the cost of qubits passing through the quantum gate can reduce the cost of qubits. The qubits contain auxiliary qubits in the process of comprehensive measurement, and the logic overhead is the cost of auxiliary qubits in the process of comprehensive measurement. In this paper, the $\mathbb{Q}$-network of RL is used to experiment, and the number of simulated qubits ranges from 3×10^{7} to 2.1×10^{8}, and compare the original overhead under different thresholds and the optimized overhead of the $\mathbb{Q}$-network, Figure 6(1) shows that when the threshold is $p_{threshold} = 0.081574$, as the number of qubits increases, both the original overhead and the $\mathbb{Q}$-network overhead increase, but the $\mathbb{Q}$-network optimized overhead is significantly lower than the original overhead. Figure 62) shows that when the threshold is $p_{threshold} = 0.09542$, as the number of qubits increases, the optimized overhead of the $\mathbb{Q}$-network is also much lower than the original overhead, although when the number of qubits is 2.1×10^{8}, the optimized $\mathbb{Q}$-network has the overhead is slightly higher than the original, but this does not affect our overall results in the slightest. At the same time, comparing the results under different thresholds in Figure 6, we can find that the larger the threshold, the greater the overhead of the quantum circuit gate.

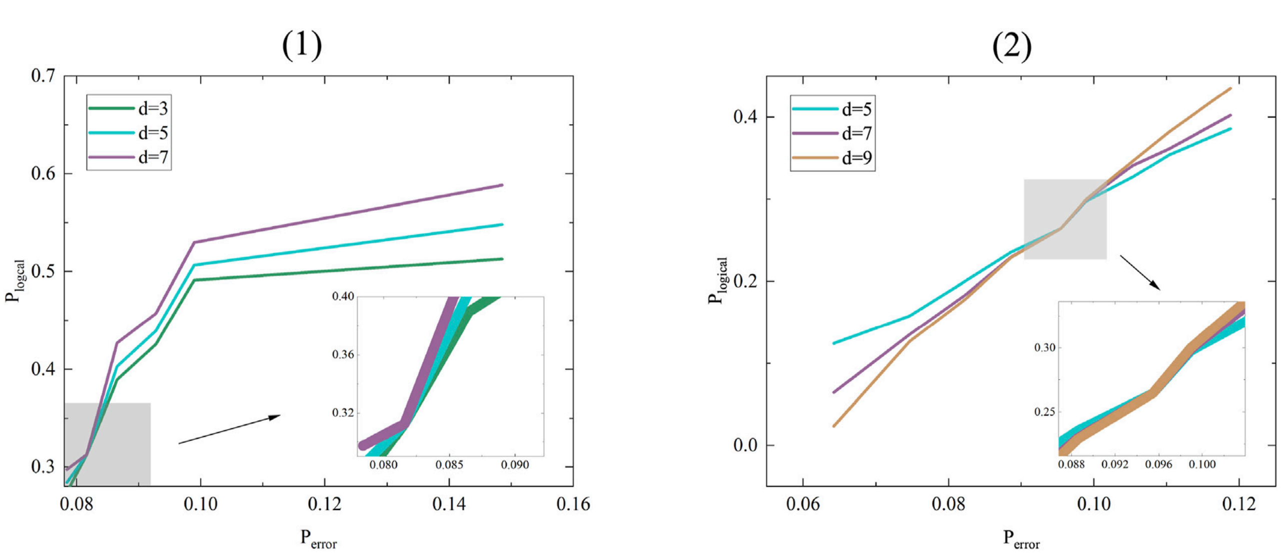


FIGURE 5
(1)Function correspondence of physical error rate p_{error}, logical error rate $p_{logical}$, and code distance d = 3, 5, 7. Threshold $p_{threshold}$ = 0.081574. (2)Function correspondence of physical error rate p_{error}, logical error rate $p_{logical}$, and code distance d = 5, 7, 9. Threshold $p_{threshold}$ = 0.09542. The abscissa represents the physical error rate, the ordinate represents the logical error rate. For better numerical analysis, the different code distances d are marked in different colours, d = 3 in green, d = 5 in blue, d = 7 in purple and d = 9 in brown.

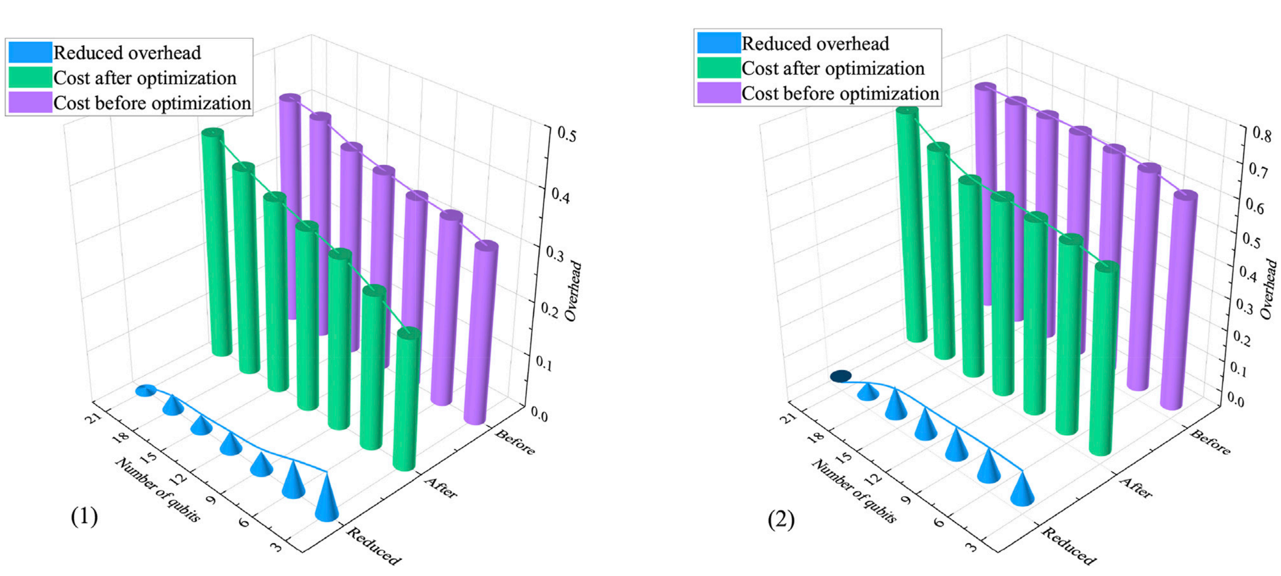


FIGURE 6
Quantum circuit gate overhead data graph. (1)When the threshold $p_{threshold}$ = 0.081574, the original cost is compared with the optimized cost of the $\mathbb{Q}$-network. (2)When the threshold $p_{threshold}$ = 0.09542, the original cost is compared with the optimized cost of the $\mathbb{Q}$-network. Among them, the abscissa represents the number of qubits, which is displayed in scientific notation, and the ordinate is the logical cost. The original cost is marked in orange, and the $\mathbb{Q}$-network optimized cost is marked in blue.

5 Conclusion

In this paper, topological QEC codes based on Semion codes in the case of noise are studied. It is a novel error correction method. Make sure that the perturbations of local errors do not destroy the global degrees of freedom through periodic measurement and inspection. Error-correcting codes protect the security and correctness of quantum information. Semion code is more innovative and flexible. The hexagonal lattice is transformed into a quadrilateral lattice through mathematical thinking, and the deep RL algorithm is input to get the error-corrected experimental results. In addition, the optimization problem of quantum circuits is also involved. Of course, this work leaves a lot to be desired. For example, the current Semion code decoder can only be input into the decoder in the form of squares and has not been completely input in the form of hexagonal grids. And we only realized that the RL decoder embedded in Semion code is feasible, but the threshold is not optimal. The follow-up work still needs to be further explored.

Data availability statement

The raw data supporting the conclusions of this article will be made available by the authors, without undue reservation.

Author contributions

H-WW (First Author): Conceptualization, Methodology, Software, Investigation, Formal Analysis, Writing–Original Draft; QC: Data Curation, Writing–Original Draft; Y-JX: Visualization, Investigation; LD: Resources, Supervision; H-YL: Software, Validation Y-MD: Visualization, Writing–Review and Editing H-YM (Corresponding Author): Conceptualization, Funding Acquisition, Resources, Supervision, Writing–Review and Editing.

Funding

Project supported by the National Natural Science Foundation of China (Grant Nos.61772295), Natural Science Foundation of Shandong Province, China (Grant Nos.ZR2021MF049, ZR2019YQ01), Project of Shandong Provincial Natural Science Foundation Joint Fund Application (ZR202108020011).

Conflict of interest

The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Publisher's note

All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers. Any product that may be evaluated in this article, or claim that may be made by its manufacturer, is not guaranteed or endorsed by the publisher.

References

1. Xin T, Wang B-X, Li K-R, Kong X-Y, Wei S-J, Wang T, et al. Nuclear magnetic resonance for quantum computing: techniques and recent achievements. *Chin Phys B* (2018) 27:020308. doi:10.1088/1674-1056/27/2/020308

2. Zhou N, Zhu K, Zou X. Multi-Party semi-quantum key distribution protocol with four-particle cluster states. *Annalen der Physik* (2019) 531:1800520. doi:10.1002/andp.201800520

3. Ma H-Y, Wang H-F, Zhang S. Implementation of the Grover quantum search algorithm in thermal cavity. *J Yanbian University(Natural Science)* (2008) 34:27–30. doi:10.16379/j.cnki.issn.1004-4353.2008.01.010

4. He Z-X, Fan X-K, Chu P-C, Ma H-Y. Anonymous communication scheme based on quantum walk on Cayley graph. *Acta Phys Sin* (2020) 69:160301. doi:10.7498/aps.69.20200333

5. Terhal BM. Quantum error correction for quantum memories. *Rev Mod Phys* (2015) 87:307–46. doi:10.1103/RevModPhys.87.307

6. Beale SJ, Wallman JJ, Gutiérrez M, Brown KR, Laflamme R. Quantum error correction decoheres noise. *Phys Rev Lett* (2018) 121:190501. doi:10.1103/PhysRevLett.121.190501

7. Huang E, Doherty AC, Flammia S. Performance of quantum error correction with coherent errors. *Phys Rev A (Coll Park)* (2018) 99:022313. doi:10.1103/PhysRevA.99.022313

8. Clemens JP, Siddiqui S, Gea-Banacloche J. Quantum error correction against correlated noise. *Phys Rev A (Coll Park)* (2004) 69:062313. doi:10.1103/physreva.69.062313

9. Poulin D. Stabilizer formalism for operator quantum error correction. *Phys Rev Lett* (2005) 95:230504. doi:10.1103/PhysRevLett.95.230504

10. Kitaev AY. Fault-tolerant quantum computation by anyons. *Ann Phys* (2003) 303:2–30. doi:10.1016/s0003-4916(02)00018-0

11. Dauphinais G, Ortiz L, Varona S, Martin-Delgado MA. Quantum error correction with the semion code. *New J Phys* (2019) 21:053035. doi:10.1088/1367-2630/ab1ed8

12. Bullivant A, Hu Y, Wan Y. Twisted quantum double model of topological order with boundaries. *Phys Rev B* (2017) 96:165138. doi:10.1103/PhysRevB.96.165138

13. Fuentes P, Etxezarreta MJ, Crespo PM, Garcia-Frias J. Approach for the construction of non-Calderbank-Steane-Shor low-density-generator-matrix–based quantum codes. *Phys Rev A (Coll Park)* (2020) 102:012423. doi:10.1103/physreva.102.012423

14. Castelnovo C. Negativity and topological order in the toric code. *Phys Rev A (Coll Park)* (2013) 88:042319. doi:10.1103/physreva.88.042319

15. Gu Z-C, Wang Z, Wen X-G. Lattice model for fermionic toric code. *Phys Rev B* (2014) 90:085140. doi:10.1103/PhysRevB.90.085140

16. Sarvepalli P, Robert R. Efficient decoding of topological color codes. *Phys Rev A (Coll Park)* (2012) 85:022317. doi:10.1103/physreva.85.022317

17. Aloshious AB, Sarvepalli PK. Erasure decoding of two-dimensional color codes. *Phys Rev A (Coll Park)* (2019) 100:042312. doi:10.1103/PhysRevA.100.042312

18. Bolens A, Markus H. Reinforcement learning for digital quantum simulation. *Phys Rev Lett* (2021) 127:110502. doi:10.1103/PhysRevLett.127.110502

19. Mills K, Michael S, Isaac T. Deep learning and the Schrödinger equation. *Phys Rev A (Coll Park)* (2017) 96:042113. doi:10.1103/physreva.96.042113

20. Zhang Y-H, Zheng P-L, Zhang Y, Deng D-L. Topological quantum compiling with reinforcement learning. *Phys Rev Lett* (2020) 125:170501. doi:10.1103/PhysRevLett.125.170501

21. Wu SL, Sun S, Guan W, Zhou C, Chan J, Cheng CL, et al. Application of quantum machine learning using the quantum kernel algorithm on high energy physics analysis at the LHC. *Phys Rev Res* (2021) 3:033221. doi:10.1103/PhysRevResearch.3.033221

22. Juan C, Torlai G. How to use neural networks to investigate quantum many-body physics. *PRX Quan* (2021) 2:040201. doi:10.1103/PRXQuantum.2.040201

23. Baireuther P, Criger B, Beenakker CWJ. Machine-learning-assisted correction of correlated qubit errors in a topological code. *Quantum* (2017) 2:48. doi:10.22331/q-2018-01-29-48

24. Baireuther P, Caio MD, Criger B, Beenakker CWJ, O'Brien TE. Neural network decoder for topological color codes with circuit level noise. *New J Phys* (2019) 21:013003. doi:10.1088/1367-2630/aaf29e

25. Wang H-W, Xue Y-J, Ma Y-L, Hua N, Ma H-Y. Determination of quantum toric error correction code threshold using convolutional neural network decoders. *Chin Phys B* (2022) 31:10303–010303. doi:10.1088/1674-1056/ac11e3

26. Levin MA, Wen X-G. String-net condensation: a physical mechanism for topological phases. *Phys Rev B* (2005) 71:045110. doi:10.1103/physrevb.71.045110

27. Lin T, Su Z, Xu Q, Xing R, Fang D. Deep Q-network based energy scheduling in retail energy market. *IEEE Access* (2020) 8:69284–95. doi:10.1109/ACCESS.2020.2983606

28. Nautrup HP, Delfosse N, Dunjko V, Briegel HJ, Friis N. Optimizing quantum error correction codes with reinforcement learning. *Quantum* (2019) 3:215. doi:10.22331/q-2019-12-16-215

29. Lo H-K, Preskill J. Non-Abelian vortices and non-Abelian statistics. *Phys Rev D* (1993) 48:4821–34. doi:10.1103/PhysRevD.48.4821

30. Forslund DW, Kindel JM, Lindman EL. Parametric excitation of electromagnetic waves. *Phys Rev Lett* (1972) 29:249–52. doi:10.1103/physrevlett.29.249

31. Harada N, Nakanishi K. Exciton chirality method and its application to configurational and conformational studies of natural products. *Acc Chem Res* (1972) 5:257–63. doi:10.1021/ar50056a001

32. Guerreiro T. Molecular machines for quantum error correction. *PRX Quan* (2021) 2:030336. doi:10.1103/prxquantum.2.030336

33. Ahn C, Wiseman HM, Milburn GJ. Quantum error correction for continuously detected errors. *Phys Rev A (Coll Park)* (2003) 67:052310. doi:10.1103/physreva.67.052310

34. Valenti A, van Nieuwenburg E, Huberand S, Greplova E. Hamiltonian learning for quantum error correction. *Phys Rev Res* (2019) 1:033092. doi:10.1103/PhysRevResearch.1.033092

35. Xu X, Benjamin SC, Yuan X. Variational circuit compiler for quantum error correction. *Phys Rev Appl* (2021) 15:034068. doi:10.1103/PhysRevApplied.15.034068

36. Nadkarni PJ, Garani SS. Quantum error correction architecture for qudit stabilizer codes. *Phys Rev A (Coll Park)* (2021) 103:042420. doi:10.1103/physreva.103.042420

37. Andreasson P, Johansson J, Liljestrand S, Granath M. Quantum error correction for the toric code using deep reinforcement learning. *Quantum* (2019) 3:183. doi:10.22331/q-2019-09-02-183

38. Dauphinais G, Poulin D. Fault-tolerant quantum error correction for non-Abelian anyons. *Commun Math Phys* (2017) 355:519–60. doi:10.1007/s00220-017-2923-9

39. Faist P, Nezami S, Albert VV, Salton G, Pastawski F, Hayden P, et al. Continuous symmetries and approximate quantum error correction. *Phys Rev X* (2020) 10:041018. doi:10.1103/physrevx.10.041018

40. Ilya D, Kovalev AA, Pryadko LP. Thresholds for correcting errors, erasures, and faulty syndrome measurements in degenerate quantum codes. *Phys Rev Lett* (2015) 115:050502. doi:10.1103/PhysRevLett.115.050502

41. Sasaki H, Horiuchi T, Kato S. Experimental study on behavior acquisition of mobile robot by deep Q-network. *J Adv Comput Intelligence Intell Inform* (2017) 21:840–8. doi:10.20965/jaciii.2017.p0840

42. Wyner A, Ziv J. The rate-distortion function for source coding with side information at the decoder. *IEEE Trans Inf Theor* (1976) 21:1–10. doi:10.1109/tit.1976.1055508

43. Raussendorf R, Harrington J, Goyal K. A fault-tolerant one-way quantum computer. *Ann Phys* (2006) 321:2242–70. doi:10.1016/j.aop.2006.01.012

44. Raussendorf R, Harrington J, Goyal K. Topological fault-tolerance in cluster state quantum computation. *New J Phys* (2007) 9:199. doi:10.1088/1367-2630/9/6/199

45. Bravyi S, Vargo A. Simulation of rare events in quantum error correction. *Phys Rev A (Coll Park)* (2013) 88:062308. doi:10.1103/physreva.88.062308

46. Stephens AM. Fault-tolerant thresholds for quantum error correction with the surface code. *Phys Rev A (Coll Park)* (2014) 89:022321. doi:10.1103/physreva.89.022321

frontiers | Frontiers in Physics

TYPE Original Research
PUBLISHED 22 August 2022
DOI 10.3389/fphy.2022.981376

Multi-party quantum private size comparison protocol with *d*-dimensional Bell states

Bing Wang[1,2,3], Li-Hua Gong[1,4] and San-Qiu Liu[1,2,3]*

[1]Jiangxi Province Key Laboratory of Fusion and Information Control, Department of Physics, Nanchang University, Nanchang, China, [2]School of Physics and Materials, Nanchang University, Nanchang, China, [3]NCU-ASIPP Magnetic Confinement Fusion Joint Lab, Institute of Fusion Energy and Plasma Application, Nanchang University, Nanchang, China, [4]Department of Electronic Information Engineering, Nanchang University, Nanchang, China

OPEN ACCESS

EDITED BY
Tianyu Ye,
Zhejiang Gongshang University, China

REVIEWED BY
Run-hua Shi,
North China Electric Power University, China
Mingxing Luo,
Southwest Jiaotong University, China
Yuling Chen,
Guizhou University, China

*CORRESPONDENCE
San-Qiu Liu,
sqlgroup@ncu.edu.cn

SPECIALTY SECTION
This article was submitted to Quantum Engineering and Technology, a section of the journal Frontiers in Physics

RECEIVED 29 June 2022
ACCEPTED 15 July 2022
PUBLISHED 22 August 2022

CITATION
Wang B, Gong L-H and Liu S-Q (2022), Multi-party quantum private size comparison protocol with d-dimensional Bell states.
Front. Phys. 10:981376.
doi: 10.3389/fphy.2022.981376

A feasible multi-party quantum private comparison (MQPC) protocol based on *d*-dimensional Bell states was proposed. In the protocol, all participants can independently encrypt their privacies and send them to a semi-honest quantum third party (TP) through authenticated channels. Then, the TP can determine the size relationship among all participants' privacies without gaining access to the private information. We verified correctness and effectiveness of the proposed protocol with some examples. In addition, compared with other similar protocols, it is not necessary to perform unitary operation on particles and only single-particle measurement is required. Furthermore, the relatively high qubit efficiency is promised. The security analysis verifies that the proposed protocol can counteract external and internal attacks in theory.

KEYWORDS

multi-party quantum private comparison, size relationship, *d*-dimensional bell state, qubit efficiency, semi-honest quantum third party

1 Introduction

Secure multi-party computation (SMC) was introduced by the famous Millionaires' problem in 1982 [1], where two millionaires want to compare their wealth and learn who is wealthier without revealing their actual property. With the combination of quantum mechanics and information science, researchers have found that processing information using quantum systems has led to many striking results, such as teleportation of quantum states and quantum algorithms that are exponentially faster than their known classical counterpart. Therefore, the quantum version of SMC has once again set off a research boom. As a particular instance of quantum SMC (QSMC), quantum private comparison (QPC) has wide applications in private bidding and auctions, secret ballot elections, commercial business, identification.

Right after Yao's millionaire problem, [2] designed an efficient and fair protocol to determine whether two millionaires are equal rich. However, as proved by [3], a quantum two-party secure computation is impossible. Therefore, a third party (e.g., a semi-honest third party) is often involved to help them achieve the task in a QSMC protocol. The semi-honest quantum third party (TP) will always follow the process of the protocol honestly.

He will not prepare other types of particles (e.g., GHZ state, single photon) and conspire with any participants or outside eavesdroppers to steal the participants' privacies. But the TP is curious to know the participants' privacies, and try to extract their private information from he knows.

In 2009, the first QPC protocol was proposed by based on Bell states [4]. With decoy particle technology, one-way hash function and unitary operation, this protocol can compare the equality. In 2010, [5] devised a novel QPC protocol to compare the equality based on GHZ states, where the unitary operation is necessary. These early QPC protocols can only compare the equality. In 2011, a new QPC protocol was presented by [6] to compare the size relationship of privacies, where the information of size was encoded into the phase of GHZ state. In 2013, Lin et al. also designed a protocol to compare the size relationship based on the d-dimensional Bell states [7]. However, the four QPC protocols mentioned above are only related to the comparison between two participants. These two-party protocols are by no means the end of the QPC research. In future secure quantum network communication, the MQPC protocol will play an important role.

Fortunately, in 2013, the first MQPC protocol was proposed based on GHZ states by [8]. Suppose there are N $(N \geq 2)$ participants, each of them has a privacy, then N participants can determine whether their privacies are the same or not with the assistance of the TP. In 2014, Luo et al. devised a novel MQPC protocol based on d-dimensional multi-particle entangled states [9]. In their protocol, N $(N \geq 2)$ participants' privacies can be sorted by size with the help of the TP, and decoy particles were used to check eavesdropping. In the same year, [10] presented two MQPC protocols in distributed mode and traveling mode respectively based on multi-particle entangled states. With the assistance of the TP, the two protocols can also compare the equality of privacies for N $(N \geq 2)$ participants. Since then, various two-party [11–13] and multi-party QPC protocols have been proposed [14–17]. In 2018, Ye et al. proposed two novel multi-party quantum private comparison protocols for size relation comparison by using d-level single-particle states. In 2021, Zhou et al. presented an efficient QPC protocol to compare the size relationship of privacies between two classical participants based on d-dimensional Bell states. It should be noted that many previous protocols involved many kinds of operations, such as quantum measurement, unitary operation, and hash function. What's more, some of them suffer from low qubit efficiency. Besides, only few MQPC protocols can compare the size relationship among the privacies.

To make the implementation of the protocol easier, a new MQPC protocol to compare the size relationship among many participants' privacies is proposed. The d-dimensional Bell states are taken as quantum resources and the TP is introduced to help participants to make private comparison. The rest of this paper is organized as follows: the proposed MQPC protocol based on the d-dimensional Bell state is detailed in Section 2. The correctness and security are analyzed in Section 3, Section 4, respectively. The comparisons of the proposed protocol and the similar QPC protocols are made in Section 5. Finally, a short conclusion is given in Section 6.

2 The proposed MQPC protocol based on *d*-dimensional bell states

Assume there are N participants (P_1, P_2, ..., P_N) and each participant P_n $(n \in \{1, 2, ..., N\})$ possesses a L-length privacy $p_n = p_n^1 p_n^2 ... p_n^L$ (if the numbers of some digits are less than L, then sufficient 0s are added to their highest digit), where, $p_n^l \in \{0, 1, ..., h-1\}$, $h = \frac{d+1}{2}$, and $l \in \{1, 2, ..., L\}$. In addition, there is a pre-shared key through a secure QKD protocol [18] among these participants denoted as $A = A^1 A^2 ... A^L$, $A^l \in \{0, 1, ..., h-1\}$. Via the help of TP, they want to compare their privacies by size without revealing any private information. Next, the d-dimensional Bell state will be reviewed first. Then, the detailed description of the proposed protocol will be given (Figure 1).

2.1 *d*-dimensional bell state

Bell state, used to describe the four maximal entangled states in two-qubit system, is the most basic quantum entangled state. Compared with other quantum entangled states, Bell state is the easiest to prepare in experiment. Therefore, Bell state is widely used to design quantum cryptographic protocol. In a d-dimensional Hilbert space, Bell state can be expressed as [19, 20]

$$\left|\psi_{u,v}\right\rangle = \frac{1}{\sqrt{d}} \sum_{k=0}^{d-1} e^{\frac{2\pi i k u}{d}} |k\rangle \otimes |k \oplus v\rangle \tag{1}$$

where $u,v \in \{0, 1, 2, ..., d-1\}$, and $\oplus$ denotes modulo d addition. Two indistinguishable orthogonal bases Z-basis $\bar{Z}$ and X-basis $\bar{X}$ in the d-dimensional quantum system are

$$\begin{aligned} \bar{Z} &= \{|j\rangle \big| j = 0, 1, ..., d-1.\} \\ \bar{X} &= \{F|j\rangle \big| j = 0, 1, ..., d-1.\} \end{aligned} \tag{2}$$

where $F|j\rangle = \frac{1}{\sqrt{d}} \sum_{k=0}^{d-1} e^{\frac{2\pi \mathrm{i}}{d} kj} |k\rangle$ with $j = 0, 1, \ldots, d-1$represents quantum Fourier transform.

2.2 The proposed MQPC protocol

Step 1: According to Eq. 1, the TP randomly prepares $L \times N$ d-dimensional Bell states and they are

$$\begin{aligned} &\left|\psi_{u_1^1,v_1^1}\right\rangle, \left|\psi_{u_2^1,v_2^1}\right\rangle, ..., \left|\psi_{u_N^1,v_N^1}\right\rangle \\ &\left|\psi_{u_1^2,v_1^2}\right\rangle, \left|\psi_{u_2^2,v_2^2}\right\rangle, ..., \left|\psi_{u_N^2,v_N^2}\right\rangle \\ &\qquad\qquad\qquad ... \\ &\left|\psi_{u_1^L,v_1^L}\right\rangle, \left|\psi_{u_2^L,v_2^L}\right\rangle, ..., \left|\psi_{u_N^L,v_N^L}\right\rangle \end{aligned} \tag{3}$$

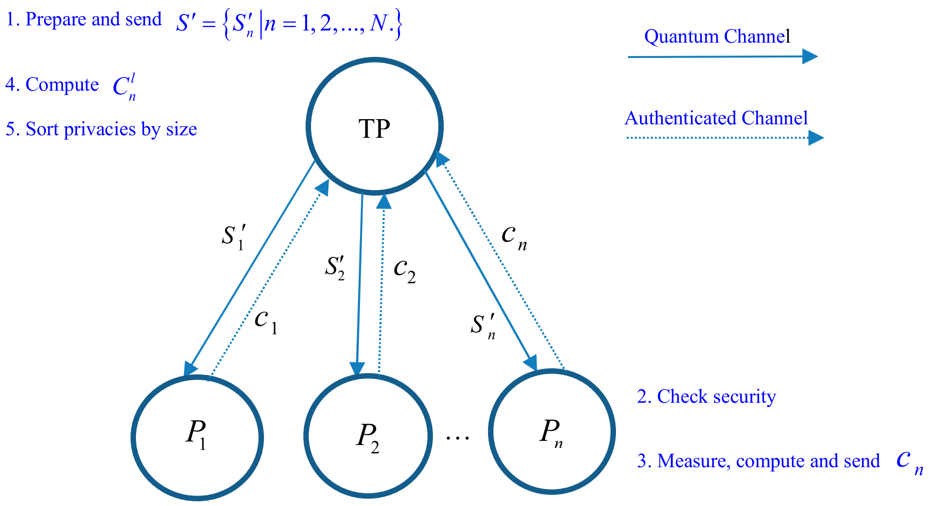


FIGURE 1
The schematic figure of the proposed protocol. The TP needs to implement steps 1, 4, 5 and each participant needs to implement steps 2, 3.

Based on these prepared Bell states in Eq. 3, he will record the v_n^l of each state and prepare $2N$ quantum sequences, namely $S = \{S_n | n = 1, 2, ..., N.\}$ and $T = \{T_n | n = 1, 2, ..., N.\}$, which contain all the first and second particles of the EPR pairs, respectively. Each particle-sequence contains L particles

$$S_n\colon\ [S_n^1, S_n^2, ..., S_n^L],$$
$$T_n\colon\ [T_n^1, T_n^2, ..., T_n^L].$$

To prevent eavesdropping, TP will prepare NL decoy particles randomly in $\bar{Z}$ or $\bar{X}$, and uniformly insert them into each sequence S_n to form a new sequence $S_n^{'}$. Then, sequence $S_n^{'}$ is sent to participant P_n via a quantum channel, while all sequences $T = \{T_n | n = 1, 2, ..., N.\}$ are kept by the TP.

Step 2: After all the quantum sequences have been received by the corresponding participants, TP will announce the position and the measurement basis of each decoy particle in sequence $S_n^{'}$. Then, each participant will check the security of the sequence received. Concretely, according to the announcement, each participant will use the right bases to measure these decoy particles and return the measurement results to TP. Then, the TP will verify these results and check whether eavesdroppers exist in the quantum channel. If the error rate is less than a predetermined threshold, the protocol will proceed to the next step; otherwise, the protocol will be terminated.

Step 3: After removing these decoy particles, each participant will measure the remaining particles with Z basis and record them as k_n^l. Then, he (she) will compute c_n^l,

$$c_n^l = k_n^l \oplus p_n^l \oplus A^l \tag{4}$$

Then, Participant P_n will obtain a sequence $c_n = c_n^1 c_n^2 ... c_n^L$ and send it to the TP via an authenticated channel.

Step 4: When confirming all sequences embedded privacy data have been received, TP will measure the particles in each sequence T_n and record them as t_n^l. Then, he will compute C_n^l,

$$C_n^l = c_n^l \oplus v_n^l \ominus t_n^l \tag{5}$$

Here, v_n^l is the record value in Step 1 and $\ominus$ denotes modulo d subtraction.

Step 5: After TP obtaining sequence $C_n = \{C_n^l | l = 1, 2, ..., L.\}$ from each participant, he will finish sorting the privacies by size. The TP takes out the same digits (the l-th digit) from sequences $C_1, C_2, \ldots, C_N$ and compute $R_{nn'}^l$,

$$R_{nn'}^l = C_n^l \ominus C_{n'}^l \tag{6}$$

Then, he can obtain $\mathrm{sign}[R_{nn'}^l]$,

$$\mathrm{sign}\left[R_{nn'}^l\right] = \begin{cases} 1, 0 < R_{nn'}^l \le h - 1; \\ 0, R_{nn'}^l = 0; \\ -1, h - 1 < R_{nn'}^l \le 2h - 2. \end{cases} \tag{7}$$

For the l-th elements of all participants' privacies $p_1^l, p_2^l, \ldots, p_N^l$, the TP can deduce their size relationship easily from $\mathrm{sign}[R_{nn'}^l]$. that is

$$\mathrm{sign}\left[R_{nn'}^l\right] = \begin{cases} 1, p_n^l > p_{n'}^l; \\ 0, p_n^l = p_{n'}^l; \\ -1, p_n^l < p_{n'}^l. \end{cases} \tag{8}$$

3 Correctness analysis

3.1 Output correctness

The quantum resource used in the protocol is the d-dimensional Bell state. According to the entanglement properties of Bell state, if one measures the particle with $\bar{Z}$, the d-dimensional Bell state will collapse into $|k\rangle|k \oplus v\rangle$. Therefore, the measurement results k_n^l and t_n^l satisfy the relationship, such that

$$k_n^l \oplus v_n^l = t_n^l \tag{9}$$

Therefore, based on Eqs 4, 5 and 6, the Eq. 9 can be deduced

$$\begin{aligned} R_{nn'}^l &= C_n^l \ominus C_{n'}^l \\ &= \left(c_n^l \oplus v_n^l \ominus t_n^l\right) \ominus \left(c_{n'}^l \oplus v_{n'}^l \ominus t_{n'}^l\right) \\ &= \left(k_n^l \oplus p_n^l \oplus A^l \oplus v_n^l \ominus t_n^l\right) \ominus \left(k_{n'}^l \oplus p_{n'}^l \oplus A^l \oplus v_{n'}^l \ominus t_{n'}^l\right) \\ &= \left(p_n^l \oplus A^l\right) \ominus \left(p_{n'}^l \oplus A^l\right) \\ &= p_n^l \ominus p_{n'}^l \end{aligned} \tag{10}$$

From Eq. 10, one can see that the value of $R_{nn'}^l$ indicates the size relationship between p_n^l and $p_{n'}^l$. Therefore, according to Eqs 7, 8 the TP can obtain the size relationship among the privacies.

3.2 Examples

Here, some examples are given for illustration the presented protocol without considering the eavesdropping checking. Let $N = 4$ and their privacies are $p_1 = 214$, $p_2 = 403$, $p_3 = 211$, $p_4 = 043$, respectively. The pre-shared key A among four participants is 123.

Step 1: TP randomly prepares 3×4 9-dimensional Bell states,

$$\begin{matrix} \left|\psi_{3_1^1,5_1^1}\right\rangle, \left|\psi_{2_2^1,1_2^1}\right\rangle, \left|\psi_{6_3^1,0_3^1}\right\rangle, \left|\psi_{4_4^1,4_4^1}\right\rangle \\ \left|\psi_{0_1^2,1_1^2}\right\rangle, \left|\psi_{1_2^2,3_2^2}\right\rangle, \left|\psi_{0_3^2,0_3^2}\right\rangle, \left|\psi_{6_4^2,7_4^2}\right\rangle \\ \left|\psi_{8_1^3,6_1^3}\right\rangle, \left|\psi_{2_2^3,6_2^3}\right\rangle, \left|\psi_{3_3^3,1_3^3}\right\rangle, \left|\psi_{5_4^3,7_4^3}\right\rangle \end{matrix} \tag{11}$$

First, he records $v_1^1 v_1^2 v_1^3 = 516$, $v_2^1 v_2^2 v_2^3 = 136$, $v_3^1 v_3^2 v_3^3 = 001$, $v_4^1 v_4^2 v_4^3 = 477$ according to Eq. 11. Then, he prepares a set of sequences $S' = \{S_n^{'} | n = 1, 2, 3, 4.\}$ and sends sequence $S_n^{'}$ to the corresponding participant via the quantum channel.

Step 2: Suppose that no eavesdropper is detected; then, move to Step 3.

Step 3: After removing these decoy particles, Participants P_1, P_2, P_3 and P_4 will measure the remaining particles with Z basis and record the measurement results. If their measurement results are $k_1 = 203$, $k_2 = 874$, $k_3 = 257$, $k_4 = 161$, then the TP's measurement results in Step 5 can be determined according to the entanglement properties of Bell state and they are

$$t_1 = 710,\ t_2 = 011,\ t_3 = 258,\ t_4 = 548 \tag{12}$$

Therefore, after all participants encode their privacies according to Eq. 4, Participants P_1, P_2, P_3 and P_4 will obtain $c_1 = 531$, $c_2 = 401$, $c_3 = 581, c_4 = 237$, separately. Then, each participant will send the encoding information to TP via an authenticated channel.

Step 4: When confirming that the encoding information from all participants has been received, the TP will measure the particles in sequence $T_n (n = 1, 2, 3, 4)$. From Step 3, one can know that the TP's measurement results must be determined as Eq. 12. Therefore, after TP computes C_n^l, he will obtain $C_1 = 337$, $C_2 = 526$, $C_3 = 333$, $C_4 = 166$.

Step 5: TP will finish sorting the privacies by size as follows

$$\begin{aligned} R_{12}^1 &= \left(C_1^1 \ominus C_2^1\right) = (3 \ominus 5) = 7,\ R_{13}^1 = \left(C_1^1 \ominus C_3^1\right) = (3 \ominus 3) = 0 \\ R_{14}^1 &= \left(C_1^1 \ominus C_4^1\right) = (3 \ominus 1) = 2,\ R_{23}^1 = \left(C_2^1 \ominus C_3^1\right) = (5 \ominus 3) = 2 \\ R_{24}^1 &= \left(C_2^1 \ominus C_4^1\right) = (5 \ominus 1) = 4,\ R_{34}^1 = \left(C_3^1 \ominus C_4^1\right) = (3 \ominus 1) = 2 \end{aligned} \tag{13}$$

Similar to Eq. 13, the TP can obtain $R_{12}^2 = 1$, $R_{13}^2 = 0$, $R_{14}^2 = 6$, $R_{23}^2 = 8$, $R_{24}^2 = 5$, $R_{34}^2 = 6$, $R_{12}^3 = 1$, $R_{13}^3 = 4$, $R_{14}^2 = 1$, $R_{23}^3 = 3$, $R_{24}^2 = 0$, $R_{34}^2 = 6$. Therefore, based on Eqs 7, 8, TP can deduce the comparison results as follows

$$\begin{aligned} \operatorname{sign}\left[R_{12}^1, R_{13}^1, R_{14}^1, R_{23}^1, R_{24}^1, R_{34}^1\right] &= \operatorname{sign}[7, 0, 2, 2, 4, 2] \\ &= -1, 0, 1, 1, 1, 1 \\ &\Rightarrow p_2^1 > p_1^1 = p_3^1 > p_4^1 \\ \operatorname{sign}\left[R_{12}^2, R_{13}^2, R_{14}^2, R_{23}^2, R_{24}^2, R_{34}^2\right] &= \operatorname{sign}[1, 0, 6, 8, 5, 6] \\ &= 1, 0, -1, -1, -1, -1 \\ &\Rightarrow p_4^2 > p_3^2 = p_1^2 > p_2^2 \\ \operatorname{sign}\left[R_{12}^3, R_{13}^3, R_{14}^3, R_{23}^3, R_{24}^3, R_{34}^3\right] &= \operatorname{sign}[1, 4, 1, 3, 0, 6] \\ &= 1, 1, 1, 1, 0, -1 \\ &\Rightarrow p_1^3 > p_2^3 = p_4^3 > p_3^3 \end{aligned}$$

Apparently, the size relationship that TP sorts without knowing participants' privacies is consistent with the actual data ($p_1 = 214$, $p_2 = 403$, $p_3 = 211$, $p_4 = 043$) given in Section 3.2. To further clarify this process, more examples are compiled in Table 1.

4 Security analysis

Assumed that the quantum and authentical channels are the ideal channels, that's to say, there is no noise in the channel and the particles can be sent to the receivers. In this section, the security of the proposed protocol will be analyzed from both external and internal attack. It is shown that no private information has been leaked according to the security analysis.

TABLE 1 Relation of essential indices for some examples.

Initial states	$L \times N$	d	p_1	p_2	p_3	k_1	k_2	k_3	c_1	c_2	c_3	A	**sign** $[R_{12}^1, R_{13}^1, R_{23}^1]$ **sign** $[R_{12}^2, R_{13}^2, R_{23}^2]$ **sign** $[R_{12}^3, R_{13}^3, R_{23}^3]$	**Size relationship**
$\|\psi_{0_1^1,4_1^1}\rangle,\|\psi_{1_2^1,3_2^1}\rangle,\|\psi_{2_3^1,0_3^1}\rangle$	2 × 3	5	21	10	11	03	14	21	41	41	04	22	1, 1,0	$p_1^1 > p_2^1 = p_3^1$
													1, 0,−1	$p_1^2 = p_3^2 > p_2^2$
$\|\psi_{3_1^2,2_1^2}\rangle,\|\psi_{1_2^2,4_2^2}\rangle,\|\psi_{3_3^2,4_3^2}\rangle$			01	12	20	22	43	34	43	20	24	20	−1,−1,−1	$p_3^1 > p_2^1 > p_1^1$
													−1, 1, 1	$p_2^2 > p_1^2 > p_3^2$
$\|\psi_{1_1^1,2_1^1}\rangle,\|\psi_{0_2^1,3_2^1}\rangle,\|\psi_{2_3^1,4_3^1}\rangle$	3 × 3	9	123	014	201	321	382	601	448	301	806	004	1,−1,−1	$p_3^1 > p_1^1 > p_2^1$
$\|\psi_{3_1^2,5_1^2}\rangle,\|\psi_{6_2^2,1_2^2}\rangle,\|\psi_{3_3^2,4_3^2}\rangle$													1, 1, 1	$p_1^2 > p_2^2 > p_3^2$
													−1, 1, 1	$p_2^3 > p_1^3 > p_3^3$
$\|\psi_{5_1^3,6_1^3}\rangle,\|\psi_{2_2^3,0_2^3}\rangle,\|\psi_{4_3^3,1_3^3}\rangle$			401	432	210	372	616	064	885	251	386	112	0, 1, 1	$p_1^1 = p_2^1 > p_3^1$
													−1,−1,1	$p_2^2 > p_3^2 > p_1^2$
													−1, 1, 1	$p_2^3 > p_1^3 > p_3^3$
$\|\psi_{5_1^1,6_1^1}\rangle,\|\psi_{6_2^1,5_2^1}\rangle,\|\psi_{5_3^1,4_3^1}\rangle$	3 × 3	7	103	201	312	314	240	616	423	453	233	012	−1,−1,−1	$p_3^1 > p_2^1 > p_1^1$
$\|\psi_{6_1^2,5_1^2}\rangle,\|\psi_{4_2^2,1_2^2}\rangle,\|\psi_{4_3^2,3_3^2}\rangle$													0,−1,−1	$p_3^2 > p_2^2 = p_1^2$
$\|\psi_{5_1^3,0_1^3}\rangle,\|\psi_{2_2^3,3_2^3}\rangle,\|\psi_{4_3^3,2_3^3}\rangle$													1, 1,−1	$p_1^3 > p_3^3 > p_2^3$
			310	220	032	646	302	161	302	645	246	123	1, 1, 1	$p_1^1 > p_2^1 > p_3^1$
													−1,−1,−1	$p_3^2 > p_2^2 > p_1^2$
													0, −1, −1	$p_3^3 > p_2^3 = p_1^3$

4.1 External attack

Eve, an external attacker, may attempt to acquire information from the participants including TP. In Step 1, Sequence $S_n^{'}$ is sent to the corresponding participant via the quantum channel. Eve may steal some useful information from sequences $S_n^{'}$ with many kinds of attacks in this step. Obviously, the security of the protocol is guaranteed by inserting the decoy particles [21, 22]. Since Eve does not know the position and the measurement basis of each decoy particle, some well-known attacks, such as intercept-resend attack, measurement-resend attack, and entanglement-measure attack can be detected with the checking mechanism [4, 23, 24]. The decoy particle technology can be thought as a variant of the eavesdropping check method of the BB84 protocol [25] which has been proven to provide unconditionally security [26]. In Step 2, the encoding information is sent to the TP via the authenticated channels. The security in this step is promised. Therefore, an external attacker cannot learn any useful information about the privacies without being detected.

4.2 Internal attack

Case 1 Internal attack from P_n

Suppose participant P_n is a dishonest participant who tries to obtain other participants' privacies in Step 1. Since P_n has no knowledge about the positions and the measurement bases of counterparts' decoy particles, the attack from the participant P_n will be detected as an external one as described in Section 4.1. Thus, the proposed protocol is immune to internal attack from dishonest P_n.

Case 2 Internal attack from TP

From Section 2.2, one can know that TP is both the sender of quantum information and the receiver of all encrypted information. Therefore, he can obtain more information than other attackers during the protocol execution. Significantly, due to TP semi-honesty, that the only thing he can do is try to extract the information from the received ciphertext $c_n^l = k_n^l \oplus p_n^l \oplus A^l$. However, he is unable to learn any information about A^l shared among these participants with a secure QKD protocol. Thus, the TP can't obtain any useful private information from c_n^l with the internal attack.

5 Discussion

In Table 2, the proposed protocol is compared with some other similar protocols with the following aspects: quantum resource used, category of QPC (size or equality), number of participants, number of TP, need for the authenticated classical channel, need for unitary operation, measurement involved, and qubit efficiency η (Defined as $\eta = b_c/b_t$, where b_c is the total number of compared qubit while b_t is the total number of qubits and classical bits used in this protocol).

In Ref. [27], we proposed a new QPC protocol to compare the size relationship of privacies between two participants. The quantum resources used in the protocol are d-dimensional GHZ states. To calculate the qubit efficiency η, we must count the number of bits consumed in the transmission of information. First, TP needs $12L$ (L is the length of each privacy) qubits to prepare $4L$ GHZ states. Second, the participants (Alice and Bob) use $4L$ qubits to send information to the TP. $2L$ is the total number of compared qubit. Hence, the qubit efficiency is $\eta = 1/8$. It is noted that the protocol can only make private comparison between two participants. In addition, both Bell measurement and single-particle measurement are needed.

In Ref. [28], the authors presented a new QPC protocol to compare the equality of privacies between two participants. The quantum resources used are GHZ states. First, the TP needs $8L$ qubits to prepare L four-particle GHZ states and $4L$ decoy states. Second, Alice needs $2L$ qubits to send information to Bob. Third, Alice and Bob need $2L$ qubits to send information to the TP. In addition, the total number of compared qubit is $2L$. Hence, the qubit efficiency is $\eta = 1/6$. In

TABLE 2 The comparisons of our QPC with other similar QPC protocols.

Compared aspects	Reference [27]	Reference [28]	Reference [29]	Reference [30]	Our protocol
Quantum resources	dD GHZ state	GHZ state	dD GHZ state	GHZ state	dD Bell state
Category of QPC	Size	Equality	Size	Equality	Size
Number of participants	2	2	N ($N \geq 2$)	N ($N \geq 2$)	N ($N \geq 2$)
Number of TP	1	1	1	2	1
Efficiency η	$\frac{1}{8}$	$\frac{1}{6}$	$\frac{1}{6}$	$\frac{1}{4}$	$\frac{1}{4}$
Need for authenticated classical channels	No	Yes	No	Yes	Yes
Need for unitary operation	No	Yes	Yes	No	No
measurement	BM and SM	BM and SM	SM	SM	SM

SM (single-particle measurement), BM (Bell measurement), dD (d-dimensional).

the protocol, both Bell measurement and single-particle measurement are involved, and unitary operation is needed.

In Ref. [29], a novel MQPC protocol for comparing the size relationship among N participants' privacies was designed. The quantum resources used are d-dimensional GHZ states. First, the TP needs $4NL$ qubits to prepare L pairs of N-particle d-dimensional GHZ states and $2NL$ decoy states. Second, each participant needs $2L$ qubits to sends information to the TP. Thus, $b_t = 4NL + 2NL$. In addition, the total number of compared bits b_c is NL. Hence, the qubit efficiency is $\eta = 1/6$. Although the authenticated channels are not necessary in advance, quantum unitary operations have to be performed in the protocol.

In Ref. [30], the authors proposed a new MQPC protocol to compare the size relationship among N participants' privacies. The quantum resources used are N-particle GHZ states. First, the TP_1 needs $2NL$ qubits to prepare L N-particle GHZ states and NL decoy states. It is note that TP_1 sends the information of the initial GHZ states to TP_2 using quantum secure direct communication protocol. Second, each participant needs $2L$ classical bits to send information to TP_1 and TP_2 via the authenticated channels. The total number of compared qubit is NL. Hence, the qubit efficiency is $\eta = 1/4$. In addition to the classic authentication channels, two TPs are required in the protocol.

In our protocol, a new MQPC protocol to compare the size relationship among N participants' privacies was proposed. The quantum resources used are d-dimensional Bell states. First, the TP_1 needs $3NL$ qubits to prepare NL d-dimensional Bell states and NL decoy particles. Second, each participants need L classical bits to send information to the TP via the authenticated classical channel. The total number of compared qubit is NL. Hence, the qubit efficiency is $\eta = 1/4$.

From Table 2, one can see that, like the protocols in [27, 29], our protocol can compare the size relationship among privacies, while in [28, 30] they can only compare the equality. When it comes to the MQPC, Refs. [27, 28] are useless. Compared with these protocols listed in Table 2, the unitary operation is not necessary, and only single-particle measurement is required in our protocol. Additionally, our protocol ensures the highest qubit efficiency only with the help of one TP. Table 2 clearly shows that the performance of the proposed protocol is better than these similar QPC protocols. However, it has to be said that the high dimensional quantum state is not easy to obtain experimentally at present. Therefore, we still need to work harder to realize the protocol based on the high dimensional quantum state in experiment.

6 Conclusion

Based on the d-dimensional Bell states, a novel MQPC protocol is presented. With the help of a semi-honest quantum TP, our protocol can determine the size relationship among N participants' privacies without any information leakage. Since the quantum measurement and unitary operation aren't required, it is easier to implement the proposed protocol. Furthermore, compared with the similar protocols, the qubit efficiency is increased. Decoy particles promise the security of the proposed protocol. Although it will take many efforts to move the theoretical research towards social practices, we will be very happy if this work plays a little facilitating role in further research of QSMC.

Data availability statement

The original contributions presented in the study are included in the article/Supplementary Material, further inquiries can be directed to the corresponding author.

Author contributions

BW: Conceptualization, methodology, investigation, formal analysis, writing—original draft; L-HG: validation, writing- reviewing and editing S-QL: Conceptualization, funding acquisition, resources, supervision, writing—review and; editing.

Funding

This work is supported by the National Natural Science Foundation of China Grant No. 62161025, the Project of Scientific and Technological Innovation Base of Jiangxi Province Grant No. 20203CCD46008, and the Jiangxi Provincial Key Laboratory of Fusion and Information Control Grant No. 20171BCD40005.

Conflict of interest

The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Publisher's note

All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers. Any product that may be evaluated in this article, or claim that may be made by its manufacturer, is not guaranteed or endorsed by the publisher.

References

1. Yao AC. Protocols for secure computations. In: Proceedings of 23rd IEEE Symposium on Foundations of Computer Science (SFCS'08); 03-05 November 1982. Washington, DC, USA: IEEE (1982). p. 160–4. doi:10.1109/SFCS.1982.38

2. Boudot F, Schoenmakers B, Traore J. A fair and efficient solution to the socialist millionaires' problem. *Discrete Appl Math* (2001) 111:23–36. doi:10.1016/s0166-218x(00)00342-5

3. Lo HK. Insecurity of quantum secure computations. *Phys Rev A (Coll Park)* (1997) 56:1154–62. doi:10.1103/physreva.56.1154

4. Yang YG, Wen QY. An efficient two-party quantum private comparison protocol with decoy photons and two-photon entanglement. *J Phys A: Math Theor* (2009) 42:055305. doi:10.1088/1751-8113/42/5/055305

5. Chen XB, Xu G, Niu XX, Wen QY, Yang YX. An efficient protocol for the private comparison of equal information based on the triplet entangled state and single-particle measurement. *Opt Commun* (2010) 283:1561–5. doi:10.1016/j.optcom.2009.11.085

6. Jia HY, Wen QY, Song TT, Gao F. Quantum protocol for millionaire problem. *Opt Commun* (2011) 284:545–9. doi:10.1016/j.optcom.2010.09.005

7. Lin S, Sun Y, Liu XF, Yao ZQ. Quantum private comparison protocol with d-dimensional Bell states. *Quan Inf Process* (2013) 12:559–68. doi:10.1007/s11128-012-0395-6

8. Chang YJ, Tsai CW, Hwang T. Multi-user private comparison protocol using GHZ class states. *Quan Inf Process* (2013) 12:1077–88. doi:10.1007/s11128-012-0454-z

9. Luo QB, Yang GW, She K, Niu WN, Wang YQ. Multi-party quantum private comparison protocol based on $$d$$ d -dimensional entangled states. *Quan Inf Process* (2014) 13:2343–52. doi:10.1007/s11128-014-0805-z

10. Wang QL, Sun HX, Huang W. Multi-party quantum private comparison protocol with $$n$$ n -level entangled states. *Quan Inf Process* (2014) 13:2375–89. doi:10.1007/s11128-014-0774-2

11. Zhang B, Liu XT, Wang J, Wang J, Tang CJ. Cryptanalysis and improvement of quantum private comparison of equality protocol without a third party. *Quan Inf Process* (2015) 14:4593–600. doi:10.1007/s11128-015-1145-3

12. Ji ZX, Zhang HG, Fan PR. Two-party quantum private comparison protocol with maximally entangled seven-qubit state. *Mod Phys Lett A* (2019) 34:1950229. doi:10.1142/s0217732319502298

13. Zhou NR, Xu QD, Du NS, Gong LH. Semi-quantum private comparison protocol of size relation with d-dimensional Bell states. *Quan Inf Process* (2021) 20:124. doi:10.1007/s11128-021-03056-6

14. Liu W, Wang YB, Wang XM. Quantum multi-party private comparison protocol using d-dimensional bell states-dimensional bell states. *Int J Theor Phys (Dordr)* (2015) 54:1830–9. doi:10.1007/s10773-014-2388-y

15. Ye CQ, Ye TY. Multi-party quantum private comparison of size relation with d-level single-particle states-level single-particle states. *Quan Inf Process* (2018) 17:252. doi:10.1007/s11128-018-2021-8

16. Cao H, Ma WP, Lü LD, He YF, Liu G. Multi-party quantum privacy comparison of size based on d-level GHZ states. *Quan Inf Process* (2019) 18:287. doi:10.1007/s11128-019-2401-8

17. Ye TY, Hu JL. Multi-party quantum private comparison based on entanglement swapping of bell entangled states within d-level quantum system. *Int J Theor Phys (Dordr)* (2021) 60(4):1471–80. doi:10.1007/s10773-021-04771-7

18. Daniel BS, Constantin B, Patrick JC, Norbert L, Ryan MC, Junji U, et al. Self-referenced continuous-variable quantum key distribution protocol. *Phys Rev X* (2015) 5:041010. doi:10.1103/physrevx.5.041010

19. Liu XS, Long GL, Tong DM, Li F. General scheme for super dense coding between multi-parties. *Phys Rev A (Coll Park)* (2002) 65:022304. doi:10.1103/physreva.65.022304

20. Liu ZH, Chen HW, Xu J, Liu WJ, Li ZQ. High-dimensional deterministic multiparty quantum secret sharing without unitary operations. *Quan Inf Process* (2013) 11:1785–95. doi:10.1007/s11128-011-0333-z

21. Lo HK, Ma X, Chen K. Decoy state quantum key distribution. *Phys Rev Lett* (2005) 94:230504. doi:10.1103/PhysRevLett.94.230504

22. Wang XB. Beating the photon-number-splitting attack in practical quantum cryptography. *Phys Rev Lett* (2005) 94:230503. doi:10.1103/PhysRevLett.94.230503

23. Deng FG, Li XH, Zhou HY. Efficient high-capacity quantum secret sharing with two-photon entanglement. *Phys Lett A* (2008) 372(12):1957–62. doi:10.1016/j.physleta.2007.10.066

24. Deng FG, Long GL, Liu XS. Two-step quantum direct communication protocol using the Einstein-Podolsky-Rosen pair block. *Phys Rev A (Coll Park)* (2003) 68(4):042317. doi:10.1103/physreva.68.042317

25. Bennett CH, Brassard G. Quantum cryptography: Public-key distribution and coin tossing. In: Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing; 14-16 Nov. 2005. Bangalore. India: IEEE Press (1984). p. 175–9.

26. Shor PW, Preskill J. Simple proof of security of the BB84 quantum key distribution protocol. *Phys Rev Lett* (2000) 85(2):441–4. doi:10.1103/physrevlett.85.441

27. Wang B, Liu SQ, Gong LH. Semi-quantum private comparison protocol of size relation with d-dimensional GHZ states. *Chin Phys B* (2022) 31:010302. doi:10.1088/1674-1056/ac1413

28. Xu QD, Chen HY, Gong LH, Zhou NR. Quantum private comparison protocol based on four-particle GHZ states. *Int J Theor Phys (Dordr)* (2020) 59:1798–806. doi:10.1007/s10773-020-04446-9

29. Huang SL, Hwang T, Gope P. Multi-party quantum private comparison with an almost-dishonest third party. *Quan Inf Process* (2015) 14:4225–35. doi:10.1007/s11128-015-1104-z

30. Hung SM, Huang SL, Hwang T, Kao SH. Multiparty quantum private comparison with almost dishonest third parties for strangers. *Quan Inf Process* (2017) 16:36. doi:10.1007/s11128-016-1498-2

TYPE Original Research
PUBLISHED 20 September 2022
DOI 10.3389/fphy.2022.1016009

Multiparticle quantum walk–based error correction algorithm with two-lattice Bose–Hubbard model

Shu-Mei Wang[1], Ying-Jie Qu[1], Hao-Wen Wang[2], Zhao Chen[2] and Hong-Yang Ma[1]*

[1]School of Science, Qingdao University of Technology, Qingdao, China, [2]School of Information and Control Engineering, Qingdao University of Technology, Qingdao, China

Check for updates

OPEN ACCESS

EDITED BY
Tianyu Ye,
Zhejiang Gongshang University, China

REVIEWED BY
Hao Cao,
Anhui Science and Technology University, China
Liyun Hu,
Jiangxi Normal University, China
Xiaoping Lou,
Hunan Normal University, China

*CORRESPONDENCE
Hong-Yang Ma,
hongyang_ma@aliyun.com

SPECIALTY SECTION
This article was submitted to Quantum Engineering and Technology, a section of the journal Frontiers in Physics

RECEIVED 10 August 2022
ACCEPTED 24 August 2022
PUBLISHED 20 September 2022

CITATION
Wang S-M, Qu Y-J, Wang H-W, Chen Z and Ma H-Y (2022), Multiparticle quantum walk–based error correction algorithm with two-lattice Bose–Hubbard model.
Front. Phys. 10:1016009.
doi: 10.3389/fphy.2022.1016009

When the evolution of discrete time quantum walk is carried out for particles, the ramble state is prone to error due to the influence of system noise. A multiparticle quantum walk error correction algorithm based on the two-lattice Bose–Hubbard model is proposed in this study. First, two point Bose–Hubbard models are constructed according to the local Euclidean generator, and it is proved that the two elements in the model can be replaced arbitrarily. Second, the relationship between the transition intensity and entanglement degree of the particles in the model is obtained by using the Bethe hypothesis method. Third, the position of the quantum lattice is coded and the quantum state exchange gate is constructed. Finally, the state replacement of quantum walk on the lattice point is carried out by switching the walker to the lattice point of quantum error correction code, and the replacement is carried out again. The entanglement of quantum particles in the double-lattice Bose–Hubbard model is simulated numerically. When the ratio of the interaction between particles and the transition intensity of particles is close to 0, the entanglement operation of quantum particles in the model can be realized by using this algorithm. According to the properties of the Bose–Hubbard model, quantum walking error correction can be realized after particle entanglement. This study introduces the popular restnet network as a training model, which increases the decoding speed of the error correction circuit by about 33%. More importantly, the lower threshold limit of the convolutional neural network (CNN) decoder is increased from 0.0058 under the traditional minimum weight perfect matching (MWPM) to 0.0085, which realizes the stable progress of quantum walk with high fault tolerance rate.

KEYWORDS

quantum error correction, multiparticle quantum walk, Bethe hypothesis, Bose–Hubbard model, threshold

1 Introduction

A quantum walk is one of the effective methods to realize quantum computation [1,2]. However, because of the randomness of quantum walk, it is difficult to correct errors when the particles are affected by system noise during particle evolution. The physical system used in this study is a homogeneous system, which extends the two-lattice Bose–Hubbard model to the Bose–Hubbard model, and the arbitrary replacement of two particles does not lead to a new quantum state of the system [3–6].

A quantum walk algorithm can be implemented on many graph structures, and its function is very significant [7–14]. Also, quantum walks have important applications in quantum cryptography and quantum communication [15,16]. Noise research in the quantum walk algorithm is also one of the key points, and general quantum walk calculation based on the Bose–Hubbard model has been proposed [17,18]. On this basis, the multiparticle quantum walk error correction algorithm based on the two-lattice Bose–Hubbard model is further studied. As early as 2003, Shapira et al. used computer simulation to study the influence of unitary noise on one-dimensional quantum walk and showed the variation of probability distribution of quantum walk under the influence of noise [19]. Also, specific noise types are studied, such as the non-Markov continuous time quantum walk algorithm with dynamic noise [20] and the quantum Bernoulli central limit theorem in the quantum walk algorithm [21]. In 2015, Ambainis et al. improved the potential barrier using the Grover algorithm, improved the amplitude of quantum walking coin state, and reduced the impact of noise during particle quantum walking [21,23]. In 2016, Wang et al. proposed to construct time-varying quantum walking with infinite degrees of freedom by using quantum Bernoulli noise [24]. In 2018, Du et al. constructed quantum gates using the quantum walk algorithm under noise, and the algorithm increased the number of addresses on the graph or the ratio of jump strength to potential could improve the coherence time, thus inhibiting the decoherence [25]. In 2019, Claudia et al. address the use of quantum walks as a quantum probe to characterize defects and perturbations occurring in complex, classical, and quantum networks [26]. These algorithms are designed to reduce the influence of noise on particles during the quantum walk.

Similar to the aforementioned algorithm, a multiparticle quantum walk error correction algorithm is proposed to reduce the influence of noise in the quantum walk. The two-lattice Bose–Hubbard model is constructed for the multiparticle quantum ramble, and it is proved that the quantum state does not change after the displacement of any two particles in the model. Using the encoding method of quantum states mentioned in the study in reference [17], entanglement of quantum states in two lattices is generated by controlling the ratio of transition intensity and interaction between particles [27]. Controlling the ratio of model parameters to generate entanglement is easier than other methods [15,28]. The convolutional neural network decoder has been introduced in detail in the study mentioned in reference [29–33]. In this study, the threshold of the quantum walk error correction circuit has been greatly improved by using the convolution operation of the decoder and the improvement of the training speed. The evolution operator of quantum walk is improved and quantum state error correction is realized. Finally, the advantages and disadvantages of the algorithm are analyzed. Figure 1 shows the core idea of the work.

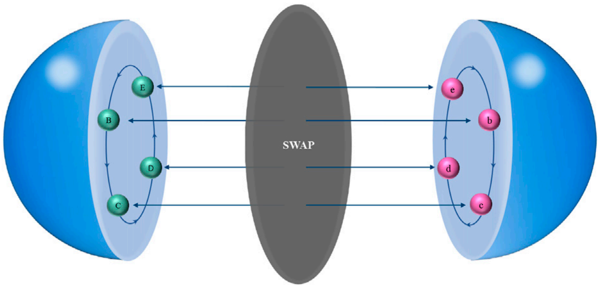


FIGURE 1
In this figure, there are three corresponding layers: the left hemisphere layer is the quantum ramble, right is the error-correcting code, and middle SWAP gate is the exchange gate. The green B → E → B node on the left is the quantum walk process and corresponds to the error correction code of the pink b-e node on the right. When the particles are in a quantum walk, they are swapped through SWAP gate to the lower network to correct errors and then switched back to the original position.

The sections of this article are organized in the following manner. In Section 2, we briefly introduce the background knowledge of discrete quantum walks. In Section 3, the two-lattice Bose–Hubbard model is constructed. In Section 4, the position of the quantum lattice is coded and the quantum state exchange gate is constructed. In Section 5, an analysis of error correction performance is performed, and Section 6concludes the study.

2 Discrete quantum walk

A quantum walk is a quantized model for a classical random walk. The discrete time models discussed here include the walker position state and the "coin" state. The position n of the walker is a vector of infinite dimensional Hilbert space $\mathcal{H}_p$, and the basis vector of Hilbert space is $\{|n\rangle: n \in \mathbf{Z}\}$, which is called the computational basis for position space.

The evolution of the walk depends on the state of a quantum coin. Suppose the walker is on position $|n\rangle$, after the quantum coin is flipped "heads", the walker goes to position $|n+1\rangle$ in the next step. If the coin is flipped "tails", the walker will go to position $|n-1\rangle$. Now, the Hilbert space of the whole ramble system is

$$\mathcal{H} = \mathcal{H}_c \otimes \mathcal{H}_p, \tag{1}$$

where $\mathcal{H}_c$ is a two-dimensional Hilbert space of the quantum coin (different walkers have different throwing operators), and the basis vector of Hilbert space is $\{|0\rangle, |1\rangle\}$. The aforementioned ground state is also the computational basis of the quantum coin space, and the computational basis for space $\mathcal{H}$ is $\{|i\rangle|n\rangle, i \in \{0, 1\}, n \in \mathbf{Z}\}$.

P is the coin operator that determines the direction of the quantum walk. The operator for the walker to move from position $|n\rangle$ to position $|n+1\rangle$ or position $|n-1\rangle$ is called the transition operator S.

$$\begin{array}{l} S|0\rangle|n\rangle = |0\rangle|n+1\rangle \\ S|1\rangle|n\rangle = |1\rangle|n-1\rangle \end{array}. \tag{2}$$

We calculated the representation of the transition operator S under the computational basis of Hilbert space $\mathcal{H}$:

$$S = |0\rangle\langle 0| \otimes \sum |n+1\rangle\langle n| + |1\rangle\langle 1| \otimes \sum |n-1\rangle\langle n|. \tag{3}$$

3 Two-lattice Bose–Hubbard model

It is assumed that the graph structure of quantum walk is G, and the vertices V in the graph represent lattice points and satisfy the local Euclidean symmetry [4]. The two-lattice Bose–Hubbard model is used to describe the discrete time quantum walk in multiparticle interaction on the graph and to correct the error of quantum walk.

To construct the two-lattice Bose–Hubbard model, we first introduce the boson creation (annihilation) operator, $b_j^\dagger (b_j)$, where $j = 1, 2, \ldots, n$, which satisfies the commutation relation:

$$\left[\hat{b}_i, \hat{b}_j\right] = 0, \quad \left[\hat{b}_i^\dagger, \hat{b}_j^\dagger\right] = 0, \quad \left[\hat{b}_i, \hat{b}_j^\dagger\right] = \delta_{ij}. \tag{4}$$

Then we get the Hamiltonian of the two-lattice Bose–Hubbard model:

$$\hat{H} = -t \sum_{k=1}^{\propto} \sum_{j_1 \cdots j_k} \tilde{b}_{j_1}^\dagger \cdots \tilde{b}_{j_k}^\dagger \sum_{j_1' \cdots j_k} \tilde{b}_{j_1}^\dagger \cdots \tilde{b}_{j_k'}^\dagger + \sum_j V\left(\hat{n}_j\right) + \sum_j \epsilon_j \hat{n}_j, \tag{5}$$

where t is the real parameter to describe the particle jumping intensity (in this work $t = 1$), ϵ_j is the local potential, and $V(\hat{n}_j)$ is the interaction between particles at the lattice point:

$$\begin{aligned} V\left(\hat{n}_j\right) &= V_2\left(\hat{n}_j\right) + V_3\left(\hat{n}_j\right) + \cdots \\ &= \frac{U_1}{2}\hat{n}_j\left(\hat{n}_j - 1\right) + \frac{U_2}{6}\hat{n}_j\left(\hat{n}_j - 1\right)\left(\hat{n}_j - 2\right) + \cdots, \end{aligned} \tag{6}$$

where $V_2(\hat{n}_j)$ is the interaction between two particles, $V_3(\hat{n}_j)$ is the interaction between three particles, U_1 and U_2 are the strength of the interaction between particles, and $\hat{n}_j = \hat{b}_j^\dagger \hat{b}_j$.

In Eq. 6, the constraint of the two sets $\{j_1, j_2, \ldots, j_k\}$ and $\{j_1', j_2', \ldots, j_k'\}$ is that the sum extends over all lattice points, and the two sets are not the same. Also, the operator operation condition is satisfied:

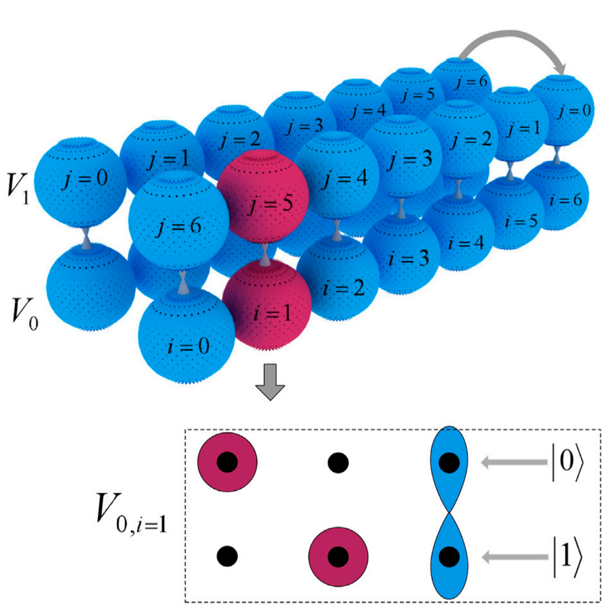


FIGURE 2
Due to the need of quantum walk error correction, two layers of network lattice (V_0 and V_1) are set in the Bose–Hubbard mode. In the 3D figure, the left side represents the original two-dimensional lattice diagram, and the right side represents the lattice encoded by using the Yang diagram method in V_1, where the lattice position in V_0 remains unchanged. The following 2D diagram describes the encoding mode of the particles in the red lattice $V_{0,\, i=1}$ and $V_{0,\, i=1} = |\Phi\rangle = |0\rangle \otimes |1\rangle \otimes | + \rangle$ (the particles in the lattice are encoded using the method described in reference [17]).

$$\tilde{b}_j = f\left(\hat{n}_j\right)\hat{b}_j, \quad \tilde{b}_j^\dagger = \hat{b}_j^\dagger f\left(\hat{n}_j\right), \quad f\left(\hat{n}_j\right) = \frac{1}{\sqrt{\hat{n}_j + 1}}, \tag{7}$$

where $\hat{n}_j = b_j^\dagger b_j$ is the number operator at the lattice point j. Operator $\{\tilde{b}_j, \tilde{b}_j^\dagger, \hat{n}_j\}$ satisfy the commutation relation:

$$\left[\hat{n}_j, \tilde{b}_j\right] = -\tilde{b}_j, \quad \left[\hat{n}_j, \tilde{b}_j^\dagger\right] = \tilde{b}_j^\dagger, \quad \left[\tilde{b}_j, \tilde{b}_j^\dagger\right] = \delta_{n_j 0}. \tag{8}$$

According to the Hamiltonian of the model, the model can make multiple particles transition at the same time without limiting the transition of two adjacent lattice points. In the study mentioned in reference [17], the limit condition of Hilbert space $\mathcal{H}$ of n boson is calculated in the 2^n dimensional computational Hilbert space $\mathcal{C}$, and the location is encoded by subset $\mathcal{H}_\mathcal{C} \subseteq \mathcal{H}$ and $|\mathcal{H}_\mathcal{C}| = 2^n$, along with an isomorphism ρ: $\mathcal{H}_\mathcal{C} \to \mathcal{C}$, where $\mathcal{C}$ and $\mathcal{H}_\mathcal{C}$ are interchangeable. The quantum state $|\Phi\rangle \in \mathcal{H}_\mathcal{C}$ in the model system provides a computer state encoding on the n-qubits, $|\Phi\rangle_\mathcal{C} = \rho(|\Phi\rangle)$. A Hamiltonian was obtained by coupling $\mathcal{H}_\mathcal{C}$ with states space $\mathcal{H}_\tau$ ($\mathcal{H}_\tau$=$\mathcal{H} \backslash \mathcal{H}_\mathcal{C}$) outside of the computational space, which generated entanglement in $\mathcal{C}$. It is proved that any initial state can be mapped to $\mathcal{H}$_{$\mathcal{C}$} and can be returned to $\mathcal{C}$ recoded as a valid computed state.

4 SWAP gate operator construction

Assume two lattices V_0 and V_1 (Figure 2), where V_0 is the location of the quantum walk and V_1 is the error-correcting coded location. The corresponding two lattices in V_0 and V_1 represent a qubit whose calculated ground state is $|0\rangle$ and $|1\rangle$, respectively. The corresponding qubits in the lattice must be entangled, and we show how quantum lattices are encoded and how qubits generate entanglement. Suppose the initial n-qubit state $|\Phi\rangle$ satisfies the following condition:

$$\sum_{i=0}^{1}\left|\langle\Phi\left|\tilde{b}^{\dagger}_{j,i}\tilde{b}_{j,i}\right|\Phi\rangle\right|^{2} = 1. \tag{9}$$

The function of the four calculated ground-state mapping relations and the creation (annihilation) operators for a 10 dimensional space is

$$\begin{aligned}
\tilde{b}^{\dagger}_{j,0}\tilde{b}^{\dagger}_{j+1,0}|00\rangle_i|00\rangle_{i+1} &= |10\rangle_i|10\rangle_{i+1} \leftrightarrow |0\rangle_i|0\rangle_{i+1},\\
\tilde{b}^{\dagger}_{j,0}\tilde{b}^{\dagger}_{j+1,1}|00\rangle_i|00\rangle_{i+1} &= |10\rangle_i|10\rangle_{i+1} \leftrightarrow |0\rangle_i|1\rangle_{i+1},\\
\tilde{b}^{\dagger}_{j,1}\tilde{b}^{\dagger}_{j+1,0}|00\rangle_i|00\rangle_{i+1} &= |10\rangle_i|10\rangle_{i+1} \leftrightarrow |1\rangle_i|0\rangle_{i+1},\\
\tilde{b}^{\dagger}_{j,1}\tilde{b}^{\dagger}_{j+1,1}|00\rangle_i|00\rangle_{i+1} &= |10\rangle_i|10\rangle_{i+1} \leftrightarrow |1\rangle_i|1\rangle_{i+1},
\end{aligned} \tag{10}$$

The Hamiltonian of the two-lattice Bose–Hubbard model is reduced to

$$\begin{aligned}
\hat{H}_1 = &-\sum_{y=1}^{N}\left(t^{y}_{01}b^{\dagger}_{j,0}b_{j,1} + t^{y}_{10}b^{\dagger}_{j,1}b_{j,0}\right)\\
&+\frac{U}{2}\sum_{j=1}^{2}\left[\hat{n}_j\left(\hat{n}_j - 1\right) + \hat{n}_j\left(\hat{n}_j - 1\right)\right],
\end{aligned} \tag{11}$$

when the interaction of two particles and the local potential ϵ_j are considered only. In Eq.6, N is the particle number, and the subscript j is the lattice position, and the parameter t_{ij} is

$$t_{ij} = t\sqrt{\frac{\hat{n}_i!\left(\hat{n}_j - y\right)!}{\hat{n}_j!\left(\hat{n}_i - y\right)!}}. \tag{12}$$

In the two-lattice Bose–Hubbard model, the six lattice points are coded according to the Yang diagram, so the lattice coding sequence is as follows:

$$|0,6\rangle|5,1\rangle|4,2\rangle|3,3\rangle|2,4\rangle|1,5\rangle|0,6\rangle\,, \tag{13}$$

According to the aforementioned Eqs 11, 12, 13, we can get the energy matrix E_6 by matrix diagonalization. From the energy matrix E_6, the eigenvalues $\{E^{(i)}_6\}^{6}_{i=0}$ of lattice particles and the ground state of the model can be obtained when determining the values of U/t, which is helpful for the establishment of the two-lattice Bose–Hubbard model. Moreover, the entangled degree calculation system mentioned in the study in reference [4] is used to calculate the entangled degree between the ground-state particles:

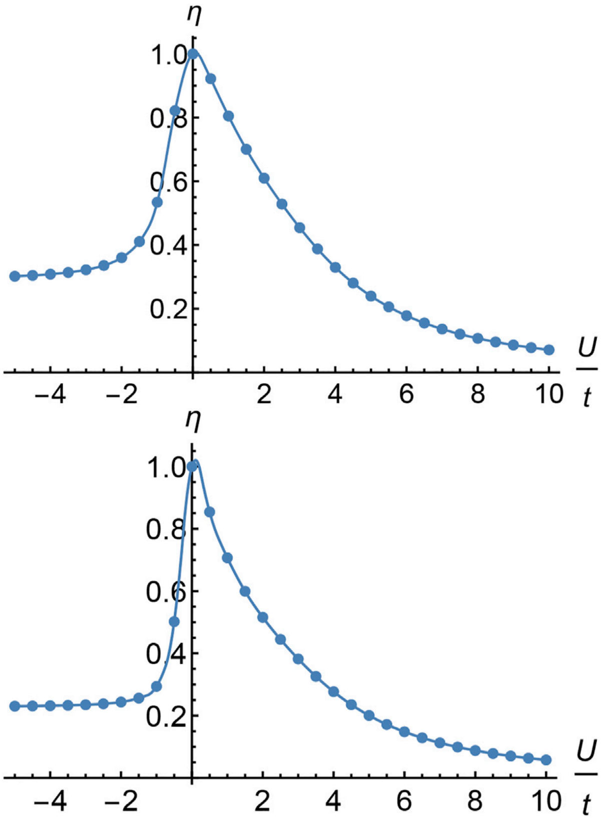


FIGURE 3
According to the Bethe assumption method, the Eq. 17 related to the degree of entanglement can be obtained, which shows the relationship between the degree of entanglement η (vertical axis) and U/t (horizontal axis). The aforementioned two figures are, respectively, the relationship curves of entanglement degree η and U/t when the total number of particles is 10 and 20. It can be seen that the degree of entanglement tends to 1 as $U/t \to 0$, so the two particles in the model can be entangled by controlling the values of parameters U/t.

$$\eta = -\frac{1}{M}\sum_{i=1}^{M} Tr\left(\phi\right)_i log_{N+1}\left(\phi\right)_i, \tag{14}$$

where N is the number of particles, M is the number of lattices, and $(\phi)_i$ is the reduced density matrix at the *ith* lattice point. The next step is to find the relationship between the specific value U/t and the degree η of entanglement. The lattice energy matrix of the seven lattice points is shown below.

$$E_6 = -t\begin{pmatrix} -\frac{15U}{t} & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -\frac{10U}{t} & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & -\frac{7U}{t} & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & -\frac{6U}{t} & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & -\frac{7U}{t} & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & -\frac{10U}{t} & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & -\frac{15U}{t} \end{pmatrix}. \tag{15}$$

According to the eigenenergy, the Bethe hypothesis method can be obtained, as follows:

$$F(m,n) = E^{(\delta)} - t - \sum_j V(\hat{n}_j) - \sum_{j=1}^{M} \epsilon_j \hat{n}_j, \tag{16}$$

where $-t\sum_{m,n}C(m,n)/F(m,n) = 1$, m and n ($m \geq n$) are the number in the lattice points, when $m = n$ and $C(m, n) = 1$ and when $m \neq n$ and $C(m, n) = 2$. According to Eq. 16, the calculation formula of entanglement is improved:

$$\eta = \sum_{m,n}^{N} \frac{1}{F(m,n)^2} log_{N+1} \frac{1}{F(m,n)^2}. \tag{17}$$

We can get the degree of entanglement between the two lattice points to 1 at $U/t \to 0$, as shown in Figure 3. The SWAP gate is obtained by limiting [4] to $U/t \approx 0$:

$$\frac{U}{t} = 4\sqrt{\frac{a^2}{(2b+1)^2} - 1} \approx 0, \quad a, b \in \mathbf{Z}, \tag{18}$$

$$SWAP = \begin{pmatrix} e^{-i\alpha\pi} & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & e^{-i\alpha\pi} \end{pmatrix}, \tag{19}$$

where $\alpha = b + \sqrt{l^2 - 4a(a+1) - 1}$ a and b need to be evaluated according to the degree of entanglement η to ensure the degree of entanglement between two particles.

5 Error correction and analysis

5.1 Quantum walk error correction

Because the generator of local Euclidean symmetry is used to construct the two-lattice Bose–Hubbard model, it is necessary to modify the quantum ramble operator. Assuming that the generator in the model (n lattices) is $\{\xi_i\}_{i=1}^{n}$, the modification of quantum walk transfer operator and coin operator is as follows:

$$P' = \sum_{p,\ q=0}^{1} |\xi_p\rangle\langle\xi_q|, \tag{20}$$

$$S' = |\xi_0\rangle\langle\xi_0| \otimes \sum_{n=0}^{N-1} |n+1\rangle\langle n| + |\xi_1\rangle\langle\xi_1| \otimes \sum_{n=1}^{N} |n-1\rangle\langle n|. \tag{21}$$

Because it is currently in a two-dimensional physical system, the aforementioned formula only takes two generative elements to construct the quantum walk evolution operator.

In the previous section, we showed that the quantum states of two corresponding lattice points can be entangled by controlling the ratio of the parameters U/t. Thus, according to the Properties of the Bose–Hubbard model, when particle qubits wander to lattice point α, it can be exchanged with another lattice point α', which becomes entangled with the particle qubits through the exchange gate and corrects the error.

In the space of N-qubits, a single-bit quantum measurement will appear at each lattice point when the evolution of the particles is in the discrete time quantum walk. The measurement operator is:

$$V = \sum_{i=0}^{N-1} \sum_{j=0}^{1} |v\rangle_{i,j} \langle v|_{i,j}, \tag{22}$$

where, $|v\rangle_{i,0}$ is the encoded quantum state in the first lattice in Figure 2, which is the state of quantum walk; $|v\rangle_{i,1}$ is the quantum state in the second lattice, which is used to assist quantum error correction. Also, the lattice locations of $|v\rangle_{i,0}$ and $|v\rangle_{i,1}$ are entangled in the model. The quantum state $|v\rangle_{i,0}$ has superposition state in the process of quantum walk:

$$|\Psi(t)\rangle = \sum_{n=0}^{N-1} \psi_{0,n}(t)|\xi_0, n\rangle + \psi_{1,n}(t)|\xi_1, n\rangle, \tag{23}$$

where $\psi_{0,n}$ and $\psi_{1,n}$ are the amplitude, $|\xi_0\rangle$ and $|\xi_1\rangle$ are the coin state, and $|n\rangle$ is the position state. In the process of quantum walk, there are mainly two kinds of errors, which are phase inversion and bit inversion. However, the amplitude in Eq. 23 is generated by the superposition state, so the detection and correction of walker errors are mainly aimed at bit inversion errors. The quantum walk error correction circuit is shown in Figure 4. In order to suppress the error generated in the quantum walk, the noise error based on the double-lattice Bose–Hubbard model in the quantum walk is reduced by reducing the circuit gate overhead. Taking depolarization noise as an example, the data map is obtained through the training of the decoder. The decoder uses the convolutional neural network [27–29] in the current hot machine learning algorithm as the dominant algorithm to decode the quantum information in the line. The specific decoding training model is shown in Figure 5. By training with different restnet layers, the accuracy and speed of training are improved; the speed is 1/3 higher than before and the accuracy reaches 99.82%.

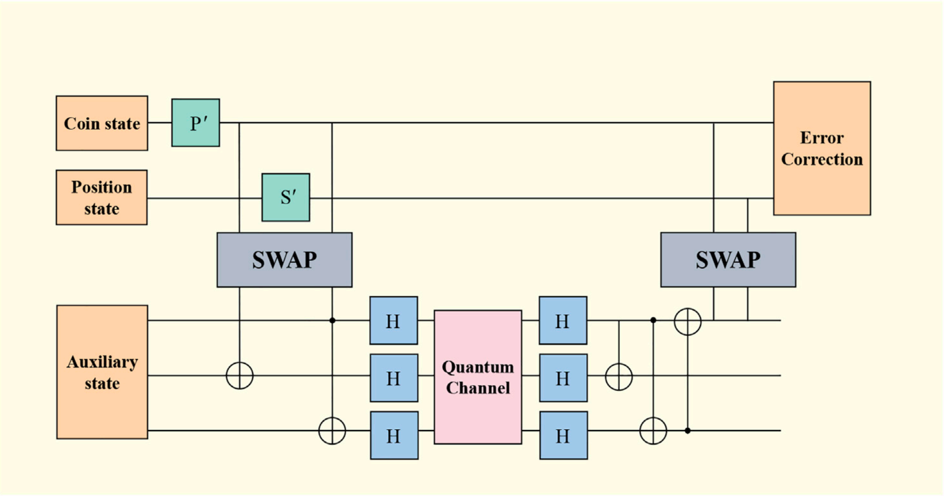


FIGURE 4
Quantum walk error correction circuit diagram. During the quantum walk, the particles are swapped into another lattice *via* the SWAP gate, which is then swapped into the lattice of quantum walk after correcting the coin state and the initial state by the quantum error-correcting code.

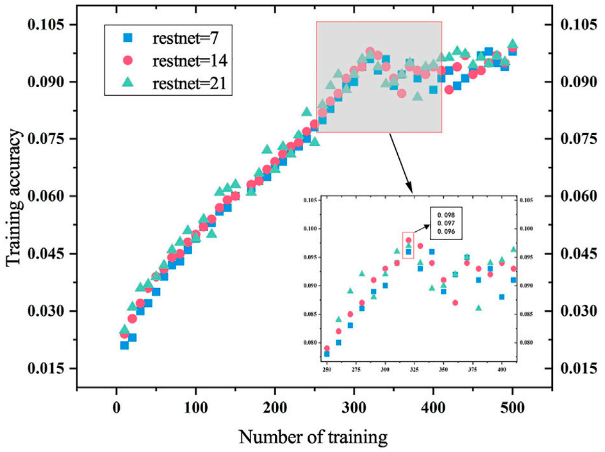


FIGURE 5
Number of training times corresponds to a function of training error rate and training accuracy. The horizontal axis represents the number of training sessions, and the vertical axis represents the training error rate and accuracy rate. Restnet=7, restnet=14, and restnet=21 are marked with blue, red, and green, separately. For intuitive viewing, zoom plots are set up to make it easier to observe the data.

TABLE 1 Unified quantization of network layers under different decoders.

	Trainable dataset	Steps	Accuracy (%)
MWPM	1.48×10^5	4.8×10^4	75.388
RestNet7	1.37×10^3	3.1×10^3	84.256
RestNet14	2.75×10^3	2.9×10^3	88.792
RestNet21	3.79×10^3	1.7×10^3	96.753

5.2 Algorithm analysis

At present, there are many research achievements in quantum walking. For example, the quantum state operator based on the Bose–Hubbard model is given in the study in reference [17], including single-bit operation, entanglement operation, and permutation operation. This study mainly studies the error correction of system noise during a quantum walk.

The algorithm is based on the two-lattice Bose–Hubbard model, and the evolution of the quantum walk algorithm is carried out. In the first section, it is proved that no new quantum state will be generated after the particles are replaced in the model [17]. Based on the model, this algorithm can correct the quantum walk error by using quantum error correction coding. In the second section, according to the Bethe hypothesis method mentioned in reference [4], we can get the relationship between energy eigenvalues, particle transition intensity, particle interaction, and entanglement (Eq. (17)). Therefore, two lattice points can be entangled by controlling the value of U/t, and the step of generating entanglement can be omitted compared with the study mentioned in reference [17].

5.3 Error correction performance analysis

We extracted non-local regularities from noise and performed transfer learning in various tasks. Applying this advantage to the cost of qubits passing through quantum gates can reduce the cost of qubits. The qubits contain auxiliary qubits in the synthetic measurement process, and the logic overhead is the cost of the auxiliary qubits during the synthetic measurement process.

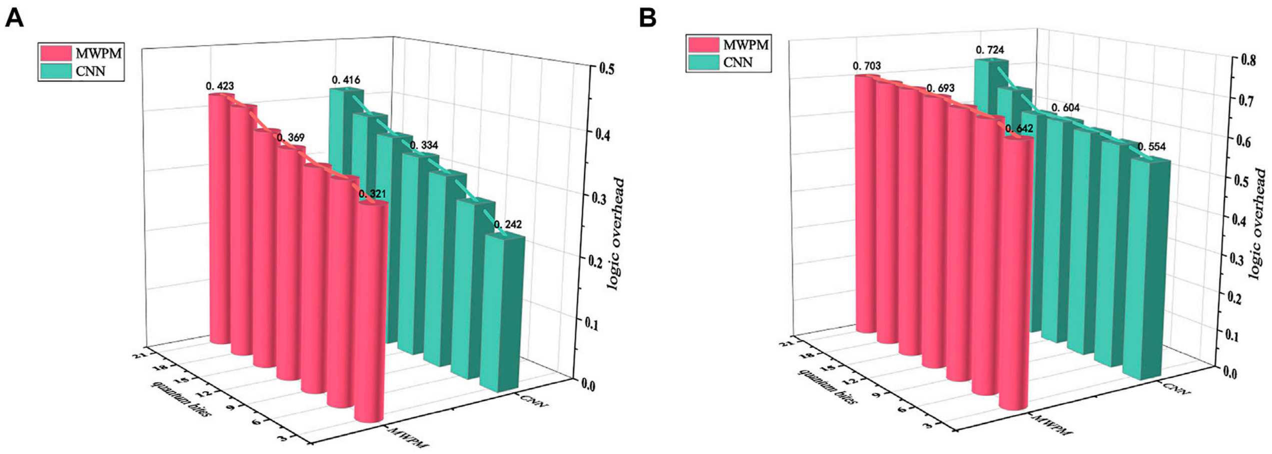


FIGURE 6
Quantum circuit gate overhead data graph. **(A)** When *threshold* = 0.005, the cost of MWPM is compared with the optimization cost of CNN network. **(B)** When *threshold* = 0.0085, the cost of MWPM is compared with the optimization cost of CNN network. Among them, the abscissa represents the number of qubits, displayed in scientific notation, and the ordinate is the logical cost. The cost of CNN is marked in pink, and the cost of CNN optimization is marked in green.

Threshold is an effective way to characterize fault tolerance performance. Specifically, applying quantum error correction for efficient quantum computing can suppress the logical error rate to arbitrarily low levels when the physical error rate of the qubits is below a certain threshold. The CNN used in this study is used for experiments. The number of simulated qubits varies from 3.8×10^3 to 1.5×10^5 bits. The specific training data quantification is shown in Table 1. Comparing the overhead of MWPM and CNN optimization with thresholds of 0.0058 and 0.0085. Figure 6A shows that with the increase of the number of qubits both the MWPM overhead and the CNN overhead increase, but the increase in CNN-optimized overhead is significantly lower than that of the MWPM overhead. Figure 6B shows that as the number of qubits increases, the optimization overhead of CNN also gets much lower than the original one; although when the number of qubits is 2.0×10^8, the overhead of the optimized CNN is slightly higher than the original one. At the same time, comparing the results under different thresholds in Figure 6, it can be found that the larger threshold, the greater the overhead of quantum circuit gate.

6 Conclusion

In this study, a multiparticle quantum walk error correction algorithm based on the two-lattice Bose–Hubbard model is proposed. This algorithm controls the proportion of the interaction between particles and the transition intensity of particles to realize the entanglement of quantum state in two lattices and then corrects the quantum walking error by using the invariant property of model particle replacement. Under the condition of the threshold of 0.0085, the restnet network layer is used as a training model, and the error noise of quantum walk is reduced by decoding the error correction circuit model, so as to achieve a more stable walk circuit. Compared with the traditional quantum walk error correction, the threshold limit is increased from 0.0058 under the traditional MWPM to 0.0085, and the speed is increased by a full 1/3. However, when the number of particles or the size of the system exceeds a certain threshold, it is impossible to accurately control the transition strength of particles and the interaction between particles, thus destroying the entanglement operation. The development of quantum convolutional neural network is relatively mature at present, and it is the focus of the next research, in preparation for further improving the fault tolerance performance.

Data availability statement

The original contributions presented in the study are included in the article/Supplementary Material; further inquiries can be directed to the corresponding author.

Author contributions

S-MW: conceptualization, methodology, and software; Y-JQ: data curation and writing—original draft preparation; H-WW:

visualization, investigation, and supervision; ZC: writing—reviewing and editing; H-YM: conceptualization, funding acquisition, and resources.

Funding

This project was supported by the National Natural Science Foundation of China (Grant No. 61772295), Natural Science Foundation of Shandong Province, China (Grant Nos. ZR2021MF049, ZR2019YQ01), and Project of Shandong Provincial Natural Science Foundation Joint Fund Application (ZR202108020011).

Conflict of interest

The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Publisher's note

All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors, and the reviewers. Any product that may be evaluated in this article, or claim that may be made by its manufacturer, is not guaranteed or endorsed by the publisher.

References

1. Aharonov Y, Davidovich L, Zagury N. Quantum random walks. *Phys Rev A (Coll Park)* (1993) 48:1687–90. doi:10.1103/PhysRevA.48.1687

2. Kempe J. Quantum random walks: An introductory overview. *Contemp Phys* (2003) 44:307–27. doi:10.1080/00107151031000110776

3. Anderson MH, Ensher JR, Matthews MR, Wieman CE, Cornell EA. Observation of bose-einstein condensation in a dilute atomic vapor. *Science* (1995) 269:198–201. doi:10.1126/science.269.5221.198

4. Zwierlein MW, Stan CA, Schunck CH, Raupach SM, Gupta S, Hadzibabic Z, et al. Observation of bose-einstein condensation of molecules. *Phys Rev Lett* (2003) 91:250401. doi:10.1103/PhysRevLett.91.250401

5. Kennedy CJ, Burton WC, Chung WC, Ketterle W. Observation of bose–einstein condensation in a strong synthetic magnetic field. *Nat Phys* (2015) 11:859–64. doi:10.1038/nphys3421

6. Aveline DC, Williams JR, Elliott ER, Dutenhoffer C, Kellogg JR, Kohel JM, et al. Observation of bose–einstein condensates in an earth-orbiting research lab. *Nature* (2020) 582:193–7. doi:10.1038/s41586-020-2346-1

7. Ghosal A, Deb P. Quantum walks over a square lattice. *Phys Rev A (Coll Park)* (2018) 98:032104. doi:10.1103/PhysRevA.98.032104

8. Wong TG. Isolated vertices in continuous-time quantum walks on dynamic graphs. *Phys Rev A* (2019) 100:062325. doi:10.1103/PhysRevA.100.062325

9. Szigeti BE, Homa G, Zimborás Z, Barankai N. Short-time behavior of continuous-time quantum walks on graphs. *Phys Rev A (Coll Park)* (2019) 100:062320. doi:10.1103/PhysRevA.100.062320

10. Cao W, Yang Y, Li D, Dong J, Zhou Y, Shi W. Quantum state transfer on unsymmetrical graphs via discrete-time quantum walk. *Mod Phys Lett A* (2019) 34:1950317. doi:10.1142/S0217732319503176

11. Zhan H. An infinite family of circulant graphs with perfect state transfer in discrete quantum walks. *Quan Inf Process* (2019) 18:369–26. doi:10.1007/s11128-019-2483-3

12. Feng Y, Shi R, Shi J, Zhou J, Guo Y. Arbitrated quantum signature scheme with quantum walk-based teleportation. *Quan Inf Process* (2019) 18:154–21. doi:10.1007/s11128-019-2270-1

13. Rhodes ML, Wong TG. Quantum walk search on the complete bipartite graph. *Phys Rev A (Coll Park)* (2019) 99:032301. doi:10.1103/PhysRevA.99.032301

14. Qiang X, Wang Y, Xue S, Ge R, Chen L, Liu Y, et al. Implementing graph-theoretic quantum algorithms on a silicon photonic quantum walk processor. *Sci Adv* (2021) 7:eabb8375. doi:10.1126/sciadv.abb8375

15. Wang Y, Lou X, Fan Z, Wang S, Huang G. Verifiable multi-dimensional (t,n) threshold quantum secret sharing based on quantum walk. *Int J Theor Phys* (2022) 61:1–17. doi:10.1007/s10773-022-05009-w

16. Lou X, Wang S, Ren S, Zan H, Xu X. Quantum identity authentication scheme based on quantum walks on graphs with ibm quantum cloud platform. *Int J Theor Phys (Dordr)* (2022) 61:40–15. doi:10.1007/s10773-022-04986-2

17. Underwood MS, Feder DL. Bose-hubbard model for universal quantum-walk-based computation. *Phys Rev A* (2012) 85:052314. doi:10.1103/PhysRevA.85.052314

18. Ye Tian-Yu, Geng Mao-Jie, Xu Tian-Jie, Chen Ying. Efficient semiquantum key distribution based on single photons in both polarization and spatial-mode degrees of freedom. *Quantum Information Processing*, 2022, 21(4) 123.

19. Shapira D, Biham O, Bracken A, Hackett M. One-dimensional quantum walk with unitary noise. *Phys Rev A (Coll Park)* (2003) 68:062315. doi:10.1103/PhysRevA.68.062315

20. Benedetti C, Buscemi F, Bordone P, Paris MG. Dynamics of quantum correlations in colored-noise environments. *Phys Rev A (Coll Park)* (2013) 87:052328. doi:10.1103/PhysRevA.87.052328

21. Wang C, Wang C, Tang Y, Ren S. Quantum walk in terms of quantum Bernoulli noise and quantum central limit theorem for quantum Bernoulli noise. *Adv Math Phys* (2018) 2018:1–9. doi:10.1155/2018/2507265

22. Ambainis A, Wong TG. Correcting for potential barriers in quantum walk search. *arXiv preprint* (2015). doi:10.48550/arXiv.1505.02035

23. Ye Tian-Yu, Li Hong-Kun, Hu Jia-Li. Semi-quantum key distribution with single photons in both polarization and spatial-mode degrees of freedom. International Journal of Theoretical Physics, 2020, 59(9) 2807–2815.

24. Wang C, Ye X. Quantum walk in terms of quantum Bernoulli noises. *Quan Inf Process* (2016) 15:1897–908. doi:10.1007/s11128-016-1259-2

25. Du Y, Lu L, Li Y. A rout to protect quantum gates constructed via quantum walks from noises. *Sci Rep* (2018) 8:7117–1. doi:10.1038/s41598-018-25550-1

26. Benedetti C, Rossi MA, Paris MG. Continuous-time quantum walks on dynamical percolation graphs. *EPL (Europhysics Letters)* (2019) 124:60001. doi:10.1209/0295-5075/124/60001

27. Cai W, Ma Y, Wang W, Zou C, Sun L. Bosonic quantum error correction codes in superconducting quantum circuits. *Fundam Res* (2021) 1:50–67. doi:10.1016/j.fmre.2020.12.006

28. Qiu T, Li H, Xie M. Coherent generation and manipulation of stationary light pulses encoded in degrees of freedom of polarization and orbital angular momentum. *Phys Rev A (Coll Park)* (2019) 100:013844. doi:10.1103/PhysRevA.100.013844

29. Chen H, Zhang Y, Kalra MK, Lin F, Chen Y, Liao P, et al. Low-dose ct with a residual encoder-decoder convolutional neural network. *IEEE Trans Med Imaging* (2017) 36:2524–35. doi:10.1109/TMI.2017.2715284

30. Xie T, Grossman JC. Crystal graph convolutional neural networks for an accurate and interpretable prediction of material properties. *Phys Rev Lett* (2018) 120:145301. doi:10.1103/PhysRevLett.120.145301

31. Li J, Zhang H, Chen JZ. Structural prediction and inverse design by a strongly correlated neural network. *Phys Rev Lett* (2019) 123:108002. doi:10.1103/PhysRevLett.123.108002

32. Maskara N, Kubica A, Jochym-O'Connor T. Advantages of versatile neural-network decoding for topological codes. *Phys Rev A (Coll Park)* (2019) 99:052351. doi:10.1103/PhysRevA.99.052351

33. Varona S, Martin-Delgado MA. Determination of the semion code threshold using neural decoders. *Phys Rev A* (2020) 102:032411. doi:10.1103/PhysRevA.102.032411

TYPE Original Research
PUBLISHED 23 September 2022
DOI 10.3389/fphy.2022.1006255

Scheme for implementing nonlocal high-fidelity quantum controlled-not gates on quantum-dot-confined electron spins using optical microcavities and photonic hyperentanglement

Yu-Hong Han[1,2,3], Cong Cao[1,4,5]*, Ling Fan [4,5] and Ru Zhang [1,2,5]

[1]State Key Laboratory of Information Photonics and Optical Communications, Beijing University of Posts and Telecommunications, Beijing, China, [2]School of Science, Beijing University of Posts and Telecommunications, Beijing, China, [3]School of Information and Communication Engineering, Beijing University of Posts and Telecommunications, Beijing, China, [4]School of Electronic Engineering, Beijing University of Posts and Telecommunications, Beijing, China, [5]Beijing Key Laboratory of Space-ground Interconnection and Convergence, Beijing University of Posts and Telecommunications, Beijing, China

Quantum information networks can transmit quantum states and perform quantum operations between different quantum network nodes, which are essential for various applications of quantum information technology in the future. In this paper, a potentially practical scheme for implementing nonlocal quantum controlled-not (CNOT) gate operations on quantum-dot-confined electron spins between two quantum network nodes is presented. The scheme can realize parallel teleportation of two nonlocal quantum CNOT gates simultaneously by employing hyperentangled photon pairs to establish quantum channel, which can effectively improve the channel capacity and operational speed. The core of the scheme are two kinds of photon-spin hybrid quantum CNOT gate working in a failure-heralded and fidelity-robust fashion. With the heralded mechanism, the nonlocal CNOT gates can be implementated with unity fidelities in principle, even if the particularly ideal conditions commonly used in other schemes are not satisfied strictly. Our analysis and calculations indicate that the scheme can be demonstrated efficiently (with efficiency exceeding 99%) with current or near-future technologies. Moreover, the utilized photon-spin hybrid quantum gates can be regarded as universal modules for many other quantum information processing (QIP) tasks. Therefore, the scheme is potential for constructing elementary quantum networks, and realizing nolocal QIP with high channel capacities, high fidelities, and high efficiencies.

KEYWORDS

quantum network, quantum CNOT gate, quantum-dot spin, optical microcavity, hyperentanglement

OPEN ACCESS

EDITED BY
Tianyu Ye,
Zhejiang Gongshang University, China

REVIEWED BY
Ma Hongyang,
Qingdao University of Technology, China
Chuan Wang,
Beijing Normal University, China

*CORRESPONDENCE
Cong Cao,
caocong@bupt.edu.cn

SPECIALTY SECTION
This article was submitted to Quantum Engineering and Technology,
a section of the journal
Frontiers in Physics

RECEIVED 29 July 2022
ACCEPTED 18 August 2022
PUBLISHED 23 September 2022

CITATION
Han Y-H, Cao C, Fan L and Zhang R (2022), Scheme for implementing nonlocal high-fidelity quantum controlled-not gates on quantum-dot-confined electron spins using optical microcavities and photonic hyperentanglement.
Front. Phys. 10:1006255.
doi: 10.3389/fphy.2022.1006255

1 Introduction

Quantum information technology, which aims to develop new theories and methods for processing information based on the laws of quantum mechanics, has developed very rapidly during the past decades. The main branches of this field, i.e., quantum communication [1], quantum computation [2–4], and quantum metrology [5, 6], have been established and become the focus of research. One of the ultimate directions for the development and integration of quantum information technology in the future is to construct quantum information networks [7–9], which are considered as spatially separated quantum network nodes connected by quantum communication channels. The fundamental characteristic of quantum networks lies in the capability to nonlocally transmit not only quantum states but also quantum operations between different quantum nodes, which makes it essential for various applications such as quantum secure direct communication [10–15] and secure multi-party quantum computation [16–21]. The quantum network can therefore significantly improve the power of quantum information processing (QIP) compared with individual QIP systems.

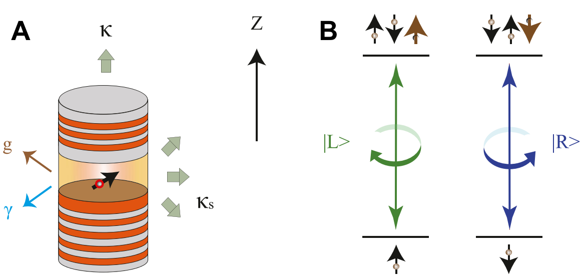


FIGURE 1
(A) Schematic diagram of a singly charged QD inside a single-sided optical micropillar cavity with two DBRs and circular cross section. g is the QD-microcavity coupling strength. γ is the exciton decay rate. κ and κ_s are the cavity-mode decay rates into the input-output mode and the leaky mode (side leakage), respectively. **(B)** The energy levels and the optical transition rule of exciton transitions. $|L\rangle$ and $|R\rangle$ represent the photonic left-circularly and right-circularly polarized states, respectively. The left-circularly polarized photon $|L\rangle$ and the right-circularly polarized photon $|R\rangle$ drive the transitions $|\uparrow\rangle \rightarrow |\uparrow\downarrow\Uparrow\rangle$ and $|\downarrow\rangle \rightarrow |\downarrow\uparrow\Downarrow\rangle$, respectively. z axis is the spin-quantization axis.

For the physical implementation of quantum networks, photon is the best carrier for fast and reliable communication over long distance, which plays the central role in the realization of nonlocal interactions between spatially distant quantum network nodes [22–24]. In particular, some interesting schemes for implementing nonlocal quantum operations between two different nodes have been proposed based on the sharing of entangled photon pairs, which act as the quantum channel for the teleportation of quantum gates [25–29]. In contrast to other schemes which rely on the transmission of a single photon through an optical channel to transmit interaction between two separate nodes, an attractive advantage of teleportation-based architectures is that the environmental noise and photon loss could be well overcome *via* entanglement purification together with quantum repeaters [30–36]. Moreover, photon possesses multiple degrees of freedom (DOFs) for encoding, such as polarization, spatial mode, frequency, time bin, and orbit angular momentum. Photon hyperentanglement [37–39], which refers to entanglements simultaneously existing in multiple DOFs of photons, has been demonstrated and proven useful in high-performance quantum communications [40–45], and hence represents a valuable quantum resource for quantum networks.

Solid-state spin systems such as electron or hole spins confined in semiconductor quantum dots (QDs) are ideal candidates for stationary qubits due to their good properties such as spin coherence and potential scalability [46–50]. Fast initialization, manipulation, and measurement of electron spins in charged QDs have been well-investigated [51–54]. Spin echo and dynamical decoupling techniques can be used to preserve the electron-spin coherence [55, 56]. With the help of optical microcavities or nanocavities, effective coupling between photons and singly charged QDs can be realized in coupled QD-cavity systems, which is crucial for realizing various quantum interfaces between single photons and spins [57–60]. With the photon-spin quantum interfaces, many QIP schemes such as universal quantum logic gates [61–67], quantum entanglement generation and analysis [68–73], and quantum entanglement purification and concentration [74–77] have been proposed. The QD-cavity systems supply ideal platforms for implementing quantum networks by constituting the quantum nodes and providing photon-spin interfaces [78, 79]. Significant progress has been achieved towards the practical demonstration of the photon-spin interfaces. For example, photon sorter [80], photon switch [81], Faraday rotation induced by a single electron or hole spin [82, 83] have been explored in experiments. These experiments were performed in the weakly-coupled cavity quantum electrodynamics (QED) regime.

In this work, we present a potentially practical scheme for implementing nonlocal quantum controlled-not (CNOT) gate operations on QD-confined electron spins between two quantum network nodes, by exploiting optical microcavities, hyperentangled photon pairs, and linear-optical elements. The scheme can realize parallel teleportation of two nonlocal quantum CNOT gates simultaneously by employing hyperentangled photon pairs to establish quantum channel, which can effectively improve the channel capacity and operational speed of the quantum network. The core units of the scheme are two kinds of photon-spin hybrid quantum CNOT gate constructed based on the interaction between an input photon and a singly charged QD mediated by a single-sided optical microcavity, which work in a failure-heralded and fidelity-robust fashion. With the help of the heralded mechanism, the nonlocal CNOT gates can be implemented with unity fidelities in principle, even if the particularly ideal conditions commonly used in other schemes are not satisfied strictly. Our analysis and calculations indicate that the scheme can be demonstrated efficiently with current or near-future technologies. Moreover, the photon-spin hybrid quantum gates used in this scheme can be regarded as universal modules, and can be used in many other QIP tasks. Therefore, the scheme has potential application prospects in constructing elementary quantum networks and realizing nonlocal QIP tasks with high channel capacities, high fidelities, and high efficiencies.

2 Interaction between an input photon and a singly charged QD mediated by a single-sided optical microcavity

As shown in Figure 1A, we consider a singly charged semiconductor QD [e.g., a self-assembled In(Ga)As QD or a GaAs interface QD] with an excess electron embedded in a single-sided optical micropillar cavity constructed by two GaAs/Al(Ga)As distributed Bragg reflectors (DBRs) and with a circular cross-section. The bottom DBR is 100% reflective and the top DBR is partially reflective so that the single-sided cavity hypothesis is valid. When we consider an input single photon interacting with the singly charged QD mediated by the single-sided optical microcavity, it has been proven that the optical property of the singly charged QD is dominated by the spin-dependent optical transitions of a negatively charged exciton (X^{-}). The X^{-} is composed of two electrons bound to one hole, and the optical transition rule is based on the Pauli exclusion principle and the conservation of total spin angular momentum. The related energy levels and the optical transition rule of X^{-} transitions is shown in Figure 1B. The left-circularly polarized photon $|L\rangle$ and the right-circularly polarized photon $|R\rangle$ drive the transitions $|\uparrow\rangle \rightarrow |\uparrow\downarrow\Uparrow\rangle$ and $|\downarrow\rangle \rightarrow |\downarrow\uparrow\Downarrow\rangle$, respectively. Here, we use $|\uparrow\rangle$ and $|\downarrow\rangle$ to represent the excess-electron spin states with spins $J_z = \frac{1}{2}$ and $-\frac{1}{2}$, respectively. $|\Uparrow\rangle$ and $|\Downarrow\rangle$ represent the heavy-hole spin states with spins $J_z = \frac{3}{2}$ and $-\frac{3}{2}$, respectively. The spin-quantization axis (z-axis) is along the normal direction of the cavity.

By solving the Heisenberg-Langevin equations of the cavity mode operator $\hat{a}$ and the X^{-} dipole operator $\hat{\sigma}_{-}$ in the interaction picture, we can calculate the optical reflection coefficient of the QD-cavity system [57]. Including losses in both the cavity and QD, as well as cavity excitation, we can attain the Heisenberg–Langevin equations as

$$\begin{aligned} \frac{d\hat{a}}{dt} &= -\left[i(\omega_c - \omega) + \frac{\kappa}{2} + \frac{\kappa_s}{2}\right]\hat{a} - g\hat{\sigma}_{-} - \sqrt{\kappa}\hat{a}_{in} + \hat{H}, \\ \frac{d\hat{\sigma}_{-}}{dt} &= -\left[i(\omega_{X^{-}} - \omega) + \frac{\gamma}{2}\right]\hat{\sigma}_{-} - g\hat{\sigma}_z\hat{a} + \hat{G}. \end{aligned} \tag{1}$$

Here, ω_c, ω, and $\omega_{X^{-}}$ represent frequencies of the cavity mode, the incident photon, and the X^{-} transition, respectively. κ and κ_s are the input-output decay rate and the leakage rate of the cavity field mode. g is the coupling strength between X^{-} and the cavity mode. γ is the X^{-} dipole decay rate. $\hat{\sigma}_z$ is the population operator. $\hat{a}_{in}$ is the input field operator, which connects to the output field operator $\hat{a}_{out}$ through the standard cavity input-output relation $\hat{a}_{out} = \hat{a}_{in} + \sqrt{\kappa}\hat{a}$. $\hat{H}$ and $\hat{G}$ are the noise operators related to reservoirs. In the approximation of weak excitation, we take $\langle\hat{\sigma}_z\rangle = -1$ and the reflection coefficient of the QD-cavity system can be described by

$$r(\Delta, g) = \frac{\left(i\Delta + \frac{\gamma}{2}\right)\left(i\Delta - \frac{\kappa}{2} + \frac{\kappa_s}{2}\right) + g^2}{\left(i\Delta + \frac{\gamma}{2}\right)\left(i\Delta + \frac{\kappa}{2} + \frac{\kappa_s}{2}\right) + g^2}. \tag{2}$$

Here we set $\omega_c = \omega_{X^{-}}$, and $\Delta = \omega_{X^{-}} - \omega = \omega_c - \omega$ is the frequency detuning between the input photon and the cavity mode. When the photon does not couple to the QD ($g = 0$), the reflection coefficient is

$$r(\Delta, 0) = \frac{i\Delta - \frac{\kappa}{2} + \frac{\kappa_s}{2}}{i\Delta + \frac{\kappa}{2} + \frac{\kappa_s}{2}}. \tag{3}$$

When the excess electron is in the spin state $|\uparrow\rangle(|\downarrow\rangle)$, only the $|L\rangle(|R\rangle)$ state photon can couple to the transition $|\uparrow\rangle\leftrightarrow|\uparrow\downarrow\Uparrow\rangle(|\downarrow\rangle\leftrightarrow|\downarrow\uparrow\Downarrow\rangle)$ and obtain the reflection coefficient $r(\Delta, g)$, while the $|R\rangle(|L\rangle)$ photon would feel an empty cavity and obtain the reflection coefficient $r(\Delta, 0)$. This is due to the optical transition rule and the cavity-QED effect. The reflection coefficients of coupled case $r(\Delta, g)$ and uncoupled case $r(\Delta, 0)$ can be significantly different, which is the so called giant circular birefringence effect [57]. As the single-photon input-output process is coherent, this description holds for superposition states as well. Therefore, when a horizontal polarized photon $|H\rangle = (|R\rangle + |L\rangle)/\sqrt{2}$ or a vertical polarized photon $|V\rangle = -i(|R\rangle - |L\rangle)/\sqrt{2}$ interacts with a QD-cavity system with the excess electron spin being prepared in the state $|\pm\rangle = (|\uparrow\rangle \pm |\downarrow\rangle)/\sqrt{2}$ initially, the photon-spin hybrid system evolves according to the following rules

$$\begin{aligned} |H\rangle|\pm\rangle &\rightarrow \left[r_{+}(\Delta)|H\rangle|\pm\rangle + ir_{-}(\Delta)|V\rangle|\mp\rangle\right]\big/\sqrt{p_1}, \\ |V\rangle|\pm\rangle &\rightarrow \left[ir_{+}(\Delta)|V\rangle|\pm\rangle + r_{-}(\Delta)|H\rangle|\mp\rangle\right]\big/\sqrt{p_1}. \end{aligned} \tag{4}$$

Here, $r_{\pm}(\Delta) = [r(\Delta, 0) \pm r(\Delta, g)]/2$, $p_1 = [|r(\Delta, 0)|^2 + |r(\Delta, g)|^2]/2$ is the probability of the photon being reflected by the QD-cavity system. That is, after the photon interacts with the QD-cavity system, the photon-spin system evolves into an orthogonally entangled state with two components: 1) due to the imperfect photon scattering process in reality, both the photon and electron spin remain unchanged with the probability of $|r_{+}(\Delta)|^2/p_1$; 2) both the photon and electron spin are flipped with the

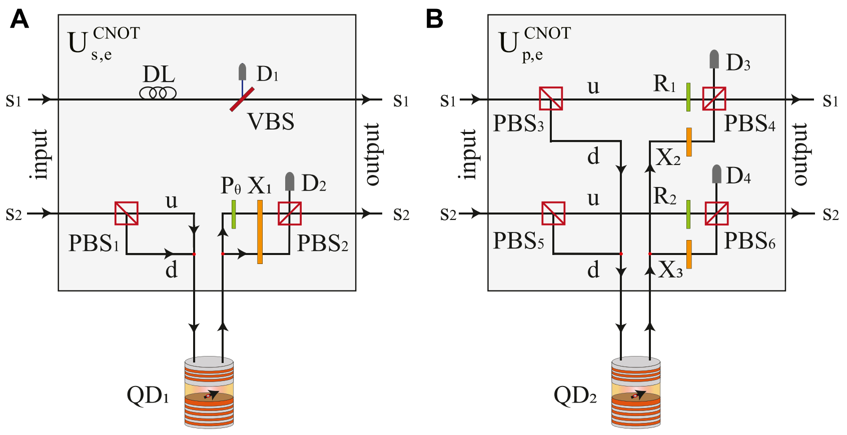


FIGURE 2
Schematics of the heralded photon-spin hybrid CNOT gates. **(A)** The spatial mode of the photon is the control qubit, and the QD-confined electron spin is the target qubit. **(B)** The polarization of the photon is the control qubit, and the QD-confined electron spin is the target qubit. All the functions of the optical elements are presented in the text.

probability of $|r_{-}(\Delta)|^2/p_1$, which is the valid interaction we use to construct the quantum gates between a single photon and an electron spin. We note that the evolution rule is general and does not depend on the particularly ideal conditions [$\kappa_s \to 0$, $g > (\kappa, \gamma)$, $|\Delta| \ll g$] usually used in other schemes.

3 Heralded photon-spin hybrid quantum CNOT gates with theoretically unity fidelities

Now we present two hybrid quantum CNOT gates, which are represented by $\mathrm{U}^{CNOT}_{s,e}$ and $\mathrm{U}^{CNOT}_{p,e}$ operation units, respectively. In the $\mathrm{U}^{CNOT}_{s,e}$ gate, the spatial-mode state of an incident photon encodes the control qubit, while the electron spin confined in QD encodes the target qubit. In the $\mathrm{U}^{CNOT}_{p,e}$ gate, the polarization state of an incident photon encodes the control qubit, while the QD spin encodes the target qubit. The quantum circuits for $\mathrm{U}^{CNOT}_{s,e}$ and $\mathrm{U}^{CNOT}_{p,e}$ are shown in Figure 2. Hereinafter, VBS represents an adjustable beam splitter with transmission coefficient $r_{-}(\Delta)$ and reflection coefficient $\sqrt{1-|r_{-}(\Delta)|^2}$. D$_i$ (i = 1, 2, 3, 4) represents a single-photon detector. DL is the delay line, which makes the photon components in spatial modes s$_1$ and s$_2$ arrive the output port simultaneously without affecting the quantum state. PBS$_j$ (j = 1, 2, . . . , 6) is a polarization beam splitter, which transmits the photonic horizontal polarization component $|H\rangle$ and reflects the vertical polarization component $|V\rangle$. $P_\theta = |H\rangle\langle H| + e^{-\frac{\pi}{2}i}|V\rangle\langle V|$ is a quantum phase gate on the polarization of the photon. X$_t$ (t = 1, 2, 3) is a half-wave plate which performs a polarization bit-flip operation $\sigma^P_X = |H\rangle\langle V| + |V\rangle\langle H|$. R$_f$ (f = 1, 2) completes the polarization rotation $|H\rangle \to r_{-}(\Delta)|H\rangle + \sqrt{1-|r_{-}(\Delta)|^2}|V\rangle$ u and d are to distinguish two different spatial modes in the quantum circuits. The red dots denote the optical switches.

As shown in Figure 2A, suppose the initial states of the input photon and the electron spin confined in QD are $|\psi_p\rangle = (k|H\rangle + l|V\rangle)(m|s_1\rangle + n|s_2\rangle)$ and $|\psi_e\rangle = \mu|+\rangle + \nu|-\rangle$, respectively. Before the photon enters the $\mathrm{U}^{CNOT}_{s,e}$ unit, the state of the photon-spin hybrid system is

$$\begin{aligned}|\psi_0\rangle &= |\psi_p\rangle \otimes |\psi_e\rangle \\ &= (k|H\rangle + l|V\rangle)(m|s_1\rangle + n|s_2\rangle) \otimes (\mu|+\rangle + \nu|-\rangle).\end{aligned} \tag{5}$$

Here, s$_1$ and s$_2$ are two spatial modes of the photon, respectively. When the photon enters the unit from the input port, the photon component in spatial mode s$_1$ passes through the delay line DL with state unchanged. The photon component in spatial mode s$_2$ passes PBS$_1$, and the $|H\rangle(|V\rangle)$ photon component interacts with the QD-cavity system *via* spatial mode $u(d)$ as described by Eq. 4. Then the photon component in spatial mode u passes P_θ and X$_1$, the photon component in spatial mode d passes X$_1$. After which, the state of the photon-spin system becomes

$$\begin{aligned}|\psi_1\rangle = m|s_1\rangle(k|H\rangle + l|V\rangle)(\mu|+\rangle + \nu|-\rangle) \\ +n\big[r_{-}(\Delta)(k|H\rangle_u + l|V\rangle_d)(\mu|-\rangle + \nu|+\rangle) \\ +r_{+}(\Delta)(k|V\rangle_u + il|H\rangle_d)(\mu|+\rangle + \nu|-\rangle)\big],\end{aligned} \tag{6}$$

where the subscripts u and d are used to distinguish the spatial modes. Then, the photon components pass through VBS and PBS$_2$, respectively. When neither of the photon detectors D$_1$ and D$_2$ click, we call this a valid state evolution, and we get the state

$$\begin{aligned}|\psi_2\rangle = r_{-}(\Delta)(k|H\rangle + l|V\rangle) \\ \times\big[m|s_1\rangle(\mu|+\rangle + \nu|-\rangle) + n|s_2\rangle(\mu|-\rangle + \nu|+\rangle)\big].\end{aligned} \tag{7}$$

Then the heralded photon-spin hybrid CNOT gate is completed, where the spatial mode of the incident photon is the control qubit and the electron spin confined in the QD is the target qubit. The polarization state of the photon does not change after this process.

On the contrary, if the photon detector D_1 or D_2 clicks, these two cases mean that errors occur in the state evolution. Any detector response means photon loss, and we get an invalid quantum state evolution result. This failure-herald mechanism guarantees the fidelity of the $U_{s,e}^{CNOT}$ unit by filtering out the errors. The QD-spin state does not change when an error occurs, and we can let a new photon enter the circuit to repeat the operation until success.

The $U_{p,e}^{CNOT}$ operation unit is shown in Figure 2B. Suppose the initial state of the photon-spin hybrid system is still $|\psi_0\rangle$. Similar to the $U_{s,e}^{CNOT}$ gate, if no photon detector responds, the photon leaves the output port and the state of the photon-spin system changes from $|\psi_0\rangle$ to

$$\begin{aligned}|\psi_3\rangle = r_-(\Delta)\left[k|H\rangle\left(\mu|+\rangle+\nu|-\rangle\right)+l|V\rangle\left(\mu|-\rangle+\nu|+\rangle\right)\right]\\ \times\left(m|s_1\rangle+n|s_2\rangle\right).\end{aligned} \tag{8}$$

The hybrid CNOT gate $U_{p,e}^{CNOT}$ is completed, in which the polarization of the incident single photon controls the electron spin confined in the QD. The spatial-mode state of the photon does not change. If the photon detector D_1 or D_2 clicks, the operation failed, and the spin state does not change. We can repeat the operation until success.

These two hybrid CNOT gates $U_{s,e}^{CNOT}$ and $U_{p,e}^{CNOT}$ have some characteristics for building quantum circuits. First, the CNOT gates can work when the particularly ideal conditions usually used in other schemes cannot be satisfied. Second, the failure of the operations can be announced by the single-photon detectors, so we can know whether the operation succeeded or not. Third, the fidelities of the CNOT gates can reach unity in principle. As modular functional units, the $U_{s,e}^{CNOT}$ and $U_{p,e}^{CNOT}$ operation units can not only be used in the proposed scheme but also in many other QIP tasks.

4 Nonlocal high-fidelity quantum controlled-not gates on QD-confined electron spins between quantum network nodes

In this section, we propose the scheme for nonlocal high-fidelity quantum CNOT gates between two remote quantum network nodes Alice and Bob, resorting to single-sided QD-cavity systems, hyperentangled photon pairs, and linear optical elements. As shown in Figure 3, the quantum network node consists of two electron spins confined in QD-cavity systems. We assume the QD-cavity systems in the scheme are identical. Network node Alice holds the electron spins AA' and the initial state is $|\Psi_{AA'}\rangle = (\alpha|+\rangle+\beta|-\rangle)_A\,(\alpha'|+\rangle+\beta'|-\rangle)_{A'}$. Network node Bob holds the electron spins BB' and the initial state is $|\Psi_{BB'}\rangle = (\gamma|+\rangle+\xi|-\rangle)_B\,(\gamma'|+\rangle+\xi'|-\rangle)_{B'}$. The subscripts A, A', B, and B' are used to distinguish the four electron spins. The coefficients satisfy the relation $|\alpha|^2+|\beta|^2=1$, $|\alpha'|^2+|\beta'|^2=1$, $|\gamma|^2+|\xi|^2=1$, and $|\gamma'|^2+|\xi'|^2=1$. The electron spin A (A') of Alice is the control qubit, while the electron spin $B(B')$ of Bob is the target qubit. The hyperentangled photon pair a and b are used to build the quantum channel and encoded in two DOFs, i.e., the

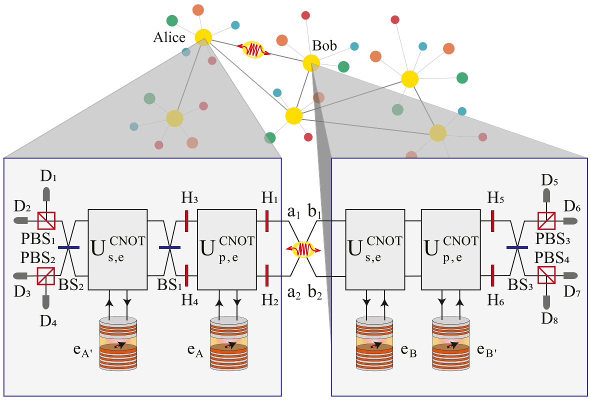


FIGURE 3
Schematic of nonlocal high-fidelity quantum CNOT gates between remote quantum network nodes. The electron spin A (A') of Alice is the control qubit, while the electron spin $B(B')$ of Bob is the target qubit. a and b are hyperentangled photon pair. BS_i (i = 1, 2, 3) is a 50:50 beam splitter used to perform a Hadamard operation on the spatial mode DOF of a photon, which completes the following transformation: $|s_1\rangle \rightarrow (|s_1\rangle + |s_2\rangle)/\sqrt{2}$ and $|s_2\rangle \rightarrow (|s_1\rangle - |s_2\rangle)/\sqrt{2}$ ($s = a, b$). H_j (j = 1, 2, . . . , 6) represents a half-wave plate to perform a Hadamard operation on the polarization of a photon, which completes the following transformation: $|H\rangle \rightarrow (|H\rangle + |V\rangle)/\sqrt{2}$ and $|V\rangle \rightarrow (|H\rangle - |V\rangle)/\sqrt{2}$. Alice and Bob holds four local single-photon detectors, respectively. i.e., D_1-D_4 and D_5-D_8. The other elements have the same function as that in Figure 2.

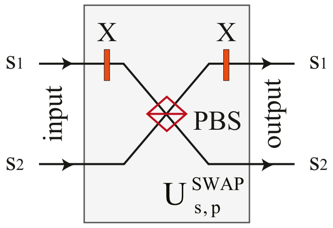


FIGURE 4
Schematic of the $U_{s,p}^{SWAP}$ unit, which swaps the polarization and spatial mode states of the incident photon. The elements have the same function as that in Figure 2.

polarization and the spatial mode. Photons a and b are initially prepared in the state $|\Psi_{ab}\rangle = \frac{1}{2}(|HH\rangle + |VV\rangle)_{ab}(|a_1b_1\rangle + |a_2b_2\rangle)$, where the subscripts a and b are used to distinguish two photons. $|a_1\rangle(|b_1\rangle)$ and $|a_2\rangle(|b_2\rangle)$ are the two spatial modes of photon $a(b)$, respectively. The scheme is detailed as follows.

Before the photons enter the circuits, the state of the system composed of photon a, photon b, electron spin AA' and BB' is

$$\begin{aligned}|\Psi\rangle_0 &= |\Psi_{ab}\rangle \otimes |\Psi_{AA'}\rangle \otimes |\Psi_{BB'}\rangle \\ &= \frac{1}{2}(|HH\rangle + |VV\rangle)_{ab}(|a_1b_1\rangle + |a_2b_2\rangle) \otimes (\alpha| + \rangle + \beta| - \rangle)_A \\ &\times (\alpha'| + \rangle + \beta'| - \rangle)_{A'} \otimes (\gamma| + \rangle + \xi| - \rangle)_B (\gamma'| + \rangle + \xi'| - \rangle)_{B'}.\end{aligned} \tag{9}$$

After the hyperentangled photon pair a and b are prepared, photon a is sent to Alice, while photon b is sent to Bob simultaneously. Photon a enters the node Alice and sequentially passes through H_1, H_2, $\mathrm{U}_{p,e}^{CNOT}$, H_3, H_4, BS_1, $\mathrm{U}_{s,e}^{CNOT}$, BS_2 in both spatial modes a_1 and a_2. If none of the photon detectors in the $\mathrm{U}_{s,e}^{CNOT}$ and $\mathrm{U}_{p,e}^{CNOT}$ units clicks, the state of the photon-spin system is changed from $|\Psi\rangle_0$ to $|\Psi\rangle_1$ in unnormalized form

$$\begin{aligned}|\Psi\rangle_1 = \frac{r_-^2(\Delta)}{2}&\left[\alpha|+\rangle_A(|a_1b_1\rangle + |a_2b_2\rangle) + \beta|-\rangle_A(|a_2b_1\rangle + |a_1b_2\rangle)\right] \\ &\otimes \left[\alpha'|+\rangle_{A'}(|HH\rangle + |VV\rangle)_{ab} + \beta'|-\rangle_{A'}(|VH\rangle + |HV\rangle)_{ab}\right].\end{aligned} \tag{10}$$

At the same time, photon b enters the node Bob and sequentially passes through $\mathrm{U}_{s,e}^{CNOT}$, $\mathrm{U}_{p,e}^{CNOT}$ in both spatial modes b_1 and b_2. If no detector in the $\mathrm{U}_{s,e}^{CNOT}$ and $\mathrm{U}_{p,e}^{CNOT}$ units clicks, the state of the system evolves into

$$\begin{aligned}|\Psi\rangle_2 = \frac{r_-^4(\Delta)}{2}&\left\{\alpha|+\rangle_A\left[|a_1b_1\rangle(\gamma| + \rangle + \xi| - \rangle)_B + |a_2b_2\rangle(\gamma| - \rangle + \xi| + \rangle)_B\right]\right. \\ &\left.+\beta|-\rangle_A\left[|a_2b_1\rangle(\gamma| + \rangle + \xi| - \rangle)_B + |a_1b_2\rangle(\gamma| - \rangle + \xi| + \rangle)_B\right]\right\} \\ &\otimes \left\{\alpha'|+\rangle_{A'}\left[\left(|HH\rangle_{ab}(\gamma'| + \rangle + \xi'| - \rangle)_{B'} + |VV\rangle_{ab}(\gamma'| - \rangle + \xi'| + \rangle)_{B'}\right]\right. \\ &\left.+\beta'|-\rangle_{A'}\left[|VH\rangle_{ab}(\gamma'| + \rangle + \xi'| - \rangle)_{B'} + |HV\rangle_{ab}(\gamma'| - \rangle + \xi'| + \rangle)_{B'}\right)\right]\right\}.\end{aligned} \tag{11}$$

Then, Hadamard operations are performed on photon b in both the polarization and the spatial mode *via* H_5, H_6, and BS_3. Before photon b gets the photon detectors D_5-D_8, the state of the system is

$$\begin{aligned}|\Psi\rangle_3 = \frac{r_-^4(\Delta)}{4}&\left\{\alpha|+\rangle_A\left[|a_1\rangle(|b_1\rangle + |b_2\rangle)(\gamma| + \rangle + \xi| - \rangle)_B + |a_2\rangle(|b_1\rangle\right.\right. \\ &\left.-|b_2\rangle)(\gamma| - \rangle + \xi| + \rangle)_B\right] + \beta|-\rangle_A\left[|a_2\rangle(|b_1\rangle + |b_2\rangle)(\gamma| + \rangle\right. \\ &\left.\left.+\xi| - \rangle)_B + |a_1\rangle(|b_1\rangle - |b_2\rangle)(\gamma| - \rangle + \xi| + \rangle)_B\right]\right\} \\ &\otimes \left\{\alpha'|+\rangle_{A'}\left[|H\rangle_a(|H\rangle + |V\rangle)_b(\gamma'| + \rangle + \xi'| - \rangle)_{B'} + |V\rangle_a(|H\rangle\right.\right. \\ &\left.-|V\rangle)_b(\gamma'| - \rangle + \xi'| + \rangle)_{B'}\right] + \beta'|-\rangle_{A'}\left[|V\rangle_a(|H\rangle + |V\rangle)_b(\gamma'| + \rangle\right. \\ &\left.\left.+\xi'| - \rangle)_{B'} + |H\rangle_a(|H\rangle - |V\rangle)_b(\gamma'| - \rangle + \xi'| + \rangle)_{B'})\right]\right\}.\end{aligned} \tag{12}$$

TABLE 1 The measurement results of the photons and the corresponding single-qubit gate rotation operations required on the electron spins.

Measurement results	The spin operations
$|a_1b_1\rangle|HH\rangle_{ab}$	$I_A \otimes I_{A'} \otimes I_B \otimes I_{B'}$
$|a_1b_1\rangle|HV\rangle_{ab}$	$I_A \otimes \sigma_{z_{A'}} \otimes I_B \otimes I_{B'}$
$|a_1b_1\rangle|VH\rangle_{ab}$	$I_A \otimes I_{A'} \otimes I_B \otimes \sigma_{x_{B'}}$
$|a_1b_1\rangle|VV\rangle_{ab}$	$I_A \otimes - \sigma_{z_{A'}} \otimes I_B \otimes \sigma_{x_{B'}}$
$|a_1b_2\rangle|HH\rangle_{ab}$	$\sigma_{z_A} \otimes I_{A'} \otimes I_B \otimes I_{B'}$
$|a_1b_2\rangle|HV\rangle_{ab}$	$\sigma_{z_A} \otimes \sigma_{z_{A'}} \otimes I_B \otimes I_{B'}$
$|a_1b_2\rangle|VH\rangle_{ab}$	$\sigma_{z_A} \otimes I_{A'} \otimes I_B \otimes \sigma_{x_{B'}}$
$|a_1b_2\rangle|VV\rangle_{ab}$	$\sigma_{z_A} \otimes - \sigma_{z_{A'}} \otimes I_B \otimes \sigma_{x_{B'}}$
$|a_2b_1\rangle|HH\rangle_{ab}$	$I_A \otimes I_{A'} \otimes \sigma_{z_B} \otimes I_{B'}$
$|a_2b_1\rangle|HV\rangle_{ab}$	$I_A \otimes \sigma_{z_{A'}} \otimes \sigma_{z_B} \otimes I_{B'}$
$|a_2b_1\rangle|VH\rangle_{ab}$	$I_A \otimes I_{A'} \otimes \sigma_{z_B} \otimes \sigma_{x_{B'}}$
$|a_2b_1\rangle|VV\rangle_{ab}$	$I_A \otimes - \sigma_{z_{A'}} \otimes \sigma_{z_B} \otimes \sigma_{x_{B'}}$
$|a_2b_2\rangle|HH\rangle_{ab}$	$-\sigma_{z_A} \otimes I_{A'} \otimes \sigma_{z_B} \otimes I_{B'}$
$|a_2b_2\rangle|HV\rangle_{ab}$	$-\sigma_{z_A} \otimes \sigma_{z_{A'}} \otimes \sigma_{z_B} \otimes I_{B'}$
$|a_2b_2\rangle|VH\rangle_{ab}$	$-\sigma_{z_A} \otimes I_{A'} \otimes \sigma_{z_B} \otimes \sigma_{x_{B'}}$
$|a_2b_2\rangle|VV\rangle_{ab}$	$-\sigma_{z_A} \otimes - \sigma_{z_{A'}} \otimes \sigma_{z_B} \otimes \sigma_{x_{B'}}$

Finally, the photons a and b pass the PBSs and get the local photon detectors D_1-D_4 and D_5-D_8, respectively. Alice and Bob communicate their measurement results through a classical communication channel. According to the results, Alice and Bob choose the corresponding single-qubit rotation operations on electron spins according to Table 1. For example, if the photon pair ab are finally detected in the state $|a_1b_1H_aH_b\rangle$, the state of the four-spin system $AA'BB'$ is

$$\begin{aligned}|\Psi_{AA'BB'}\rangle = \frac{r_-^4(\Delta)}{4}&\left[\alpha|+\rangle_A(\gamma| + \rangle + \xi| - \rangle)_B + \beta|-\rangle_A(\gamma| - \rangle + \xi| + \rangle)_B\right] \\ &\otimes \left[\alpha'|+\rangle_{A'}(\gamma'| + \rangle + \xi'| - \rangle)_{B'} + \beta'|-\rangle_{A'}(\gamma'| - \rangle + \xi'| + \rangle)_{B'}\right],\end{aligned} \tag{13}$$

which means two CNOT gates between the spins AA' of Alice and the spins BB' of Bob have been implemented. If the photons are detected in the state $|a_1b_2V_aV_b\rangle$, Alice should perform a σ_z operation on the electron spin A and a $-\sigma_z$ operation on the spin A', and Bob should perform a σ_x operation on the spin B'. After the operations above, the state $|\Psi_{AA'BB'}\rangle$ can be obtained. Other situations can be seen in Table 1. Moreover, if any photon detector in the $\mathrm{U}_{s,e}^{CNOT}$ or $\mathrm{U}_{p,e}^{CNOT}$ unit clicks, it declares a failed operation, and we can restart the process just *via* launching a new pair of hyperentangled photons.

So far, we have described the teleportation of two nonlocal CNOT gates operations on spin qubits between two quantum network nodes in parallel assisted by single-sided QD-cavity systems. Electron spin A (A') of Alice is the control qubit, while the electron spin $B(B')$ of Bob is the target qubit. Two CNOT gates are achieved simultaneously. The modular functional units make the circuit more flexible and extensible. For instance, if we let the electron spin A (A') of Alice control $B'(B)$ of Bob, we only need to let photon b pass through a linear optical $U_{s,p}^{SWAP}$ unit shown in Figure 4 before the $U_{s,e}^{CNOT}$, which swaps the spatial mode and polarization states of the incident photon.

5 Discussion and summary

In this section, we discuss the performance of the scheme, which can be characterized by fidelity and efficiency. We define the fidelity as $F = |\langle\Psi_r|\Psi_i\rangle|^2$, where $|\Psi_r\rangle$ is the final state of the system composed of four electron spins hold by two network nodes Alice and Bob in reality, and $|\Psi_i\rangle$ is the final state of the system in ideal conditions, which should be

$$\begin{aligned}|\Psi_i\rangle = \frac{1}{4}&\left[\alpha|+\rangle_A(\gamma|+\rangle+\xi|-\rangle)_B+\beta|-\rangle_A(\gamma|-\rangle+\xi|+\rangle)_B\right]\\ &\otimes\left[\alpha'|+\rangle_{A'}(\gamma'|+\rangle+\xi'|-\rangle)_{B'}+\beta'|-\rangle_{A'}(\gamma'|-\rangle+\xi'|+\rangle)_{B'}\right].\end{aligned} \tag{14}$$

Consider the cavity QED parameters (g, κ, κ_s, γ), the final state of the system in unnormalized form is

$$\begin{aligned}|\Psi_r\rangle &= |\Psi_{AA'BB'}\rangle\\ &= \frac{r_-^4(\Delta)}{4}\left[\alpha|+\rangle_A(\gamma|+\rangle+\xi|-\rangle)_B+\beta|-\rangle_A(\gamma|-\rangle+\xi|+\rangle)_B\right]\\ &\quad\otimes\left[\alpha'|+\rangle_{A'}(\gamma'|+\rangle+\xi'|-\rangle)_{B'}+\beta'|-\rangle_{A'}(\gamma'|-\rangle+\xi'|+\rangle)_{B'}\right].\end{aligned} \tag{15}$$

The average fidelity of the scheme is

$$\begin{aligned}\bar{F} &= \overline{|\langle\Psi_r|\Psi_i\rangle|^2}\\ &= \frac{1}{4\pi^4}\int_0^{2\pi}d\theta_A\int_0^{2\pi}d\theta_{A'}\int_0^{2\pi}d\phi_B\int_0^{2\pi}d\phi_{B'}\frac{|\langle\Psi_r|\Psi_i\rangle|^2}{\langle\Psi_r|\Psi_r\rangle} = 1,\end{aligned} \tag{16}$$

where $\cos\theta_A = \alpha$, $\sin\theta_A = \beta$, $\cos\theta_{A'} = \alpha'$, $\sin\theta_{A'} = \beta'$, $\cos\phi_B = \gamma$, $\sin\phi_B = \xi$, $\cos\phi_{B'} = \gamma'$, and $\sin\phi_{B'} = \xi'$. The fidelity of the scheme is unity in principle. The herald mechanism of the $U_{s,e}^{CNOT}$ and $U_{p,e}^{CNOT}$ operation units filters out the errors and announces them via single-photon detectors, which guarantees high fidelity. We can conclude that the fidelity is robust to the cavity QED parameters (g, κ, κ_s, γ) and photon loss.

The efficiency of the scheme is defined as the probability that the hyperentangled photon pair are detected by the local single-photon detectors of Alice and Bob. In other words, the efficiency is the probability that none of the single-photon detectors of $U_{s,e}^{CNOT}$ or $U_{p,e}^{CNOT}$ operation units clicks, and the network nodes Alice and Bob each have a local single-photon detector click. The efficiency can be described as

$$\begin{aligned}\eta &= \left|r_-(\Delta)^4\right|^2 = \left|\frac{r(\Delta,0)-r(\Delta,g)}{2}\right|^8\\ &= \left|\frac{-4g^2/\kappa^2}{(2i\Delta/\kappa+1+\kappa_s/\kappa)\left[(2i\Delta/\kappa+\gamma/\kappa)(2i\Delta/\kappa+1+\kappa_s/\kappa)+4g^2/\kappa^2\right]}\right|^8,\end{aligned} \tag{17}$$

which depends on cavity-QED parameters. The relation between the absolute amplitude of $r_-(\Delta)$, the cavity-QED parameters (g, κ, κ_s, γ), and the frequency detuning Δ is depicted in Figure 5, where we take $\gamma = 0.01\kappa$. As shown in Figure 5, we take the slices $g/\kappa = 0.5$, $g/\kappa = 1$, $g/\kappa = 2.4$, $\kappa_s/\kappa = 0$, $\kappa_s/\kappa = 0.05$, and $\kappa_s/\kappa = 0.1$ for examples. We can conclude that $|r_-(\Delta)|$ can get relevant high values not only around the resonant frequency $\Delta = 0$ but also at some other frequency detuning such as $\Delta = \pm g$. The cavity side leakage and loss rate κ_s/κ decrease $|r_-(\Delta)|$ slightly.

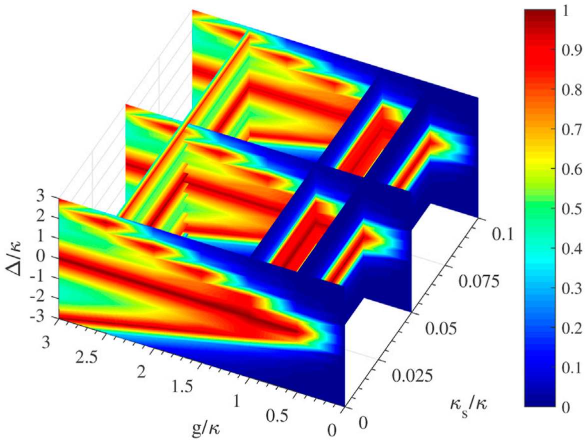


FIGURE 5
The absolute amplitude $|r_-(\Delta)|$ of $r_-(\Delta)$ vs. the cavity QED parameters (g, κ, κ_s, γ) and the frequency detuning Δ. The slices shown are $g/\kappa = 0.5$, $g/\kappa = 1$, $g/\kappa = 2.4$, $\kappa_s/\kappa = 0$, $\kappa_s/\kappa = 0.05$, and $\kappa_s/\kappa = 0.1$. $\gamma = 0.01\kappa$.

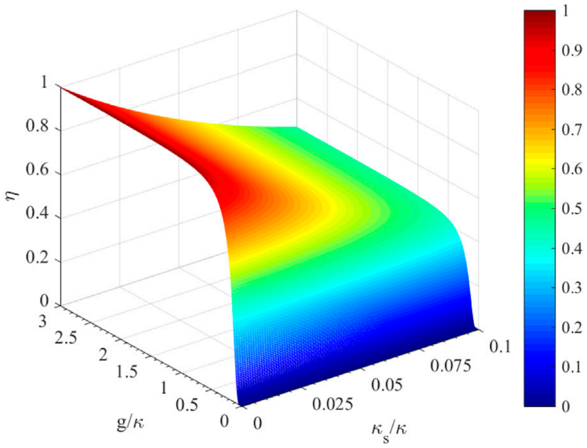


FIGURE 6
The efficiency η vs. g/κ and κ_s/κ at the resonant frequency $\Delta = 0$. $\gamma = 0.01\kappa$.

When the system works under the resonance frequency ($\Delta = 0$), the efficiency η is the function of the coupling strength g/κ and the cavity decay rate κ_s/κ under given γ. The relation between η and the cavity QED parameters (g, κ, κ_s, γ) under the resonant frequency $\Delta = 0$ is shown in Figure 6. When the side leakage is negligible, the efficiency is 92.35% at $g = 0.5\kappa$, 98.021% at $g = \kappa$, and 99.65% at $g = 2.4\kappa$. The scheme has high efficiency without the strict requirement of the strong-coupling condition. When $\kappa_s = 0.05\kappa$, the efficiency is 62.26% at $g = 0.5\kappa$, 66.28% at $g = \kappa$, and 67.44% at $g = 2.4\kappa$. The scheme still works when the side leakage is taken into account. To obtain high efficiency, the side leakage and the cavity loss rate κ_s/κ should be controlled as small as possible. The side leakage κ_s can be reduced by engineering the fabrication and adjusting the material, structure and size of the cavity.

The hyperentangled photon pairs can be generated by combinations of the techniques used for creating entanglement in a single DOF [37, 38], such as with the assistance of an optical cavity [84, 85] or spontaneous four-wave mixing [86]. The bandwidth of the hyperentangled pules should be narrow than the linewidth of the cavity mode. The superposition state of an electron spin can be prepared assisted by nanosecond ESR pulses or picosecond optical pulses [53]. The fast single-qubit rotation operations on the electron spin can be achieved by ultrafast optical pulses or optically controlled geometric phases [54]. The dark counts of photon detectors may lead to false-positive responses that affect the efficiency slightly. Other factors such as the imperfect hyperentangled sources and the linear elements would affect the performance of the scheme, and can be improved by the manufacturing process.

In summary, assisted by single-sided QD-cavity systems, we presented two robust photon-spin hybrid CNOT gates with a herald mechanism, i.e., the $U^{CNOT}_{s,e}$ and $U^{CNOT}_{p,e}$ operation units. The units can work without the strict requirement of strong coupling. Single-photon detectors can herald the failure of the operation. The fidelities of the units can get unity in principle. Utilizing the units, we propose a parallel teleportation scheme of two nonlocal quantum CNOT gates between two remote quantum network nodes, Alice and Bob. Electron spins A and A' of Alice simultaneously control electron spins B and B' of Bob, respectively. The scheme has some characteristics. First, we use hyperentangled photon pairs to build the quantum channel for nonlocal operations, which can effectively improve the channel capacity. Second, with the herald mechanism, the fidelities of the nonlocal CNOT gates can be raised to unity in principle. Third, teleporting two CNOT gates in parallel can save quantum resources and accelerate computing speed. Fourth, the scheme with the modular design has good flexibility. The advantages above make the scheme feasible with current technology, which may open promising possibilities for nonlocal quantum computation and quantum information networks. To construct a practical multi-node quantum network, a series of cascade cavities with coupled quantum memories or registers are required. Although our scheme could weaken the requirements for coupling strength and cavity leakage to some extent, it is still a technical challenge to connect multiple different cavities while keeping all cavities in the required coupling conditions. Therefore, we have great expectations for the optimization of microcavity parameters design and the improvement of the microfabrication process.

Data availability statement

The raw data supporting the conclusions of this article will be made available by the authors, without undue reservation.

Author contributions

All authors listed have made a substantial, direct, and intellectual contribution to the work and approved it for publication.

Funding

The project was supported by Fund of State Key Laboratory of Information Photonics and Optical Communications (Beijing University of Posts and Telecommunications) (No. IPOC2022ZT07), P. R. China. This work was also supported by the National Natural Science Foundation of China (NSFC) under Grant Nos. 61701035 and 61671085.

Conflict of interest

The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Publisher’s note

All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers. Any product that may be evaluated in this article, or claim that may be made by its manufacturer, is not guaranteed or endorsed by the publisher.

References

1. Gisin N, Thew R. Quantum communication. *Nat Photon* (2007) 1:165–71. doi:10.1038/nphoton.2007.22

2. Ekert A, Jozsa R. Quantum computation and shor's factoring algorithm. *Rev Mod Phys* (1996) 68:733–53. doi:10.1103/revmodphys.68.733

3. Grover LK. Quantum mechanics helps in searching for a needle in a haystack. *Phys Rev Lett* (1997) 79:325–8. doi:10.1103/physrevlett.79.325

4. Long GL. Grover algorithm with zero theoretical failure rate. *Phys Rev A (Coll Park)* (2001) 64:022307. doi:10.1103/physreva.64.022307

5. Giovannetti V, Lloyd S, Maccone L. Quantum metrology. *Phys Rev Lett* (2006) 96:010401. doi:10.1103/physrevlett.96.010401

6. Giovannetti V, Lloyd S, Maccone L. Advances in quantum metrology. *Nat Photon* (2011) 5:222–9. doi:10.1038/nphoton.2011.35

7. Wehner S, Elkouss D, Hanson R. Quantum internet: A vision for the road ahead. *Science* (2018) 362:eaam9288. doi:10.1126/science.aam9288

8. Awschalom D, Berggren KK, Bernien H, Bhave S, Carr LD, Davids P, et al. Development of quantum interconnects (quics) for next-generation information technologies. *PRX Quan* (2021) 2:017002. doi:10.1103/prxquantum.2.017002

9. Long GL, Pan D, Sheng YB, Xue Q, Lu J, Hanzo L. An evolutionary pathway for the quantum internet relying on secure classical repeaters. (2022) arXiv preprint arXiv:2202.03619.

10. Long GL, Liu XS. Theoretically efficient high-capacity quantum-key-distribution scheme. *Phys Rev A (Coll Park)* (2002) 65:032302. doi:10.1103/physreva.65.032302

11. Deng FG, Long GL, Liu XS. Two-step quantum direct communication protocol using the einstein-podolsky-rosen pair block. *Phys Rev A (Coll Park)* (2003) 68:042317. doi:10.1103/physreva.68.042317

12. Deng FG, Long GL. Secure direct communication with a quantum one-time pad. *Phys Rev A (Coll Park)* (2004) 69:052319. doi:10.1103/physreva.69.052319

13. Niu PH, Zhou ZR, Lin ZS, Sheng YB, Yin LG, Long GL. Measurement-device-independent quantum communication without encryption. *Sci Bull* (2018) 63:1345–50. doi:10.1016/j.scib.2018.09.009

14. Zhou Z, Sheng Y, Niu P, Yin L, Long G, Hanzo L. Measurement-device-independent quantum secure direct communication. *Sci China Phys Mech Astron* (2020) 63:230362. doi:10.1007/s11433-019-1450-8

15. Yang YF, Duan LZ, Qiu TR, Xie XM. Controlled quantum secure direct communication based on four-qubit cluster states and quantum search algorithm. *Front Phys* (2022) 10:875441. doi:10.3389/fphy.2022.875441

16. Crépeau C, Gottesman D, Smith A. Secure multi-party quantum computation. In: *Proceedings of the thiry-fourth annual ACM symposium on Theory of computing* (2002). p. 643–52.

17. Clementi M, Pappa A, Eckstein A, Walmsley IA, Kashefi E, Barz S. Classical multiparty computation using quantum resources. *Phys Rev A (Coll Park)* (2017) 96:062317. doi:10.1103/physreva.96.062317

18. Yang HY, Ye TY. Secure multi-party quantum summation based on quantum Fourier transform. *Quan Inf Process* (2018) 17:129. doi:10.1007/s11128-018-1890-1

19. Fan L, Cao C. A synchronous quantum blind signature scheme with entanglement swapping. *Int J Quan Inform* (2019) 17:1950007. doi:10.1142/s0219749919500072

20. Yi X, Cao C, Fan L, Zhang R. Quantum secure multi-party summation protocol based on blind matrix and quantum Fourier transform. *Quan Inf Process* (2021) 20:249. doi:10.1007/s11128-021-03183-0

21. Gao LZ, Zhang X, Lin S, Wang N, Guo GD. Authenticated multiparty quantum key agreement for optical-ring quantum communication networks. *Front Phys* (2022) 10:962781. doi:10.3389/fphy.2022.962781

22. Cirac JI, Zoller P, Kimble HJ, Mabuchi H. Quantum state transfer and entanglement distribution among distant nodes in a quantum network. *Phys Rev Lett* (1997) 78:3221–4. doi:10.1103/physrevlett.78.3221

23. Ritter S, Nölleke C, Hahn C, Reiserer A, Neuzner A, Uphoff M, et al. An elementary quantum network of single atoms in optical cavities. *Nature* (2012) 484:195–200. doi:10.1038/nature11023

24. Reiserer A, Rempe G. Cavity-based quantum networks with single atoms and optical photons. *Rev Mod Phys* (2015) 87:1379–418. doi:10.1103/revmodphys.87.1379

25. Zhou XF, Zhang YS, Guo GC. Nonlocal gate of quantum network *via* cavity quantum electrodynamics. *Phys Rev A (Coll Park)* (2005) 71:064302. doi:10.1103/physreva.71.064302

26. Wang HF, Zhu AD, Zhang S, Yeon KH. Optically controlled phase gate and teleportation of a controlled-not gate for spin qubits in a quantum-dot-microcavity coupled system. *Phys Rev A (Coll Park)* (2013) 87:062337. doi:10.1103/physreva.87.062337

27. Wang TJ, Wang C. Parallel quantum computing teleportation for spin qubits in quantum dot and microcavity coupled system. *IEEE J Sel Top Quan Electron* (2014) 21:91–7. doi:10.1109/jstqe.2014.2321523

28. Liu AP, Cheng LY, Guo Q, Su SL, Wang HF, Zhang S. Heralded teleportation of a controlled-not gate for nitrogen-vacancy centers coupled to a microtoroid resonator. *Laser Phys* (2019) 29:025205. doi:10.1088/1555-6611/aaf90c

29. Wan Y, Kienzler D, Erickson SD, Mayer KH, Tan TR, Wu JJ, et al. Quantum gate teleportation between separated qubits in a trapped-ion processor. *Science* (2019) 364:875–8. doi:10.1126/science.aaw9415

30. Briegel HJ, Dür W, Cirac JI, Zoller P. Quantum repeaters: The role of imperfect local operations in quantum communication. *Phys Rev Lett* (1998) 81:5932–5. doi:10.1103/physrevlett.81.5932

31. Dür W, Briegel HJ, Cirac JI, Zoller P. Quantum repeaters based on entanglement purification. *Phys Rev A (Coll Park)* (1999) 59:169–81. doi:10.1103/physreva.59.169

32. Sheng YB, Deng FG, Zhou HY. Efficient polarization-entanglement purification based on parametric down-conversion sources with cross-kerr nonlinearity. *Phys Rev A (Coll Park)* (2008) 77:042308. doi:10.1103/physreva.77.042308

33. Cao C, Wang C, Ly H, Zhang R. Atomic entanglement purification and concentration using coherent state input-output process in low-q cavity qed regime. *Opt Express* (2013) 21:4093–105. doi:10.1364/oe.21.004093

34. Cao C, Chen X, Duan Y, Fan L, Zhang R, Wang T, et al. Concentrating partially entangled w-class states on nonlocal atoms using low-q optical cavity and linear optical elements. *Sci China Phys Mech Astron* (2016) 59:100315. doi:10.1007/s11433-016-0253-x

35. Hu XM, Huang CX, Sheng YB, Zhou L, Liu BH, Guo Y, et al. Long-distance entanglement purification for quantum communication. *Phys Rev Lett* (2021) 126:010503. doi:10.1103/physrevlett.126.010503

36. Huang CX, Hu XM, Liu BH, Zhou L, Sheng YB, Li CF, et al. Experimental one-step deterministic polarization entanglement purification. *Sci Bull* (2022) 67:593–7. doi:10.1016/j.scib.2021.12.018

37. Kwiat PG. Hyper-entangled states. *J Mod Opt* (1997) 44:2173–84. doi:10.1080/09500349708231877

38. Deng FG, Ren BC, Li XH. Quantum hyperentanglement and its applications in quantum information processing. *Sci Bull* (2017) 62:46–68. doi:10.1016/j.scib.2016.11.007

39. Xu W, Wang T, Cao C, Wang C. High dimensional quantum logic gates and quantum information processing. *Chin Sci Bull* (2019) 64:1691–701. doi:10.1360/n972019-00252

40. Simon DS, Sergienko AV. High-capacity quantum key distribution via hyperentangled degrees of freedom. *New J Phys* (2014) 16:063052. doi:10.1088/1367-2630/16/6/063052

41. Wang XL, Cai XD, Su ZE, Chen MC, Wu D, Li L, et al. Quantum teleportation of multiple degrees of freedom of a single photon. *Nature* (2015) 518:516–9. doi:10.1038/nature14246

42. Cao C, Wang TJ, Mi SC, Zhang R, Wang C. Nonlocal hyperconcentration on entangled photons using photonic module system. *Ann Phys* (2016) 369:128–38. doi:10.1016/j.aop.2016.03.003

43. Williams BP, Sadlier RJ, Humble TS. Superdense coding over optical fiber links with complete bell-state measurements. *Phys Rev Lett* (2017) 118:050501. doi:10.1103/physrevlett.118.050501

44. Sheng YB, Zhou L, Long GL. One-step quantum secure direct communication. *Sci Bull* (2022) 67:367–74. doi:10.1016/j.scib.2021.11.002

45. Zhou L, Sheng YB. One-step device-independent quantum secure direct communication. *Sci China Phys Mech Astron* (2022) 65:250311. doi:10.1007/s11433-021-1863-9

46. Loss D, DiVincenzo DP. Quantum computation with quantum dots. *Phys Rev A (Coll Park)* (1998) 57:120–6. doi:10.1103/physreva.57.120

47. Imamog A, Awschalom DD, Burkard G, DiVincenzo DP, Loss D, Sherwin M, et al. Quantum information processing using quantum dot spins and cavity qed. *Phys Rev Lett* (1999) 83:4204–7. doi:10.1103/physrevlett.83.4204

48. Delteil A, Sun Z, Gao W, Togan E, Faelt S, Imamoğlu A. Generation of heralded entanglement between distant hole spins. *Nat Phys* (2016) 12:218–23. doi:10.1038/nphys3605

49. Prechtel JH, Kuhlmann AV, Houel J, Ludwig A, Valentin SR, Wieck AD, et al. Decoupling a hole spin qubit from the nuclear spins. *Nat Mater* (2016) 15:981–6. doi:10.1038/nmat4704

50. Wang K, Xu G, Gao F, Liu H, Ma RL, Zhang X, et al. Ultrafast coherent control of a hole spin qubit in a germanium quantum dot. *Nat Commun* (2022) 13:206. doi:10.1038/s41467-021-27880-7

51. Atature M, Dreiser J, Badolato A, Hogele A, Karrai K, Imamoglu A. Quantum-dot spin-state preparation with near-unity fidelity. *Science* (2006) 312:551–3. doi:10.1126/science.1126074

52. Berezovsky J, Mikkelsen M, Gywat O, Stoltz N, Coldren L, Awschalom D. Nondestructive optical measurements of a single electron spin in a quantum dot. *Science* (2006) 314:1916–20. doi:10.1126/science.1133862

53. Press D, Ladd TD, Zhang B, Yamamoto Y. Complete quantum control of a single quantum dot spin using ultrafast optical pulses. *Nature* (2008) 456:218–21. doi:10.1038/nature07530

54. Kim ED, Truex K, Xu X, Sun B, Steel D, Bracker A, et al. Fast spin rotations by optically controlled geometric phases in a charge-tunable inas quantum dot. *Phys Rev Lett* (2010) 104:167401. doi:10.1103/physrevlett.104.167401

55. Press D, De Greve K, McMahon PL, Ladd TD, Friess B, Schneider C, et al. Ultrafast optical spin echo in a single quantum dot. *Nat Photon* (2010) 4:367–70. doi:10.1038/nphoton.2010.83

56. West JR, Lidar DA, Fong BH, Gyure MF. High fidelity quantum gates via dynamical decoupling. *Phys Rev Lett* (2010) 105:230503. doi:10.1103/physrevlett.105.230503

57. Hu C, Young A, O'brien J, Munro W, Rarity J. Giant optical faraday rotation induced by a single-electron spin in a quantum dot: applications to entangling remote spins via a single photon. *Phys Rev B* (2008) 78:085307. doi:10.1103/physrevb.78.085307

58. Hu C, Munro W, O'Brien J, Rarity J. Proposed entanglement beam splitter using a quantum-dot spin in a double-sided optical microcavity. *Phys Rev B* (2009) 80:205326. doi:10.1103/physrevb.80.205326

59. Cao C, Duan YW, Chen X, Zhang R, Wang TJ, Wang C. Implementation of single-photon quantum routing and decoupling using a nitrogen-vacancy center and a whispering-gallery-mode resonator-waveguide system. *Opt Express* (2017) 25:16931–46. doi:10.1364/oe.25.016931

60. Wang K, Gao YP, Jiao R, Wang C. Recent progress on optomagnetic coupling and optical manipulation based on cavity-optomagnonics. *Front Phys (Beijing)* (2022) 17:42201. doi:10.1007/s11467-022-1165-2

61. Bonato C, Haupt F, Oemrawsingh SS, Gudat J, Ding D, van Exter MP, et al. Cnot and bell-state analysis in the weak-coupling cavity qed regime. *Phys Rev Lett* (2010) 104:160503. doi:10.1103/physrevlett.104.160503

62. Wei HR, Deng FG. Universal quantum gates for hybrid systems assisted by quantum dots inside double-sided optical microcavities. *Phys Rev A (Coll Park)* (2013) 87:022305. doi:10.1103/physreva.87.022305

63. Luo MX, Wang X. Parallel photonic quantum computation assisted by quantum dots in one-side optical microcavities. *Sci Rep* (2014) 4:5732. doi:10.1038/srep05732

64. Li T, Deng FG. Error-rejecting quantum computing with solid-state spins assisted by low-Qoptical microcavities. *Phys Rev A (Coll Park)* (2016) 94:062310. doi:10.1103/physreva.94.062310

65. Xia BY, Cao C, Han YH, Zhang R. Universal photonic three-qubit quantum gates with two degrees of freedom assisted by charged quantum dots inside single-sided optical microcavities. *Laser Phys* (2018) 28:095201. doi:10.1088/1555-6611/aac904

66. Cao C, Han YH, Zhang L, Fan L, Duan YW, Zhang R. High-fidelity universal quantum controlled gates on electron-spin qubits in quantum dots inside single-sided optical microcavities. *Adv Quan Technol* (2019) 2:1900081. doi:10.1002/qute.201900081

67. Han YH, Cao C, Fan L, Zhang R. Heralded high-fidelity quantum hyper-cnot gates assisted by charged quantum dots inside single-sided optical microcavities. *Opt Express* (2021) 29:20045–62. doi:10.1364/oe.426325

68. Wang TJ, Lu Y, Long GL. Generation and complete analysis of the hyperentangled bell state for photons assisted by quantum-dot spins in optical microcavities. *Phys Rev A (Coll Park)* (2012) 86:042337. doi:10.1103/physreva.86.042337

69. Ren BC, Wei HR, Hua M, Li T, Deng FG. Complete hyperentangled-bell-state analysis for photon systems assisted by quantum-dot spins in optical microcavities. *Opt Express* (2012) 20:24664–77. doi:10.1364/oe.20.024664

70. Wang GY, Ai Q, Ren BC, Li T, Deng FG. Error-detected generation and complete analysis of hyperentangled bell states for photons assisted by quantum-dot spins in double-sided optical microcavities. *Opt Express* (2016) 24:28444–58. doi:10.1364/oe.24.028444

71. Zheng Y, Liang L, Zhang M. Error-heralded generation and self-assisted complete analysis of two-photon hyperentangled bell states through single-sided quantum-dot-cavity systems. *Sci China Phys Mech Astron* (2019) 62:970312. doi:10.1007/s11433-018-9338-8

72. Cao C, Zhang L, Han YH, Yin PP, Fan L, Duan YW, et al. Complete and faithful hyperentangled-bell-state analysis of photon systems using a failure-heralded and fidelity-robust quantum gate. *Opt Express* (2020) 28:2857–72. doi:10.1364/oe.384360

73. Fan L, Cao C. Deterministic cnot gate and complete bell-state analyzer on quantum-dot-confined electron spins based on faithful quantum nondemolition parity detection. *J Opt Soc Am B* (2021) 38:1593–603. doi:10.1364/josab.415321

74. Wang C, Zhang Y, Jin G. Entanglement purification and concentration of electron-spin entangled states using quantum-dot spins in optical microcavities. *Phys Rev A (Coll Park)* (2011) 84:032307. doi:10.1103/physreva.84.032307

75. Wang C. Efficient entanglement concentration for partially entangled electrons using a quantum-dot and microcavity coupled system. *Phys Rev A (Coll Park)* (2012) 86:012323. doi:10.1103/physreva.86.012323

76. Cao C, Fan L, Chen X, Duan YW, Wang TJ, Zhang R, et al. Efficient entanglement concentration of arbitrary unknown less-entangled three-atom w states via photonic faraday rotation in cavity qed. *Quan Inf Process* (2017) 16:98. doi:10.1007/s11128-017-1549-3

77. Liu YT, Wu YM, Du FF. Self-error-rejecting multipartite entanglement purification for electron systems assisted by quantum-dot spins in optical microcavities. *Chin Phys B* (2022) 31:050303. doi:10.1088/1674-1056/ac4489

78. Lodahl P. Quantum-dot based photonic quantum networks. *Quan Sci Technol* (2017) 3:013001. doi:10.1088/2058-9565/aa91bb

79. Borregaard J, Sørensen AS, Lodahl P. Quantum networks with deterministic spin–photon interfaces. *Adv Quan Technol* (2019) 2:1800091. doi:10.1002/qute.201800091

80. Bennett A, Lee J, Ellis D, Farrer I, Ritchie D, Shields A. A semiconductor photon-sorter. *Nat Nanotechnol* (2016) 11:857–60. doi:10.1038/nnano.2016.113

81. Sun S, Kim H, Solomon GS, Waks E. A quantum phase switch between a single solid-state spin and a photon. *Nat Nanotechnol* (2016) 11:539–44. doi:10.1038/nnano.2015.334

82. Arnold C, Demory J, Loo V, Lemaître A, Sagnes I, Glazov M, et al. Macroscopic rotation of photon polarization induced by a single spin. *Nat Commun* (2015) 6:6236. doi:10.1038/ncomms7236

83. Androvitsaneas P, Young AB, Schneider C, Maier S, Kamp M, Höfling S, et al. Charged quantum dot micropillar system for deterministic light-matter interactions. *Phys Rev B* (2016) 93:241409. doi:10.1103/physrevb.93.241409

84. Barreiro JT, Langford NK, Peters NA, Kwiat PG. Generation of hyperentangled photon pairs. *Phys Rev Lett* (2005) 95:260501. doi:10.1103/physrevlett.95.260501

85. Suo J, Dong S, Zhang W, Huang Y, Peng J. Generation of hyper-entanglement on polarization and energy-time based on a silicon micro-ring cavity. *Opt Express* (2015) 23:3985–95. doi:10.1364/oe.23.003985

86. Zhao TM, Ihn YS, Kim YH. Direct generation of narrow-band hyperentangled photons. *Phys Rev Lett* (2019) 122:123607. doi:10.1103/physrevlett.122.123607

frontiers | Frontiers in Physics

TYPE Original Research
PUBLISHED 06 October 2022
DOI 10.3389/fphy.2022.1023992

OPEN ACCESS

EDITED BY
Nanrun Zhou,
Shanghai University of Engineering Sciences, China

REVIEWED BY
Lihua Gong,
Nanchang University, China
Mahmoud Abdel-Aty,
Sohag University, Egypt

*CORRESPONDENCE
Mingqiang Wang,
wangmingqiang@sdu.edu.cn

SPECIALTY SECTION
This article was submitted to Quantum Engineering and Technology, a section of the journal Frontiers in Physics

RECEIVED 20 August 2022
ACCEPTED 09 September 2022
PUBLISHED 06 October 2022

CITATION
Xu L and Wang M (2022), Quantum voting protocol without quantum memory.
Front. Phys. 10:1023992.
doi: 10.3389/fphy.2022.1023992

Quantum voting protocol without quantum memory

Lidong Xu and Mingqiang Wang*

School of Mathematics, Shandong University, Jinan, China

Most of the quantum voting protocols are impractical due to the currently limited quantum storage capabilities. In this article, based on the interference principle of light, we proposed a new quantum voting protocol without quantum memory. In our protocol, the ballot is a sequence of non-orthogonal coherent states, the voting information is encoded by implying different phase shifts on the coherent states, and the vote counting is carried out by performing USD measurement on the coherent states. Particularly, the design of USD measurement on coherent states eliminates the need for quantum storage. Our protocol satisfies the general security requirements of quantum voting protocols and can resist various attacks. In addition, our protocol can be implemented by only linear optics and thus can be experimentally achieved with current technology.

KEYWORDS

quantum voting, USD measurement, coherent state, QKD, linear optical

1 Introduction

As is known, electronic voting is extensively used in various fields of modern life such as proposal collection and elections. In 1982, Chaum [1] proposed the first privacy-assured voting protocol. Since then, a lot of voting protocols have been constructed where the security of them depends on some difficult mathematical problems, for example, the protocols proposed by Ku and Wang [2] and Jan and Tai [3]. However, with the development of quantum information and quantum computing, as shown by Grover [4]; Shor [5]; Shi [6]; Shi [7]; Zidan et al. [8]; Abdel-Aty et al. [9]; and Zidan et al. [10], the previous voting protocols are under increasing security threat and so cannot meet the security requirements of electronic voting protocols. Since the security of quantum cryptography is guaranteed by the laws of quantum mechanics including the unclonability of quantum states and the principle of uncertainty, it becomes one of the hot issues to design a secure and efficient quantum voting protocol.

In recent years, many secure and efficient quantum voting protocols have been proposed with different features such as anonymous voting, large-scale voting, and traveling ballot. In 2006, Hillery et al. [11] designed a quantum voting protocol that can prevent voters' cheating by resisting each voter to vote more times. In the same year, Hillery [12] first proposed the traveling ballot protocol and distributed ballot protocol which clearly divided the quantum voting protocols into two modes. In 2007, Vaccaro et al. [13] proposed a quantum voting protocol by using quantum entanglement states and summarized the basic rules that a quantum voting scheme should satisfy. In 2011, Horonshko and Kilin [14] proposed a voting protocol that protects the privacy of voters from malicious tallyman and dishonest voters. In 2019, Wang et al. [15] proposed a fault-tolerant quantum protocol that can resist the collective-phasing noise and the collective-rotation noise.

Note that, all of the aforementioned voting protocols are based on quantum entanglement technology. Compared with quantum entangled states, quantum orthogonal product states mentioned by Jiang and Xu [16] and single-particle states are easy to obtain and manipulate. So, quantum voting protocols using non-entangled states have started attracting people's attention. In 2018, Xu et al. [17] constructed a quantum voting protocol by choosing a single-particle state from a set of mutually unbiased bases (MUBs). In 2020, based on locally indistinguishable orthogonal product states, Jiang and Wang [18] proposed a quantum voting scheme that can resist known quantum attacks and has high efficiency.

In this article, we propose a new quantum voting protocol that uses the non-orthogonal coherent states as information carriers. In our protocol, the management center distributes a voting code to each voter over an encryption channel, which plays the role of voting certification. The center also sends these voting codes in a disordered way to the tallyman for vote counting, over an encryption channel. Then, the management center sends a sequence of coherent states as the blank ballot to the first voter. The ballot travels from the first voter to the last one where each voter casts ones vote by applying the phase shift $R(\pi)$ or $R(0)$ on some coherent states based on ones voting code and finally arrives at the tallyman. The tallyman measures the received coherent states by the USD measurement and counts the votes by comparing the original bits used to generate the blank ballot with the measurement outcomes.

Compared with other existing quantum voting protocols, our voting protocol has two outstanding advantages. In the voting process, instead of entangled states or single-particle states, the voting information is encoded into a sequence of non-orthogonal states which can be produced by VCSEL. The phase shift and USD measurement on non-orthogonal states can be performed only by linear optics, which are widely available commercial components. So, our voting protocol can be experimentally achieved with current technology. On the other hand, when receiving the sequence of non-orthogonal states, the receivers immediately implement the USD measurement, which eliminates the need for quantum storage in our protocol. In addition, we also analyze our protocol's security from almost all aspects mentioned in the previous works, such as correctness, anonymity, resisting malicious attacks, legality, non-repeatability, and verifiability.

In this article, we use the non-orthogonal coherent states to design a quantum voting protocol. The rest of this article is structured as follows: Section 2 introduces some basic theories involved in our voting protocol, Section 3 elaborates on our quantum voting protocols, and Section 4 gives the security analysis of the protocol. In the last section, we present the conclusions of this article.

2 Preliminaries

2.1 Notations

In this article, we use boldface lowercase letters to represent sequences of numbers and bit strings, such as $\mathbf{s}$, $\boldsymbol{s_T}$, $\boldsymbol{s_i}$, $\mathbf{r}$. The sequences of quantum states are denoted as bold Greek letters, for example, $\boldsymbol{\rho_r}$, $\boldsymbol{\rho_r^i}$. When the letters are non-boldface, they denote the elements of the sequences, such as $s_i, s_i^{(j)}, r_i, \rho_i$. Particularly, when we write $\boldsymbol{s} - \boldsymbol{s_T}$, where $\boldsymbol{s_T}$ is some subsequence of $\boldsymbol{s}$, it means the complement sequence of $\boldsymbol{s_T}$ with respect to $\boldsymbol{s}$. In addition, the unitary operator that rotates the phase of the coherent state by θ is written as $R(\theta)$.

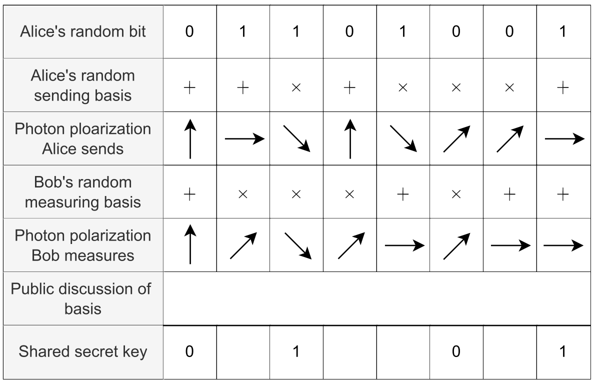
2.2 Quantum key distribution

In the early 1980s, Bennett and Barassard [19] first proposed a scheme to deal with the problem of key distribution based on quantum physics. From then on, a variety of quantum key distribution protocols were proposed, such as the works of Bennett [20]; Scarani et al. [21]; Broadbent and Schaffner [22]; Abdulbast and Khaled [23]; and Ye et al. [24], making quantum key distribution (QKD) the most successful practical application of quantum mechanics to information processing. In recent years, QKD devices have become more and more mature and have entered the application of commercial communication.

The security of QKD is guaranteed by the principles of quantum mechanics and has been proven against any eavesdropper, who has unbounded computational ability. When the key is prepared, as long as the message is to be sent and the key is used only once (one-time pad; OTP), the ciphertext cannot be decrypted by any amount of computation, even by the most powerful computers. The first security proof that considered an unbounded adversary was given by Mayers [25]; Biham et al. [26]; Mayers [27]; and Biham et al. [28], more than a decade after. Another decade after the first such proof, König et al. [29] showed that the security criterion used was insufficient: even though it guarantees that an eavesdropper cannot guess the key, this only holds if the key is never used. If a part of the key is revealed to the eavesdropper, for example, by using it to encrypt a message known to her, the rest becomes insecure. Fortunately, Canetti [30] and Canetti et al. [31] introduced a general framework, universally composable (UC) framework, to define cryptographic security. The security of QKD was discussed within the framework by Ben-Or et al. [32]. They proved that QKD also satisfies the universally composable security under the UC framework, that is, the QKD protocol can be safely used as a sub-protocol to compound with any other (secure) protocols.

Next, we briefly recall the first QKD scheme, BB84, proposed by Bennett and Brassard in 1984, as follows:

Alice prepares a sequence of n photons each in one of the four states($|0\rangle$, $|1\rangle$, $| + \rangle$, $|\times\rangle$) and sends it to Bob over the quantum



Alice's random bit	0	1	1	0	1	0	0	1
Alice's random sending basis	+	+	×	+	×	×	×	+
Photon ploarization Alice sends	↑	→	↘	↑	↘	↗	↗	→
Bob's random measuring basis	+	×	×	×	+	×	+	+
Photon polarization Bob measures	↑	↗	↘	↗	→	↗	→	→
Public discussion of basis								
Shared secret key	0		1			0		1

FIGURE 1
Example of BB84 protocol, where Alice and Bob shared a 4-bit common string from a random bit sequence chosen by Alice.

channel. Bob measures it in either the + or × basis. Now, both Alice and Bob have a list of n pairs (bit and basis). Alice and Bob communicate over the classical channel and compare the "basis" value of each item and discard those in which they used different bases. Now, Alice and Bob have a list of approximately $n/2$ bits, called the raw key. Alice and Bob reveal a random sample of the bits of their raw keys to estimate the error rate in the quantum channel, thus in turn Eve's information. In the absence of errors, the raw key is identical for Alice and Bob, while Eve has no information. If there are errors, Alice and Bob have to correct them and erase the information that Eve could have obtained by communicating over the classical channel. At the end, Alice and Bob share either a truly secret key or nothing at all. Figure 1 shows the process of BB84 scheme when $n = 4$.

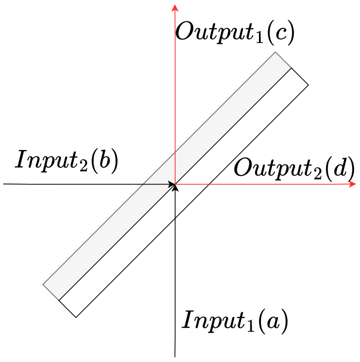


FIGURE 2
Beam splitter is an optical device that can split one beam of light into two beams. It is a key part of most interferometers. When two beams of light get into the beam splitter from *Input*$_1$ and *Input*$_2$, respectively, each of them will be split into two beams. *Output*$_1$ and *Output*$_2$ will output the interfering results of the split beams.

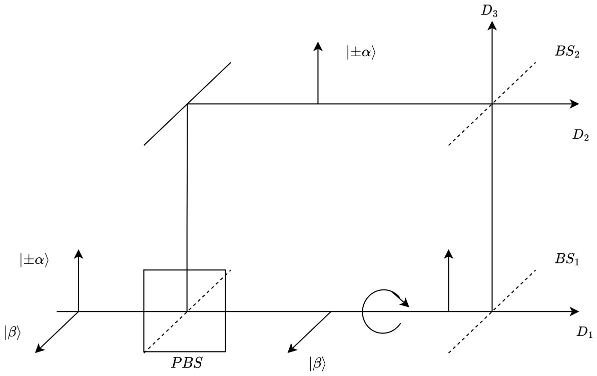


FIGURE 3
USD measurement device.

2.3 Coherent states and USD measurement

A coherent state is a quantum state, which closely resembles a classical electromagnetic wave and can be produced by a single-mode laser such as the vertical-cavity surface-emitting laser (VCSEL), according to the works of Loudon [33]. We adopt the notation $|\alpha e^{i\theta}\rangle$ to represent a coherent state, where α is a real positive amplitude and θ is the phase of the quantum state. As is known, the principles of quantum mechanics prohibit determining the phase of a coherent state with complete certainty if we only have access to the quantum state. The principles were introduced rigorously in the book written by Barnett [34] and Nielsen and Chuang [35]. So, the phase of a coherent state can be thought as the secret information, which cannot be revealed in a conclusive way. Coherent states are comparatively easy to generate and manipulate, and this makes them a far more practical choice for use in quantum information protocols than single photons. So, since 2006, many experimental quantum cryptography schemes using coherent states have been proposed and demonstrated experimentally, for example, the schemes proposed by Andersson et al. [36]; Clarke et al. [37]; Dunjko et al. [38]; Collins et al. [39]; and Donaldson et al. [40]. In these schemes, the classical secret information is encoded by the sender in a sequence of non-orthogonal coherent states, which are distinguished by the receivers using the USD measurement.

Since beam splitters are central to the measurement of two-photon interference phenomena, the USD measurement device employs them as basic optical components. Figure 2 shows the representation of a beam splitter.

The relations between the inputs and outputs are as follows:

$$c = \mathcal{R}b + \mathcal{T}a,$$
$$d = \mathcal{R}a + \mathcal{T}b,$$

```
Subroutine 1

Parameters: classical message length $n$.
Parties: The sender $A$ and the receiver $B$.
1. $A$ and $B$ share a $n$-bit secret key through the QKD scheme;
2. $A$ performs a bit-wise XOR on the $n$-bit message with the $n$-bit key, and sends the result to $B$;
3. $B$ performs a bit-wise XOR on the message he received from $A$ with his $n$-bit key, then he will get the classical message.
```

FIGURE 4
Transportation of a classical message from one party to another, while no third party can get any information about this message.

where $\mathcal{R}$ and $\mathcal{T}$ are the reflection and transmission coefficients, respectively.

Next, let us describe the optical realization of USD measurement between two non-orthogonal coherent states suggested in [1995]. The sender (Alice) generates and sends the weak coherent states $|\pm\alpha\rangle$ with phase encoding 0 or π and the strong coherent state $|\beta\rangle$ to the receiver (Bob), where $|\pm\alpha\rangle$ has vertical polarization and $|\beta\rangle$ has horizontal polarization. When receiving the two states, Bob separates them using a polarization beam splitter (*PBS*). Then, Bob rotates $|\beta\rangle$ to vertical polarization and sends it mainly through a transmitting beam splitter (BS_1) to detector D_1. A small fraction of $|\beta\rangle$, equaling to $|\alpha\rangle$, is reflected to BS_2 where it interferes with $|\pm\alpha\rangle$ and then goes toward two detectors D_2 and D_3. A count in D_2 corresponds to phase 0, while a count in D_3 corresponds to π. No count in both D_2 and D_3 means an inconclusive result. The optical realization of USD measurement between two non-orthogonal coherent states suggested in [1995] can be described in Figure 3.

Finally, we give the optimal probability of obtaining an unambiguous outcome in USD measurement, which is mentioned in the works of Ivanovic [41]; Peres [42]; and Dieks [43]. Given two non-orthogonal coherent states $|\alpha\rangle$ and $|-\alpha\rangle$, if an individual quantum system Q is either in state $|\alpha\rangle$ or in state $|-\alpha\rangle$, then the optimal probability of obtaining an unambiguous outcome in the USD measurement on Q depends on the amplitude α and is given by

$$p_{USD} = 1 - e^{-2\alpha^2}.$$

Obviously, the probability p_{USD} will tend to 1 when α tends to infinity. So, the amplitude α can be chosen based on the practical requirement.

3 Quantum voting protocol

In this section, we describe our protocol in three stages: the initial stage, the voting stage, and the counting stage. There are $n + 2$ participants in our protocol, including the management center (M) as a trusted participant who will not disclose any information on the voters' voting codes, the tallyman (T) who is responsible to count the number of votes, and n voters (V_1, V_2, . . ., V_N). In the initial stage, M sends a voting code to each voter, then mixes up all the voting codes, and sends them to T. In the voting stage, T sends the quantum ballot to V_1. Then, V_1 encodes V_1's vote by applying the phase shift R(0) or $R(\pi)$ on some coherent states of the ballot based on V_1's voting codes and sends the resulting ballot to V_2, and so on. After V_n finishes the voting, V_n sends the resulting ballot to T. In the counting stage, T measures each coherent states of the received ballot by USD measurement and counts the number of votes.

3.1 Encryption channel

Before describing our protocol, we introduce how to set up an encryption channel at first. This channel will be used in our protocol to transmit classical sequences without being revealed to anyone other than the receiver.

It is well known that QKD can be implemented only by linear optics, so the aforementioned subroutine is feasible with current technology. The security of QKD is guaranteed by the principles of quantum mechanics and has been rigorously proven by Mayers [25]; Biham et al. [26]; Mayers [27]; and Biham et al. [28]. Thus, we can conclude that the QKD protocols can be against any eavesdropper, who has unbounded computational ability. When considering using the QKD as a subroutine in other protocols, the proof of the security of QKD under the UC framework is given by Ben-Or et al. [32], which makes the aforementioned subroutine that can be securely composed into our protocol. Figure 4 shows the establishment of the encryption channel.

3.2 Our protocol

Our protocol can be applied in the following scenario: the management center acts as a trusted party and supervises all other participants, including voters and tallyman. The tasks of voters and tallyman are the same as normal voting protocols. In addition, when there is a disagreement on the number of votes between the voters and tallyman, the management center can verify the result. Now, we describe our protocol in detail.

The initial stage:

1) The management center M sets up a bulletin board and announces the voters and tallyman and their order on the bulletin board.
2) M randomly chooses L elements from the sequence $\boldsymbol{s} = (1, 2, \ldots, 2nL)$ as V_1's voting code, denoted by $\mathbf{s_1} = (s_1^{(1)}, s_1^{(2)}, \ldots, s_1^{(L)})$. Then, V_1 randomly chooses L elements from the remaining numbers as V_2's voting code,

denoted by $\boldsymbol{s_2} = (s_2^{(1)}, s_2^{(2)}, \ldots, s_2^{(L)})$, and so on. Finally, the last member randomly chooses L elements from the remaining $(n + 1)$ numbers as V_n's voting code, denoted by $\boldsymbol{s_n} = (s_n^{(1)}, s_n^{(2)}, \ldots, s_n^{(L)})$.

3) M rearranges $s_i^{(j)}$ ($i = 1, 2, \ldots, n$ and $j = 1, 2, \ldots, L$) in an incremental manner to form a subsequence of $\boldsymbol{s}$, denoted by $\boldsymbol{s_T}$.
4) M sends $\boldsymbol{s_i}$ to V_i and $\boldsymbol{s_T}$ to T by calling Subroutine 1.

The voting stage:

1) M and T discuss to determine a sequence $\boldsymbol{r} = (r_1, r_2, \ldots, r_{2nL}) \in \{-1,1\}^{2nL}$ by BB84 protocol, and then M generates a sequence $\boldsymbol{\rho_r} = (\rho_1, \rho_2, \ldots, \rho_{2nL})$ of coherent states, where $\rho_i = |r_i\alpha\rangle\langle r_i\alpha|$. Here, $\boldsymbol{\rho_r}$ is called the ballot.
2) M sends $\boldsymbol{\rho_r}$ to the first voter V_1.
3) After receiving $\boldsymbol{\rho_r}$, the voter V_1 starts to vote based on V_1's voting code. If V_1 decides to vote the current candidate, then V_1 applies $R(\pi)$ to each element of $(\rho_{s_1^{(1)}}, \rho_{s_1^{(2)}}, \ldots, \rho_{s_1^{(L)}})$ and performs nothing on the rest states of ρ_r. If V_1 does not want to vote for the current candidate, then V_1 performs nothing on the element of $\boldsymbol{\rho_r}$. V_1 sends the sequence of resulting states, denoted by $\boldsymbol{\rho_r^1}$, to V_2.
4) For $2 \leq i \leq n - 1$, suppose the voter V_i has received $\boldsymbol{\rho_r^{i-1}}$, then V_i starts to vote based on V_i's voting code. If V_i decides to vote the current candidate, then V_i applies $R(\pi)$ to each element of $(\rho_{s_i^{(1)}}, \rho_{s_i^{(2)}}, \ldots, \rho_{s_i^{(L)}})$ and performs nothing on the rest states of ρ_r. If V_i does not want to vote the current candidate, then V_i performs nothing on the element of $\boldsymbol{\rho_r^{i-1}}$. V_i sends the sequence of resulting states, denoted by $\boldsymbol{\rho_r^i}$, to V_{i+1}.
5) After receiving $\boldsymbol{\rho_r^{n-1}}$, V_n votes based on V_n's voting code just as other voters carry out. Then, V_n sends the sequence of resulting states, denoted by $\boldsymbol{\rho_r^n}$, to T.

The counting stage:

1) The tallyman T measures each element of $\boldsymbol{\rho_r^n}$ by USD measurement and records the measuring results as a sequence $\mathbf{r}' = (r_1', r_2', \ldots, r_{2nL}')$, where $r_i' = 1$ if the measuring result of the ith state is $|\alpha\rangle$, $r_i' = -1$ if the measuring result of the ith state is $|-\alpha\rangle$, and $r_i' = 0$ if the measuring result is ambiguous.
2) T compares r_i and r_i' for each $i \in \boldsymbol{s} - \boldsymbol{s_T}$ and counts the number of mismatches for the unambiguous measuring results. If the number is larger than $s_a p_{USD} nL$, T aborts the protocol. Otherwise, T continues the next step.
3) T compares r_i with r_i' for each $i \in \boldsymbol{s_T}$ and counts the number of mismatches for the unambiguous measuring results. If the number is inside $[(p_{USD} - \delta)kL, (p_{USD} + \delta)kL]$, then the number of votes is k.
4) T announces the measurement result $\mathbf{r}' = (r_1', r_2', \ldots, r_{2nL}')$ and the number of votes on the bulletin board.

Remark: s_a is the mismatch tolerance for the set $\{(r_i, r_i'): i \in \boldsymbol{s} - \boldsymbol{s_T}\}$, and δ is the unambiguous count tolerance.

According to the analysis in the next section, our protocol has six important properties, which are mentioned in the previous works. Here, we list them as follows:

1) Correctness: the protocol will abort only with a negligible probability and output a correct number of votes with an overwhelming probability.
2) Anonymity: only the voter knows what the voter votes.
3) Resisting malicious attack: any malicious Eve can change the number of votes and cannot be detected by the tallyman T with a negligible probability.
4) Legality: only the legitimate voters can vote.
5) Non-repeatability: each legitimate voter can vote just once.
6) Verifiability: each voter can ask the management center to verify whether the voter's vote has been calculated correctly.

4 Analysis

In this section, we analyze our protocol from six aspects: correctness, anonymity, resisting malicious attack, legality, non-repeatability, and verifiability.

4.1 Correctness

In this scenario, all parties in the protocol are assumed to be honest, and no attack occurs. We discuss the correctness in two aspects: our protocol will abort only with a negligible probability, and it will output a correct number of votes with an overwhelming probability.

Let X_1 be the empirical number of mismatches in Step 2 of the counting stage, then the expectation μ of X_1 is 0. Obviously, our protocol will abort whenever $X_1 \geq s_a p_{USD} nL$. So, the probability of "the protocol aborts" is

$$P_a = P[X_1 \geq s_a p_{USD} nL]. \tag{1}$$

According to Hoeffding's inequalities, we obtain

$$P_a = P[X_1 \geq s_a p_{USD} nL] \leq \exp\left(-2\left(s_a p_{USD}\right)^2 nL\right). \tag{2}$$

This means that P_a decreases exponentially as L increases, and thus our protocol will abort only with a negligible probability for some large enough L.

Now, let us consider the counting process. Suppose that the number of votes is k and X_2 is the empirical number of matches in Step 3 of the counting stage, then the expectation of X_2 is $p_{USD}kL$. It follows that the probability of "the number of votes is wrong" is

$$P_w = P[|X_2 - p_{USD}kL| \geq \delta]. \tag{3}$$

By Hoeffding's inequalities, we claim that

$$P_w = P\left[|X_2 - p_{USD}kL| \geq \delta\right] \leq 2\exp\left(-2\delta^2 nL\right). \quad (4)$$

Clearly, the probability P_w is decreasing exponentially as the L is increasing. So, our protocol will output a correct number of votes with an overwhelming probability for some large enough L.

4.2 Anonymity

Obviously, there are two extreme situations where the privacy is meaningless. When the number of votes is 0, all voters have not voted the candidate. When the number of votes is n, all voters have voted the candidate. Next, we skip these situations to discuss the voter's privacy.

To verify whether a voter V_i has voted the current candidate, a curious participant needs to know V_i's voting code, the sequence $\mathbf{r}$, and the sequence $\mathbf{r}'$. If the curious participant has no information about V_i's voting code, then the participant could not determine on which coherent states the phase was shifted. If the curious participant has no information about the sequence $\mathbf{r}$ or the sequence $\mathbf{r}'$, then the participant will not know how V_i voted for the current candidate.

Since the voting codes are transmitted from M to the voters over encryption channels, V_i can only obtain V_i's own voting code $\boldsymbol{s_i}$, while V_i does not know any information of other voters' voting codes. Furthermore, in the voting stage, the original sequence $\boldsymbol{r}$ was randomly selected by M and T. So, no one can obtain the voting results by comparing the original bit r_i with the corresponding measurement outcomes r_i^j except T, even if T intercepts some sequence $\boldsymbol{\rho_r^j}$ and measures all elements of it. Thus, the voting result is anonymous for each voter.

In the initial stage, the management center M sends $\boldsymbol{s_T}$, which is a rearrangement of $s_i^{(j)}$ $(i = 1, 2, \ldots, n$ and $j = 1, 2, \ldots, L)$ in an incremental manner, to the tallyman T. So, T can only know which coherent state has been changed by the voters but cannot know which voter has changed the state. Thus, T can only obtain the number of votes but cannot determine how each voter voted, that is, the voting result is anonymous for the tallyman.

4.3 Resisting malicious attack

According to the aforementioned analysis, our protocol can resist the attack of dishonest parties. But, what happens if there is a malicious Eve who wants to make T get the wrong number of votes?

First of all, let us consider the malicious Eve's two possible strategies:

- When the voting code s_i of some voter V_i is transmitted over the encryption channel, Eve selects enough bits of s_i to perform XOR with 1. In this way, Eve can change V_i's voting code, and thus the voter V_i will apply a phase shift on coherent states at some incorrect position of the ballot. This will possibly affect the correctness of vote counting by the tallyman.
- When some voter V_i sends V_i's ballot ρ_i^r over the quantum channel to the next receiver, Eve intercepts it and applies $R(\pi)$ on enough states of it. As a result, V_i's vote will be reversed, and thus the tallyman will obtain the incorrect number of votes in the counting stage.

Since Eve knows neither the voter V_i nor the sequence $\boldsymbol{\rho_r^i}$ of coherent states from V_i to V_{i+1}, Eve's choices of bits or coherent states are random. So, there is no difference between changing some bits of V_i's voting code by XOR and changing some coherent states of $\boldsymbol{\rho_r^i}$ by the phase shift for Eve's aim. Based on this fact, we focus on the case that Eve applies $R(\pi)$ on some coherent states of ρ_r^i when V_i votes. In fact, we only need to consider that Eve applies $R(\pi)$ on some coherent states of ρ_r^n when V_n votes.

Suppose the actual number of votes is k and Eve applies $R(\pi)$ on l coherent states of the sequence $\boldsymbol{\rho_r^n}$, then the expectation of the number of changed states by Eve at the position of voting codes is $\frac{l}{2}$ and the expectation of the number of changed states by Eve at other positions is $\frac{l}{2}$. So, the expectation of the number of not being the original states at the position of voting codes is

$$\frac{(n-k)L}{nL}\frac{l}{2} - \frac{kL}{nL}\frac{l}{2} = \frac{(n-2k)l}{2n}, \ when\ n \geq 2k, \quad (5)$$

or

$$\frac{kL}{nL}\frac{l}{2} - \frac{(n-k)L}{nL}\frac{l}{2} = \frac{(2k-n)l}{2n}, \ when\ n < 2k, \quad (6)$$

and the expectation of the number of not being the original states at the other positions is $\frac{l}{2}$.

Next, we first consider the case of $n \geq 2k$. Let XnL be the empirical number of changed states by Eve at the position of voting codes, where X is the empirical change ratio. Then, by Hoeffding's inequalities, we have that

$$P\left(|\ XnL - \frac{(n-2k)p_{USD}l}{2n}\ | \geq \varepsilon nL\right) = P\left(|\ X - \frac{(n-2k)p_{USD}l}{2n^2L}\ | \geq \varepsilon\right) \leq 2\,exp\left(-2\varepsilon^2 L\right). \quad (7)$$

Let YnL be the empirical number of not being the original states at other positions, where Y is the empirical change ratio. Then, by Hoeffding's inequalities, we have that

$$P\left(|\ YnL - \frac{1}{2}p_{USD}l\ | \geq \varepsilon nL\right) = P\left(|\ Y - \frac{l}{2nL}p_{USD}\ | \geq \varepsilon\right) \leq 2\,exp\left(-2\varepsilon^2 L\right), \quad (8)$$

where ε is any small positive number. So, the empirical number of changed states by Eve at the positions of voting codes will be inside $[\frac{(n-2k)p_{USD}l}{2n^2L} - \varepsilon nL, \frac{(n-2k)P_{USD}l}{2n^2L} + \varepsilon nL]$, with an overwhelming probability for large enough L, and the empirical number of not

TABLE 1 Comparison with other quantum voting protocols.

	Wang et al[15]	**Xu et al[17]**	**Jiang and Wang [18]**	**Our protocol**
Number of participants	n + 3	n + 3	n + 3	n + 2
Quantum resources	Entangled states	Orthogonal product states	Single-particle states	Non-orthogonal coherent states
Measurement technology	Basis measurement	Basis measurement	Basis measurement	USD measurement
Quantum memory	Yes	Yes	Yes	No

being the original states at the other positions will be inside $[\frac{1}{2}p_{USD}l - \varepsilon nL, \frac{1}{2}p_{USD}l + \varepsilon nL]$, with an overwhelming probability for large enough L.

To successfully change the number k of votes, Eve should increase or decrease at least L coherent states, which are not the original ones at the position of voting codes, and guarantee that the number of not being the original states at the other positions is less than $s_a p_{USD} nL$, that is,

$$\frac{(n-2k)P_{USD}l}{2n} - \varepsilon nL \geq p_{USD}L, \tag{9}$$

$$\frac{1}{2}p_{USD}l + \varepsilon nL \leq s_a p_{USD} nL. \tag{10}$$

Note that, inequality 9 implies that $l \geq \frac{2(p_{USD}+\varepsilon n)nL}{(n-2k)p_{USD}}$, and inequality 10 implies that $l \leq \frac{2(s_a p_{USD}-\varepsilon)nL}{p_{USD}}$. If the tallyman T sets $s_a < \frac{p_{USD}+\varepsilon n}{(n-2k)p_{USD}} + \frac{\varepsilon}{p_{USD}}$, then $\frac{2(s_a p_{USD}-\varepsilon)nL}{p_{USD}} < \frac{2(p_{USD}+\varepsilon n)nL}{(n-2k)p_{USD}}$. This means that no matter how many coherent states Eve selects to apply the phase shift $R(\pi)$, Eve cannot achieve the aim both to change the number k of votes and not to be detected by the tallyman T.

For the case of $n < 2k$, a similar discussion will yield the requirement that $s_a < \frac{p_{USD}+\varepsilon n}{(2k-n)p_{USD}} + \frac{\varepsilon}{p_{USD}}$. Since the number k of votes is uncertain and between 1 and n, it is enough for T to set $s_a < \frac{1}{n} + \frac{2\varepsilon}{p_{USD}}$.

4.4 Legality

Only eligible voters can vote in the voting stage. Each voter who has the qualification to vote must be announced on the bulletin board and distributed a voting code by the voting management center M over an encryption channel. For an illegal voter, any legal voter will not send the ballot to the illegal voter. Even obtained the ballot, the illegal voter has no way to know a voting code and so does not know which coherent states should be operated. According to the analysis of malicious attack, any random phase shifts on elements of the ballot will be either invalid or detected by the tallyman at the counting stage.

4.5 Non-repeatability

According to the analysis of the malicious attack, any voter's illegal operation after voter's first voting will yield two possible results. If the voter changes the coherent states at the position of voter's voting codes, then the voter will turn voter's own voting. If the voter changes the coherent states at the other positions, then either voter's operation is not valid when the number of changed coherent states at the position of other voters' voting codes is less than L or voter's operation is detected by the tallyman when the number of changed coherent states at the other positions is more than $2s_a L$.

4.6 Verifiability

After the tallyman T publishes the measurement results and the voting results on the bulletin board, each voter can check whether voter's voting is tampered or missed according to voter's voting code. If there is a dispute, the voter can apply to the management center for arbitration (M distributes ballot $\boldsymbol{\rho_r}$ to the first voter and sends $\boldsymbol{r}$ to T over an encryption channel). As a scrutineer of the voting process, the management center knows both classical information $\boldsymbol{r}$ of the ballot $\boldsymbol{\rho_r}$ and voters' voting codes. Once the tallyman announces the measurement outcomes, any deception carried out by voters or the tallyman can be found by the management center M.

5 Conclusion

In this article, we propose a quantum voting protocol without quantum memory by using the coherent states, USD measurement, and QKD technology. Our protocol satisfies the general security requirements of the quantum voting protocols such as correctness, anonymity, resisting malicious attack, legality, non-repeatability, and verifiability. If the parameters in the protocol are properly chosen, our protocol will abort or output a wrong number of votes only with a negligible probability.

Compared with other existing quantum voting protocols, our voting protocol has two outstanding advantages. In the voting process, instead of entangled states or single-particle states, the voting information is encoded into a sequence of non-orthogonal states which can be produced by VCSEL. The phase shift and USD measurement on non-orthogonal states can be performed only by linear optics, which are widely available commercial components. So, thus our voting protocol can be experimentally achieved with current technology. On the other hand, when receiving the sequence of non-orthogonal states, the receivers immediately implement the USD measurement, which eliminates the need for quantum storage in our protocol. The comparison with other existing protocols is given in Table 1.

The most important advantage of our quantum voting protocol lies in that the tallyman measures the sequence of coherent states immediately after the tallyman receives it, by the USD measurement. So, our protocol does not require any quantum memory to store the coherent states. In this way, the limitation of quantum storage capabilities faced by other voting protocols no longer exists.

To sum up, our voting protocol not only satisfies the security required by quantum voting protocols but also takes into account the infeasibility in reality. We believe that our voting protocol will have a good application prospect.

Data availability statement

The original contributions presented in the study are included in the article/Supplementary material; further inquiries can be directed to the corresponding author.

Author contributions

All authors listed have contributed to this work equally and approved it for publication.

Funding

This research was supported by the National Key Research and Development Program of China (No. 2021YFA1000600), the National Key Research and Development Program of China (Grant No. 2018YFA0704702), and the National Natural Science Foundation of China (Grant No. 61832012).

Conflict of interest

The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Publisher's note

All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors, and the reviewers. Any product that may be evaluated in this article, or claim that may be made by its manufacturer, is not guaranteed or endorsed by the publisher.

References

1. Chaum D. Untraceable electronic mail, return addresses, and digital pseudonyms. *Commun ACM* (1982) 24:84–90. doi:10.1145/358549.358563

2. Ku W-C, Wang S-D. A secure and practical electronic voting scheme. *Comp Commun* (1999) 22:279–86. doi:10.1016/S0140-3664(98)00241-2

3. Jan J-K, Tai C-C. A secure electronic voting protocol with ic cards. *J Syst Softw* (1997) 39:93–101. doi:10.1016/S0164-1212(96)00166-5

4. Grover LK. A fast quantum mechanical algorithm for database search. In: *28th annual ACM symposium on the theory of computing*. Philadelphia: STOC (1996). p. 212–9. doi:10.1145/237814.237866

5. Shor P. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J Comput* (1999) 26:1484–509. doi:10.1137/S0097539795293172

6. Shi Y-P. A brief introduction to quantum computing and quantum information(i). *Math Model Its Appl* (2018) 7:1–10.

7. Shi Y-P. A brief introduction to quantum computing and quantum information(ii). *Math Model Its Appl* (2018) 7:1–11.

8. Zidan M, Abdel-Aty A-H, Younes A, Zanaty EA, El-khayat I. A novel algorithm based on entanglement measurement for improving speed of quantum algorithms. *Appl Math Inf Sci* (2018) 12:265–9. doi:10.18576/amis/120127

9. Abdel-Aty A-H, Kadry H, Zidan M, Al-Sbou Y, Zanaty EA, Abdel-Aty M. A quantum classification algorithm for classification incomplete patterns based on entanglement measure. *J Intell Fuzzy Syst* (2020) 38:2809–16. doi:10.3233/JIFS-179566

10. Zidan M, Aldulaimi S, Eleuch H. Analysis of the quantum algorithm based on entanglement measure for classifying boolean multivariate function into novel hidden classes: Revisited. *Appl Math Inf Sci* (2021) 15:643–7. doi:10.18576/amis/150513

11. Hillery M, Ziman M, Bielikova M, Buzek V. Towards quantum-based privacy and voting. *Phys Lett A* (2006) 349:75–81. doi:10.1016/j.physleta.2005.09.010

12. Hillery M, Ziman M, Buzek V, Bielikova M. Quantum voting and privacy protection: First steps. *Phys Lett A* (2006) 349:75–81. doi:10.1016/j.physleta.2005.09.010

13. Vaccaro JA, Spring J, Chefles A. Quantum protocols for anonymous voting and surveying. *Phys Rev A (Coll Park)* (2007) 75:012333. doi:10.1103/PhysRevA.75.012333

14. Horonshko D, Kilin S. Quantum anonymous voting with anonymity check. *Phys Lett A* (2011) 375:1172–5. doi:10.1016/j.physleta.2011.01.038

15. Wang S-L, Zhang S, Wang Q, Shi R-H. Fault-tolerant quantum anonymous voting protocol. *Int J Theor Phys (Dordr)* (2019) 58:1008–16. doi:10.1007/s10773-018-3992-z

16. Jiang D-H, Xu G-B. Nonlocal sets of orthogonal product states in an arbitrary multipartite quantum system. *Phys Rev A (Coll Park)* (2020) 102:032211. doi:10.1103/PhysRevA.102.032211

17. Xu Y-Z, Huang Y-F, Lu W, Li L-Z. A quantum electronic voting scheme with d-level single particles. In: Huang D, Gromiha M, Han K, Hussain A, editors. *Intelligent computing methodologies. ICIC 2018. Lecture notes in computer science*, 10956 (2018). p. 710–5.

18. Jiang D-H, Wang J, Liang XQ, Xu GB, Qi HF. Quantum voting scheme based on locally indistinguishable orthogonal product states. *Int J Theor Phys (Dordr)* (2020) 59:436–44. doi:10.1007/s10773-019-04337-8

19. Bennett C, Barassard G. Quantum cryptography: Public key distribution and coin tossing. *Theor Comput Sci* (1984) 560:7–11. doi:10.1016/j.tcs.2014.05.025

20. Bennett CH. Quantum cryptography using any two nonorthogonal states. *Phys Rev Lett* (1992) 68:3121–4. doi:10.1103/PhysRevLett.68.3121

21. Scarani V, Acín A, Ribordy G, Gisin N. Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations. *Phys Rev Lett* (2004) 92:057901. doi:10.1103/PhysRevLett.92.057901

22. Broadbent A, Schaffner C. Quantum cryptography beyond quantum key distribution. *Des Codes Cryptogr* (2016) 78:351–82. doi:10.1007/s10623-015-0157-4

23. Abdulbast AA, Khaled ME. Qkd protocol based on entangled states by trusted third party. In: Proceeding of the 2017 IEEE Long Island Systems, Applications and Technology Conference (LISAT); May 2017; Farmingdale, NY, USA (2017). p. 1–5. doi:10.1109/LISAT.2017.8001969

24. Ye T-Y, Geng M-J, Xu T-J, Chen Y. Efficient semiquantum key distribution based on single photons in both polarization and spatial-mode degrees of freedom. *Quan Inf Process* (2022) 21:123. doi:10.1007/s11128-022-03457-1

25. Mayers D. Quantum key distribution and string oblivious transfer in noisy channels. In: Koblitz N, editor. *Advances in cryptology — crypto '96. Crypto 1996. Lecture notes in computer science*, 1109 (1996). p. 343–57.

26. Biham E, Boyer M, Boykin OP, Roychowdhury V, More T. A proof of the security of quantum key distribution (extended abstract). In: Proceedings of the Thirty-Second Annual ACM Symposium on Theory of Computing(STOC'00); May 2000. Portland, OR: Association for Computing Machinery (2000). p. 715–24. doi:10.1145/335305.335406

27. Mayers D. Unconditional security in quantum cryptography. *J ACM* (2001) 48:351–406. doi:10.1145/382780.382781

28. Biham E, Boyer M, Boykin OP, Mor T, Roychowdhury V. A proof of the security of quantum key distribution. *J Cryptology* (2006) 19:381–439. doi:10.1007/s00145-005-0011-3

29. König R, Renner R, Bariska A, Maurer U. Small accessible quantum information does not imply security. *Phys Rev Lett* (2007) 98:140502. doi:10.1103/PhysRevLett.98.140502

30. Canetti R. *Universally composable security: A new paradigm for cryptographic protocols*. Cryptology ePrint Archive (2000). [Dataset] Paper 2000/067. available at: https://eprint.iacr.org/2000/067.

31. Canetti R, Dodis Y, Pass R, Walfish S. Universally composable security with global setup. In: Vadhan S, editor. *Theory of cryptography TCC 2007. Lecture notes in computer science*, 4392 (2007). p. 41–50. doi:10.1007/978-3-540-70936-7_4

32. Ben-Or M, Horodecki M, Leung DW, Mayers D, Oppenheim J. The universal composable security of quantum key distribution. In: Kilian J, editor. *Theory of cryptography TCC 2005. Lecture notes in computer science)*, 3378 (2005). p. 41–50. doi:10.1007/978-3-540-30576-7_21

33. Loudon R. *The quantum theory of light*. Oxford University Press (2000).

34. Barnett S *Quantum information*, 16. Oxford University Press (2009).

35. Nielsen MA, Chuang IL. *Quantum computation and quantum information*. Cambridge University Press (2010).

36. Andersson E, Curty M, Jex I. Experimentally realizable quantum comparison of coherent states and its applications. *Phys Rev A (Coll Park)* (2006) 74:022304. doi:10.1103/PhysRevA.74.022304

37. Clarke PJ, Collins RJ, Dunjko V, Andersson E, Jeffers J, Buller GS. Experimental demonstration of quantum digital signatures using phase encoded coherent states of light. *Nat Commun* (2012) 3:1174–8. doi:10.1038/NCOMMS2172

38. Dunjko V, Wallden P, Andersson E. Quantum digital signatures without quantum memory. *Phys Rev Lett* (2014) 112:040502. doi:10.1103/PhysRevLett.112.040502

39. Collins RJ, Donaldson RJ, Dunjko V, Wallden P, Clarke PJ, Andersson E, et al. Realization of quantum digital signatures without the requirement of quantum memory. *Phys Rev Lett* (2014) 113:040502. doi:10.1103/physrevlett.113.040502

40. Donaldson RJ, Collins RJ, Kleczkowska K, Amiri R, Wallden P, Dunjko V, et al. Experimental demonstration of kilometer-range quantum digital signatures. *Phys Rev A (Coll Park)* (2016) 93:012329. doi:10.1103/PhysRevA.93.012329

41. Ivanovic ID. How to differentiate between non-orthogonal states. *Phys Lett A* (1987) 123:257–9. doi:10.1016/0375-9601(87)90222-2

42. Peres A. How to differentiate between non-orthogonal states. *Phys Lett A* (1988) 128:19. doi:10.1016/0375-9601(88)91034-1

43. Dieks D. Overlap and distinguishability of quantum states. *Phys Lett A* (1988) 126:303–6. doi:10.1016/0375-9601(88)90840-7

frontiers | Frontiers in Physics

TYPE Original Research
PUBLISHED 13 October 2022
DOI 10.3389/fphy.2022.1023443

OPEN ACCESS

EDITED BY
Tianyu Ye,
Zhejiang Gongshang University, China

REVIEWED BY
Xiangfu Zou,
Wuyi University, China
Xiaoping Lou,
Hunan Normal University, China

*CORRESPONDENCE
Yuan Tian,
tinyuen@xauat.edu.cn

SPECIALTY SECTION
This article was submitted to Quantum Engineering and Technology, a section of the journal Frontiers in Physics

RECEIVED 19 August 2022
ACCEPTED 15 September 2022
PUBLISHED 13 October 2022

CITATION
Tian Y, Li J, Ye C and Li C (2022), Multi-party semi-quantum key distribution protocol based on hyperentangled Bell states.
Front. Phys. 10:1023443.
doi: 10.3389/fphy.2022.1023443

Multi-party semi-quantum key distribution protocol based on hyperentangled Bell states

Yuan Tian[1]*, Jian Li[2], Chongqiang Ye[3] and Chaoyang Li[4]

[1]College of Information and Control Engineering, Xi'an University of Architecture and Technology, Xi'an, China, [2]School of Cyberspace Security, Beijing University of Post and Telecommunications, Beijing, China, [3]Information Security Center, State Key Laboratory of Networking and Switching Technology, Beijing University of Post and Telecommunications, Beijing, China, [4]College of Software Engineering, Zhengzhou University of Light Industry, Zhengzhou, China

Semi-quantum key distribution allows generating a raw key between two communication participants, in which the sender is a quantum participant and the receiver is a classical participant. This article presents an original semi-quantum key distribution protocol based on hyperentangled Bell states. The hyperentangled Bell states can be entangled simultaneously in polarization and spatial degrees of freedom, enhancing channel capacity. According to the characteristics of hyperentangled Bell states, the proposed protocol is more efficient than the protocol based on Bell states. Moreover, the measure−resend attack, the intercept−resend attack, and the entangle−measure attack are analyzed in detail. The security analysis demonstrates that the proposed protocol is secure. In addition, a multi-party semi-quantum key distribution scheme based on hyperentangled Bell states is proposed, which can realize key distribution between one quantum participant and multiple classical participants.

KEYWORDS

quantum cryptography, semi-quantum key distribution, hyperentangled Bell states, polarization degree of freedom, spatial degree of freedom

1 Introduction

A traditional cryptographic protocol is the foundation of information security in public network channels [1–3]. With the successful development of quantum computers and quantum computing, the traditional classical encryption algorithm based on mathematical problems has been seriously threatened [4]. Different from traditional cryptography, quantum cryptography is based on quantum physics [5] and information science to guarantee communication security [6]. Therefore, quantum information processing has gained increasing attention for potential applications such as quantum communication technology and quantum computing. Quantum communication technology is based on quantum cryptography to solve the potential problem of channel eavesdropping, which has provable security. Quantum communication includes quantum key distribution (QKD) [7, 8], quantum secure direction communication (QSDC) [9, 10], quantum secret sharing (QSS) [11, 12], quantum private comparison (QPC) [13, 14] etc. Quantum key distribution protocol, as a significant field of quantum cryptography, is a quantum cryptography protocol, which can be verified theoretically and experimentally.

The BB84 protocol [15], the initial quantum key distribution protocol, was presented by Bennett and Brassard in 1984. It guarantees the secure transmission of keys between two participants. The BB84 protocol had gained widespread attention when it was proposed, and many researchers began to study the QKD protocol since BB84 was presented, such as Ekert91 protocol [16], BBM92 protocol [17], SARG04 protocol [18], and so on. In recent years, the latest protocols and the development of QKD were presented [19–22]. However, the traditional QKD protocols require all communication participants to have quantum capability and quantum devices [23], which are too complex and expensive to realize. At present, only a few environments can be implemented. These are also important factors hindering QKD's current development.

Aiming at the problems faced in complex quantum operations and expensive quantum devices, the concept of "semi-quantum" was proposed for the first time by Boyer et al. [24]. They proposed the first semi-quantum key distribution protocol in 2007. Alice, a sender, has quantum capability, and Bob, a receiver, has classical capability. The classical capability is restricted within the following operations : (1) reflecting the qubits with no disturbance ; (2) measuring the qubits with basis Z; (3) preparing the fresh qubits with basis Z; and (4) reordering the qubits *via* delay lines. Because the concept of "semi-quantum" requires less quantum power and resources and is easy to implement, it has received extensive attention, has been studied by an increasing number of scholars, and even extended to other directions such as semi-quantum distribution (SQKD) protocols [25–33], semi-quantum secret sharing (SQSS) protocols [34–37], semi-quantum private comparison (SQPC) protocols [38–41], etc. In 2009, Zou et al. [25] put forward five SQKD protocols based on three quantum states, two quantum states, and one quantum state, and strong proofs are given. In 2011, an SQKD protocol based on Bell states was devised by Wang et al. [26]. Without invoking the classical participant's measurement capability, an efficient SQKD protocol was designed by Zou et al. [27] in 2015. In 2017, an SQKD protocol that limits the quantum sender's measurement capabilities was presented by Krawec et al. [28]. Two semi-quantum key distribution protocols based on GHZ states were proposed by Zhu et al. [29] in 2018. The presented protocol had higher noise tolerance than the "fully quantum" protocol. Iqbal et al. [30] designed an SQKD protocol based on high-dimensional quantum states which increased the noise tolerance in 2019. In 2020, Ye et al. [31] proposed a novel SQKD based on single photons in both polarization and spatial-mode degrees of freedom, which improved the capacity of quantum communication. In 2021, Tian et al. [32] presented an efficient SQKD based on EPR and single-particle hybridization, which has higher efficiency than that found in the similar literature. An efficient SQKD protocol based on single photons in both polarization and spatial-mode degrees of freedom was proposed by Ye et al. [33], which has double quantum communication capacity.

The hyperentangled states not only contain the entanglement between multi-particles but also multi-dimensional entanglements, such as spatial degree of freedom and polarization degree of freedom [42]. The way to transmit secret information safely is to measure the spatial degree of freedom and polarization degree of freedom of a photon by hyperentangled Bell state measurement to change the spatial degree of freedom and polarization degree of freedom of another photon.

To improve the efficiency and security of information transmission, reducing the responsibility of the protocol, this study proposes a semi-quantum key distribution protocol based on hyperentangled Bell states. In addition, the security analysis of the protocol shows that the proposed protocol can effectively resist the measure–resend attack, intercept–resend attack, and entangle–measure attack. It is demonstrated that the proposed protocol is efficient and secure. In the process of key distribution, sometimes not only two participants but also multiple participants are required. Considering that more scenarios are applicable, we design a semi-quantum key distribution protocol that satisfies multiple participants and achieves more than the previous key distribution between two participants.

This article is organized as follows: Section 2 proposes the semi-quantum distribution protocol, Section 3 gives the security proof and comparison of the protocol, Section 4 designs the multi-party semi-quantum distribution protocol, and Section 5 summarizes it.

2 Semi-quantum key distribution protocol

In this section, we introduce the hyperentangled Bell states and propose an SQKD protocol based on the hyperentangled Bell states.

2.1 The hyperentangled Bell states

We present the hyperentangled Bell states as follows:

$$|\Phi\rangle_{ps}^{12} = |\mu\rangle_{p}^{12} \otimes |\nu\rangle_{s}^{12}, \tag{1}$$

where 1 and 2 represent the two qubits in the hyperentangled Bell states and p, s represent the polarization degree of freedom and the spatial degree of freedom, respectively.

Under the polarization degree of freedom $|\mu\rangle_{p}^{12}$, the Bell states can be described as follows:

$$|\phi^{\pm}\rangle_p^{12} = \frac{1}{\sqrt{2}}(|HH\rangle \pm |VV\rangle), \tag{2}$$

$$|\psi^{\pm}\rangle_p^{12} = \frac{1}{\sqrt{2}}(|HV\rangle \pm |VH\rangle), \tag{3}$$

where $|H\rangle$, $|V\rangle$ are the horizontal and the vertical polarizations, respectively.

Under the spatial degree of freedom $|\nu\rangle_s^{12}$, the Bell state can be described as follows:

$$|\phi^{\pm}\rangle_s^{12} = \frac{1}{\sqrt{2}}(|RR\rangle \pm |LL\rangle), \tag{4}$$

$$|\psi^{\pm}\rangle_s^{12} = \frac{1}{\sqrt{2}}(|RL\rangle \pm |LR\rangle), \tag{5}$$

where $|R\rangle$, $|L\rangle$ are orthogonal spatial states.

2.2 Protocol

Based on hyperentangled Bell states, the quantum sender Alice and the classical receiver Bob can produce secure keys. In this protocol, Alice has full quantum capabilities, with the potential to generate and measure the qubits with an arbitrary basis. Bob has classical capabilities, with the potential to only prepare and measure the qubits with Z basis. The proposed protocol comprises the following six steps.

Step 1: Alice generated $N = 4n$ hyperentangled Bell states, which are chosen from sets $\{|\phi^{\pm}\rangle_p^{12} \otimes |\phi^{\pm}\rangle_s^{12}, |\psi^{\pm}\rangle_p^{12} \otimes |\phi^{\pm}\rangle_s^{12}, |\psi^{\pm}\rangle_p^{12} \otimes |\psi^{\pm}\rangle_s^{12}, |\phi^{\pm}\rangle_p^{12} \otimes |\psi^{\pm}\rangle_s^{12}\}$, where 1, 2 represent the two particles of each state. Alice implemented particle 1 to compose the sequence $A = \{A_1, A_2, \ldots, A_N\}$ and particle 2 to compose the sequence $B = \{B_1, B_2, \ldots, B_N\}$. Then, she held the A sequence in her hands and transmitted the B sequence to Bob.

Step 2: When Bob received the qubits, he randomly performed two operations. CTRL operation: reflecting the qubits to Alice with no disturbance and SIFT operation: measuring the qubits with base $Z_P \otimes Z_S$ and resending the same states to Alice.

Step 3: When the qubits arrived, Alice notified Bob that she has received them. Bob announced the operations of qubits, which he performed.

Step 4: Alice and Bob conducted eavesdropping detection. For CTRL particles, Alice combined particle 2 with the corresponding particle 1 and recorded hyperentangled Bell state measurements. The measurement results should be the same as what Alice sent. If the error rate exceeds the threshold value, Alice and Bob will terminate this protocol. Otherwise, they will move on to the next step.

Step 5: For SIFT particles, Alice carried out $Z_P \otimes Z_S$ base measurement on particle 1. Alice randomly selected n measurement results from particle 1, in which Bob chose SIFT operation. Alice and Bob checked the error rate, and Alice's measurements should be equal to Bob's measurements. If the error rate is higher than the threshold value, the protocol will be discarded. Otherwise, they will proceed with the next step.

Step 6: Alice and Bob performed error correcting code (ECC) and privacy amplification (PA) for the remaining n measurement results, in which Bob chose SIFT operation to obtain the final keys.

Table 1 gives a description of Alice's and Bob's operations when Alice transmitted $|\phi^+\rangle_p^2 \otimes |\phi^+\rangle_s^2$ to Bob.

3 Security analysis and comparison

A malicious eavesdropper, Eve, attempted to obtain the significant keys between Alice and Bob in this communication. Eve may attack keys by the measure–resend attack, intercept–resend attack, and entangle–resend attack.

3.1 Measure–resend attack

When Alice transmitted qubits to Bob *via* the quantum channel, Eve measured qubits from Alice and sent the measured qubits to Bob. Eve is eager to obtain the significant operations, which is chosen by Bob. Unfortunately, no matter what measures Eve took, errors will be introduced. When Alice and Bob conduct eavesdropping detection, Eve will be found.

Without loss of generality, Alice prepared the hyperentangled Bell states $|\phi^+\rangle_p^{12} \otimes |\phi^+\rangle_s^{12}$ and sent the particle 2 sequence to Bob. The security analysis of hyperentangled Bell states $|\phi^-\rangle_p^{12} \otimes |\phi^-\rangle_s^{12}$, $|\psi^{\pm}\rangle_p^{12} \otimes |\phi^{\pm}\rangle_s^{12}$, $|\psi^{\pm}\rangle_p^{12} \otimes |\psi^{\pm}\rangle_s^{12}$ and $|\phi^{\pm}\rangle_p^{12} \otimes |\psi^{\pm}\rangle_s^{12}\}$ are similar to $|\phi^+\rangle_p^{12} \otimes |\phi^+\rangle_s^{12}$.

Eve intercepted the particles and recorded base $Z_P \otimes Z_S$ measurement on $|\phi^+\rangle_p^2 \otimes |\phi^+\rangle_s^2$. The qubit is collapsed to $|0\rangle \otimes |0\rangle$, $|0\rangle \otimes |1\rangle$, $|1\rangle \otimes |0\rangle$, or $|1\rangle \otimes |1\rangle$, each with 25% probability. After measurement, we suppose that Eve transmitted the states $|0\rangle \otimes |0\rangle$ to Bob (if Eve's measurement results are the rest of three results, the analysis is similar to the mentioned analysis). When Bob received the qubits, he chose CTRL operation or SIFT operation at random. If Bob chose CTRL operation, Alice performed hyperentangled Bell state measurement on the reflected qubit and the remaining qubit. Because Eve destroyed particle 2 from the hyperentangled Bell states, particle 2 has been changed, which is differently sent by Alice. The hyperentangled Bell states are collapsed to $|\phi^+\rangle_p^{12} \otimes |\phi^+\rangle_s^{12}$, $|\phi^-\rangle_p^{12} \otimes |\phi^+\rangle_s^{12}$, $|\phi^+\rangle_p^{12} \otimes |\phi^-\rangle_s^{12}$ and $|\phi^-\rangle_p^{12} \otimes |\phi^-\rangle_s^{12}$, each with 25% probability. Alice can gain the initial measurement results $|\phi^+\rangle_p^{12} \otimes |\phi^+\rangle_s^{12}$ with 1/4 probability. Therefore, Eve will be detected with the probability of 75% by the security check of Step 4. If Bob chose CTRL operation, there is no error introduced in this case. So Eve will not be detected.

Therefore, the proposed protocol can resist the measure–resend attack.

TABLE 1 One example description of Alice's and Bob's operations.

Alice's transmission	Bob's operation	Returned result	Usage
$\lvert\phi^+\rangle_p^2 \otimes\lvert\phi^+\rangle_s^2$	CTRL	$\lvert\phi^+\rangle_p^2 \otimes\lvert\phi^+\rangle_s^2$	Eavesdropping detection
$\lvert\phi^+\rangle_p^2 \otimes\lvert\phi^+\rangle_s^2$	SIFT	$\lvert 0\rangle_p^2 \otimes\lvert 0\rangle_s^2$	Eavesdropping detection/obtaining the raw keys
$\lvert\phi^+\rangle_p^2 \otimes\lvert\phi^+\rangle_s^2$	SIFT	$\lvert 0\rangle_p^2 \otimes\lvert 1\rangle_s^2$	Eavesdropping detection/obtaining the raw keys
$\lvert\phi^+\rangle_p^2 \otimes\lvert\phi^+\rangle_s^2$	SIFT	$\lvert 1\rangle_p^2 \otimes\lvert 0\rangle_s^2$	Eavesdropping detection/obtaining the raw keys
$\lvert\phi^+\rangle_p^2 \otimes\lvert\phi^+\rangle_s^2$	SIFT	$\lvert 1\rangle_p^2 \otimes\lvert 1\rangle_s^2$	Eavesdropping detection/obtaining the raw keys

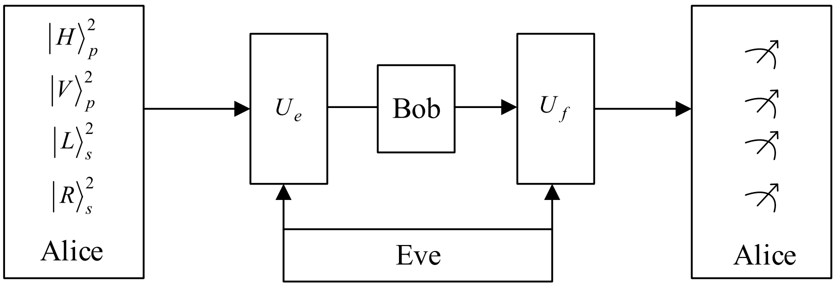


FIGURE 1
Entangle–measure attacks with two operations U_e and U_f.

3.2 Intercept–resend attack

When Alice transmitted qubits to Bob *via* the quantum channel, Eve intercepted qubits from Alice and resent faked qubits, which were generated by Eve to Bob. Eve wanted to figure out which operation Bob had chosen. Unfortunately, irrespective of the measures taken by Eve, errors will be introduced. When Alice and Bob conduct eavesdropping detection, Eve will be found.

Without loss of generality, Alice prepares the hyperentangled Bell states $|\phi^+\rangle_p^{12} \otimes|\phi^+\rangle_s^{12}$ and sends the particle 2 sequence to Bob. The security analysis of hyperentangled Bell states $|\psi^-\rangle_p^{12} \otimes|\phi^-\rangle_s^{12}$, $|\psi^\pm\rangle_p^{12} \otimes|\psi^\pm\rangle_s^{12}$ and $|\phi^\pm\rangle_p^{12} \otimes|\psi^\pm\rangle_s^{12}\}$ are similar to $|\phi^+\rangle_p^{12} \otimes|\phi^+\rangle_s^{12}$.

Eve intercepted the particles and generated hyperentangled Bell states $|\phi^-\rangle_p^{12} \otimes|\phi^-\rangle_s^{12}$ (if Eve generated the remaining three hyperentangled Bell states, the analysis is similar to the mentioned analysis). Eve transmitted particle 2 to Bob because Eve reflected the qubits directly from Alice, and if Bob selected CTRL operation, there is no error introduced in this case. If Bob selects SIFT operation, the received qubits will be measured with base $Z_P \otimes Z_S$, and the qubits will collapse to $|0\rangle \otimes|0\rangle$, $|0\rangle \otimes|1\rangle$, $|1\rangle \otimes|0\rangle$, and $|1\rangle \otimes|1\rangle$, each with 25% probability. When Alice received qubits, the received qubits with base $Z_P \otimes Z_S$ will be measured with ease, and the qubits will collapse to $|0\rangle \otimes|0\rangle$, $|0\rangle \otimes|1\rangle$, $|1\rangle \otimes|0\rangle$, and $|1\rangle \otimes|1\rangle$, each with 25% probability. Alice and Bob obtain the same measurement results with 1/4 probability. Therefore, Eve can be detected with the probability of 75% by the security check of Step 5.

Therefore, the proposed protocol can resist the intercept–resend attack.

3.3 Entangle–measure attack

When Alice transmitted qubits to Bob *via* the quantum channel, Eve entangled the ancillary qubits to the transmitted qubits from Alice. When the qubits were transmitted back to Alice, Eve measured the transmitted qubits to obtain Bob's measurement results. The implementation of the entangle–measure attack is shown in Figure 1. Unfortunately, irrespective of the measures taken by Eve, errors will be introduced. When Alice and Bob conduct eavesdropping detection, Eve will be found.

Without loss of generality, it is assumed that Alice sent $|\phi^+\rangle_p^2 \otimes|\phi^+\rangle_s^2$ to Bob and Eve performed unitary operation U_e to entangle the ancillary qubit $|e\rangle$ with the target qubits and sent to Bob. When the qubits returned to Alice, Eve measured the ancillary qubit $|e\rangle$ to get the information. For the target qubits $|\phi^+\rangle_p^2 \otimes|\phi^+\rangle_s^2$, which are sent by Alice, after U_e, the states become as follows:

$$U_e\left(|H\rangle_p^2 \otimes |R\rangle_s^2\right)|e\rangle = \left(|H\rangle_p^2|e_{hh}\rangle + |V\rangle_p^2|e_{hv}\rangle\right) \otimes \left(|R\rangle_s^2|e_{rr}\rangle + |L\rangle_s^2|e_{rl}\rangle\right), \tag{6}$$

TABLE 2 Comparison.

Protocol	Quantum resource	Communication capacity	Information carried	Qubit efficiency
[24]	Single photon	1	1	8.3%
[26]	Bell states	1	2	16.6%
[29]	GHZ states	1	3	7.1%
[33]	Single photon	2	2	22.2%
Proposed protocol	Hyperentangled Bell states	2	4	16.6%

$$U_e\left(|H\rangle_p^2 \otimes |L\rangle_s^2\right)|e\rangle = \left(|H\rangle_p^2|e_{hh}\rangle + |V\rangle_p^2|e_{hv}\rangle\right) \otimes \left(|R\rangle_s^2|e_{lr}\rangle + |L\rangle_s^2|e_{ll}\rangle\right), \tag{7}$$

$$U_e\left(|V\rangle_p^2 \otimes |R\rangle_s^2\right)|e\rangle = \left(|H\rangle_p^2|e_{vh}\rangle + |V\rangle_p^2|e_{vv}\rangle\right) \otimes \left(|R\rangle_s^2|e_{rr}\rangle + |L\rangle_s^2|e_{rl}\rangle\right), \tag{8}$$

$$U_e\left(|V\rangle_p^2 \otimes |L\rangle_s^2\right)|e\rangle = \left(|H\rangle_p^2|e_{vh}\rangle + |V\rangle_p^2|e_{vv}\rangle\right) \otimes \left(|R\rangle_s^2|e_{lr}\rangle + |L\rangle_s^2|e_{ll}\rangle\right), \tag{9}$$

where $|e_{hh}\rangle$, $|e_{hv}\rangle$, $|e_{vh}\rangle$, $|e_{vv}\rangle$, $|e_{rr}\rangle$, $|e_{rl}\rangle$, $|e_{lr}\rangle$, and $|e_{ll}\rangle$ are the pure ancillary states, which are controlled by the operation U_e.

Eve expected to pass the eavesdropping detection, where the operation U_e does not introduce errors. According to Eqs. 6–9, it can be inferred that

$$|e_{hv}\rangle = |e_{rl}\rangle = |e_{lr}\rangle = |e_{vh}\rangle = 0. \tag{10}$$

Then, Eve sent the qubits to Bob. Bob selected CTRL operation or SIFT operation on the qubits when he received them, and Bob returned the qubits to Alice. Eve carried out unitary operation U_f on the qubits which Bob transmitted back to Alice.

Case 1: Bob performed SIFT operation and returned the qubits to Alice. Eve performed U_f on the states sent back to Alice.

$$U_f\left(|H\rangle_p^2|e_{hh}\rangle \otimes |R\rangle_s^2|e_{rr}\rangle\right) = |H\rangle_p^2|f_{hh}\rangle \otimes |R\rangle_s^2|f_{rr}\rangle, \tag{11}$$

$$U_f\left(|H\rangle_p^2\middle|e_{hh}\rangle \otimes \left(|L\rangle_s^2|e_{ll}\rangle\right) = |H\rangle_p^2|f_{hh}\rangle \otimes |L\rangle_s^2|f_{ll}\rangle, \tag{12}$$

$$U_f\left(|V\rangle_p^2|e_{vv}\rangle \otimes |R\rangle_s^2|e_{rr}\rangle\right) = |V\rangle_p^2|f_{vv}\rangle \otimes |R\rangle_s^2|f_{rr}\rangle, \tag{13}$$

$$U_f\left(|V\rangle_p^2|e_{vv}\rangle \otimes |L\rangle_s^2|e_{ll}\rangle\right) = |V\rangle_p^2|f_{vv}\rangle \otimes |L\rangle_s^2|f_{ll}\rangle. \tag{14}$$

Case 2: Bob performed CTRL operation and did nothing on the qubits. Therefore, after entangling the ancillary particle on the hyperentangled Bell states, the states become as follows:

$$\begin{aligned}
&U_f\left(|\phi^+\rangle_p^{12} \otimes |\phi^+\rangle_s^{12}\right)\\
&= \frac{1}{\sqrt{2}}\left(\left(|H^1\rangle\left(|H^2\rangle|f_{hh}\rangle + |V^2\rangle|f_{hv}\rangle\right) + |V^1\rangle\left(|H^2\rangle|f_{vh}\rangle + |V^2\rangle|f_{vv}\rangle\right)\right)\right.\\
&\quad \left.\otimes \left(|R^1\rangle\left(|R^2\rangle|f_{rr}\rangle + |L^2\rangle|f_{rl}\rangle\right) + |L^1\rangle\left(|R^2\rangle|f_{lr}\rangle + |L^2\rangle|f_{ll}\rangle\right)\right)\right)\\
&= \frac{1}{\sqrt{2}}\left(\left(|H^1H^2\rangle|f_{hh}\rangle + |H^1V^2\rangle|f_{hv}\rangle + |V^1H^2\rangle|f_{vh}\rangle + |V^1V^2\rangle|f_{vv}\rangle\right)\right.\\
&\quad \left.\otimes \left(|R^1R^2\rangle|f_{rr}\rangle + |R^1L^2\rangle|f_{rl}\rangle + |L^1R^2\rangle|f_{lr}\rangle + |L^1L^2\rangle|f_{ll}\rangle\right)\right)\\
&= \frac{1}{2}\left(\left(\left(|\phi^+\rangle_p^{12} + |\phi^-\rangle_p^{12}\right)|f_{hh}\rangle + \left(|\psi^+\rangle_p^{12} + |\psi^-\rangle_p^{12}\right)|f_{hv}\rangle\right.\right.\\
&\quad \left.+\left(|\psi^+\rangle_p^{12} - |\psi^-\rangle_p^{12}\right)|f_{vh}\rangle + \left(|\phi^+\rangle_p^{12} - |\phi^-\rangle_p^{12}\right)|f_{vv}\rangle\right)\\
&\quad \otimes \left(\left(|\phi^+\rangle_s^{12} + |\phi^-\rangle_s^{12}\right)|f_{rr}\rangle + \left(|\psi^+\rangle_s^{12} + |\psi^-\rangle_s^{12}\right)|f_{rl}\rangle\right.\\
&\quad \left.\left.+\left(|\psi^+\rangle_s^{12} - |\psi^-\rangle_s^{12}\right)|f_{lr}\rangle + \left(|\phi^+\rangle_s^{12} - |\phi^-\rangle_s^{12}\right)|f_{ll}\rangle\right)\right)\\
&= \frac{1}{2}\left(|\phi^+\rangle_p^{12}|f_{hh}\rangle + |\phi^-\rangle_p^{12}|f_{hh}\rangle + \left(|\psi^+\rangle_p^{12} + |\psi^-\rangle_p^{12}\right)|f_{hv}\rangle\right.\\
&\quad \left.+\left(|\psi^+\rangle_p^{12} - |\psi^-\rangle_p^{12}\right)|f_{vh}\rangle + |\phi^+\rangle_p^{12}|f_{vv}\rangle - |\phi^-\rangle_p^{12}|f_{vv}\rangle\right)\\
&\quad \otimes \left(|\phi^+\rangle_s^{12}|f_{rr}\rangle + |\phi^-\rangle_s^{12}|f_{rr}\rangle + \left(|\psi^+\rangle_s^{12} + |\psi^-\rangle_s^{12}\right)|f_{rl}\rangle\right.\\
&\quad \left.+\left(|\psi^+\rangle_s^{12} - |\psi^-\rangle_s^{12}\right)|f_{lr}\rangle + |\phi^+\rangle_s^{12}|f_{ll}\rangle - |\phi^-\rangle_s^{12}|f_{ll}\rangle\right)\\
&= \frac{1}{2}\left(|\phi^+\rangle_p^{12}\left(|f_{hh}\rangle + |f_{vv}\rangle\right) + |\phi^-\rangle_p^{12}\left(|f_{hh}\rangle - |f_{vv}\rangle\right) + \left(|\psi^+\rangle_p^{12} + |\psi^-\rangle_p^{12}\right)|f_{hv}\rangle\right.\\
&\quad \left.+\left(|\psi^+\rangle_p^{12} - |\psi^-\rangle_p^{12}\right)|f_{vh}\rangle\right)\\
&\quad \otimes \left(|\phi^+\rangle_s^{12}\left(|f_{rr}\rangle + |f_{ll}\rangle\right) + |\phi^-\rangle_s^{12}\left(|f_{rr}\rangle - |f_{ll}\rangle\right) + \left(|\psi^+\rangle_s^{12} + |\psi^-\rangle_s^{12}\right)|f_{rl}\rangle\right.\\
&\quad \left.+\left(|\psi^+\rangle_s^{12} - |\psi^-\rangle_s^{12}\right)|f_{lr}\rangle\right).
\end{aligned} \tag{15}$$

Eve expected to pass the eavesdropping detection, so U_f should not change the states which were sent by Alice. Therefore, from Eq. 15, it can be inferred that

$$|f_{hh}\rangle - |f_{vv}\rangle = 0, \tag{16}$$

$$|f_{rr}\rangle - |f_{ll}\rangle = 0, \tag{17}$$

$$|f_{hv}\rangle = |f_{vh}\rangle = |f_{rl}\rangle = |f_{lr}\rangle = 0. \tag{18}$$

According to Eqs. 16–18, Eqs. 11–14 can be rewritten as follows:

$$U_f\left(|H\rangle_p^2|e_{hh}\rangle \otimes |R\rangle_s^2|e_{rr}\rangle\right) = |H\rangle_p^2|f_{hh}\rangle \otimes |R\rangle_s^2|f_{rr}\rangle, \tag{19}$$

$$\begin{aligned} U_f\left(|H\rangle_p^2|e_{hh}\rangle \otimes |L\rangle_s^2|e_{ll}\rangle\right) &= |H\rangle_p^2|f_{hh}\rangle \otimes |L\rangle_s^2|f_{ll}\rangle \\ &= |H\rangle_p^2|f_{hh}\rangle \otimes |L\rangle_s^2|f_{rr}\rangle, \end{aligned} \tag{20}$$

$$\begin{aligned} U_f\left(|V\rangle_p^2|e_{vv}\rangle \otimes |R\rangle_s^2|e_{rr}\rangle\right) &= |V\rangle_p^2|f_{vv}\rangle \otimes |R\rangle_s^2|f_{rr}\rangle \\ &= |V\rangle_p^2|f_{hh}\rangle \otimes |R\rangle_s^2|f_{rr}\rangle, \end{aligned} \tag{21}$$

$$\begin{aligned} U_f\left(|V\rangle_p^2|e_{vv}\rangle \otimes |L\rangle_s^2|e_{ll}\rangle\right) &= |V\rangle_p^2|f_{vv}\rangle \otimes |L\rangle_s^2|f_{ll}\rangle \\ &= |V\rangle_p^2|f_{hh}\rangle \otimes |L\rangle_s^2|f_{rr}\rangle. \end{aligned} \tag{22}$$

According to the aforementioned equations, Eve's probes are dependent on the corresponding states. Once Eve acquired the information, the eavesdropping behavior will introduce the error and be detected. So, Eve cannot acquire any valuable information.

For security analysis of qubits $|\psi^-\rangle_p^{12} \otimes |\phi^-\rangle_s^{12}$, $|\psi^\pm\rangle_p^{12} \otimes |\psi^\pm\rangle_s^{12}$, $|\psi^\pm\rangle_p^{12} \otimes |\phi^\pm\rangle_s^{12}$, and $|\phi^\pm\rangle_p^{12} \otimes |\psi^\pm\rangle_s^{12}$ are similar to $|\phi^+\rangle_p^{12} \otimes |\phi^+\rangle_s^{12}$.

Consequently, the proposed protocol can resist the entangle–measure attack.

3.4 Comparison

The efficiency of key distribution can be improved by using the properties of hyperentangled Bell states. For example, Bell states can transmit two bits of classical information each time, while hyperentangled Bell states can transmit four bits of classical information each time, twice as much as Bell states. Specifically, the proposed protocols transmitted two bits in each interaction, and the previous SQKD based on the Bell state can only transmit one bit.

The efficiency qubit can use equation $\eta = c/(q + b)$ for calculation, where c represents the compared classical participants, q represents particles generated by the quantum participant, and b represents particles generated by the classical participant. In Boyer et al. [24], the quantum resource is single photon; Alice prepared eight particles, and Bob measured and prepared four particles. Hence, $\eta = c/(q + b) = 1/(8 + 4) = 1/12$. Wang et al. [26] used the Bell states to describe an SQPC protocol, wherein Alice generated four particles and Bob measured and prepared two particles. Therefore, $\eta = c/(q + b) = 1/(4 + 2) = 1/6$. Zhu et al. [29] employed GHZ states to construct an SQPC protocol. Therefore, $\eta = c/(q + b) = 1/(12 + 2) = 1/14$. In Ye et al. [33], the single photon in two degrees of freedom is used to implement quantum key distribution. Alice prepared six particles, and Bob measured and prepared three particles. So, $\eta = c/(q + b) = 2/(6 + 3) = 2/9$. In the proposed protocol, SQKD is based on hyperentangled Bell states, Alice randomly prepared eight particles, and Bob measured and prepared four particles. Hence, $\eta = c/(q + b) = 2/(8 + 4) = 1/6$.

Table 2 shows the comparison between the proposed protocol and some protocols. It can be seen that this protocol and protocol [33] expand the degree of freedom of particles from a single degree of freedom to two degrees of freedom. This increases the communication capacity. The proposed protocol takes Bell states as an example to discuss the multiple degrees of freedom of the entangled state, which provides an indication for further research of various entangled states (GHZ states, cluster states, *etc.*).

4 Multi-party semi-quantum key distribution protocol

In this section, the previously proposed protocol is extended to a multi-party semi-quantum key distribution protocol (MPSQKD), which can realize that one quantum participant distributes keys among T ($T > 1$) classical participants.

Here, set U_1, U_2, . . . , U_T is referred as existing classical participants. In MPSQKD, only Alice has full quantum capability and can perform any quantum operation. Others are limited to measuring and preparing qubits with base $Z_P \otimes Z_S$ and realize the key distribution with the help of Alice. The following steps are part of the MPSQKD protocol.

Step 1: Alice generated $2^{T+1}N$ hyperentangled Bell states in the set $\{|\phi^{\pm}\rangle_p^{12} \otimes |\phi^{\pm}\rangle_s^{12}, |\psi^{\pm}\rangle_p^{12} \otimes |\phi^{\pm}\rangle_s^{12}, |\psi^{\pm}\rangle_p^{12} \otimes |\psi^{\pm}\rangle_s^{12}, |\phi^{\pm}\rangle_p^{12} \otimes |\psi^{\pm}\rangle_s^{12}\}$. Subsequently, Alice transmitted particle 2 of each hyperentangled Bell state to the first user U_1.

Step 2: T classical participants are sorted in the order of U_1, U_2, . . . , U_T. The former classical participant randomly selected measurement or reflection operation and then back to the latter participant. The last participant randomly selected a measurement or reflection operation back to Alice.

Step 3: After Alice received all the qubits, U_1, U_2, . . . , U_T published their specific choices.

Step 4: According to the operation of their choices, Alice will take a different operation.

Case 1: When all classical participants chose SIFT operation, the measurement results of U_1, U_2, . . . , U_T will be raw keys.

Case 2: When all classical participants chose CTRL operation, Alice will check whether an eavesdropper arises. The results announced by Alice should be the same as prepared. Once the error rate is higher than the threshold, the protocol will be terminal.

Case 3: the classical participants discarded the qubits whose operations performed differently.

Step 5: T classical participants recorded some measurement results to check the eavesdropper of Case 1.

Step 6: U_1, U_2, . . . , U_T will own the final keys after promulgating the error correcting code (ECC) and privacy amplification (PA) data.

5 Conclusion

In this study, a novel semi-quantum key distribution protocol based on the hyperentangled Bell states is proposed. Alice has quantum capability and transmitted the hyperentangled Bell states to the classical participant Bob. Bob randomly performed two operations on the received qubits. Communication participants used the hyperentangled Bell states to realize the secure transmission. The security analysis proves that this scheme can effectively resist the measure–resend attack, intercept–resend attack, and entangle–measure attack. Hence, the proposed protocol is secure. The hyperentangled states dramatically improves the efficiency of key transmission, which effectively improves the efficiency and feasibility of the protocol. Moreover, a multi-party scenario protocol based on the hyperentangled Bell stats is presented, realizing key distribution for multiple classical participants. The proposed protocol is the first SQKD protocol based on multi-degree of freedom entangled states, which has a certain guiding role for future research.

Data availability statement

The original contributions presented in the study are included in the article/Supplementary Material; further inquiries can be directed to the corresponding author.

Author contributions

YT is responsible for proposing innovative points, designing protocol steps, analyzing and designing, and writing paper. JL is responsible for the overall structure and content design of the paper. CY is responsible for paper preparation, protocol correctness and security analysis. CL is responsible for the polishing and proofreading of paper.

Funding

This work is supported by the Open Fund of Advanced Cryptography and System Security Key Laboratory of Sichuan Province No. SKLACSS-202108, the National Natural Science Foundation of China under Grant Nos. 92046001 and 61962009, the Fundamental Research Funds for the Central Universities under Grant 2019XD-A02, and the Open Research Project of the State Key Laboratory of Media Convergence and Communication under Grant KLMCC2020KF006.

Acknowledgments

We would like to thank the anonymous reviewers for their detailed reviews and valuable comments, which have enhanced the quality of this manuscript.

Conflict of interest

The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Publisher's note

All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors, and the reviewers. Any product that may be evaluated in this article, or claim that may be made by its manufacturer, is not guaranteed or endorsed by the publisher.

References

1. Xia ZH, Jiang LQ, Liu DD, Li LH, Jeon B. Boew: A content-based image retrieval scheme using bag-of-encrypted-words in cloud computing. *IEEE Trans Comput* (2019)(1) 1.

2. Xia ZH, Wang L, Tang J, Xiong N, Weng J. A privacy-preserving image retrieval scheme using secure local binary pattern in cloud computing. *IEEE Trans Netw Sci Eng* (2020) 8(1):318–30. doi:10.1109/tnse.2020.3038218

3. Xia ZH, Zhou WH, Xiong LZ, Weng J, Xiong NX. Str: Secure computation on additive shares using the share-transform-reveal strategy. *IEEE Trans Comput* (2021) 1. doi:10.1109/tc.2021.3073171

4. Aumasson JP. The impact of quantum computing on cryptography. *Computer Fraud Security* (2017) 2017(6):8–11. doi:10.1016/s1361-3723(17)30051-9

5. Diffie W, Hellman M. New directions in cryptography. *IEEE Trans Inf Theor* (1976) 22(6):644–54. doi:10.1109/tit.1976.1055638

6. Pan XB, Chen XB, Xu G, Ahmad H, Yang YX, Li ZP, et al. Controlled quantum network coding without loss of information. *Comput Mater Continua* (2021) 69(3): 3967–79. doi:10.32604/cmc.2021.017087

7. Guo GP, Li CF, Shi BS, Li J, Guo GC. Quantum key distribution scheme with orthogonal product states. *Phys Rev A (Coll Park)* (2001) 64(4):042301. doi:10.1103/physreva.64.042301

8. Kronberg DA, Nikolaeva AS, Kurochkin YV, Fedorov AK. Quantum soft filtering for the improved security analysis of the coherent one-way quantum-key-distribution protocol. *Phys Rev A (Coll Park)* (2020) 101(3):032334. doi:10.1103/physreva.101.032334

9. Deng FG, Long GL, Liu XS. Two-step quantum direct communication protocol using the Einstein-Podolsky-Rosen pair block. *Phys Rev A (Coll Park)* (2003) 68(4): 042317–114. doi:10.1103/physreva.68.042317

10. Sun Z, Song L, Huang Q, Yin L, Long G, Lu J, et al. Toward practical quantum secure direct communication: A quantum-memory-free protocol and code design. *IEEE Trans Commun* (2020) 68(9):5778–92. doi:10.1109/tcomm.2020.3006201

11. Hillery M, Nek V., Berthiaume A. Quantum secret sharing. *Phys Rev A (Coll Park)* (1999) 59(3):1829–34. doi:10.1103/physreva.59.1829

12. Yang CW, Tsai CW. Efficient and secure dynamic quantum secret sharing protocol based on Bell states. *Quan Inf Process* (2020) 19(5):162–14. doi:10.1007/s11128-020-02662-0

13. Yang YG, Wen QY. An efficient two-party quantum private comparison protocol with decoy photons and two-photon entanglement. *J Phys A: Math Theor* (2009) 42(5):055305. doi:10.1088/1751-8113/42/5/055305

14. Lang YF. Quantum private comparison using single Bell state. *Int J Theor Phys (Dordr)* (2021) 60:4030–6. doi:10.1007/s10773-021-04937-3

15. Bennett CH, Brassard G. Quantum cryptography: Public key distribution and coin tossing. In: *Proceedings of the IEEE international conference on computers, systems and signal processing*. Bangalore (1984). p. 175–9.

16. EkertArtur K. Quantum cryptography based on Bell's theorem. *Phys Rev Lett* (1991) 67(6):661–3. doi:10.1103/physrevlett.67.661

17. Bennett CH. Quantum cryptography using any two nonorthogonal states. *Phys Rev Lett* (1992) 68:3121–4. doi:10.1103/physrevlett.68.3121

18. Scarani V, Acin A, Ribordy G, Gisin N. Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulses implementations. *Phys Rev Lett* (2004) 92(5):057901.1–057901.4.

19. Yan X, Zhou N, Gong L, Wang Y, Wen X. High-dimensional quantum key distribution based on qudits transmission with quantum Fourier transform. *Quan Inf Process* (2019) 18(9):271–14. doi:10.1007/s11128-019-2368-5

20. Srikara S, Thapliyal K, Pathak A. Continuous variable B92 quantum key distribution protocol using single photon added and subtracted coherent states. *Quan Inf Process* (2020) 19(10):371–16. doi:10.1007/s11128-020-02872-6

21. Wu X, Wang Y, Huang D, Guo Y. Multi-mode plug-and-play dual-phase-modulated continuous-variable quantum key distribution. *Quan Inf Process* (2021) 20(4):143–21. doi:10.1007/s11128-021-03076-2

22. Li CY, Ye CQ, Tian Y, Chen XB, Li J. Cluster-state-based quantum secret sharing for users with different abilities. *Quan Inf Process* (2021) 20(12):385–14. doi:10.1007/s11128-021-03327-2

23. Bennett CH, Wiesner SJ. Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states. *Phys Rev Lett* (1992) 69(20):2881–4. doi:10.1103/physrevlett.69.2881

24. Boyer M, Kenigsberg D, Mor T. Quantum key distribution with classical Bob. *Phys Rev Lett* (2007) 99(14):140501. doi:10.1103/physrevlett.99.140501

25. Zou X, Qiu D, Li L, Wu L, Li L. Semi-quantum key distribution using less than four quantum states. *Phys Rev A (Coll Park)* (2009) 79(5):052312–1747. doi:10.1103/physreva.79.052312

26. Wang J, Zhang S, Zhang Q, Tang CJ. Semi-quantum key distribution using entangled states. *Chin Phys Lett* (2011) 28(10):100301. doi:10.1088/0256-307x/28/10/100301

27. Zou X, Qiu D, Zhang S, Mateus P. Semi-quantum key distribution without invoking the classical party's measurement capability. *Quan Inf Process* (2015) 14(8):2981–96. doi:10.1007/s11128-015-1015-z

28. Krawec WO, Geiss EP. Limited resource semi-quantum key distribution. arXiv preprint arXiv:1710.05076 (2017).

29. Zhu KN, Zhou NR, Wang YQ, Wen XJ. Semi-quantum key distribution protocols with GHZ states. *Int J Theor Phys (Dordr)* (2018) 57(12):3621–31. doi:10.1007/s10773-018-3875-3

30. Iqbal H, Krawec WO. Semi-quantum cryptography. *Quan Inf Process* (2020) 19(3):97–52. doi:10.1007/s11128-020-2595-9

31. Ye TY, Li HK, Hu JL. Semi-quantum key distribution with single photons in both polarization and spatial-mode degrees of freedom. *Int J Theor Phys (Dordr)* (2020) 59(9):2807–15. doi:10.1007/s10773-020-04540-y

32. Tian Y, Li J, Yuan KG, Li CY, Li HJ, Chen XB. An efficient semi-quantum key distribution protocol based on EPR and single-particle hybridization. *Quan Inf Comput* (2021) 21(7-8):563–76. doi:10.26421/qic21.7-8-3

33. Ye TY, Geng MJ, Xu TJ, Chen Y. Efficient semiquantum key distribution based on single photons in both polarization and spatial-mode degrees of freedom. *Quan Inf Process* (2022) 21(4):123–1. doi:10.1007/s11128-022-03457-1

34. Tsai CW, Chang YC, Lai YH, Yang CW. Cryptanalysis of limited resource semi-quantum secret sharing. *Quan Inf Process* (2020) 19(8):224–8. doi:10.1007/s11128-020-02690-w

35. Li XY, Chang Y, Zhang SB. Multi-party semi-quantum secret sharing scheme based on Bell states. In: *International conference on artificial intelligence and security*. Cham: Springer (2020). p. 280–8.

36. Tian Y, Li J, Chen XB, Ye CQ, Li HJ. An efficient semi-quantum secret sharing protocol of specific bits. *Quan Inf Process* (2021) 20(6):217–1. doi:10.1007/s11128-021-03157-2

37. Wang Y, Lou X, Fan Z, Wang S, Huang G. Verifiable multi-dimensional (t, n) threshold quantum secret sharing based on quantum walk. *Int J Theor Phys (Dordr)* (2022) 61(2):24–17. doi:10.1007/s10773-022-05009-w

38. Ye TY, Ye CQ. Measure-resend semi-quantum private comparison without entanglement. *Int J Theor Phys (Dordr)* (2018) 57(12):3819–34. doi:10.1007/s10773-018-3894-0

39. Jiang LZ. Semi-quantum private comparison based on Bell states. *Quan Inf Process* (2020) 19(6):180–21. doi:10.1007/s11128-020-02674-w

40. Tian Y, Li J, Chen XB, Ye CQ, Li CY, Hou YY. An efficient semi-quantum private comparison without pre-shared keys. *Quan Inf Process* (2021) 20(11): 360–13. doi:10.1007/s11128-021-03294-8

41. Ye CQ, Li J, Chen XB, Tian Y. Efficient semi-quantum private comparison without using entanglement resource and pre-shared key. *Quan Inf Process* (2021) 20(8):1–19.

42. Yang YG, Wen QY, Zhu FC. Multi-party multi-level quantum key distribution protocol based on entanglement swapping. *Acta Phys Sin* (2005) 54(12):5544–8. doi:10.7498/aps.54.5544

frontiers | Frontiers in Physics

TYPE Original Research
PUBLISHED 18 October 2022
DOI 10.3389/fphy.2022.1028630

EDITED BY
Tianyu Ye,
Zhejiang Gongshang University, China

REVIEWED BY
Guodong Ye,
Guangdong Ocean University, China
Xingbin Liu,
Southwest University, China

*CORRESPONDENCE
Wei-Ping Zou,
zwp@ncu.edu.cn

SPECIALTY SECTION
This article was submitted to Quantum Engineering and Technology, a section of the journal Frontiers in Physics

RECEIVED 26 August 2022
ACCEPTED 23 September 2022
PUBLISHED 18 October 2022

CITATION
Ma Y, Yu F-F, Gong L-H and Zou W-P (2022), Fast quantum image encryption scheme based on multilayer short memory fractional order Lotka-Volterra system and dual-scale triangular map. *Front. Phys.* 10:1028630.
doi: 10.3389/fphy.2022.1028630

Fast quantum image encryption scheme based on multilayer short memory fractional order Lotka-Volterra system and dual-scale triangular map

Yan Ma[1], Fang-Fang Yu[2], Li-Hua Gong[2] and Wei-Ping Zou[1]*

[1]Department of Computer Science and Technology, Nanchang University, Nanchang, China,
[2]Department of Electronic Information Engineering, Nanchang University, Nanchang, China

The Caputo fractional order Lotka-Volterra system is time-consuming in practical applications, since its starting point is fixed. To tackle this problem, a short memory fractional order Lotka-Volterra system (SMFrLVS) is proposed, where the chaotic attractor of the short memory fractional order Lotka-Volterra system is achieved by the predictor-corrector method. Then, a multilayer fractional order Lotka-Volterra system with short memory (MSMFrLVS) is introduced, whose chaotic behaviors are explored *via* Poincare sections and frequency power spectra. A quantum image encryption algorithm is proposed by combining MSMFrLVS with quantum dual-scale triangular map. A quantum circuit of the dual-scale triangular map is designed with ADDER-MOD2^n. At the permutation stage, the plaintext image is transformed into quantum form with the generalized quantum image representation model. The resulting quantum image is divided into sub-blocks and scrambled by the quantum dual-scale triangular map. Subsequently, the intra and the inter permutation operations on bit-planes are realized by sorting pseudo-random sequence and by quantum Gray code, respectively. At the diffusion stage, the initial values of the MSMFrLVS are generated with a plaintext correlation mechanism. The ciphertext image can be acquired by carrying out three-level diffusion operations. It is demonstrated that the proposed quantum image encryption algorithm performs better than some typical image encryption algorithm in terms of security, robustness, computational complexity and encryption speed.

KEYWORDS

quantum image encryption, fractional order differential equation, Lotka-Volterra system, predictor-corrector method, quantum dual-scale triangular map

1 Introduction

Lots of efficient quantum image encryption algorithms have been developed [1–5]. Since chaotic systems have good dynamic characteristics, they are very suitable for quantum image encryption [6–8]. Dai et al. presented an image encryption and compression algorithm based on 4D hyper-chaotic Henon map [9]. Zhou et al.

designed a secure quantum image encryption algorithm based on 5D hyper-chaotic system [10]. Ye et al. explored a fast image encryption scheme based on public key cryptosystem, quantum logistic map and the substitution-permutation network [11]. Khan et al. proposed a fast quantum image encryption scheme based on affine transform and fractional order Lorenz-like chaotic dynamical system [12]. Signing et al. provided an image encryption algorithm by combining a chameleon chaotic system with dynamic DNA coding [13]. Wang et al. researched a color image encryption scheme by combining hyper-chaotic system with improved quantum revolving gate [14]. Li et al. proposed an image encryption scheme by combining quantum chaos with discrete fractional wavelet transform [15]. Wu et al. designed a quantum image encryption based on 2D logistic map and quantum Baker map [16]. Hu et al. presented an efficient quantum color image encryption scheme using a new 3D chaotic system [17]. Kamran et al. proposed a secure image encryption algorithm based on quantum walk and chaos [18].

There have been numerous proposals for quantum image encryption algorithms with image scrambling methods [19–21]. Hu et al. proposed a quantum image encryption algorithm based on Arnold transform and wavelet transform, where the wavelet coefficients are scrambled by the Arnold transform [22]. Liu et al. designed a quantum image encryption algorithm by combining general Arnold transform with substitution tables (S-box) scrambling [23]. Liu et al. developed a quantum block image encryption algorithm with quantum Arnold transform based on the superposition property of quantum states [24]. Zhou et al. suggested a multi-image encryption scheme based on quantum 3D Arnold transform [25]. However, these methods have some limitations and cannot be used to scramble the rectangle image. For any rectangle image, it should be expanded into the square image or divided into many square images before scrambling, which will add extra space and increase computational complexity.

A fast quantum image encryption scheme for a rectangle image based on the MSMFrLVS and quantum dual-scale triangular map is proposed. During the encryption process, the plaintext image is represented with the generalized quantum image representation (GQIR) model, the image sub-blocks are shuffled with quantum dual-scale triangular map. Subsequently, the bit-level permutation is performed by the random sequence generated by the MSMFrLVS and quantum Gray code, respectively. Then, the three-level diffusion operations among the pixel values, binary bits and pixel bits are implemented by the chaotic sequences originated by the MSMFrLVS. Simulation analyses show the proposed quantum image encryption algorithm has good encryption performance and can resist any key sensitivity attacks and any brute-force attacks.

The rest of this paper is organized as follows: The basic knowledge of the GQIR for images, the MSMFrLVS and the Gray code are introduced in Section 2. The quantum circuits of dual-scale triangular map are designed in Section 3. The proposed quantum image encryption scheme is shown in Section 4. Numerical simulation analyses are described in Section 5. Finally, a conclusion is given in Section 6.

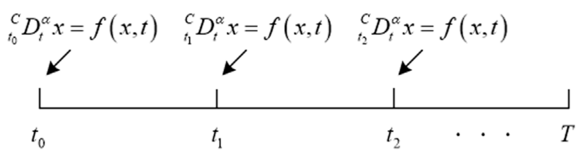

${}_{t_0}^{C}D_t^{\alpha}x = f(x,t)$
${}_{t_1}^{C}D_t^{\alpha}x = f(x,t)$
${}_{t_2}^{C}D_t^{\alpha}x = f(x,t)$
t_0
t_1
t_2
· · ·
T

FIGURE 1
Short memory fractional order system.

2 Preliminaries

2.1 Generalized quantum image representation

In Ref. [26], the generalized quantum image representation (GQIR) can store arbitrary integer numbers $H \times W$ quantum images with $\lceil \log_2 H \rceil + \lceil \log_2 W \rceil + q$ qubits, where q is the image color depth, $\lceil \log_2 H \rceil$ and $\lceil \log_2 W \rceil$ remarked as h and ω are the sizes of the Y-axis coordinate information and the X-axis coordinate information, respectively. Hence, an $H \times W$ quantum image $|I\rangle$ with GQIR can be expressed as

$$
\begin{aligned}
|I\rangle &= \frac{1}{(\sqrt{2})^{h+\omega}}\left(\sum_{Y=0}^{H-1}\sum_{X=0}^{W-1} \otimes_{i=0}^{q-1}|C_{YX}^{i}\rangle|YX\rangle\right)\\
|YX\rangle &= |y_0 y_1 \cdots y_{h-1}\rangle|x_0 x_1 \cdots x_{\omega-1}\rangle, y_i, x_i \in \{0,1\},\\
|C_{YX}\rangle &= |C_{YX}^{0} C_{YX}^{1} \cdots C_{YX}^{q-1}\rangle, C_{YX}^{i} \in \{0,1\}
\end{aligned}
\quad (1)
$$

where $|YX\rangle$ and $|C_{YX}\rangle$ are the location information and the color information, respectively.

2.2 Multilayer short memory fractional order Lotka-Volterra system

2.2.1 Short memory fractional order system

The α order Caputo fractional derivative of function $f(t)$ is defined as [27]

$$
{}_{t_0}^{C}D_t^{\alpha} f(t) = \frac{1}{\Gamma(1-\alpha)}\int_{t_0}^{t}\frac{f(s)}{(t-s)^{\alpha}}\mathrm{d}s, \quad 0<\alpha<1, \quad (2)
$$

where $\Gamma(\cdot)$ is the Gamma function. The standard Caputo fractional order system is illustrated as

$$ {}_{t_0}^{C}D_t^{\alpha} x(t) = f(t, x(t)), \quad x(t) = x_0, \tag{3}$$

where t_0 is the fixed starting point of the fractional order system.

The standard fractional order system Eq. 3 stores memory from $t = t_0$. Wu et al. proposed a short memory fractional order system which holds memory from $t\star = t_k$ and provides more freedom in the real-world applications [28], as shown in Figure 1. Let the interval $[t_0, T]$ be divided into m_1 subintervals of length $n_1 h_1$ such that $[t_0, T] = [t_0, t_1] \cup [t_1, t_2] \cup \cdots \cup [t_{m_1-1}, t_{m_1}]$, n_1 is an integer and $h_1 = (T - t_0)/N_1$. The short memory fractional order system is given as

$$\begin{cases} {}_{t_*}^{C}D_t^{\alpha} x(t) = f(x, t), & x(t_0) = x_0 \\ t_* = t_k, & t \in [t_k, t_{k+1}], k = 0, \ldots, m_1 - 1 \end{cases}. \tag{4}$$

2.2.2 Short memory fractional order Lotka-Volterra system

The fractional order Lotka-Volterra chaotic system is defined as [29].

$$\begin{array}{l} {}_{t_0}^{C}D_t^{\alpha_1} x = \gamma x + e x^2 - \varpi x y - \lambda z x^2 \\ {}_{t_0}^{C}D_t^{\alpha_2} y = -\mu y + \tau x y \\ {}_{t_0}^{C}D_t^{\alpha_3} z = -\xi z + \sigma z x^2 \end{array}, \tag{5}$$

where $\alpha_i\,(i = 1, 2, 3)$ represents the fractional order of the system Eq. 5, γ denotes the intrapopulation natural growth rate of the prey, ϖ denotes the effect of the predator on the prey, μ is the intrapopulation natural growth rate of the predator, τ is the positive effect of the prey on the predator, the parameters $\gamma, \varpi, \mu, \tau$, and the constants e, ξ, σ are positive.

We define the SMFrLVS as

$$\begin{array}{l} {}_{t_*}^{C}D_t^{\alpha_1} x = \gamma x + e x^2 - \varpi x y - \lambda z x^2 \\ {}_{t_*}^{C}D_t^{\alpha_2} y = -\mu y + \tau x y \\ {}_{t_*}^{C}D_t^{\alpha_3} z = -\xi z + \sigma z x^2 \end{array}. \tag{6}$$

In Eq. 6, the starting point of the SMFrLVS is the variable point $t\star$ rather than a fixed point t_0 such that the SMFrLVS improves the speed of the numerical computation.

2.2.3 Predictor-corrector method for the SMFrLVS

The predictor-corrector method is one of the most widely methods used in the chaotic analysis of the fractional order system, which explains the approximate solution of the nonlinear fractional order differential equations. The SMFrLVS is solved by the predictor-corrector method as follows.

For the interval $[t_0, t_1]$, the predicted values are given as

$$\begin{array}{l} x_1^p = x_0 + \dfrac{h_1^{\alpha_1}}{\alpha_1 \Gamma(\alpha_1)} \left(\gamma x_0 + e x_0^2 - \varpi x_0 y_0 - \lambda z_0 x_0^2\right) \\ y_1^p = y_0 + \dfrac{h_1^{\alpha_2}}{\alpha_2 \Gamma(\alpha_2)} \left(-\mu y_0 + \tau x_0 y_0\right) \\ z_1^p = z_0 + \dfrac{h_1^{\alpha_3}}{\alpha_3 \Gamma(\alpha_3)} \left(-\xi z_0 + \sigma z_0 x_0^2\right) \end{array}. \tag{7}$$

The numerical solutions are determined by

$$\begin{array}{l} x_1 = x_0 + \dfrac{h_1^{\alpha_1}}{\Gamma(\alpha_1+2)} \left[(1+\alpha_1)\left(\gamma x_0 + e x_0^2 - \varpi x_0 y_0 - \lambda z_0 x_0^2\right) + \gamma x_1^p + e x_1^p 2 - \varpi x_1^p y_1^p - \lambda z_1^p x_1^{p2}\right] \\ y_1 = y_0 + \dfrac{h_1^{\alpha_2}}{\Gamma(\alpha_2+2)} \left[(1+\alpha_2)\left(-\mu y_0 + \tau x_0 y_0\right) + \tau x_1^p y_1^p - \mu y_1^p\right] \\ z_1 = z_0 + \dfrac{h_1^{\alpha_3}}{\Gamma(\alpha_3+2)} \left[(1+\alpha_3)\left(-\xi z_0 + \sigma z_0 x_0^2\right) + \sigma z_1^p x_1^{p2} - \xi z_1^p\right] \end{array}. \tag{8}$$

For $t \in [t_k, t_{k+1}]$, $1 \le k \le m_1 - 1$, and $m_1 \ge 2$, the predicted values are defined as

$$\begin{array}{l} x_{k+i+1}^p = x_k + \dfrac{h_1^{\alpha_1}}{\Gamma(\alpha_1)} \displaystyle\sum_{j=0}^{i} b_{j,i+1} \left(\gamma x_k + e x_k^2 - \varpi x_k y_k - \lambda z_k x_k^2\right) \\ y_{k+i+1}^p = y_k + \dfrac{h_1^{\alpha_2}}{\Gamma(\alpha_2)} \displaystyle\sum_{j=0}^{i} b_{j,i+1} \left(-\mu y_k + \tau x_k y_k\right) \\ z_{k+i+1}^p = z_k + \dfrac{h_1^{\alpha_3}}{\Gamma(\alpha_3)} \displaystyle\sum_{j=0}^{i} b_{j,i+1} \left(-\xi z_k + \sigma z_k x_k^2\right) \end{array}, \tag{9}$$

where the coefficient $b_{j,i+1}$ is expressed as

$$b_{j,i+1} = \frac{1}{\alpha}\left[(i+1-j)^{\alpha} - (i-j)^{\alpha}\right]. \tag{10}$$

The numerical solutions are defined as

$$\begin{array}{l} x_{k+i+1} = x_k + \dfrac{h_1^{\alpha_1}}{\Gamma(\alpha_1+2)} \left(\displaystyle\sum_{j=0}^{i} a_{j,i+1}\left(\gamma x_{k+j} + e x_{k+j}^2 - \varpi x_{k+j} y_{k+j} - \lambda z_{k+j} x_{k+j}^2\right) \right. \\ \qquad \left. + \gamma x_{k+i+1}^p + e x_{k+i+1}^{p2} - \varpi x_{k+i+1}^p y_{k+i+1}^p - \lambda z_{k+i+1}^p x_{k+i+1}^{p2} \right) \\ y_{k+i+1} = y_k + \dfrac{h_1^{\alpha_2}}{\Gamma(\alpha_2+2)} \left[\displaystyle\sum_{j=0}^{i} a_{j,i+1}\left(-\mu y_{k+j} + \tau x_{k+j} y_{k+j}\right) + \tau x_{k+i+1}^p y_{k+i+1}^p - \mu y_{k+i+1}^p \right], \\ z_{k+i+1} = z_k + \dfrac{h_1^{\alpha_3}}{\Gamma(\alpha_3+2)} \left[\displaystyle\sum_{j=0}^{i} a_{j,i+1}\left(-\xi z_{k+j} + \sigma z_{k+j} x_{k+j}^2\right) + \sigma z_{k+i+1}^p x_{k+i+1}^{p2} - \xi z_{k+i+1}^p \right] \end{array} \tag{11}$$

where the coefficient $a_{j,i+1}$ is given as

$$a_{j,i+1} = \begin{cases} i^{\alpha+1} - (i-\alpha)(i+1)^{\alpha}, & j = 1; \\ (i-j+2)^{\alpha+1} + (i-j)^{\alpha+1} - 2(i-j+1)^{\alpha+1}, & 1 < j \le i; \\ 1, & j = i+1. \end{cases} \tag{12}$$

The parameters are set as $\gamma = 1$, $\varpi = 1$, $\mu = 1$, $\tau = 1$, $e = 2$, $\xi = 3$, $\sigma = 2.7$, $h_1 = 0.01$, $N_1 = 5000$, and the initial values are taken as $[1, 1.4, 1]$. When $\alpha_i\,(i = 1, 2, 3) = 0.8$, the chaotic attractors of the SMFrLVS with phase portraits are plotted in Figure 2. When $\alpha_i\,(i = 1, 2, 3) = 0.95$, the chaotic attractors of the SMFrLVS with phase portraits are described in Figure 3. The SMFrLVS can significantly save time and is more suitable for practical applications than the fractional order Lotka-Volterra system, since the SMFrLVS starts from $t\star$, as shown in Table 1.

2.2.4 Multilayer short memory fractional order Lotka-Volterra system

We propose the MSMFrLVS as follows

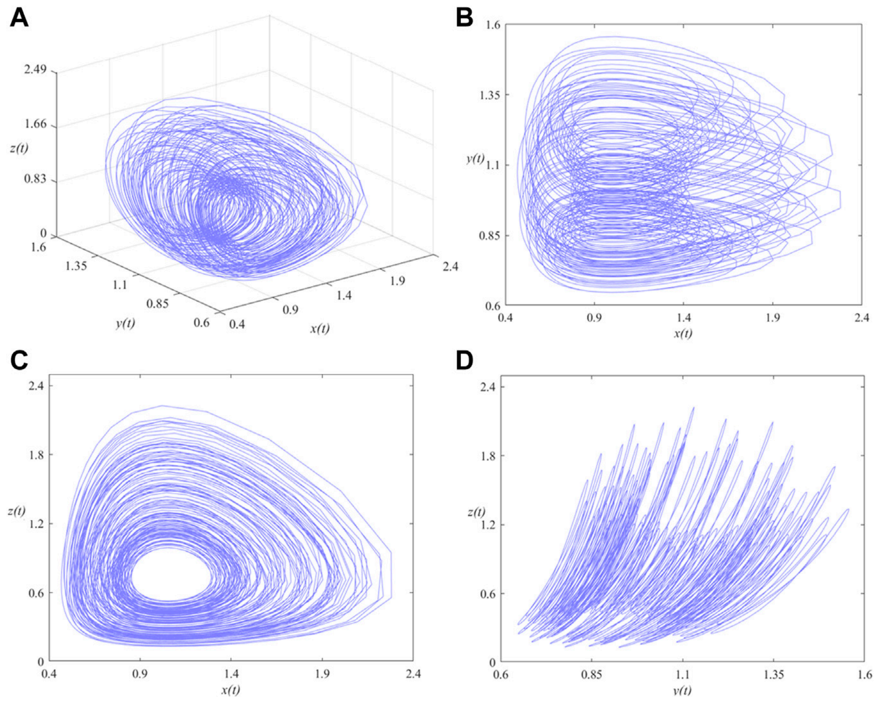


FIGURE 2
Phase portraits of the SMFrLVS when α_i (i = 1, 2, 3) = 0.8 in: **(A)** x-y-z space, **(B)** x-y, **(C)** x-z, **(D)** y-z planes.

$$\begin{cases} {}^{C}_{t_*}D_t^{\alpha_1'}x = \gamma x + e x^2 - \varpi x y - \lambda z x^2 \\ {}^{C}_{t_*}D_t^{\alpha_2'}y = -\mu y + \tau x y \\ {}^{C}_{t_*}D_t^{\alpha_3'}z = -\xi z + \sigma z x^2 \\ {}^{C}_{t_*}D_t^{\alpha_4'}w = \left(v x^2 - 1\right)\tanh(w) \end{cases}, \tag{13}$$

where the parameters $\gamma, \varpi, \mu, \tau$, and the constants $e, \xi, \sigma, v$are positive, $\alpha_i' (i = 1, 2, 3, 4)$ represent the fractional order of the MSMFrLVS, the starting point of the MSMFrLVS is t_*. The numerical solutions of the MSMFrLVS are acquired with the predictor-corrector method, the chaotic attractors of the MSMFrLVS with phase portraits are depicted in Figure 4, when $\alpha_i' (i = 1, 2, 3, 4) = 0.95$ and N_1 takes 2000, 3000, 4000, 5000, the values of other parameters remain unchanged, it is illustrated that the number of layers of the MSMFrLVS increases with the increase of N_1. When $N_1 = 5000$ and $\alpha_i' (i = 1, 2, 3, 4) = 0.7, 0.8, 0.85, 0.9$, the values of other parameters remain unchanged, the chaotic attractors of the MSMFrLVS with phase portraits are displayed in Figure 5, it is shown that the number of layers of the MSMFrLVS decreases as the increase of the fractional order.

It is difficult to describe the orbits of a chaotic system concisely due to the disorder of the orbits. One of the ideas is to reduce the dimension of description and simplify the trajectory of the space into a series of discrete points, thus the Poincare section is observed. A large number of points observed at the intersection of the phase space trajectory and the Poincare section are a feature of the chaotic motion, as shown in Figure 6. In addition, the continuous frequency power spectrum is generally regarded as an indicator of chaos, the frequency power spectra of the MSMFrLVS are plotted in Figure 7.

2.3 Gray code

Gray code is a signal coding method and generally used in the digital conversions [30]. Gray code can be expressed as

$$\begin{cases} \phi_i = \delta_i \oplus \delta_{i+1}, i = 0, 1, \ldots, q-1 \\ \phi_q = \delta_q \end{cases}, \tag{14}$$

where δ is a positive integer with binary code $\delta = \delta_q \delta_{q-1} \cdots \delta_1 \delta_0$.

3 Quantum realization of the dual-scale triangular map

3.1 Quantum representation of the dual-scale triangular map

Li et al. [31] proposed 2D dual-scale triangular map which can be utilized to scramble a rectangle image directly. For a given

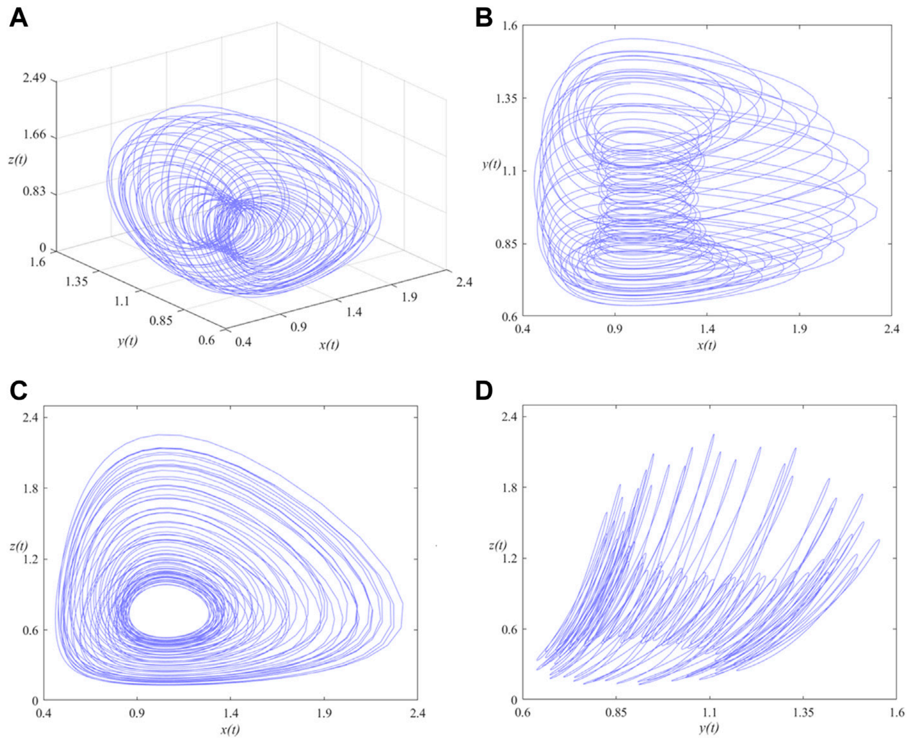


FIGURE 3
Phase portraits of the SMFrLVS when α_i (i = 1, 2, 3) = 0.95 in: **(A)** x-y-z space, **(B)** x-y, **(C)** x-z, **(D)** y-z planes.

$M \times N$ matrix, (x, y) represent the pixel coordinates and (x', y') corresponding to the changed pixel coordinates. 2D dual-scale triangular map is defined as

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} a & 0 \\ c & d \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \text{mod} \begin{bmatrix} M \\ N \end{bmatrix}, \tag{15}$$

where a, c and d are non-negative integers. Note that a and M should be co-prime, so should d and N.

The inverse dual-scale triangular map is

$$\begin{cases} x = \left(a^{-1}x'\right)\text{mod}\,M \\ y = \left(d^{-1}y' - px + s\right)\text{mod}\,N \end{cases}, \tag{16}$$

where $p = d^{-1}c$ and $s = \text{ceil}\,(cM/N) \cdot N \cdot d^{-1}$, ceil (x) denotes that each element of x is rounded to the nearest integer greater than or equal to that element. $(a^{-1}a)\text{mod}\,M = 1$ and $(d^{-1}d)\text{mod}\,N = 1$.

According to the classical dual-scale triangular map, the quantum representation of the dual-scale triangular map can be expressed as

$$\begin{cases} |x'\rangle = |a x \text{mod}\, 2^m\rangle \\ |y'\rangle = |(cx + dy)\text{mod}\, 2^n\rangle \end{cases}. \tag{17}$$

Correspondingly, the quantum representation of the inverse dual-scale triangular map can be defined as

$$\begin{cases} |x\rangle = |a^{-1}x'\text{mod}\, 2^m\rangle \\ |y\rangle = \left|\left(d^{-1}y' - px + s\right)\text{mod}\, 2^n\right\rangle \end{cases}. \tag{18}$$

3.2 Quantum circuits for the dual-scale triangular map and the inverse dual-scale triangular map

3.2.1 Quantum circuits for the dual-scale triangular map

According to Eq. 17, the states $|x'\rangle$ and $|y'\rangle$ are independent of each other. Therefore, the quantum circuits of $|x'\rangle$ and $|y'\rangle$ can be designed.

(1) Quantum circuit $|x'\rangle$. According to Eq. 17, $|x'\rangle$ can be achieved with a steps.

$$|x, x\rangle \rightarrow |x, 2x\text{mod}\, 2^m\rangle \rightarrow \cdots \rightarrow |x, a x\text{mod}\, 2^m\rangle. \tag{19}$$

$a x\text{mod}\, 2^m$ from the first step to the last step can be acquired with the ADDER-MOD2^m network [32], as shown in Figure 8A.

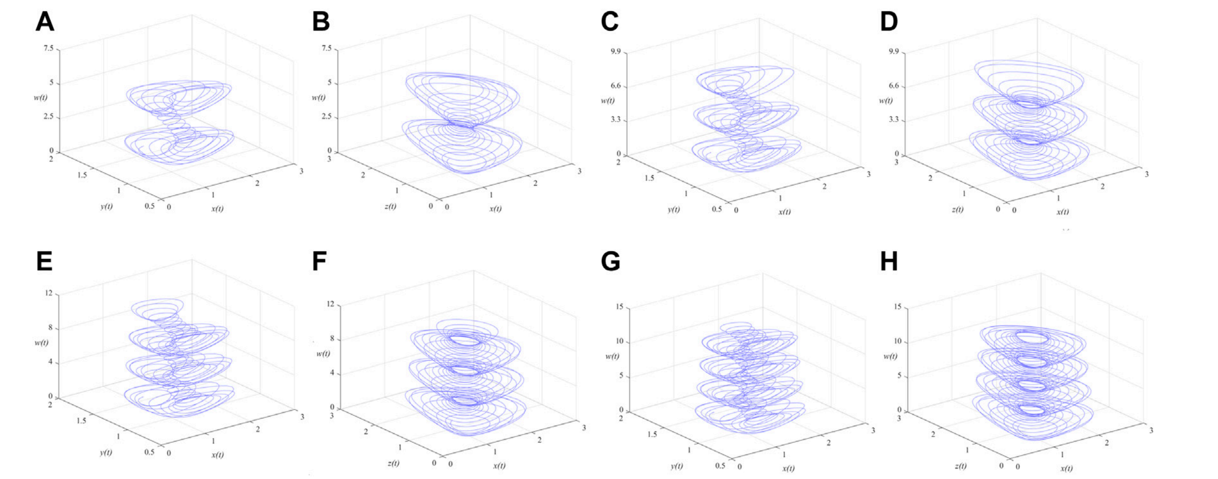


FIGURE 4
Phase portraits of the MSMFrLVS in *x*-*y*-*w* space and *x*-*z*-*w* space: **(A,B)**: N_1 = 2000, **(C,D)**: N_1 = 3000, **(E,F)**: N_1 = 4000, **(G,H)**: N_1 = 5000.

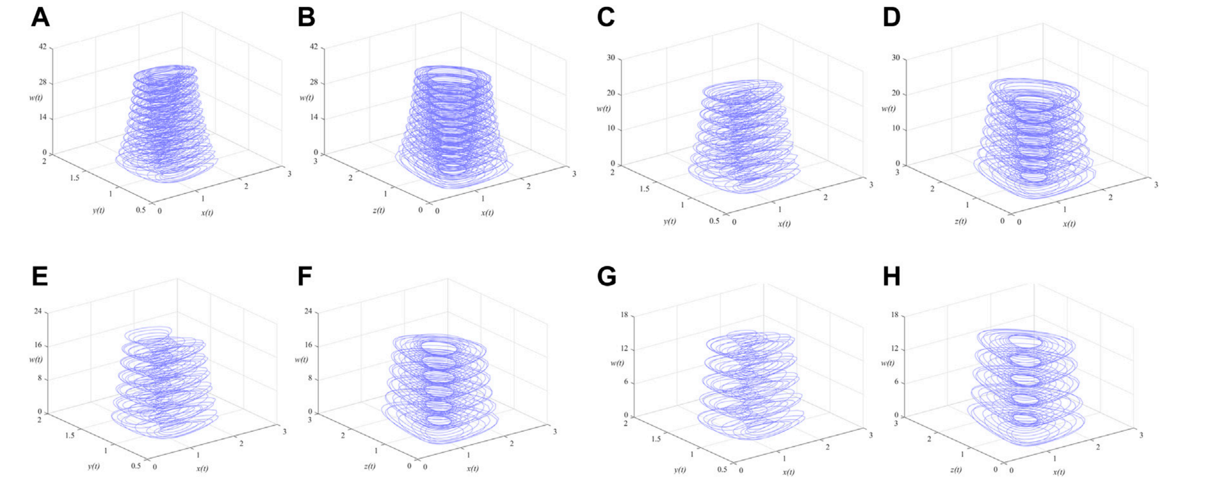


FIGURE 5
Phase portraits of the MSMFrLVS in *x*-*y*-*w* space and *x*-*z*-*w* space: **(A,B)**: $\alpha_i' = 0.7$, **(C,D)**: $\alpha_i' = 0.8$, **(E,F)**: $\alpha_i' = 0.85$, **(G,H)**: $\alpha_i' = 0.9$

TABLE 1 Time comparison between the SMFrLVS and the fractional order Lotka-Volterra system.

N_1	The SMFrLVS (s)	Fractional order Lotka-Volterra system (s)
4,000	0.863	14.575
8,000	0.992	66.054
16,000	1.077	226.386
30,000	1.272	1306.923
40,000	1.437	1802.287
50,000	1.624	3,256.137

(2) Quantum circuit $|y'\rangle$. According to Eq. 17, $|y'\rangle$ can be realized with $c+d+1$ steps.

$$|x,x\rangle \to |x, 2x\bmod 2^n\rangle \to\cdots\to |x, cx\bmod 2^n\rangle \to |y, cx\bmod 2^n\rangle \to |y, (cx+y)\bmod 2^n\rangle \to\cdots\to |y, (cx+dy)\bmod 2^n\rangle. \tag{20}$$

It shows that $cx\bmod 2^n$ from the first step to the c-th step can be obtained with the ADDER-MOD2^n network. In the $(c+1)$-th step, x is substituted for y. $(cx+dy)\bmod 2^n$ from the $(c+2)$-th step to the last step can be constructed with the ADDER-MOD2^n network. The quantum circuit $|y'\rangle$ is depicted in Figure 8B.

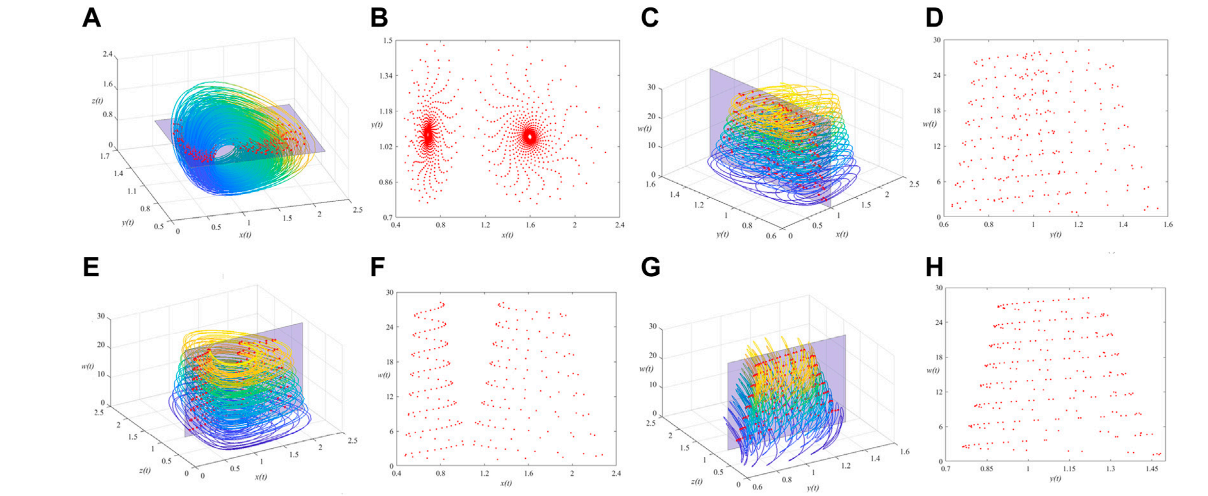


FIGURE 6
3D view of the MSMFrLVS and the Poincare section in: **(A,B)**: *x*-*y*-*z* space, **(C,D)**: *x*-*y*-*w* space, **(E,F)**: *x*-*z*-*w* space, **(G,H)**: *y*-*z*-*w* space.

3.2.2 Quantum circuits for the inverse dual-scale triangular map

To recover the plaintext image from the scrambled image, the quantum circuits of $|x\rangle$ and $|y\rangle$ should be involved. From Eq. 18, the inverse transform uses subtraction operation. A theorem stated in [32] provides a solution to realizing the subtraction operation.

$$(x-y)\bmod 2^n = (x+(\bar{y}+1))\bmod 2^n, \tag{21}$$

where $\bar{y} = \overline{y_{n-1}y_{n-2}\ldots y_0}$, $\overline{y_i} = 1-y_i$, $i = n-1, n-2, \ldots, 0$.

(1) Quantum circuit $|x\rangle$. From Eq. 18, it requires a^{-1} steps to realize $|x\rangle$, as illustrated in Figure 9A. $|x\rangle$ can be constructed as

$$|x', x'\rangle \rightarrow \cdots \rightarrow |x', a^{-1}x' \bmod 2^m\rangle. \tag{22}$$

$a^{-1}x' \bmod 2^m$ from the first step to the last step can be created with the ADDER-MOD2^m network.

(2) Quantum circuit $|y\rangle$. By recalling Eq. 18, $|y\rangle$ can be implemented with $p+d^{-1}+6$ steps, as depicted in Figure 9B.

$$\begin{aligned}&|\bar{x}, \bar{x}\rangle \rightarrow \cdots \rightarrow |\bar{x}, p\bar{x} \bmod 2^n\rangle \rightarrow |p, p\bar{x} \bmod 2^n\rangle \rightarrow |p, p(\bar{x}+1) \bmod 2^n\rangle \\ &\rightarrow |y', p(\bar{x}+1) \bmod 2^n\rangle \rightarrow \cdots \rightarrow |y', (p(\bar{x}+1)+d^{-1}y') \bmod 2^n\rangle \\ &\rightarrow |s, (p(\bar{x}+1)+d^{-1}y') \bmod 2^n\rangle \rightarrow |s, (p(\bar{x}+1)+d^{-1}y'+s) \bmod 2^n\rangle.\end{aligned} \tag{23}$$

It demonstrates that $p\bar{x} \bmod 2^n$from the first step to the p-th step can be obtained with the ADDER-MOD2^n network. $\bar{x}$ is superseded by p in the $(p+1)$-th step. In the $(p+2)$-th step, $p(\bar{x}+1) \bmod 2^n$ is acquired with the help of the ADDER-MOD2^n operation. In the $(p+3)$-th step, p is replaced by y'. From the $(p+4)$-th step to the $(p+d^{-1}+4)$-th step, $(p(\bar{x}+1)+d^{-1}y') \bmod 2^n$ is generated with the ADDER-MOD2^n network. In the $(p+d^{-1}+5)$-th step, y' is substituted for s. In the last step, $(p(\bar{x}+1)+d^{-1}y'+s) \bmod 2^n$ is accomplished by the ADDER-MOD2^n network.

4 Quantum image encryption and decryption algorithm

4.1 Quantum image encryption algorithm

The proposed quantum image encryption scheme based on the MSMFrLVS and quantum dual-scale triangular map is shown in Figure 10. The plaintext image is represented with the GQIR model. During the permutation stage, the position information of the quantum image is shuffled by the block-level permutation and the intra and the inter bit-level permutation operations, while the color information of the quantum image remains unchanged. In the diffusion stage, three-level diffusion operations including pixel values, binary bits and pixel bits are accomplished for the scrambled image.

Assume the plaintext image of size $N \times M$ with a color depth q to be encrypted is expressed as $|I\rangle$ and its GQIR representation can be written as

$$|I\rangle = \frac{1}{(\sqrt{2})^{n+m}} \sum_{Y=0}^{2^n-1} \sum_{X=0}^{2^m-1} \bigotimes_{j=0}^{q-1} |C_{YX}^j\rangle |YX\rangle. \tag{24}$$

The specific encryption algorithm involves the following steps.

Step 1: Block-level scrambling is performed. To effectively realize the block-level arrangement, the plaintext image

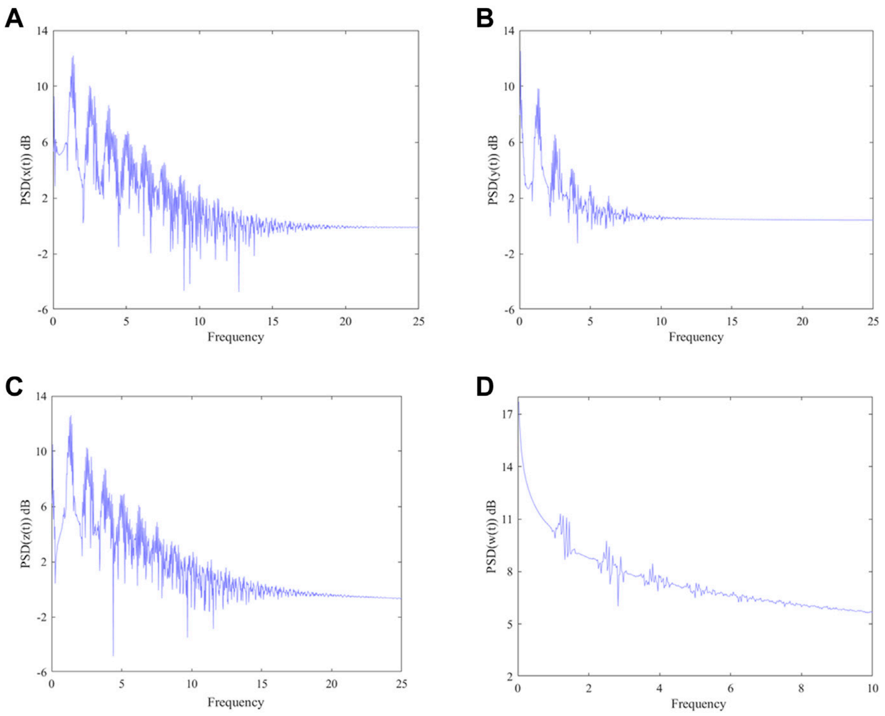


FIGURE 7
Frequency power spectra of the MSMFrLVS in: **(A)** x, **(B)** y, **(C)** z, **(D)** w planes.

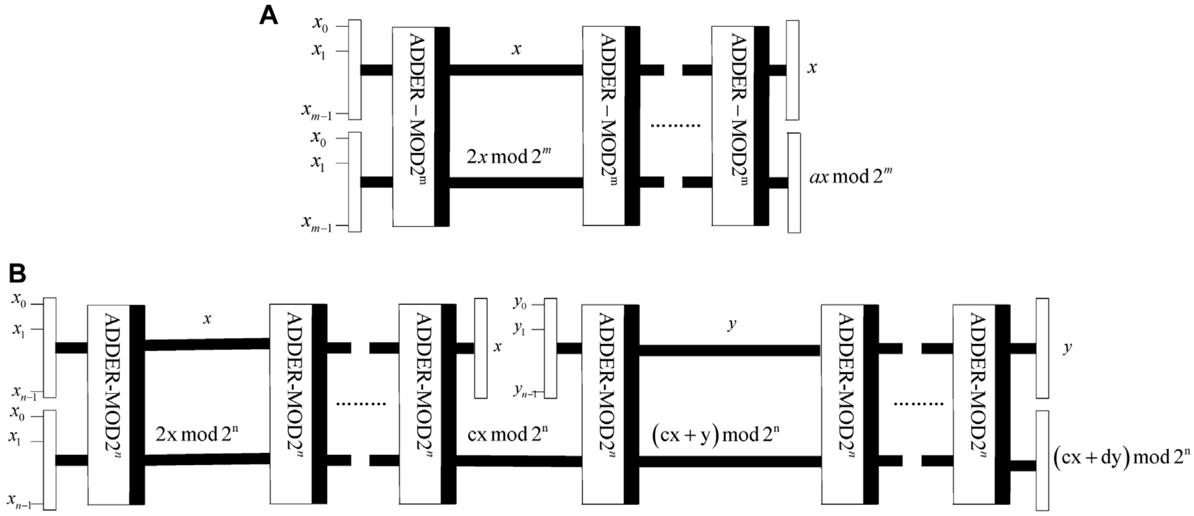


FIGURE 8
Quantum circuits:**(A)** $|x'\rangle$, **(B)** $|y'\rangle$.

should be decomposed into sub-blocks. If the block size is $2^{w_1} \times 2^{w_1}$, then the number of blocks is $2^{n-w_1} \times 2^{m-w_1}$ after division. Assume that $\mathrm{Q}_{\mathrm{dst}}$ represents the quantum dual-scale triangular map which is applied on the $n - w_1$ and $m - w_1$ qubits and the scrambled block image $|I_b\rangle$ can be acquired.

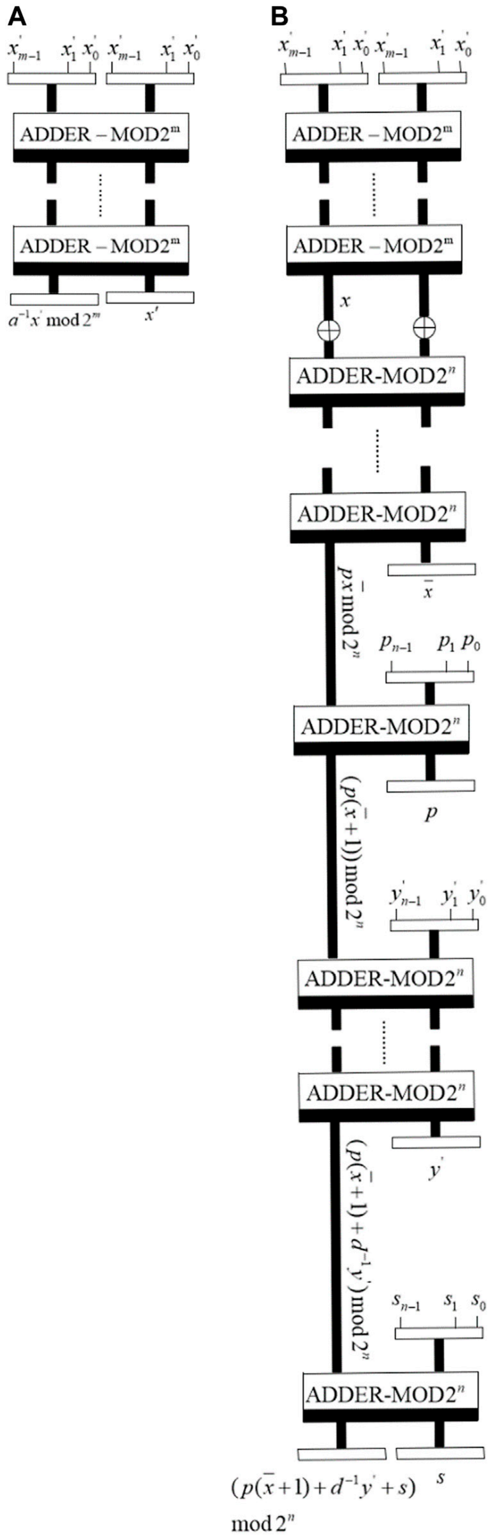


FIGURE 9
Quantum circuit **(A)** $|x\rangle$, **(B)** $|y\rangle$.

$$
\begin{aligned}
|I_b\rangle = Q_{\text{dst}}|I\rangle &= \frac{1}{(\sqrt{2})^{n+m}}\sum_{Y=0}^{2^n-1}\sum_{X=0}^{2^m-1}\bigotimes_{j=0}^{q-1}|C_{YX}^j\rangle Q_{\text{dst}}|YX\rangle \\
&= \frac{1}{(\sqrt{2})^{n+m}}\sum_{Y=0}^{2^n-1}\sum_{X=0}^{2^m-1}\bigotimes_{j=0}^{q-1}|C_{YX}^j\rangle Q_{\text{dst}}\left(|y_{n-1}y_{n-2}\cdots y_0\rangle|x_{m-1}x_{m-2}\cdots x_0\rangle\right) \\
&= \frac{1}{(\sqrt{2})^{n+m}}\sum_{Y=0}^{2^n-1}\sum_{X=0}^{2^m-1}\bigotimes_{j=0}^{q-1}|C_{YX}^j\rangle Q_{\text{dst}}\left(|y_{n-1}y_{n-2}\cdots y_{w_1}\rangle\right)\left|y_{w_1-1}\cdots y_0\right\rangle \\
&\quad Q_{\text{dst}}\left(|x_{m-1}x_{m-2}\cdots x_{w_1}\rangle\right)\left|x_{w_1-1}\cdots x_0\right\rangle \\
&= \frac{1}{(\sqrt{2})^{n+m}}\sum_{Y=0}^{2^n-1}\sum_{X=0}^{2^m-1}\bigotimes_{j=0}^{q-1}|C_{YX}^j\rangle\left|y'_{n-1}\ y'_{n-2}\ \cdots y'_{w_1}\ y_{w_1-1}\cdots y_0\right\rangle\left|x'_{m-1}\ x'_{m-2}\ \cdots x'_{w_1}\ x_{w_1}\cdots x_0\right\rangle.
\end{aligned}
\tag{25}
$$

According to Eq. 17, the scrambled position qubits $|y'_{n-1}\ y'_{n-2}\ \cdots y'_{w_1}\ \rangle$ and $|x'_{m-1}\ x'_{m-2}\ \cdots x'_{w_1}\ \rangle$ can be obtained as

$$
\begin{cases}
|y'_{n-1}\ y'_{n-2}\ \cdots y'_{w_1}\ \rangle = Q_{\text{dst}}\left(y_{n-1}y_{n-2}\cdots y_{w_1}\right) \\
\qquad = \left(c|x_{n-1}x_{n-2}\cdots x_{w_1}\rangle + d\left|y_{n-1}y_{n-2}\cdots y_{w_1}\right\rangle\right)\bmod 2^{n-w_1} \\
|x'_{m-1}\ x'_{m-2}\ \cdots x'_{w_1}\ \rangle = Q_{\text{dst}}\left(x_{m-1}x_{m-2}\cdots x_{w_1}\right) = \left(a|x_{m-1}x_{m-2}\cdots x_{w_1}\rangle\right)\bmod 2^{m-w_1}
\end{cases}.
\tag{26}
$$

The circuit of image block-level permutation based on Q_{dst} is depicted in Figure 11.

Step 2. : To improve the security of the system, a plaintext correlation mechanism is employed to obtain the initial values of the MSMFrLVS. The method is expressed as

$$
\begin{cases}
x'(0) = x(0) + \sum_{i=1}^{8} h_i \times 10^{-6} + \dfrac{h_9 \oplus h_{10} \oplus \cdots h_{16}}{10^{10}} \\
y'(0) = y(0) + \sum_{i=17}^{24} h_i \times 10^{-6} + \dfrac{h_{25} \oplus h_{26} \oplus \cdots h_{32}}{10^{10}} \\
z'(0) = z(0) + \sum_{i=33}^{40} h_i \times 10^{-6} + \dfrac{h_{41} \oplus h_{42} \oplus \cdots h_{48}}{10^{10}} \\
w'(0) = w(0) + \sum_{i=49}^{56} h_i \times 10^{-6} + \dfrac{h_{57} \oplus h_{58} \oplus \cdots h_{64}}{10^{10}}
\end{cases},
\tag{27}
$$

where $x(0)$, $y(0)$, $z(0)$ and $w(0)$ are the initial values of Eq. 13, h_i is a 256-bit hash value, $x'(0)$, $y'(0)$, $z'(0)$ and $w'(0)$ are the updated initial values of Eq. 13. Obviously, the new initial values are related to the plaintext image.

Step 3: The initial values $x'(0)$, $y'(0)$, $z'(0)$ and $w'(0)$ are iterated with Eq. 13 $m' + 2^n \times 2^m$ times, m' is set to 100. To avoid the harmful effect of transient procedure, a new chaotic sequence $\{\Upsilon_i | i = 1, 2, \ldots, 2^n \times 2^m\}$ is obtained after abandoning the former m' elements, where $\Upsilon \in \{x, y, z, w\}$.

Step 4: The new chaotic sequence is transformed into integer sequence, $\{\Upsilon_i^* | i = 1, 2, \cdots, 2^n \times 2^m\}$,

$$
\Upsilon_i^* = \left|\lfloor (\Upsilon_i - \lfloor \Upsilon_i \rfloor) \times 10^{14} \rfloor\right| \bmod 256,
\tag{28}
$$

where $\lfloor \Upsilon \rfloor$ rounds Υ to the nearest integer towards zero.

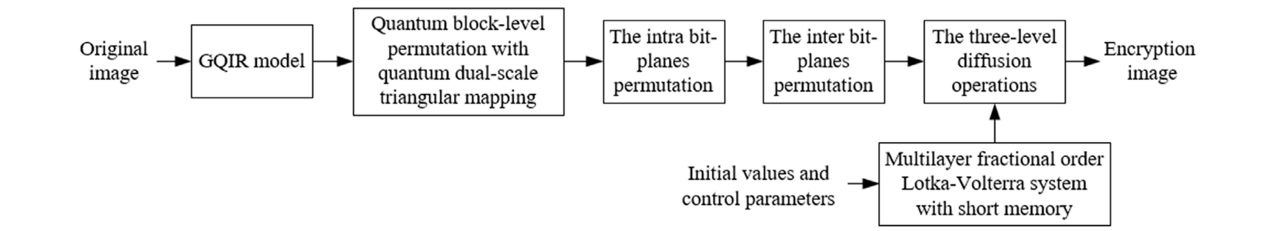

Original image
GQIR model
Quantum block-level permutation with quantum dual-scale triangular mapping
The intra bit-planes permutation
The inter bit-planes permutation
The three-level diffusion operations
Encryption image
Initial values and control parameters
Multilayer fractional order Lotka-Volterra system with short memory

FIGURE 10
Flowchart of image encryption algorithm.

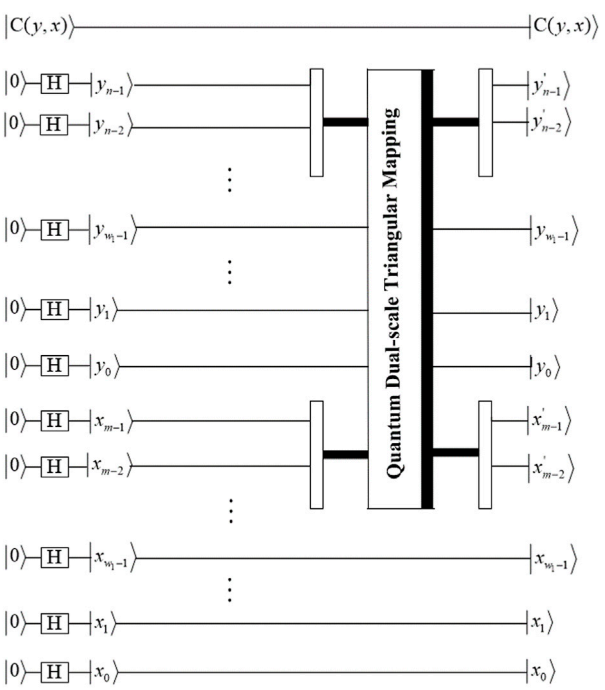


FIGURE 11
Quantum circuit for the block-level permutation based on Q_{dst}.

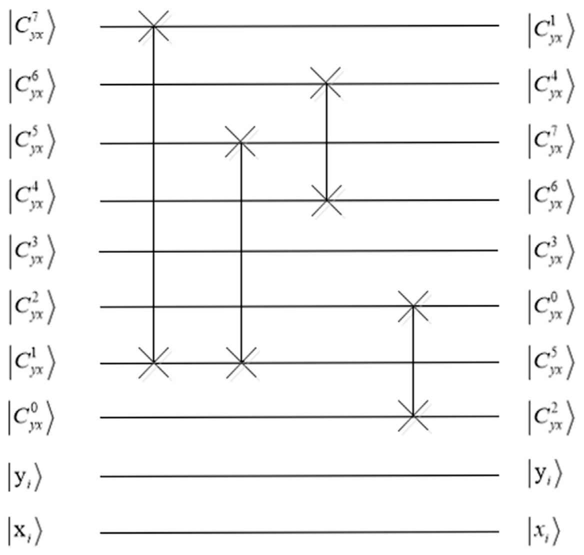


FIGURE 12
Quantum circuit of the intra bit-planes permutation.

Step 5. : Bit-level permutation includes the intra bit-planes permutation and the inter bit-planes permutation. The intra bit-planes permutation is accomplished by sorting the sequence $\{x_i^*|i=1,2,\cdots,8\}$ in ascending order. The corresponding quantum circuit is shown in Figure 12, where the exchange of bit-planes is implemented with quantum swap gate.

For pixel (Y,X), a quantum sub-operation φ_{YX} can be constructed as

$$\varphi_{YX} = I \otimes \sum_{y=0}^{2^n-1}\sum_{x=0,YX\neq yx}^{2^m-1} |yx\rangle\langle yx| + G_{YX}\otimes |YX\rangle\langle YX|. \quad (29)$$

where G_{YX} to realize bit-planes permutation operation is defined as

$$\begin{aligned} G_{YX}|C(y,x)\rangle &= G_{YX}\left|c_{yx}^7 c_{yx}^6 c_{yx}^5 c_{yx}^4 c_{yx}^3 c_{yx}^2 c_{yx}^1 c_{yx}^0\right\rangle \\ &= \left|c_{yx}^1 c_{yx}^4 c_{yx}^7 c_{yx}^6 c_{yx}^3 c_{yx}^0 c_{yx}^5 c_{yx}^2\right\rangle \end{aligned}, \quad (30)$$

By applying the quantum sub-operation φ_{YX} on the block-level permutation image $|I_b\rangle$, the bit-planes of pixel (Y,X) are scrambled.

$$\begin{aligned} \varphi_{YX}|I_b\rangle &= \frac{1}{(\sqrt{2})^{n+m}}\varphi_{YX}\left(\sum_{y=0}^{2^n-1}\sum_{x=0,YX\neq yx}^{2^m-1}|C(y,x)\rangle|yx\rangle + |C(Y,X)\rangle|YX\rangle\right) \\ &= \frac{1}{(\sqrt{2})^{n+m}}\sum_{y=0}^{2^n-1}\sum_{x=0,YX\neq yx}^{2^m-1}|C(y,x)\rangle|yx\rangle + \varphi_{YX}\left(\left|c_{yx}^7 c_{yx}^6 c_{yx}^5 c_{yx}^4 c_{yx}^3 c_{yx}^2 c_{yx}^1 c_{yx}^0\right\rangle|YX\rangle\right) \\ &= \frac{1}{(\sqrt{2})^{n+m}}\sum_{y=0}^{2^n-1}\sum_{x=0,YX\neq yx}^{2^m-1}|C(y,x)\rangle|yx\rangle + \left|c_{yx}^1 c_{yx}^4 c_{yx}^7 c_{yx}^6 c_{yx}^3 c_{yx}^0 c_{yx}^5 c_{yx}^2\right\rangle|YX\rangle. \end{aligned} \quad (31)$$

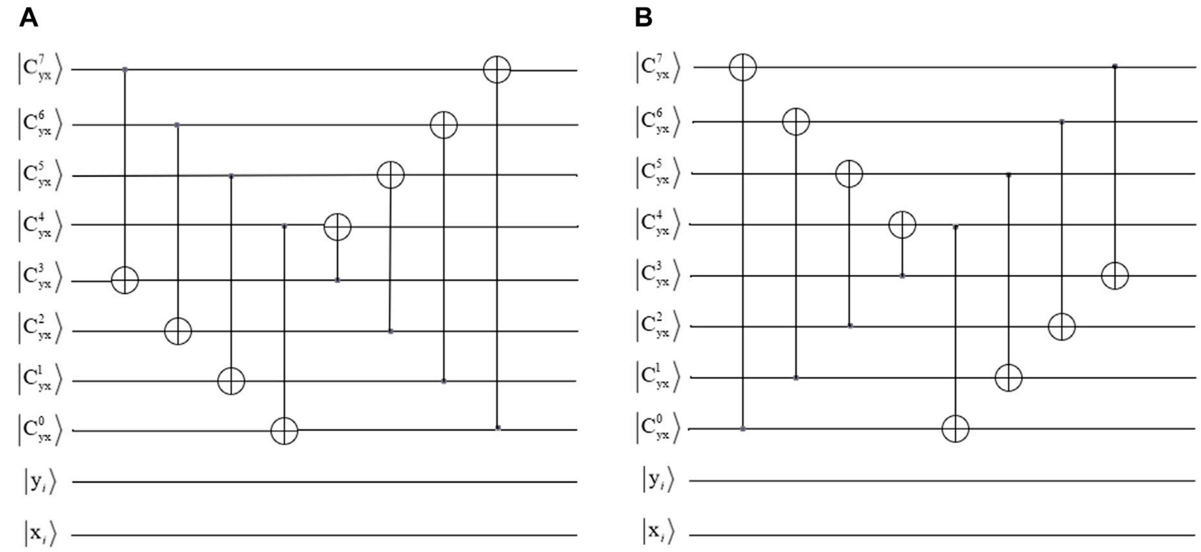


FIGURE 13
Circuits **(A)** Quantum Gray code, **(B)** Inverse quantum Gray code.

To complete bit-planes scrambling of all the pixels, a quantum operation S is defined,

$$\begin{aligned} |I_k\rangle = S|I_b\rangle &= \prod_{Y=0}^{2^n-1}\prod_{X=0}^{2^m-1}\varphi_{YX}|I_b\rangle \\ &= \frac{1}{(\sqrt{2})^{n+m}}\sum_{Y=0}^{2^n-1}\sum_{X=0}^{2^m-1}\left|c^1_{yx}c^4_{yx}c^7_{yx}c^6_{yx}c^3_{yx}c^0_{yx}c^5_{yx}c^2_{yx}\right\rangle|YX\rangle \\ &= \frac{1}{(\sqrt{2})^{n+m}}\sum_{y=0}^{2^n-1}\sum_{x=0}^{2^m-1}|C'(y,x)\rangle|yx\rangle. \end{aligned} \tag{32}$$

Step 6. : The inter bit-planes permutation is accomplished with quantum Gray code. By scrambling quantum image $|I_k\rangle$ with quantum Gray code, the scrambled quantum image $|I_s\rangle$ is obtained. The circuit of quantum Gray code is shown in Figure 13A.

Step 7. : The sequence $\{w_i^{'}|i = 1, 2, \cdots, 2^n \times 2^m\}$ is given by

$$w_i^{'} = w_i^* \bmod 3. \tag{33}$$

The scrambled quantum image $|I_s\rangle$ is chosen to perform diffusion operations among pixel values, binary bits and pixel bits according to the sequence $\{w_i^{'}|i = 1, 2, \cdots, 2^n \times 2^m\}$.

Step 8. : If $w_i^{'} = 0$, then the pixel values diffusion operation is performed.

$$\begin{cases} \text{aa} = \text{floor}\left(\frac{1}{2} \times 10^4 \sin\left(4 \sin y^*(i) + 1\right)\right) \bmod 256 \\ \text{bb} = \text{floor}\left(0.9 \cos 3.9\pi z^*(i) \times (1 - z^*(i)) \times 10^4\right) \bmod 256 \\ I_e(i) = (I_s(i) + \text{aa} \oplus \text{bb}) \bmod 256 \end{cases} \cdot \tag{34}$$

If $w_i^{'} = 1$, then the binary bits diffusion operation is performed.

$$I_e(i) = I_s(i) \oplus y^*(i) \oplus z^*(i). \tag{35}$$

If $w_i^{'} = 2$, then the pixel bits diffusion operation is performed.

$$\begin{cases} a_1 = \text{floor}\left(\frac{y^*(i)}{100}\right) \\ b_1 = \text{floor}\left(\frac{y^*(i) - 100a_1}{10}\right) \\ c_1 = \text{floor}\left(y^*(i) - 100a_1 - 10b_1\right) \end{cases}, \tag{36}$$

$$\begin{cases} a_{11} = \left[a_1 + \text{floor}\left(0.99 \sin 0.99 \times 10^4 \pi a_1\right) \bmod 100\right] \bmod 10 \\ b_{11} = \left[b_1 + \text{floor}\left(0.99 \sin 0.99 \times 10^4 \pi b_1\right) \bmod 100\right] \bmod 10 \\ c_{11} = \left[c_1 + \text{floor}\left(0.99 \sin 0.99 \times 10^4 \pi c_1\right) \bmod 100\right] \bmod 10 \end{cases}, \tag{37}$$

$$\text{abc} = (100a_{11} + 10b_{11} + c_{11}) \bmod 256, \tag{38}$$

$$I_e(i) = \left[\text{abc} + \text{floor}\left(0.99 \sin 2\pi 10^4 z^*(i)\right) + I_s(i)\right] \bmod 256. \tag{39}$$

According to Eq. 36, the hundreds place a_1, tens place b_1, and one place c_1. They were then entered into Eq. 37 to obtain a_{11}, b_{11}, and c_{11}. They are then substituted in Eq. 38 and combined to yield *abc*. Finally, the quantum ciphertext image $|I_e\rangle$ can be generated by substituting them into Eq. 39.

4.2 Quantum image decryption algorithm

The decryption process is the reverse process of the encryption process, the specific image decryption process is as follows.

Step 1: The encryption quantum image $|I_e\rangle$ performs three-level diffusion operations with the integer sequences $\{y_i^*|i = 1, 2, \ldots 2^n \times 2^m\}$ and $\{z_i^*|i = 1, 2, \ldots 2^n \times 2^m\}$, the scrambled quantum image $|I_s\rangle$ is retrieved.

Step 2. : The quantum image $|I_k\rangle$ is retrieved by the inverse quantum Gray code on the scrambled quantum image $|I_s\rangle$, the circuit of the inverse quantum Gray code is depicted in Figure 13B.

Step 3: The quantum image $|I_b\rangle$ is obtained by the inverse bit-planes exchange operation S^{-1} on the quantum image $|I_k\rangle$.

$$\begin{aligned}
|I_b\rangle &= S^{-1}|I_k\rangle = \prod_{Y=0}^{2^n-1}\prod_{X=0}^{2^m-1}\varphi_{YX}^{-1}|I_k\rangle \\
&= \frac{1}{(\sqrt{2})^{n+m}}\sum_{Y=0}^{2^n-1}\sum_{X=0}^{2^m-1} G_{YX}^{-1}|c_{YX}^1 c_{YX}^4 c_{YX}^7 c_{YX}^6 c_{YX}^3 c_{YX}^0 c_{YX}^5 c_{YX}^2\rangle \otimes |YX\rangle \\
&= \frac{1}{(\sqrt{2})^{n+m}}\sum_{Y=0}^{2^n-1}\sum_{X=0}^{2^m-1} |c_{YX}^7 c_{YX}^6 c_{YX}^5 c_{YX}^4 c_{YX}^3 c_{YX}^2 c_{YX}^1 c_{YX}^0\rangle \otimes |YX\rangle.
\end{aligned} \tag{40}$$

Step 4: The plaintext image can be recovered by performing inverse Q_{dst} on the quantum image $|I_b\rangle$.

$$\begin{aligned}
|I\rangle &= Q_{\mathrm{dst}}^{-1}|I_b\rangle \\
&= \frac{1}{(\sqrt{2})^{n+m}}\sum_{Y=0}^{2^n-1}\sum_{X=0}^{2^m-1}\bigotimes_{j=0}^{q-1}|C_{YX}^j\rangle Q_{dst}^{-1}\left(|y'_{n-1}\ y'_{n-2}\ \cdots y'_{w_1}\ y_{w_1-1}\cdots y_0\rangle|x'_{m-1}\ x'_{m-2}\ \cdots x'_{w_1}\ x_{w_1}\cdots x_0\rangle\right) \\
&= \frac{1}{(\sqrt{2})^{n+m}}\sum_{Y=0}^{2^n-1}\sum_{X=0}^{2^m-1}\bigotimes_{j=0}^{q-1}|C_{YX}^j\rangle Q_{dst}^{-1}|y'_{n-1}\ y'_{n-2}\ \cdots y'_{w_1}\ \rangle|y_{w_1-1}\cdots y_0\rangle Q_{dst}^{-1}|x'_{m-1}\ x'_{m-2}\ \cdots x'_{w_1}\ \rangle|x_{w_1-1}\cdots x_0\rangle \\
&= \frac{1}{(\sqrt{2})^{n+m}}\sum_{Y=0}^{2^n-1}\sum_{X=0}^{2^m-1}\bigotimes_{j=0}^{q-1}|C_{YX}^j\rangle|y_{n-1}y_{n-2}\cdots y_0\rangle|x_{m-1}x_{m-2}\cdots x_0\rangle \\
&= \frac{1}{(\sqrt{2})^{n+m}}\sum_{Y=0}^{2^n-1}\sum_{X=0}^{2^m-1}\bigotimes_{j=0}^{q-1}|C_{YX}^j\rangle|YX\rangle.
\end{aligned} \tag{41}$$

5 Numerical simulation and discussion

The numerical simulations are run on a MATLAB R2019b platform due to a lack of equipment. To test the effectiveness and reliability of the proposed quantum image encryption algorithm, the plaintext images in Figures 14A–C are image "Barbara" of size 580 × 720, image "Arnav" of size 248 × 300, and color image "Girls" of size 321 × 481 × 3 [33–35]. The block size w_1 has been set to four. The simulation parameters are as follows: $a = 1, c = 2, d = 1, \gamma = 1, \varpi = 1, \mu = 1, \tau = 1, e = 2, \xi = 3, \sigma = 2.7, h_1 = 0.01, N_1 = 5000, x(0) = 1, y(0) = 1.4, z(0) = 1$ and $w(0) = 1$. The relevant ciphertext images are shown in Figures 14D–F. Because all ciphertext images are encrypted and exhibit chaotic behavior, attacks will have an enormously difficult time extracting the original plaintext images. When decrypted with the correct keys, Figures 14G–I show the corresponding decrypted images. There is no discernible difference between the original plaintext image and the decrypted image, indicating that the proposed fast quantum image encryption scheme based on a multilayer short memory fractional order Lotka-Volterra system and a dual-scale triangular map is effective.

The proposed algorithm was evaluated using three types of statistical property analyses, comprising histogram, correlation of adjacent pixels, and information entropy. The histogram assures that plaintext images and ciphertext images are different from each other. The association between two neighboring pixels was shown by the correlation of adjacent pixels. The information entropy looks at the encryption effect of the ciphertext images. In order to verify the proposed algorithm's resistance to various attacks, differential attack analysis, noise attack analysis, and shear attack analysis were also carried out. To show the space and sensitivity of the keys, key space analysis and key sensitivity analysis are then done. The proposed algorithm's computational complexity was then described. Last but not least, tests and comparisons of the encryption and decryption times in seconds were performed. All of the preceding analyses will guarantee that proposed algorithms would both be technically proficient and efficient.

5.1 Statistical property analysis

5.1.1 Histogram

The histograms of the color images "Girls," "Sailboat," and "Goldhill" are shown in Figures 15A–C, and the histograms of the corresponding ciphertext images are shown in Figures 15D–F. It is demonstrated that the histograms of ciphertext images differ noticeably from those of plaintext images. The pixel values of ciphertext images are evenly distributed and completely different from those of plaintext images. It demonstrates that the proposed quantum image encryption scheme can withstand the histogram attack.

Furthermore, the chi-square test is used to precisely measure the difference between the ciphertext image and the plaintext image.

$$\chi^2 = \sum_{L=0}^{255}\frac{(o_L - e_L)^2}{e_L}, \tag{42}$$

where o_L is the observed number of the L-th gray level and e_L is the expected number of the L-th gray level. Table 2 displays the results of the chi-square test on ciphertext and plaintext images. Table 2 shows that the chi-square values of ciphertext images are

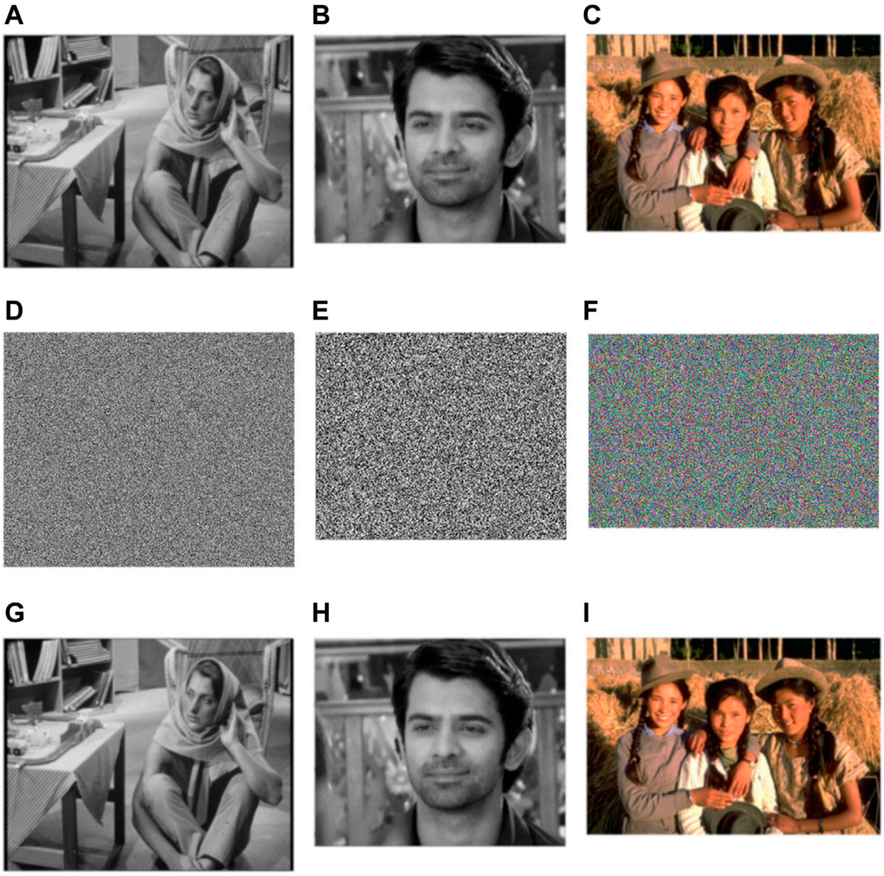


FIGURE 14
Plaintext images, ciphertext images and decryption images: **(A)** "Barbara," **(B)** "Arnav," **(C)** "Girls," **(D)** "Barbara," **(E)** "Arnav," **(F)** "Girls," **(G)** "Barbara," **(H)** "Arnav," **(I)** "Girls." ("Barbara" is from the University of Southern California's signal and image process institute image dataset, "Arnav" is from the IMDB-WIKI 500k dataset, "Girls" is from the Berkeley segmentation dataset (BSD) 500 dataset.).

less than 5% of the significance level, demonstrating that the proposed encryption scheme can withstand the histogram attack.

5.1.2 Correlation of adjacent pixels

Assume that N pairs of adjacent pixels need to be randomly selected from the image to be investigated, and the gray values are recorded as (x, y), the correlation coefficient between two vectors is defined as

$$C_{XY} = \frac{\sum_{i=1}^{N}\left(x_i - \frac{1}{N}\sum_{i=1}^{N}x_i\right)\left(y_i - \frac{1}{N}\sum_{i=1}^{N}y_i\right)}{\sqrt{\sum_{i=1}^{N}\left(x_i - \frac{1}{N}\sum_{i=1}^{N}x_i\right)^2 \sum_{i=1}^{N}\left(y_i - \frac{1}{N}\sum_{i=1}^{N}y_i\right)^2}}. \tag{43}$$

The correlation distribution of plaintext image "Girls" and ciphertext image "Girls" in horizontal, vertical and diagonal directions are depicted in Figure 16. The correlation coefficients of plaintext images and ciphertext images are edited in Table 3. As can be seen from Figure 16 and Table 3, the correlations between the adjacent pixels of plaintext images are extremely strong, while the correlations between the adjacent pixels of ciphertext images are close to 0, which are almost no correlations. Compared with [10, 24], the proposed image encryption scheme has stronger capacity to resist the correlation analysis attack.

5.1.3 Information entropy

The information entropy $H(x)$ calculation formula is written as

$$H(x) = -\sum_{i=0}^{255} p(x_i)\log_2 p(x_i), \tag{44}$$

where $p(x_i)$ represents the probability of the gray value i. The theoretical value of information entropy for a gray-scale random image with level 256 is 8 bits. The information entropy of

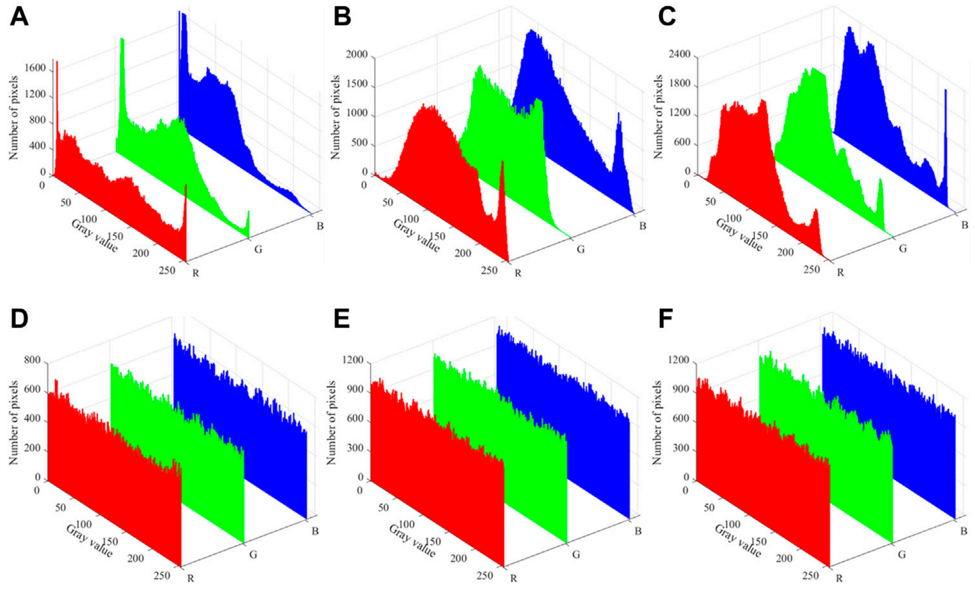


FIGURE 15
Histograms of plaintext images and ciphertext images: **(A)** "Girls," **(B)** "Sailboat," **(C)** "Goldhill," **(D)** "Girls," **(E)** "Sailboat," **(F)** "Goldhill."

TABLE 2 Chi-square test.

Image		Plaintext image	Ciphertext image
Barbara		1.6314e+05	235.6696
Arnav		4.0976e+04	278.3243
Bridge		1.5584e+05	265.5647
Lake		1.5144e+05	259.4658
Baboon		1.4652e+04	265.2458
	R channel	1.4164e+05	236.4007
Girls	G channel	1.1872e+05	206.2859
	B channel	1.6640e+05	234.2054
	R channel	1.6543e+05	256.5642
Sailboat	G channel	1.2564e+05	286.2656
	B channel	1.3654e+05	266.6462
	R channel	1.5621e+05	269.5354
Goldhill	G channel	1.4365e+05	275.3564
	B channel	1.6543e+05	265.3564
Critical value (5%)		293.2478	293.2478

plaintext images and ciphertext images is listed in Table 4. It is demonstrated that the information entropy of each ciphertext image approaches the theoretical value, whereas the information entropy of each plaintext image deviates significantly from the theoretical value, and the image encryption effect outperforms [10, 24].

5.2 Differential attack analysis

To quantitatively measure the difference between two images of the same size, Number of Pixels Change Rate (NPCR) and Unified Average Changing Intensity (UACI) can be performed.

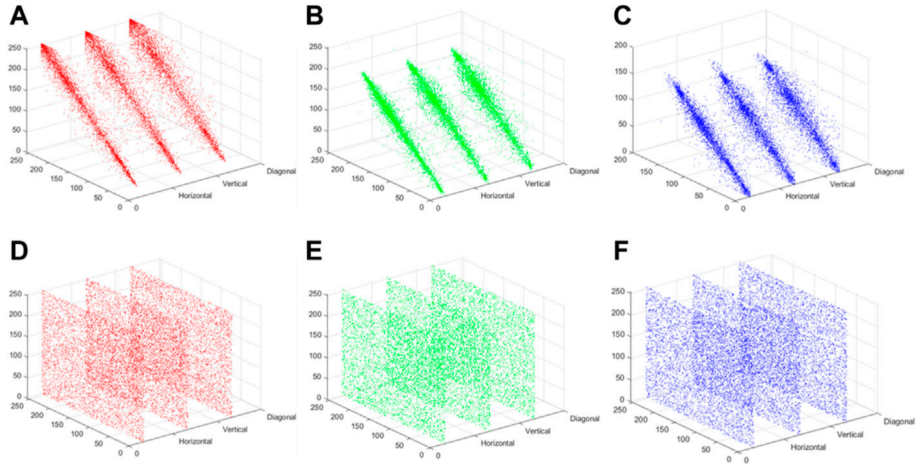


FIGURE 16
Correlation distribution of two adjacent horizontal, vertical and diagonal pixels of "Girls": **(A)** R channel, **(B)** G channel, **(C)** B channel; Correlation distribution of two adjacent horizontal, vertical and diagonal pixels of encryption "Girls": **(D)** R channel, **(E)** G channel, **(F)** B channel.

$$\begin{cases} \text{NPCR} = \sum_{j=1}^{N}\sum_{i=1}^{M}\frac{D(i,j)}{M\times N}\times 100\% \\ \text{UACI} = \sum_{j=1}^{N}\sum_{i=1}^{M}\frac{|c_1(i,j)-c_2(i,j)|}{M\times N\times 255}\times 100\% \end{cases}. \tag{45}$$

Besides NPCR and UACI, Block Average Changing Intensity (BACI) can also measure the difference between two random images.

$$\text{BACI} = \frac{1}{(M-1)(N-1)}\sum_{i=1}^{(M-1)(N-1)}\frac{m_i}{255}. \tag{46}$$

If the NPCR of the two images is 100%, and the UACI is close to the theoretical value, but the visual effects of the two images are similar, it indicates that NPCR and UACI are still insufficient in describing the differences between the two images, and BACI makes up for this deficiency. The theoretical value of BACI is 26.7712%. From Table 5, NPCR, UACI and BACI are all close to the theoretical values. Therefore, the proposed encryption scheme is very sensitive to any small changes of the pixel of plaintext image.

5.3 Key space analysis

The key space of the image cryptosystem should be large enough to resist brute force attack effectively. The key space should be at least 2^{128}. In the proposed scheme, the key space contains the parameters of quantum dual-scale triangular map, the initial values of the MSMFrLVS and the hash value of plaintext image. The key space of quantum dual-scale triangular map is estimated to be 10^8. The precision of the initial values of the MSMFrLVS is 10^{15}, the total key space is $10^8 + 10^{15\times 4} + 2^{256}$. Therefore, the key space of the proposed algorithm is large enough to resist the brute-force attack.

5.4 Key sensitivity analysis

A good image encryption system should have strong key sensitivity. To be more precise, the key sensitivity of the system is evaluated by the mean-squared error (MSE).

$$\text{MSE} = \frac{1}{M\times N}\sum_{x=1}^{M}\sum_{y=1}^{N}[D(x,y)-I(x,y)]^2, \tag{47}$$

where $M\times N$ denotes the image size, $D(x,y)$ and $I(x,y)$ represents the pixel values of decryption image and plaintext image at the position (x,y), respectively. Figures 17B–E show the MSE curves with wrong keys $x_0 + 10^{-14}$, $y_0 + 10^{-14}$, $z_0 + 10^{-14}$ and $w_0 + 10^{-14}$, respectively. As can be seen from Figure 17, the ciphertext images obtained under the condition of minor changes of the keys are quite different. Since the keys are randomly selected from the key space, it can be explained that each key in the key space is valid and sensitive.

5.5 Shear attack analysis

In addition to the noise attack, the ciphertext image is also susceptible to malicious cutting by the attacker during the process of transmission and processing, therefore it is necessary to analyze the anti-clipping ability of the proposed algorithm. Figure 18 shows the ciphertext images of different

TABLE 3 Correlation coefficients of adjacent pixels.

Correlation coefficient		Horizontal	Vertical	Diagonal
Plaintext Barbara		0.9803	0.9806	0.9591
Ciphertext Barbara		0.0079	−0.0087	−0.0035
Plaintext Arnav		0.9844	0.9837	0.9730
Ciphertext Arnav		0.0097	0.0100	−0.0138
Plaintext Baboon		0.9763	0.9356	0.9435
Ciphertext Baboon		0.0053	0.0059	0.0043
Plaintext Bridge		0.9786	0.9442	0.9624
Ciphertext Bridge		0.0023	0.0045	0.0026
	R channel	0.9678	0.9494	0.9304
Plaintext Girls	G channel	0.9456	0.9247	0.8827
	B channel	0.9162	0.8944	0.8352
	R channel	−0.0093	−0.0303	−0.0049
Ciphertext Girls	G channel	−0.0177	−0.0203	0.0057
	B channel	−0.0155	0.0052	−0.0117
Plaintext Sailboat	R channel	0.9356	0.9869	0.9364
	G channel	0.9468	0.9576	0.9567
	B channel	0.9256	0.9564	0.8967
	R channel	−0.0053	0.0134	0.0036
Ciphertext Sailboat	G channel	0.0054	−0.0023	0.0054
	B channel	−0.0034	0.0098	−0.0068
Reference [10]		−0.0423	0.0202	−0.0212
Reference [24]		0.0295	0.0187	0.0393

TABLE 4 Information entropy.

Images		Plaintext image (bit)	Ciphertext image (bit)
Barbara		7.6578	7.9996
Arnav		7.4914	7.9973
Baboon		7.4465	7.9985
Bridge		7.2645	7.9976
Lake		7.6548	7.9992
	R channel	7.7771	7.9975
Girls	G channel	7.5523	7.9981
	B channel	7.2687	7.9975
	R channel	7.6782	7.9968
Sailboat	G channel	7.6485	7.9978
	B channel	7.4356	7.9986
	R channel	7.6897	7.9991
Goldhill	G channel	7.8562	7.9981
	B channel	7.7568	7.9985
Reference [10]		7.1273	7.9970
Reference [24]		7.0097	7.9970

clipping regions and their corresponding decryption images. From Figure 18, the resolution of decryption images varies with the cutting degree of ciphertext images, but the crucial information of the decryption images can still be identified. Therefore, the proposed encryption algorithm has a certain ability to resist the shear attack.

TABLE 5 NPCR, UACI and BACI.

Image		NPCR%	UACI%	BACI%
Barbara		99.6090	33.4476	26.7930
Arnav		99.5820	33.3371	26.6211
Baboon		99.6032	33.4562	26.7568
Bridge		99.5962	33.3685	26.6238
Lake		99.5658	33.3456	26.8664
Girls	R channel	99.6237	33.4665	26.8179
	G channel	99.6538	33.3546	26.7534
	B channel	99.5456	33.1562	26.6481
Sailboat	R channel	99.6023	33.4356	26.5562
	G channel	99.6548	33.3346	26.7652
	B channel	99.5964	33.3450	26.6724
Goldhill	R channel	99.6432	33.3315	26.6482
	G channel	99.6023	33.3725	26.7315
	B channel	99.6130	33.4456	26.6856

5.6 Computational complexity

Assume that I is an $M \times N$ image, and N is greater than M. The computational complexity of the proposed quantum image encryption algorithm primarily depends on quantum dual-scale triangular map, the intra bit-planes permutation and quantum XOR operation. In the block-level permutation stage, the basic gates of ADDER-MOD2^n are $28n - 12$ and the complexity of the ADDER-MOD2^n is about $140n$ [1]. Hence, the computational complexity of quantum dual-scale triangular map is $O(n)$. In addition, the intra bit-planes permutation involves four quantum swap gates, and each swap gate is achieved by three C-NOT gates, thus the intra bit-planes permutation is realized by $12n$ basic gates, the computational complexity of the intra bit-planes permutation is $O(n)$. What's more, the quantum XOR operation needs $8n - 16$ Toffoli gates [36], and each Toffoli gate is composed of six C-NOT gates, thus the quantum XOR operation involves $384n - 768$ basic gates, and the computational complexity of the quantum XOR operation is $O(n)$. Consequently, the computational complexity of the proposed quantum algorithm is $O(n)$, while the computational complexity of the corresponding classical image encryption scheme is $O(2^{2n})$. Obviously, the proposed quantum image encryption algorithm is better than its classical counterparts in terms of computational complexity.

5.7 Noise attack analysis

Assume that the ciphertext image "Arnav" is added with the Gaussian noise.

$$C' = C + kG, \tag{48}$$

where C' and C are the noisy ciphertext images and the noise-free ciphertext images, k represents noise intensity, G is the Gaussian noise with zero mean and unit standard deviation. Figure 19A shows

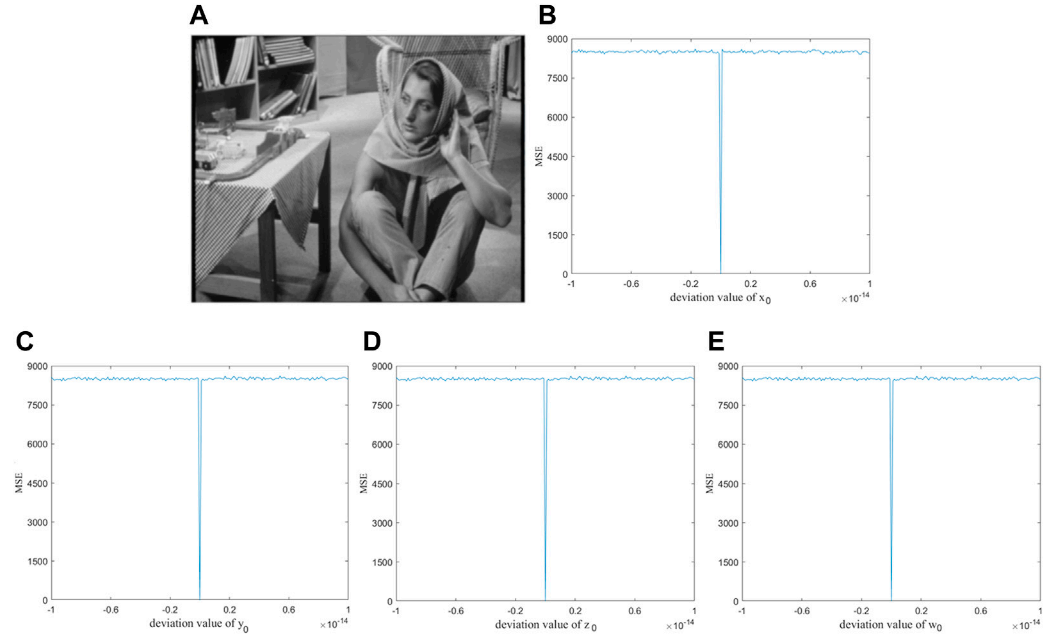


FIGURE 17
(A) Plaintext image, MSE curves: **(B)** x_0, **(C)** y_0, **(D)** z_0, **(E)** w_0.

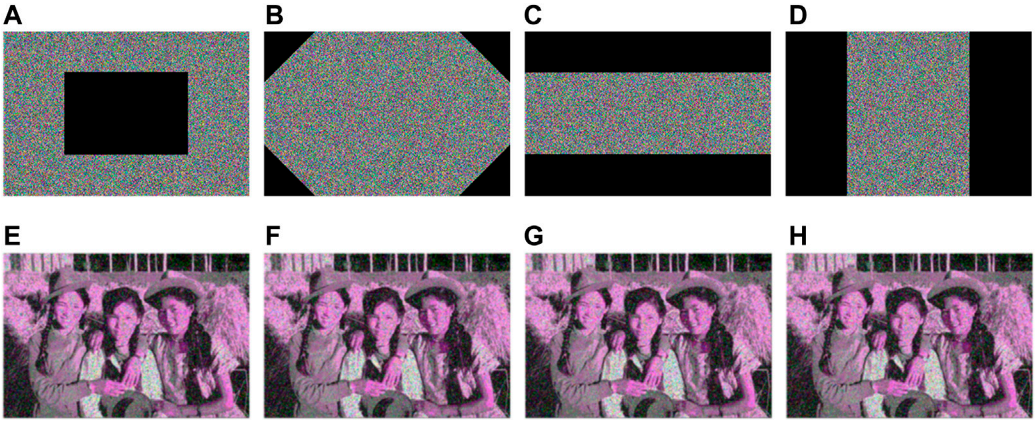


FIGURE 18
Sheared images in different position: **(A–D)**, the corresponding decryption images: **(E–H)**.

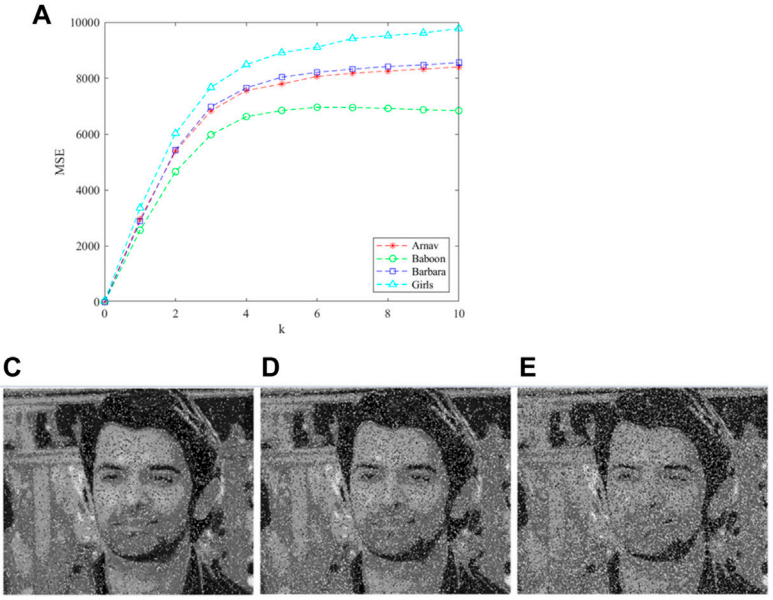


FIGURE 19
Results of noise attack: **(A)** MSE curve, noise intensities: **(B)** $k = 2$, **(C)** $k = 4$, **(D)** $k = 6$, **(E)** $k = 8$.

the MSE curves with different noise intensities, Figures 19B–E give the decryption images with noise intensities 2, 4, 6 and 8. From Figure 19, with the increase of noise intensity, decryption images become more and more blurred, but the outline of decryption images can still be seen clearly, the proposed image encryption scheme can resist the noise attack to some degree.

5.8 Encryption time analysis

The length of the execution time is an index to evaluate the quality of an encryption algorithm. The execution time of the proposed algorithm and Refs. [9, 12, 16, 17] are listed in Table 6. In [9, 16, 17], the pseudo-random sequences are originated by iterating the 4D hyper-chaotic Henon map, 2D logistic map and 3D chaotic system, respectively, which take too much time. In [12], the encryption process is time-consuming owing to the

TABLE 6 Encryption and decryption time in second.

Time(s)	Proposed scheme	[9]	[12]	[16]	[17]
Encryption time	0.9235	1.2540	1.2230	1.9450	1.9123
Decryption time	0.9582	2.3540	1.1958	2.2895	2.0012

fractional-order Lorenz-like chaotic system. In our algorithm, the initial point of the MSMFrLVS is variable such that the algorithm can save the encryption time greatly, thus the proposed image encryption algorithm can be developed for fast image encryption.

6 Conclusion

The quantum image encryption scheme is proposed by combining the MSMFrLVS with the quantum dual-scale triangular map. The block-level permutation, intra and inter bit-plane permutations, and three-level diffusion operations are used to implement the encryption process. The independent parameters of quantum dual-scale triangular map, the initial values and the control parameters of the MSMFrLVS and the hash value of plaintext image consist of the keys of the proposed quantum image encryption algorithm. As a result, the encryption system's key space is sufficiently large. Numerical simulation analyses demonstrate the proposed algorithm's reliability and effectiveness, and it requires less computation time. Furthermore, the proposed image encryption algorithm has lower computational complexity than its conventional counterparts. In the future, we will focus on combining quantum image encryption with semi-quantum cryptography protocols [37] in order to propose an algorithm with improved security and quantum communication capacity.

Data availability statement

The original contributions presented in the study are included in the article/supplementary material, further inquiries can be directed to the corresponding author.

Author contributions

YM: Conceptualization, methodology, investigation; F-FY: Formal analysis, writing—original draft; L-HG: Validation, writing- reviewing and editing; W-PZ: Conceptualization, funding acquisition, resources, supervision, writing—review and editing.

Funding

This work is supported by the National Natural Science Foundation of China (Grant No. 61861029), the Top Double 1000 Talent Programme of Jiangxi Province (Grant No. JXSQ2019201055).

Conflict of interest

The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Publisher's note

All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers. Any product that may be evaluated in this article, or claim that may be made by its manufacturer, is not guaranteed or endorsed by the publisher.

References

1. Zhou NR, Hua TX, Gong LH, Pei DJ, Liao QH. Quantum image encryption based on generalized Arnold transform and double random-phase encoding. *Quan Inf Process* (2015) 14(4):1193–213. doi:10.1007/s11128-015-0926-z

2. Malik A, Dhall S, Gupta S. An improved bit plane image encryption technique using RC4 and quantum chaotic demeanour. *Multimed Tools Appl* (2020) 80(5): 7911–37. doi:10.1007/s11042-020-09973-5

3. Zhu HH, Chen XB, Yang YX. A multimode quantum image representation and its encryption scheme. *Quan Inf Process* (2021) 20(9):315. doi:10.1007/s11128-021-03255-1

4. Zhang JL, Huang ZJ, Li X, Wu MQ, Wang XY, Dong YM. Quantum image encryption based on quantum image decomposition. *Int J Theor Phys (Dordr)* (2021) 60(8):2930–42. doi:10.1007/s10773-021-04862-5

5. Wang L, Ran QW, Ma J. Double quantum color images encryption scheme based on DQRCI. *Multimed Tools Appl* (2020) 79(9-10):6661–87. doi:10.1007/s11042-019-08514-z

6. Vagish KD, Rajakumaran C, Kavitha R. Chaos based encryption of quantum images. *Multimed Tools Appl* (2020) 79(33-34):23849–60. doi:10.1007/s11042-020-09043-w

7. Zhou NR, Huang LX, Gong LH, Zeng QW. Novel quantum image compression and encryption algorithm based on DQWT and 3D hyper-chaotic Henon map. *Quan Inf Process* (2020) 19(9):284. doi:10.1007/s11128-020-02794-3

8. Wang Y, Chen LQ, Yu KL, Gao Y, Ma Y. An image encryption scheme based on logistic quantum chaos. *Entropy* (2022) 24(2):251. doi:10.3390/e24020251

9. Dai JY, Ma Y, Zhou NR. Quantum multi-image compression-encryption scheme based on quantum discrete cosine transform and 4D hyper-chaotic Henon map. *Quan Inf Process* (2021) 20(7):246. doi:10.1007/s11128-021-03187-w

10. Zhou NR, Chen WW, Yan XY, Wang YQ. Bit-level quantum color image encryption scheme with quantum cross-exchange operation and hyper-chaotic system. *Quan Inf Process* (2018) 17(6):137. doi:10.1007/s11128-018-1902-1

11. Ye GD, Jiao KX, Huang XL, Goi BM, Yap WS. An image encryption scheme based on public key cryptosystem and quantum logistic map. *Sci Rep* (2020) 10(1): 21044. doi:10.1038/s41598-020-78127-2

12. Khan M, Rasheed A. A fast quantum image encryption algorithm based on affine transform and fractional-order Lorenz-like chaotic dynamical system. *Quan Inf Process* (2022) 21(4):134. doi:10.1007/s11128-022-03474-0

13. Signing VRF, Tegue GAG, Kountchou M, Njitacke ZT, Tsafack N, Nkapkop JDD, et al. A cryptosystem based on a chameleon chaotic system and dynamic DNA coding. *Chaos Solitons Fractals* (2022) 155:111777. doi:10.1016/j.chaos.2021.111777

14. Wang XY, Su YN, Luo C, Nian FZ, Teng L. Color image encryption algorithm based on hyperchaotic system and improved quantum revolving gate. *Multimed Tools Appl* (2022) 81(10):13845–65. doi:10.1007/s11042-022-12220-8

15. Li CM, Yang XZ. An image encryption algorithm based on discrete fractional wavelet transform and quantum chaos. *Optik* (2022) 260:169042. doi:10.1016/j.ijleo.2022.169042

16. Wu WQ, Wang Q. Quantum image encryption based on Baker map and 2D logistic map. *Int J Theor Phys (Dordr)* (2022) 61(3):64. doi:10.1007/s10773-022-04979-1

17. Hu WB, Dong YM. Quantum color image encryption based on a novel 3D chaotic system. *J Appl Phys* (2022) 131(11):114402. doi:10.1063/5.0084611

18. Kamran MI, Khan MA, Alsuhibany SA, Ghadi YY, Arshad AJ, Ahmad J, et al. A highly secured image encryption scheme using quantum walk and chaos. *Comput Mater Contin* (2022) 73(1):657–72. doi:10.32604/cmc.2022.028876

19. Alhumyani H, El-Banby GM, El-Sayed HS, El-Samie F, Faragallah OS. Efficient generation of cancelable face templates based on quantum image Hilbert permutation. *Electronics* (2022) 11(7):1040. doi:10.3390/electronics11071040

20. Zhong HY, Li GD. Multi-image encryption algorithm based on wavelet transform and 3D shuffling scrambling. *Multimed Tools Appl* (2022) 81:24757–76. doi:10.1007/s11042-022-12479-x

21. Chen C, Zhang HY, Wu B. Image encryption based on arnod transform and fractional chaotic. *Symmetry (Basel)* (2022) 14(1):174. doi:10.3390/sym14010174

22. Hu WW, Zhou RG, Luo J, Jiang SX, Luo GF. Quantum image encryption algorithm based on Arnold scrambling and wavelet transforms. *Quan Inf Process* (2020) 19(3):82. doi:10.1007/s11128-020-2579-9

23. Liu H, Zhao B, Huang L. Quantum image encryption scheme using Arnold transform and S-box scrambling. *Entropy* (2019) 21(4):343. doi:10.3390/e21040343

24. Liu XB, Xiao D, Huang W, Liu C. Quantum block image encryption based on Arnold transform and sine chaotification model. *IEEE Access* (2019) 7:57188–99. doi:10.1109/ACCESS.2019.2914184

25. Zhou NR, Yan XY, Liang HR, Tao XY, Li GY. Multi-image encryption scheme based on quantum 3D Arnold transform and scaled Zhongtang chaotic system. *Quan Inf Process* (2018) 17(12):338. doi:10.1007/s11128-018-2104-6

26. Zhou RG, Liu X, Luo J. Quantum circuit realization of the bilinear interpolation method for GQIR. *Int J Theor Phys (Dordr)* (2017) 56(9):2966–80. doi:10.1007/s10773-017-3463-y

27. Li Y, Chen YQ, Podlubny I. Stability of fractional-order nonlinear dynamic systems: Lyapunov direct method and generalized Mittag-Leffler stability. *Comput Math Appl* (2010) 59(5):1810–21. doi:10.1016/j.camwa.2009.08.019

28. Wu GC, Deng ZG, Baleanu D, Zeng DQ. New variable-order fractional chaotic systems for fast image encryption. *Chaos* (2019) 29(8):083103. doi:10.1063/1.5096645

29. Agrawal SK, Srivastava M, Das S. Synchronization between fractional-order ravinovich-fabrikant and lotka-volterra systems. *Nonlinear Dyn* (2012) 69(4):2277–88. doi:10.1007/s11071-012-0426-y

30. El-Latif AAA, Abd-El-Atty B, Talha M. Robust encryption of quantum medical images. *IEEE Access* (2018) 6:1073–81. doi:10.1109/ACCESS.2017.2777869

31. Li PS, Zheng Q, Hong JG, Xing CH. 2D triangular mappings and their applications in scrambling rectangle image. *Inf Tech J* (2008) 7(1):40–7. doi:10.3923/itj.2008.40.47

32. Jiang N, Wang L. Analysis and improvement of the quantum Arnold image scrambling. *Quan Inf Process* (2014) 13(7):1545–51. doi:10.1007/s11128-014-0749-3

33. University of Southern California. Signal and Image Processing Institute. USC-SIPI Image Database (1997) Available at: http://sipi.usc.edu/database (Online Accessed March 15, 2021).

34. Rothe R, Timofte R, Gool LV. Deep expectation of real and apparent age from a single image without facial landmarks. *Int J Comput Vis* (2018) 126(2):144–57. doi:10.1007/s11263-016-0940-3

35. Arbelaez P, Maire M, Fowlkes C, Malik J. Contour detection and hierarchical image segmentation. *IEEE Trans Pattern Anal Mach Intell* (2011) 33(5):898–916. doi:10.1109/TPAMI.2010161

36. Ralph TC, Resch KJ, Gilchrist A. Efficient Toffoli gates using qudits. *Phys Rev A (Coll Park)* (2007) 75(2):022313. doi:10.1103/PhysRevA.75.022313

37. Ye TY, Geng MJ, Xu TJ, Chen Y. Efficient semiquantum key distribution based on single photons in both polarization and spatial-mode degrees of freedom. *Quan Inf Process* (2021) 21(4):123. doi:10.1007/s11128-022-03457-1

frontiers | Frontiers in Physics

TYPE Original Research
PUBLISHED 18 October 2022
DOI 10.3389/fphy.2022.1028014

Quantum attacks on two-round even-mansour

BinBin Cai[1,2], Fei Gao[1] and Gregor Leander[3]*

[1]State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing, China, [2]Henan Key Laboratory of Network Cryptography Technology, Zhengzhou, China, [3]Ruhr University Bochum, Bochum, Germany

Check for updates

OPEN ACCESS

EDITED BY
Tianyu Ye,
Zhejiang Gongshang University, China

REVIEWED BY
Gang Xu,
North China University of Technology, China
Yefeng He,
Xi'an University of Posts and Telecommunications, China
Jun Zhu,
Guangxi Normal University, China

*CORRESPONDENCE
Gregor Leander,
gregor.leander@rub.de

SPECIALTY SECTION
This article was submitted to Quantum Engineering and Technology, a section of the journal Frontiers in Physics

RECEIVED 25 August 2022
ACCEPTED 20 September 2022
PUBLISHED 18 October 2022

CITATION
Cai B, Gao F and Leander G (2022), Quantum attacks on two-round even-mansour.
Front. Phys. 10:1028014.
doi: 10.3389/fphy.2022.1028014

Even-Mansour is one of the most important constructions in symmetric cryptography, both from a theoretical and practical perspective. With the rapid development of quantum computing, the security of Even-Mansour construction in quantum setting needs to be considered. For one round Even-Mansour construction, it is well settled by classical and quantum attacks. While for the iterated scheme, the situation is much more complex. In this paper, we study the next case in line in detail and depth: quantum attacks against two rounds case. We first make an asymptotic comparison with existing classical and quantum attacks. Then we give concrete resource estimation for the proposed quantum attacks on round reduced LED cipher and AES^2. The resource estimation allows to deduce the most efficient attacks based on the trade-off of the number of qubits and Toffoli depth.

KEYWORDS

even-mansour, grover algorithm, grover-meets-simon algorithm, offline simon algorithm, resource estimation

1 Introduction

The Even-Mansour (EM) construction [1] is a minimal block cipher that has been widely studied since its outstanding simplicity and provable classical security [1, 2]. It is made up of a n-bit public permutation P and two n-bit secret subkeys K_1 and K_2, *i.e.*, $E(x) = P(x \oplus K_1) \oplus K_2$, where n is the block size. When P is a public random permutation, EM construction has been proven to be indistinguishable from a random permutation when $D \cdot T = \Omega(2^n)$, where D and T are the number of queries to the encryption oracle $E(x)$ and permutation oracle P respectively. At EUROCRYPT 2012, Bogdanov *et al.* [3] studied EM construction into an r-round iterated EM scheme, which is defined as

$$E(x) = P_r(\cdots P_2(P_1(x \oplus K_1) \oplus K_2) \oplus K_3 \cdots \oplus K_r) \oplus K_{r+1},$$

where $P_1, \ldots, P_r$ are r independent permutations and $K_1, \ldots, K_{r+1}$ are $(r+1)$ n-bit subkeys. This construction was proven to be secure up to $2^{2n/3}$ queries against distinguishing attack for $r \geq 2$ [3] and subsequently improved to $2^{rn/(r+1)}$ queries [4, 5].

Recently, the security analysis of symmetric cryptography in quantum setting has also become a hot issue in cryptography research [6], in addition to quantum cryptography [7–10]. There are two different models for quantum cryptanalysis against symmetric cipher based on the notions for pseudorandom function security in quantum setting, standard security and quantum security [11]. The standard security and quantum security are also denoted as Q1 model and Q2 model respectively by Kaplan *et al.* [12]. In Q1 model, the adversaries could only access the encryption oracle classically but process data with quantum operations. While in Q2 model, the adversaries could query the encryption oracle with quantum superpositions and process data with quantum operations.

In 2012, Kuwakado and Morri [13] proposed a quantum key-recovery attack against EM construction in Q2 model. Compared with the classical key-recovery attack, the quantum attack can attain exponential acceleration. In other words, the EM construction has been broken in Q2 model. Very recently, at EUROCRYPT 2022, Alagic *et al.* [14] proved a lower bound that $\approx 2^{n/3}$ queries are necessary for attacking EM construction in Q1 model. In 2014, Kaplan [15] gave the quantum meet-in-the-middle attack (QMITM attack) against iterated block ciphers in Q1 model. For two-round iterated EM (2EM) construction with two alternating subkeys and 2EM construction with independent subkeys, the attack requires the time and memory complexities of $\mathcal{O}(2^n)$ and $\Omega(2^n)$ quantum queries to permutation oracle to recover all subkeys. However, the QMITM attack which reduces key-recovery to claw finding problem [16] is a general attack that may not be as effective for 2EM constructions. Therefore, we aim at investigating more efficient quantum key-recovery attacks on 2EM constructions in this paper. The constructions we focused on are 2EM construction with identical subkeys, 2EM construction with two alternating subkeys and 2EM construction with independent subkeys which we refer as

$$\begin{aligned}
\mathbf{2EM_1}&:\quad E_1(x) = P_2(P_1(x \oplus K) \oplus K) \oplus K,\\
\mathbf{2EM_2}&:\quad E_2(x) = P_2(P_1(x \oplus K_1) \oplus K_2) \oplus K_1,\\
\mathbf{2EM_3}&:\quad E_3(x) = P_2(P_1(x \oplus K_1) \oplus K_2) \oplus K_3.
\end{aligned}$$

At FSE 2013, Nikolić *et al.* [17] proposed the first nontrivial classical attack on $2\mathrm{EM}_1$ construction which requires the time complexity of $2^n \ln n/n$ with $2^n \ln n/n$ known plaintexts. Later, Dinur *et al.* [18] improved this attack to reduce the data complexity to $2^{\lambda n}$ known plaintexts, where $0 < \lambda < 1$. Meanwhile, they also presented an attack against $2\mathrm{EM}_3$ construction with the time complexity of $\mathcal{O}(2^n \sqrt{\ln n/n})$ and $2^n \sqrt{\ln n/n}$ chosen plaintexts. However, the above attacks against $2\mathrm{EM}_1$ construction are based on multi-collisions techniques, which require time and memory complexities close to 2^n. In 2016, Dinur *et al.* [19] presented an alternative attack on $2\mathrm{EM}_1$ construction with linear algebra techniques. This attack requires a time complexity of $2^n/\lambda n$ and memory complexity of $2^{\lambda n}$, but with $2^n/\lambda n$ chosen plaintexts. Subsequently, Isobe *et al.* [20] introduced meet-in-the-middle techniques into the attack against $2\mathrm{EM}_1$ construction which requires the time and memory complexities of $2^n \ln n/n$ with $2^n \ln n/n$ chosen plaintexts. Furthermore, they also described a low data-complexity and a time-optimized variant attacks. The low data-complexity attack requires the time and memory complexities of $2^n \ln n/n$ with $2^{\lambda n}$ chosen plaintexts. The time-optimized one requires the time complexity of $2^n\beta/n$ and memory complexity of $2^n/2^\beta$ with $2^n\beta/n$ chosen plaintexts, where $\log n \le \beta \lll n$. More recently, Leurent *et al.* [21] proposed three key-recovery attacks on $2\mathrm{EM}_1$ construction which are related to the 3-XOR problem. The basic attack requires the time complexity of $2^n/n$ and memory complexity of $2^{2n/3}$ with $2^{2n/3}$ known plaintexts in a balanced case. The variant attack based on 3-SUM algorithm requires the time complexity of $2^n \ln^2 n/n^2$ and memory complexity of $2^{2n/3}$ with $2^{2n/3}$ known plaintexts, but it is unpractical for realistic block size. The low data-complexity attack requires the time complexity of $2^n/\lambda n$ and memory complexity of $2^{\lambda n}$ with λn known plaintexts.

Besides, there are also other quantum attacks against iterated EM construction such as the quantum slide attack on iterated EM construction with identical permutations and subkeys in Q2 model [12] and the quantum related-key attack against iterated EM cipher with identical permutations and independent subkeys in Q2 model [22]. However, these

TABLE 1 Comparison of previous quantum attacks and our attacks on $2\mathrm{EM}_2$ and $2\mathrm{EM}_3$ constructions, where "Data" represents encryption queries, "Queries" signifies calls to P_i, "Q-memory" and "C-memory" denote quantum memory and classical memory respectively.

Target	Model	Data	Queries	Time	Q-memory	C-memory	References
$2\mathrm{EM}_2$	Q2	$\mathcal{O}(2^n)$	0	$\mathcal{O}(2^n)$	$\mathcal{O}(n)$	0	[23]
	Q1	$\mathcal{O}(1)$	$\Omega(2^n)$	$\mathcal{O}(2^n)$	$\mathcal{O}(n)$	$\mathcal{O}(2^n)$	[15]
	Q2	$\mathcal{O}(n\cdot 2^{n/2})$	$\mathcal{O}(n\cdot 2^{n/2})$	$\mathcal{O}(n^3\cdot 2^{n/2})$	$\mathcal{O}(n^2)$	0	Section 3.2
	Q2	$\mathcal{O}(n)$	$\mathcal{O}(n\cdot 2^{n/2})$	$\mathcal{O}(n^3\cdot 2^{n/2})$	$\mathcal{O}(n^2)$	$\mathcal{O}(n)$	Section 3.2
	Q1	$\mathcal{O}(2^{2n/3})$	$\mathcal{O}(n\cdot 2^{2n/3})$	$\mathcal{O}(n^3\cdot 2^{2n/3})$	$\mathcal{O}(n^2)$	$\mathcal{O}(n)$	Section 3.2
$2\mathrm{EM}_3$	Q2	$\mathcal{O}(2^{3n/2})$	0	$\mathcal{O}(2^{3n/2})$	$\mathcal{O}(n)$	0	[23]
	Q1	$\mathcal{O}(1)$	$\Omega(2^n)$	$\mathcal{O}(2^n)$	$\mathcal{O}(n)$	$\mathcal{O}(2^n)$	[15]
	Q2	$\mathcal{O}(n\cdot 2^{n/2})$	$\mathcal{O}(n\cdot 2^{n/2})$	$\mathcal{O}(n^3\cdot 2^{n/2})$	$\mathcal{O}(n^2)$	0	Section 3.2
	Q2	$\mathcal{O}(n)$	$\mathcal{O}(n\cdot 2^{n/2})$	$\mathcal{O}(n^3\cdot 2^{n/2})$	$\mathcal{O}(n^2)$	$\mathcal{O}(n)$	Section 3.2
	Q1	$\mathcal{O}(2^{2n/3})$	$\mathcal{O}(n\cdot 2^{2n/3})$	$\mathcal{O}(n^3\cdot 2^{2n/3})$	$\mathcal{O}(n^2)$	$\mathcal{O}(n)$	Section 3.2

TABLE 2 Comparison of attacks against 2-step LED-64. Assume that one evaluation of the cipher as one complexity unit and the evaluation of one permutation costs 1/2 unit.

Data	Queries	Time	Memory	References
$2^{58.7}$	$2^{60.5}$	$2^{60.9}$	2^{60}	[17]
2^{45}	$2^{60.7}$	$2^{60.7}$	2^{60}	[18] ($\lambda = 0.7$)
2^{60}	2^{59}	$2^{60.6}$	2^{16}	[19] ($\lambda = 1/4$)
2^{60}	2^{60}	$2^{61.3}$	2^{60}	[20]
2^{8}	2^{62}	$2^{62.6}$	2^{62}	[20]
2^{61}	2^{57}	$2^{61.7}$	2^{58}	[20] ($\beta = 8$)
2^{42}	2^{43}	2^{58}	2^{42}	[21]
2^{42}	2^{43}	$2^{56.1}$	2^{42}	[21]
2^{4}	2^{60}	2^{61}	2^{16}	[21] ($\lambda = 1/4$)
2^{32}	0	2^{32}	2^{6} qubits	Section 3.1

TABLE 3 Comparison of quantum attacks against 2-step LED-128.

Model	Data	Queries	Time	Q-memory	C-memory	References
Q2	2^{64}	0	2^{64}	2^{7}	0	[23]
Q1	1	2^{64}	2^{64}	2^{7}	2^{64}	[15]
Q2	2^{39}	2^{39}	2^{50}	2^{12}	0	Section 3.2
Q2	2^{6}	2^{38}	2^{50}	2^{12}	2^{6}	Section 3.2
Q1	2^{47}	$2^{46.5}$	$2^{58.5}$	2^{12}	2^{6}	Section 3.2

quantum attacks are in Q2 model and only consider iterated EM construction with identical permutations.

Contributions. in this paper, we study quantum key-recovery attacks against 2EM constructions. The main contributions of this paper include the following two aspects.

First, we consider the security of two-round Even-Mansour constructions with independent permutations in quantum setting. Several quantum key-recovery attacks on 2EM constructions are proposed. For $2EM_1$ construction, the presented quantum key-recovery attack adopts Grover algorithm [23] directly. Compared with the classical attack with optimal query complexity (including the queries to cipher and permutation), *i.e.,* the observed by Leurent *et al.* [21], our attack reduces the query complexity by a factor of $2^{n/6}$. For $2EM_2$ and $2EM_3$ constructions, we consider Grover-meets-Simon algorithm [24] (GMS algorithm) and Offline Simon algorithm [25] (OS algorithm) on constructed functions. The proposed quantum attacks against $2EM_2$ and $2EM_3$ constructions require $\tilde{O}(2^{2n/3})$ and $\tilde{O}(2^{n/2})$ queries in Q1 and Q2 model, where $\tilde{O}$ means ignoring logarithmic factors. In the case of $2EM_2$ construction, the query complexity of our attacks is less than Grover search by a factor of $2^{n/3}$ and $2^{n/2}$ in Q1 and Q2 model respectively. In the case of $2EM_3$ construction, the query complexity of our attacks is better than Grover search by a factor of $2^{5n/6}$ and 2^{n} in Q1 and Q2 model. When compared with the QMITM attack against $2EM_2$ and $2EM_3$ constructions, the query complexity of our attacks is reduced by a factor of $2^{n/3}$ and $2^{n/2}$ in Q1 and Q2 model.

TABLE 4 Comparison of attacks against AES^{2}.

Model	Data	Queries	Time	Q-memory	C-memory	References
/	2^{128}	2^{129}	$2^{129.6}$	0	2^{128}	[3]
/	$2^{125.4}$	$2^{126.8}$	$2^{126.8}$	0	$2^{125.4}$	[18]
Q2	2^{192}	0	2^{192}	$2^{8.6}$	0	[23]
Q1	1	2^{128}	2^{128}	$2^{8.6}$	2^{128}	[15]
Q2	2^{72}	2^{72}	2^{85}	2^{14}	0	Section 3.2
Q2	2^{7}	2^{71}	2^{85}	2^{14}	2^{7}	Section 3.2
Q1	2^{90}	2^{90}	2^{104}	2^{14}	2^{7}	Section 3.2

TABLE 5 Resource estimation for constructed functions of target ciphers, where #Toffoli/CNOT/NOT represents the number of Toffoli gates, CNOT gates and NOT gates respectively.

	Algorithm	Model	Target cipher	Toffoli depth	#Toffoli	#CNOT	#NOT	width
$f(i, x)$	GMS	Q2	2-step LED-128	304	7296	9280	1536	352
$f(i, x)$	OS	Q1&Q2	2-step LED-128	304	4864	6080	1024	208
$f(i, x)$	GMS	Q2	AES^2	22016	66032	328656	3264	1820
$f(i, x)$	OS	Q1&Q2	AES^2	22016	33016	164072	1632	910

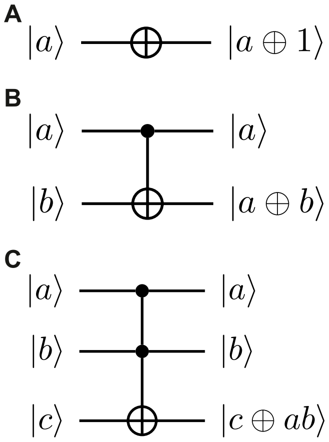


FIGURE 1
Quantum gates of **(A)** NOT gate, **(B)** CNOT gate and **(C)** Toffoli gate.

Besides, the classical memory complexity of our attacks can attain exponential acceleration compared with the QMITM attack on 2EM$_2$ and 2EM$_3$ constructions. It is worth noting that the presented quantum attacks could break 2EM$_3$ construction with $\mathcal{O}(n \cdot 2^{n/2})$ queries in Q2 model, which is less than the classical indistinguishable bound for 2EM$_3$ construction, *i.e.,* $2^{2n/3}$ queries. The comparison of previous quantum attacks and our attacks on 2EM$_2$ and 2EM$_3$ constructions is shown in Table 1.

Second, we apply the presented quantum attacks on 2-step LED-64, 2-step LED-128 and full AES^2. Then we design the quantum circuits for proposed attacks and give the corresponding resource estimation. According to the result of resource estimation, the cost imposed by the attacks based on GMS algorithm and attacks with OS algorithm in Q2 model is close. The extra overhead generated by the attacks based on GMS algorithm is mainly due to their more complex classifier oracles. Besides, the attacks based on OS algorithm in Q1 model cost more resources than corresponding attacks in Q2 model since the attacks in Q1 model require more iterations to search more bits exhaustively. Moreover, there is no doubt that the presented quantum attacks on 2-step LED-128 and AES^2 cost much less than the corresponding Grover attacks, except for the number of qubits.

Organization. The rest of the paper is organized as follows. In the next section, some essential preliminaries are introduced. The quantum attacks on 2EM constructions and their application to specific ciphers are presented in Sect. 3. In Sect. 4, we give the quantum resource estimation of the proposed quantum attacks on corresponding ciphers. Finally, a short conclusion is given in Sect. 5.

2 Preliminaries

In this section, some relevant preliminaries are given.

2.1 Quantum algorithms

2.1.1 Grover algorithm

Problem 1. (Grover [23]). Assume that there exists only one marked item x' in the N-scale unstructured datasets, the goal is to find x', *where* $N = 2^n$. *In other words, let* f: $\{0,1\}^n \rightarrow \{0, 1\}$ *be a function such that* $f(x) = 0$ *for all* $0 \leq x < 2^n$ *except* x', *for which* $f(x') = 1$, *find* x'.

To solve this problem, any deterministic classical algorithms need to make $\mathcal{O}(2^n)$ queries to $f(x)$. However, Grover algorithm can solve this problem with a probability close to 1 by performing Grover iteration about $\frac{\pi}{4}\sqrt{2^n}$ times. Therefore, the query complexity of Grover algorithm is $\mathcal{O}(\sqrt{2^n})$, which is a square speed-up compared to the classical counterpart. Furthermore, the generalization of Grover algorithm (*i.e.,* Quantum Amplitude Amplification, QAA) is given in the following theorem.

Theorem 1. (Brassard et al. [26]). Let $\mathcal{A}$ be any quantum algorithm performed on q qubits without *measurement. Let* $\mathcal{B}$: $\mathbb{F}_2^q \rightarrow \{0, 1\}$ *be a function that classifies the outcomes of* $\mathcal{A}$

as good or bad and $p > 0$ *be the initial success probability that a measurement of* $\mathcal{A}|0\rangle$ *is good. Set* $k = \lceil \frac{\pi}{4\theta} \rceil$, *where* θ *is defined as* $\sin^2(\theta) = p$. *Besides, define the unitary operator* $Q = -\mathcal{A}S_0\mathcal{A}^{-1}S_{\mathcal{B}}$, *where* $S_{\mathcal{B}}$ *changes the sign of the good state*

$$|x\rangle = \begin{cases} -|x\rangle, & \text{if } \mathcal{B}(x) = 1 \\ |x\rangle, & \text{if } \mathcal{B}(x) = 0 \end{cases},$$

while S_0 *changes the sign of zero state* $|0\rangle$ *only. Finally, the measurement after the operation of* $Q^k\mathcal{A}|0\rangle$ *will obtain the good state with probability at least* $\max\{1 - p, p\}$.

```
Step 1. Prepare the quantum state $|0^{\otimes n}\rangle$.
Step 2. Perform a Hadamard transform $H^{\otimes n}$ on the register:
        $|\psi\rangle = H^{\otimes n}|0^{\otimes n}\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle.$
Step 3. Construct the quantum oracle $O : |x\rangle \overset{O}{\to} (-1)^{f(x)}|x\rangle$, where $f(x) = 1$ if $x$ is the
        marked item, otherwise $f(x) = 0$.
Step 4. Apply Grover iteration for $R$ ($R \approx \frac{\pi}{4}\sqrt{2^n}$) times:
        $[(2|\psi\rangle\langle\psi| - I)O]^R|\psi\rangle \approx |x'\rangle.$
Step 5. Measure the register and obtain $x'$.
```

Algorithm 1. Grover algorithm [23]

2.1.2 Simon algorithm

Problem 2. (Simon [27]). Let *f*: $\{0,1\}^n \to \{0,1\}^n$ be a function. Promise that there exists $s \in \{0,1\}^n$ such that for any $(x, y) \in \{0,1\}^n$, $[f(x) = f(y)] \Leftrightarrow [x \oplus y \in \{0^n, s\}]$ *is satisfied. The goal is to find the period s.*

By performing Simon algorithm, one can obtain a random vector *y* such that $y \cdot s = 0$. Therefore, $(n - 1)$ independent vectors orthogonal to period *s* can be obtained by repeating Simon algorithm for $\mathcal{O}(n)$ times. Then one can recover the period *s* with linear algebra classically. Thus, the query complexity of Simon algorithm is $\mathcal{O}(n)$.

According to EM construction, Kuwakado and Morri [13] introduce the function $f(x) = E(x) \oplus P(x) = P(x \oplus K_1) \oplus K_2 \oplus P(x)$. It is obvious that $f(x) = f(x \oplus K_1)$ and the period *s* is K_1. Hence, they can recover the subkey K_1 with Simon algorithm and then obtain the value of K_2 easily.

2.1.3 Grover-meets-simon algorithm

Problem 3. (Leander et al. [24]). Let *f*: $\{0,1\}^m \times \{0,1\}^n \to \{0,1\}^\text{i}$ be a function, where *m* is in $\mathcal{O}(n)$. There exists a unique $i_0 \in \{0,1\}^\text{m}$ such that for any $x \in \{0,1\}^n$, $f(i_0, x) = f(i_0, x \oplus s)$ is satisfied, where $s \in \{0,1\}^n$. The goal is to find the unique i_0 and the period *s*.

The problem can be solved by GMS algorithm which requires the query complexity of $\mathcal{O}(n \cdot 2^{m/2})$ and time complexity of $\mathcal{O}(n^3 \cdot 2^{m/2})$.

At Asiacrypt 2017, Leander and May [24] proposed GMS algorithm to attack the FX construction [28] that $Enc(x) = E_{K_0}(x \oplus K_1) \oplus K_2$. They consider the function $f(k, x) = Enc(x) \oplus E_k(x) = E_{K_0}(x \oplus K_1) \oplus K_2 \oplus E_k(x)$. Obviously, the function $f(k, x)$ is periodic with period K_1 for all *x* when $k = K_0$. Otherwise $f(k, x)$ is not periodic. In such a case, they design the following GMS algorithm to recover all subkeys of FX construction.

2.1.4 Offline Simon algorithm

Problem 4. (Bonnetain et al. [25]). Let *f*: $\{0,1\}^m \times \{0,1\}^n \to \{0,1\}^l$ and *g*: $\{0,1\}^n \to \{0,1\}^\text{l}$ be functions, where *m* is in $\mathcal{O}(n)$. There exists a unique $i_0 \in \{0,1\}^m$ such that for any $x \in \{0,1\}^n$, $f(i_0, x) \oplus g(x) = f(i_0, x \oplus s) \oplus g(x \oplus s)$ is satisfied, where $s \in \{0,1\}^n$. The goal is to find the unique i_0 and the period *s*.

```
Step 1. Prepare the quantum state $|0^{\otimes n}\rangle|0^{\otimes n}\rangle$.
Step 2. Apply a Hadamard transform $H^{\otimes n}$ to the first register:
        $\frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle|0^{\otimes n}\rangle.$
Step 3. Apply a quantum query to the function $f$:
        $\frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle|f(x)\rangle.$
Step 4. Measure the second register and then the first register collapses to the state:
        $\frac{1}{\sqrt{2}}(|z\rangle + |z \oplus s\rangle).$
Step 5. Reapply a Hadamard transform $H^{\otimes n}$ to the first register:
        $\frac{1}{\sqrt{2}} \frac{1}{\sqrt{2^n}} \sum_{y \in \{0,1\}^n} (-1)^{y \cdot z}(1 + (-1)^{y \cdot s})|y\rangle.$
Step 6. Measure the first register and obtain $y$.
```

Algorithm 2. Simon algorithm [27]

To solve this problem, we can adopt OS algorithm. The OS algorithm requires $\mathcal{O}(n)$ quantum queries to *g*, $\mathcal{O}(n \cdot 2^{m/2})$ quantum queries to *f* and the time complexity of $\mathcal{O}(n^3 \cdot 2^{m/2})$.

Furthermore, we can also solve this problem with OS algorithm in Q1 model if the function *g* can be only queried classically. Concretely, it is similar to executing OS algorithm in Q2 model except that the quantum state $|\psi_g\rangle$ in steps 2 and 6 now should be prepared by querying the whole codebook of *g*. Hence, it requires $\mathcal{O}(2^n)$ classical queries to *g*, $\mathcal{O}(n \cdot 2^{m/2})$ quantum queries to *f* and the time complexity of $\mathcal{O}(n^3 \cdot 2^{m/2})$.

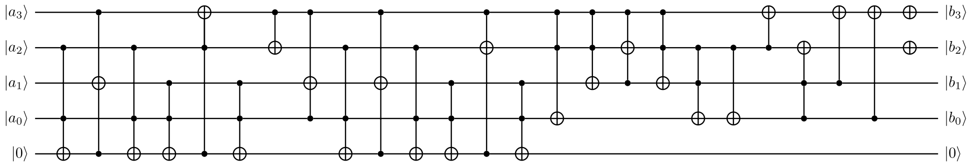


FIGURE 2
Quantum circuit of S-box used in SubCells: $|a\rangle|0\rangle \to |S(a)\rangle|0\rangle$, where $|a_3\rangle$ is the most significant qubit.

2.2 Target ciphers

Next, we introduce three ciphers that belong to 2EM_1, 2EM_2 and 2EM_3 constructions respectively.

2.2.1 LED

At CHES 2011, Guo *et al.* [29] proposed a 64-bit resource-constrained block cipher named LED. The step function F_i of LED is a 4-round AES-like permutation where the addition of the subkeys is replaced with addition of constants. There are two primary variants of LED.**LED − 64** uses a 64-bit key in each step as a subkey and the number of steps is 8. It is clear that 2-step LED-64 belongs to 2EM_1 construction.**LED − 128** divides a 128-bit key into $K_1 \| K_2$ as the subkeys alternatively and the number of steps is 12. Obviously, 2-step LED-128 belongs to 2EM_2 construction.

Algorithmic idea : apply Grover search over $i \in \{0,1\}^m$ and the classifier $\mathcal{B}$ identifies the periodicity of $f(i,\cdot)$ using Simon algorithm.

The quantum algorithm $\mathcal{A}$:

Step 1. Prepare the quantum state $|0^{\otimes m}\rangle|0^{\otimes \ell n}\rangle|0^{\otimes \ell l}\rangle$, where $\ell = \mathcal{O}(n)$.

Step 2. Apply Hadamard transforms $H^{\otimes(m+\ell n)}$ to the first $(m+\ell n)$ qubits:

$$\sum_{i\in\{0,1\}^m, x_1,\cdots,x_\ell\in\{0,1\}^n} |i\rangle|x_1\rangle\cdots|x_\ell\rangle|0^{\otimes \ell l}\rangle,$$

where the amplitude is omitted for ease of exposition.

Step 3. Perform quantum querise to f for i and each x:

$$\sum_{i\in\{0,1\}^m, x_1,\cdots,x_\ell\in\{0,1\}^n} |i\rangle|x_1\rangle\cdots|x_\ell\rangle|f(i,x_1) \| \cdots \| f(i,x_\ell)\rangle.$$

Step 4. Apply Hadamard transforms $H^{\otimes \ell n}$ to $|x_1\rangle\cdots|x_\ell\rangle$:

$$\sum_{i\in\{0,1\}^m, x_1,\cdots,x_\ell,u_1,\cdots,u_\ell\in\{0,1\}^n} |i\rangle(-1)^{u_1\cdot x_1}|u_1\rangle\cdots(-1)^{u_\ell\cdot x_\ell}|u_\ell\rangle|f(i,x_1) \| \cdots \| f(i,x_\ell)\rangle.$$

The classifier $\mathcal{B}$: $(i,u_1,\cdots,u_\ell) \in \{0,1\}^{m+\ell n} \to \{0,1\}$:

Test 1. If $\dim(\langle u_1,\cdots,u_\ell\rangle) \neq n-1$, output 0. Otherwise, use Lemma 2 of Ref. [24] to compute a candidate period $s' \in \{0,1\}^n$.

Test 2. For fixed i check whether $f(i,z) = f(i, z \oplus s')$ holds for some given z. If all identities hold, output 1. Otherwise, output 0.

Both Test 1 and Test 2 are satisfied, the classifier $\mathcal{B}$ outputs 1. Otherwise, output 0.

Algorithm 3. Grover-meets-Simon algorithm [24]

2.2.2 AES^2

AES^2 is a 128-bit cipher designed by Bogdanov et al. [3] at EUROCRYPT 2012. It belongs to 2EM_3 construction, where each of the public permutations P_1 and P_2 is based on an invocation of full AES-128 with a pre-fix and publicly known key. The subkeys are composed of three independently chosen 128-bit secret subkeys K_1, K_2 and K_3.

3 Quantum attacks

In this section, several quantum key-recovery attacks on 2EM_1, 2EM_2 and 2EM_3 constructions and the corresponding applications are given.

3.1 Quantum key-recovery Attack on 2EM_1 construction

Based on 2EM_1 construction, the function $E_1(x) = P_2(P_1(x \oplus K) \oplus K) \oplus K$ is obtained. In such a case, we adopt Grover algorithm on this function directly. Therefore, the query complexity and time complexity of this attack are both $\mathcal{O}(2^{n/2})$.

Step 1. Prepare the quantum state $\otimes^{cn}|0^{\otimes n}\rangle|0^{\otimes l}\rangle$, where c is a small constant.

Step 2. Perform Hadamard transforms $\otimes^{cn}H^{\otimes n}$ and cn quantum queries to g:

$$|\psi_g\rangle = \otimes^{cn}\left(\sum_{x\in\{0,1\}^n} |x\rangle|g(x)\rangle\right),$$

where the amplitude is ommitted for ease of exposition.

Step 3. Create the uniform superposition:

$$|\psi_g\rangle \otimes \sum_{i\in\{0,1\}^m} |i\rangle.$$

Step 4. Apply Grover iteration for $\mathcal{O}(2^{m/2})$ times, where the classifier in Grover iteration is to check whether $f(i,x) \oplus g(x)$ is periodic.

Step 5. Measure the register and obtain i_0.

Step 6. Apply Simon algorithm on $f(i_0,x) \oplus g(x)$ to obtain the period s.

Algorithm 4. Offline Simon algorithm [25]

3.1.1 The Application to 2-step LED-64

We can attack 2-step LED-64 by applying Grover algorithm on $E(x) = F_2(F_1(x \oplus K) \oplus K) \oplus K$ directly, where the block size is 64. Thus, the attack requires the query and time complexities of 2^{32}. The comparison of attacks against 2-step LED-64 is summarized in Table 2.

3.2 Quantum key-recovery Attacks on 2EM_2 and 2EM_3 constructions

For 2EM_2 construction, we consider the function

$$\begin{aligned} f(i,x) &= E_2(x) \oplus P_2(P_1(x) \oplus i) \\ &= P_2(P_1(x \oplus K_1) \oplus K_2) \oplus K_1 \oplus P_2(P_1(x) \oplus i). \end{aligned}$$

It is easily seen that $f(i, x)$ has the period K_1 when $i = K_2$ since

$$\begin{aligned} f(K_2, x \oplus K_1) &= P_2(P_1(x \oplus K_1 \oplus K_1) \oplus K_2) \oplus K_1 \oplus P_2(P_1(x \oplus K_1) \oplus K_2) \\ &= P_2(P_1(x) \oplus K_2) \oplus K_1 \oplus P_2(P_1(x \oplus K_1) \oplus K_2) \\ &= f(K_2, x). \end{aligned}$$

Therefore, we can employ GMS algorithm on $f(i, x)$ to recover K_1 and K_2 which requires the query complexity of $\mathcal{O}(n \cdot 2^{n/2})$ and time complexity of $\mathcal{O}(n^3 \cdot 2^{n/2})$.

Furthermore, the recovery of subkeys K_1 and K_2 can also be reduced to **Problem 4** by defining functions f: $\{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ and g: $\{0,1\}^n \to \{0,1\}^n$ as

$$\begin{aligned} f(i,x) &= P_2(P_1(x) \oplus i), \\ g(x) &= E_2(x). \end{aligned}$$

Similarly, we can obtain that

$$f(K_2, x \oplus K_1) \oplus g(x \oplus K_1) = f(K_2, x) \oplus g(x)$$

when $i = K_2$. Then we can recover all subkeys with OS algorithm. In such a case, the quantum attack requires $\mathcal{O}(n)$ queries to $g(x)$, $\mathcal{O}(n \cdot 2^{n/2})$ queries to $f(i, x)$ and the time complexity of $\mathcal{O}(n^3 \cdot 2^{n/2})$.

On the other hand, we can also solve this problem with OS algorithm in Q1 model if the cryptographic function $E_2(x)$

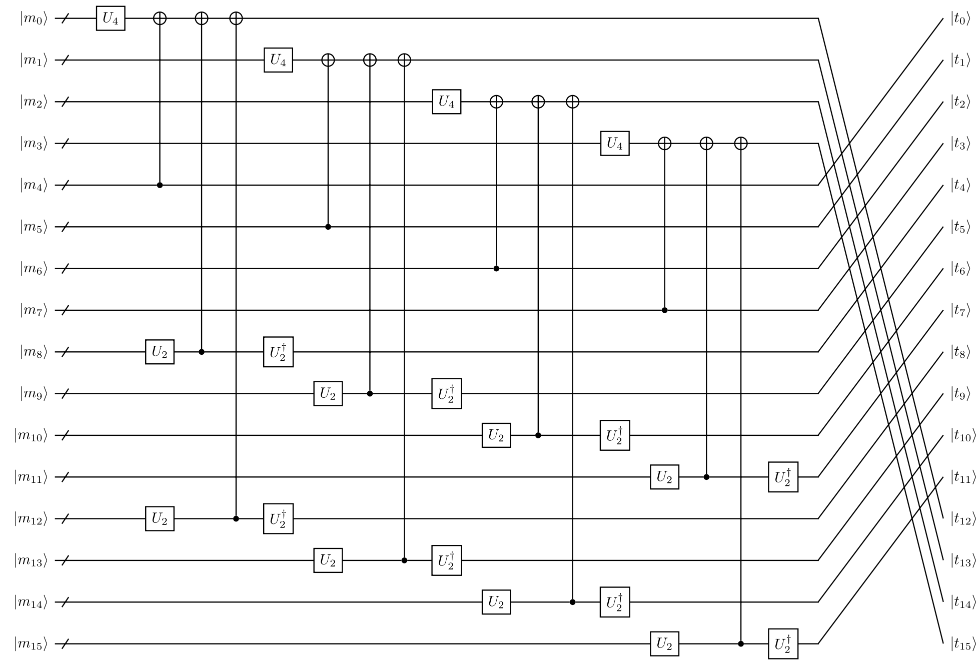


FIGURE 3
Quantum circuit of matrix A, where U_2 and U_4 are quantum circuits of operations 2 and 4 respectively. $U_2^\dagger$ represents the inverse quantum circuit of U_2. Each m_j and t_j contains four qubits, where j = 0, 1, . . . , 15.

can be accessed only classically. Now the functions f: $\{0,1\}^{n+(n-u)} \times \{0,1\}^u \rightarrow \{0,1\}^n$ $(0 \leq u \leq n)$ and g: $\{0,1\}^u \rightarrow \{0,1\}^n$ are defined as

$$\begin{aligned} &f(i\|j, x) = P_2(P_1(x\|j) \oplus i) \quad (j \in \{0,1\}^{n-u}),\\ &g(x) = E_2(x\|0^{n-u}). \end{aligned}$$

obviously, $f(K_2\|K_1^2, x) \oplus g(x)$ has the period K_1^1 when $i\|j = (K_2\|K_1^2, x \oplus K_1^1) \oplus g(x \oplus K_1^1) K_2\|K_1^2$ since

$$\begin{aligned} &f(K_2\|K_1^2, x \oplus K_1^1) \oplus g(x \oplus K_1^1)\\ &= P_2(P_1((x \oplus K_1^1)\|K_1^2) \oplus K_2) \oplus P_2(P_1((x \oplus K_1^1\|0^{n-u}) \oplus K_1) \oplus K_2) \oplus K_1\\ &= P_2(P_1((x\|0^{n-u}) \oplus K_1) \oplus K_2) \oplus P_2(P_1(x\|K_1^2) \oplus K_2) \oplus K_1\\ &= f(K_2\|K_1^2, x) \oplus g(x), \end{aligned}$$

where the subkey $K_1 = K_1^1\|K_1^2$ and $|K_1^1| = u$, $|K_1^2| = n - u$. Therefore, we can apply OS algorithm on above functions in Q1 model to recover subkeys K_1 and K_2. Then, the attack requires $\mathcal{O}(2^u)$ classical queries to $g(x)$, $\mathcal{O}(n \cdot 2^{(2n-u)/2})$ quantum queries to f $(i\|j, x)$ and the time complexity of $\mathcal{O}(n^3 \cdot 2^{(2n-u)/2})$. Specially, the number of classical queries to $g(x)$ and quantum queries to f $(i\|j, x)$ are balanced when $u = \frac{2n}{3}$.

The quantum key-recovery attack against 2EM$_3$ construction is similar to the case of 2EM$_2$ construction, except that the functions we considered here are

$$\begin{cases} f(i, x) = E_3(x) \oplus P_2(P_1(x) \oplus i), & \textbf{Problem 3}\\ f(i, x) = P_2(P_1(x) \oplus i), \;\; g(x) = E_3(x), & \textbf{Problem 4 in Q2 model}\\ f(i\|j, x) = P_2(P_1(x\|j) \oplus i), \;\; g(x) = E_3(x\|0^{n-u}), & \textbf{Problem 4 in Q1 model} \end{cases}.$$

Finally, we can easily obtain the value of K_3 with additional encryption after recovering subkeys K_1 and K_2. Hence, the query and time complexities of the quantum attacks on 2EM$_3$ construction are the same as the case of 2EM$_2$ construction.

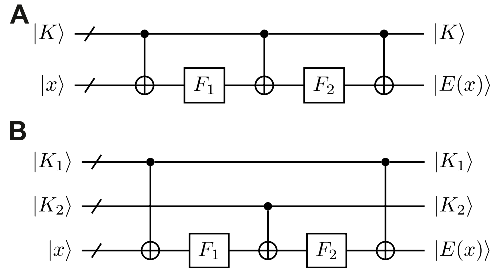


FIGURE 4
Quantum circuit of **(A)** 2-step LED-64 and **(B)** 2-step LED-128, here ancilla qubits are not represented.

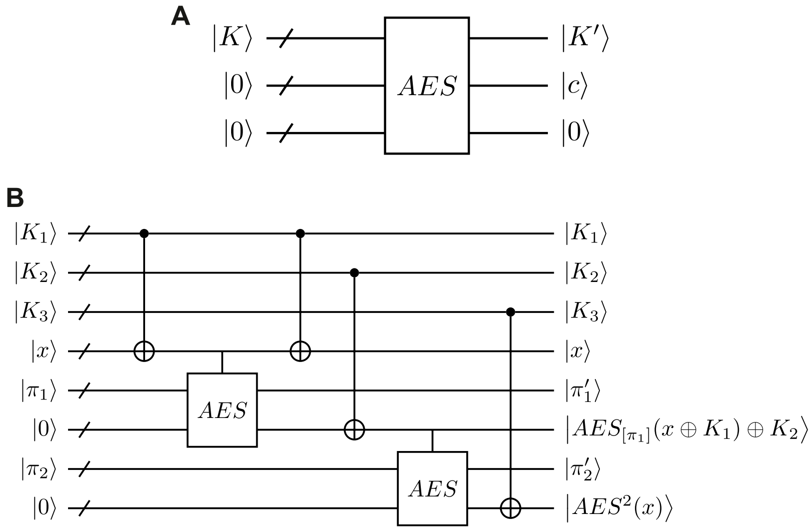


FIGURE 5
Quantum circuit of **(A)** AES, where the box of AES means the quantum circuit of AES-128 in Ref. [35], K' is the subkey of the 10th round in AES and c is the ciphertext; **(B)** AES^2, where the vertical line above the AES box indicates that 128 × 2 CNOT gates are performed instead of 128 × 2 NOT gates in the quantum circuit of AES-128. The ancilla qubits and unused outputs are not represented.

3.2.1 The applications to 2-step LED-128 and AES$_2$

According to the structure of 2-step LED-128, we can obtain the cryptographic function

$$E(x) = F_2(F_1(x \oplus K_1) \oplus K_2) \oplus K_1,$$

where $|K_1| = |K_2| = 64$. In order to attack 2-step LED-128, we consider the function

$$\begin{aligned} f(i,x) &= E(x) \oplus F_2(F_1(x) \oplus i) \\ &= F_2(F_1(x \oplus K_1) \oplus K_2) \oplus K_1 \oplus F_2(F_1(x) \oplus i) \end{aligned}$$

in **Problem 3**. Now, we can adopt GMS algorithm on $f(i, x)$ directly. Hence, this attack requires the query complexity of 2^{39} and time complexity of 2^{50}.

Furthermore, we can also utilize OS algorithm to recover K_1 and K_2 of 2-step LED-128. First, we define the functions

$$\begin{aligned} &f(i,x) = F_2(F_1(x) \oplus i), \\ &g(x) = E(x). \end{aligned}$$

Then the subkeys can be recovered with OS algorithm on $f(i, x)$ and $g(x)$. The quantum attack requires 2^6 quantum queries to $E(x)$, 2^{38} quantum queries to $f(i, x)$ and time complexity of 2^{50}. On the other hand, we can also consider functions

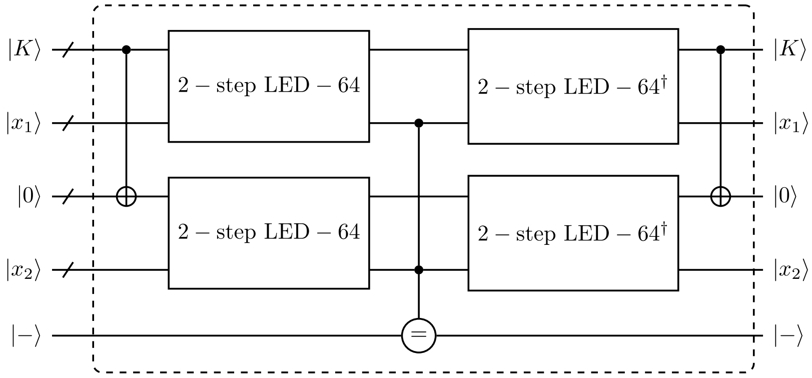


FIGURE 6
Grover oracle for 2-step LED-64.

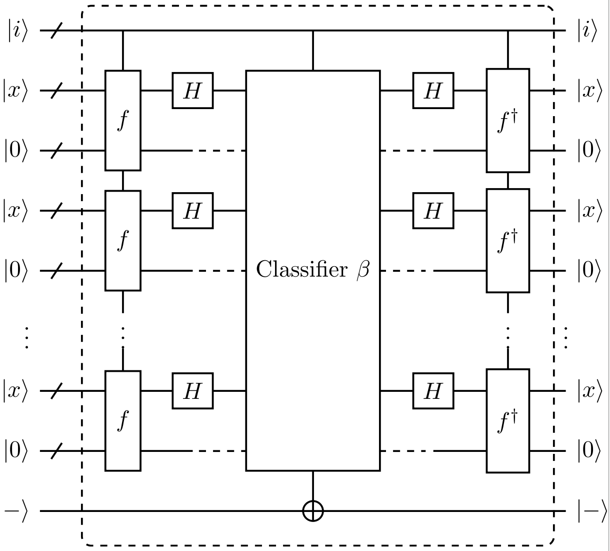


FIGURE 7
Iterative oracle for GMS algorithm, the quantum circuit for classifier β is given in Supplementary Figure S5 of Supplementary B.

$$f(i\|j,x) = F_2(F_1(x\|j) \oplus i),$$
$$g(x) = E(x\|0^{n-u})$$

and apply OS algorithm on $f(i\|j, x)$ and $g(x)$ in Q1 model when $E(x)$ can be queried only classically. In such a case, the quantum attack requires 2^{47} classical queries to $E(x)$, $2^{46.5}$ quantum queries to $f(i\|j, x)$ and time complexity of $2^{58.5}$ when $u = 47$. The comparison of quantum attacks against 2-step LED-128 is summarized in Table 3.

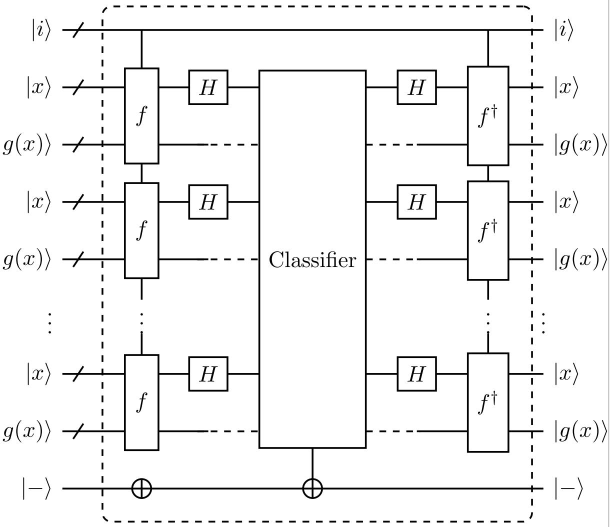


FIGURE 8
Iterative oracle for OS algorithm, the quantum circuit for classifier is provided in Supplementary Figure S6 of Supplementary B.

In order to attack AES_2, we need to construct functions in the case of 2EM_3 construction described in Section 3.2 with block size 128. Thus, the subkeys of AES^2 can be recovered by GMS algorithm with the query complexity of 2^{72} and time complexity of 2^{85}. Furthermore, we can also attack AES^2 with OS algorithm in Q1 and Q2 model respectively. In Q1 model, the attack requires 2^{90} classical queries to $E(x)$, 2^{90} quantum queries to $f(i\|j, x)$ and the time complexity of 2^{104} when $u = 90$. In Q2 model, the attack requires 2^7 quantum queries to $E(x)$, 2^{71} queries to $f(i, x)$ and the time complexity of 2^{85}. The comparison of attacks against AES^2 is summarized in Table 4.

Tables 3 and 4 show that the quantum attacks we proposed in Q1 and Q2 models are more efficient than existing classical and quantum attacks in time complexity and query complexity when we consider queries of cryptographic function and public permutations, except that more qubits are needed.

4 Resource estimation

We first give some quantum gates that are used in quantum implementations of classical circuits in Figure 1. Note that the last qubit is target qubit and other qubits are control qubits in CNOT and Toffoli gates.

4.1 Resource estimation of target ciphers

Next, we give the quantum resource estimation of 2-step LED-64, 2-step LED-128 and AES^2 respectively.

4.1.1 Resource estimation of 2-step LED-64 and 2-step LED-128

The internal state of LED contains 64 bits, arranged in 16 nibbles. Each nibble represents an element from GF(2^4) with the underlying polynomial for field multiplication given by $X^4 + X + 1$. The step function F_i of LED cipher is a 4-round AES-like permutation. Each of these four rounds consists of operations AddConstants, SubCells, ShiftRows and MixColumnsSerial.

AddConstants. The operation consists of XOR-ing of a 32-bit round constant to the internal state of LED. Thus, it can be realized by using 32 NOT gates in quantum circuit.

SubCells. LED cipher uses a 4-bit to 4-bit S-box of PRESENT [30], which is applied in parallel 16 times to the internal state of LED. According to Algorithm 3 of Ref. [31], the quantum circuit of the S-box is redesigned in Figure 2, which requires Toffoli depth 19, 19 Toffoli gates, 5 CNOT gates, 2 NOT gates and 5 qubits. Therefore, we can obtain the resource estimation of SubCells by multiplying the resources of the S-box by 16, except

TABLE 6 Resource estimation for iterative oracle of GMS algorithm and OS algorithm, where Clifford gate denotes the CNOT gate and Hadamard gate.

Algorithm	Model	Target cipher	Toffoli depth	#Toffoli	#Clifford	#NOT	width
GMS	Q2	2-step LED-128	62327	4759241	4516500	762376	25152
GMS	Q2	AES^2	12508008	83407802	368607419	3734666	365444
OS	Q1&Q2	2-step LED-128	4954	2887806	1966081	327809	26880
OS	Q1&Q2	AES^2	53626	31698174	105088001	1044737	270848

for the Toffoli depth since that these 16 S-boxes are applied in parallel.

ShiftRows. After the operation ShiftRows, the internal state is changed into a special permutation. Hence, we do not have to perform any operation for the quantum circuit of ShiftRows since it corresponds to a permutation of qubits. In this case, we only need to adjust the position of subsequent operations to ensure that the correct input wire is used.

MixColumnsSerial. The MixColumnsSerial performs four applications of matrix A, which is equivalent to matrix M:

$$(A)^4 = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 4 & 1 & 2 & 2 \end{pmatrix}^4 = \begin{pmatrix} 4 & 1 & 2 & 2 \\ 8 & 6 & 5 & 6 \\ B & E & A & 9 \\ 2 & 2 & F & B \end{pmatrix} = M.$$

The first scheme of implementing MixColumnsSerial is to realize matrix A. In order to design the quantum circuit of matrix A, the quantum circuit of operations 2 and 4 in A should be considered first. It is easy to obtain that $2 \cdot (a_3, a_2, a_1, a_0) = (a_2, a_1, a_3 \oplus a_0, a_3)$ and $4 \cdot (a_3, a_2, a_1, a_0) = (a_1, a_3 \oplus a_0, a_3 \oplus a_2, a_2)$. Hence, the implementation of operations 2 and 4 cost 1 and 2 CNOT gates respectively. Now, we can design the quantum circuit of matrix A based on operations 2 and 4 in Figure 3.

According to Figure 3, we can derive that the quantum circuit of matrix A requires $(2 + 4 + 6 + 6) \times 4 = 72$ CNOT gates. Thus, the resource estimation for operation MixColumnsSerial is $72 \times 4 = 288$ CNOT gates.

The second scheme is to consider the matrix M directly. From SageMath [32], we can obtain the PLU decomposition

$$\begin{aligned} M &= \begin{pmatrix} 4 & 1 & 2 & 2 \\ 8 & 6 & 5 & 6 \\ B & E & A & 9 \\ 2 & 2 & F & B \end{pmatrix} \\ &= \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 0 & 0 \\ 2 & 1 & 0 & 0 \\ 6 & 2 & 1 & 0 \\ 9 & 6 & 2 & 1 \end{pmatrix} \cdot \begin{pmatrix} 4 & 1 & 2 & 2 \\ 0 & 4 & 1 & 2 \\ 0 & 0 & 4 & 1 \\ 0 & 0 & 0 & 4 \end{pmatrix}. \end{aligned}$$

Similarly, we can easily obtain that $6 \cdot (a_3, a_2, a_1, a_0) = (a_2 \oplus a_1, a_3 \oplus a_1 \oplus a_0, a_2 \oplus a_0, a_3 \oplus a_2)$ and $9 \cdot (a_3, a_2, a_1, a_0) = (a_0, a_3, a_2, a_1 \oplus a_0)$, which can be achieved with 5 and 1 CNOT gates respectively. Then, we can know that the matrix L and U require $4\times([(1 + 4 + 1) + (5 + 4 + 5) + (1 + 4 + 1)] + [(5 + 4 + 5) + (1 + 4 + 1)] + (1 + 4 + 1)) = 208$ and $4 \times ([2 + 4 + (1 + 4 + 1) + (1 + 4 + 1)] + [2 + 4 + (1 + 4 + 1)] + (2 + 4) + 2) = 152$ CNOT gates respectively. Therefore, the resource estimation for operation MixColumnsSerial is $208 + 152 = 360$ CNOT gates in second scheme. Comparing these two schemes, we adopt first one to implement the operation MixColumnsSerial since it requires fewer CNOT gates.

Taking all these into consideration, we can derive that the resource estimation of one round AES-like permutation costs Toffoli depth 19, 304 Toffoli gates, 368 CNOT gates, 64 NOT gates and 80 qubits. Then the quantum circuits of 2-step LED-64 and 2-step LED-128 are presented in Figure 4. In such a case, the quantum circuit of 2-step LED-64 requires Toffoli depth 152, 2432 Toffoli gates, 3136 CNOT gates, 512 NOT gates and 144 qubits. The quantum circuit of 2-step LED-128 costs Toffoli depth 152, 2432 Toffoli gates, 3136 CNOT gates, 512 NOT gates and 208 qubits.

TABLE 7 Resource estimation for proposed quantum attacks on target ciphers, where all figures are in log base 2. The values of u of OS algorithm in Q1 model for 2-step LED-128 and AES^2 are 47 and 90, respectively.

Algorithm	Model	Target cipher	Toffoli depth	#Toffoli	#Clifford	#NOT	width
GMS	Q2	2-step LED-128	47.6	53.8	53.8	51.2	14.6
GMS	Q2	AES^2	87.2	90.0	92.1	85.5	18.5
OS	Q2	2-step LED-128	43.9	53.1	52.6	50.0	14.7
OS	Q2	AES^2	79.4	88.6	90.3	83.6	18.0
OS	Q1	2-step LED-128	52.4	61.6	61.1	58.5	14.7
OS	Q1	AES^2	98.4	107.6	109.3	102.6	18.0

4.1.2 Resource estimation of AES^2

The construction of AES^2 is defined by fixing two randomly chosen 128-bit AES-128 keys, which specify the permutations P_1 and P_2. The subkeys are comprised of three independently chosen 128-bit secret keys K_1, K_2 and K_3. Let AES[K] denotes the whole AES-128 encryption with the 128-bit key K. Hence, the encryption of AES^2 is defined as

$$\mathrm{AES}^2(x) = \mathrm{AES}[\pi_2](\mathrm{AES}[\pi_1](x \oplus K_1) \oplus K_2) \oplus K_3,$$

where two 128-bit keys π_1 and π_2 are defined based on the first 256 bits of the binary digit expansion of π. Recently, the implementation of AES quantum circuit received more and more attention [33–35]. Based on the fewer qubits principle, we take the quantum circuit of AES-128 from Ref. [35] for quntum circuit design of AES^2. As shown in Figure 5A, this quantum circuit costs Toffoli depth 11008, 16508 Toffoli gates, 81652 CNOT gates, 1072 NOT gates and 270 qubits. In Ref. [35], the XOR of a 128-bit plaintext in first round of AES-128 is considered as XOR-ing of a 128-bit constant, which is achieved by performing 128 NOT gates on the key of AES-128 first and then canceled by 128 NOT gates again. However, the 128-bit plaintext is a quantum superposition in our proposed quantum attacks. Hence, we need to adopt 128 × 2 CNOT gates instead of 128 × 2 NOT gates here. Therefore, the quantum circuit of AES-128 used in the quantum circuit design of AES^2 requires Toffoli depth 11008, 16508 Toffoli gates, 81908 CNOT gates, 816 NOT gates and 270 qubits. In such a case, we can easily design the quantum circuit of AES^2 in Figure 5B and obtain the resource estimation of AES^2 with Toffoli depth 22016, 33016 Toffoli gates, 164328 CNOT gates, 1632 NOT gates and 1038 qubits. Note that the ancilla qubits involved in first AES quantum circuit can be reused in second AES quantum circuit.

4.2 Resource estimation of Grover algorithm on 2-step LED-64

In order to adopt Grover algorithm on 2-step LED-64, we need to design the Grover oracle for 2-step LED-64 first. When designing the Grover oracle, the number of plaintext-ciphertext pairs required to recover the correct key uniquely should be considered. At EUROCRYPT 2020, Jaques *et al.* [34] stated that when the number of required plaintext-ciphertext pairs $\nu \geq \lceil \frac{m}{n} \rceil$, the probability of uniquely recovering the correct key is about $e^{-2^{m-\nu n}}$, where n and m are block size and key size for a block cipher respectively.

Hence, the number of required plaintext-ciphertext pairs for 2-step LED-64 should be $\nu \geq 1$ since $m = n = 64$. Then the probability of finding a unique key is around 0.37 for $\nu = 1$. For $\nu = 2$, the probability is about 0.99. Thus, we consider the case of $\nu = 2$ when designing the Grover oracle for 2-step LED-64. Therefore, the quantum circuit of the Grover oracle for 2-step LED-64 is illustrated in Figure 6, which requires Toffoli depth 317, 9981 Toffoli gates, 12672 CNOT gates, 2304 NOT gates and 383 qubits. In the quantum circuit of Grover oracle for 2-step LED-64, each comparison of n-bit known ciphertext and n-qubit output of 2-step LED-64 oracle requires Toffoli depth $2\lceil \log_2 n \rceil$, 2 (n − 1) Toffoli gates, $2n$ NOT gates and (n − 1) ancilla qubits.

In the process of Grover algorithm, $\lfloor \frac{\pi}{4} 2^{m/2} \rfloor$ iterations of Grover operator are performed. While estimating the resources, we only consider the cost incurred by Grover oracle. Since compared with the cost incurred by Grover oracle, the cost imposed by other operations in Grover operator is relatively small in terms of magnitude and can be ignored. In such a case, the resources of Grover oracle for 2-step LED-64 are multiplied by $\lfloor \frac{\pi}{4} 2^{m/2} \rfloor$ for estimating the resources of Grover algorithm on 2-step LED-64, which costs Toffoli depth $2^{40.0}$, $2^{44.9}$ Toffoli gates, $2^{45.3}$ CNOT gates, $2^{42.8}$ NOT gates and $2^{8.6}$ qubits. Note that the width is still the same as in Grover oracle since we assume that no parallelization is involved.

4.3 Resource estimation of proposed quantum attacks on 2-step LED-128 and AES^2

The resource estimation of proposed quantum attacks on 2-step LED-128 and AES^2 can be considered in a similar way as Grover algorithm since that Grover algorithm, GMS algorithm and OS algorithm all need to perform an iterative operator. Thus, we should consider the resource estimation of iterative oracle for target ciphers first. Here, the resource estimation of constructed functions for target ciphers in proposed quantum attacks is given in Table 5 and the corresponding quantum circuits see Supplementary A.

Now, the quantum circuits of iterative oracle for GMS algorithm and OS algorithm are designed in Figure 7 and Figure 8 respectively.

In Figure 7, the classifier β for GMS algorithm contains Test 1 and Test 2 (see also Supplementary Figure S5 of Supplementary B). When both two test conditions are satisfied, the phase of target qubit will be flipped. Test 1 of classifier β. The Test 1 of classifier β includes the checking of dim $(\langle u_1, \ldots, u_\ell \rangle)$ and the calculation of candidate period s'. The first phase includes the computation of triangular basis and the rank checking of triangular basis. Based on Algorithm 4 of Ref. [36], we can obtain that the computation of triangular basis requires Toffoli depth $\ell(4 + \lceil \log_2 n \rceil) + \sum_{i=2}^{n} (4 + \lceil \log_2 (n-i+1) \rceil)$, $\ell n^2 + \ell n$ Toffoli gates and ℓ + n (n + 1)/2 + n (n − 1) ancilla qubits, where the value of ℓ is $2(n + \sqrt{n})$ [24]. For the rank checking of triangular basis, it requires Toffoli depth $2\lceil \log_2 n \rceil$, 2 (n − 1) Toffoli gates, $2n$ NOT gates and (n − 1) ancilla qubits. The second phase is the calculation of the candidate period. Bonnetain *et al.* [36] showed that the realizing of computing orthogonal vectors (*i.e.,* Algorithm 5 in Ref. [36]) costs Toffoli depth $n(n-1)$, $n(n-1)$ Toffoli gates, n CNOT gates and n ancilla qubits. However, there is a mistake that the Toffoli depth and Toffoli gates should be $n\ (n-1)/2$. Thus, we can obtain that the resource estimation for Test 1 of classifier β requires Toffoli depth $\ell(4+\lceil\log_2 n\rceil)+\sum_{i=2}^{n}(4+\lceil\log_2(n-i+1)\rceil)+2\lceil\log_2 n\rceil+n(n-1)/2$, $\ell n^2+\ell n+2\ (n-1)+n\ (n-1)/2$ Toffoli gates, n CNOT gates, $2n$ NOT gates and $\ell+n\ (n+1)/2+n\ (n-1)+n$ ancilla qubits by combining all these terms. Note that there are $(n-1)$ ancilla qubits missing since the ancilla qubits in the process of rank checking can be reused in the computation of orthogonal vectors. In this case, we only need $\max\{n-1,\ n\}$ ancilla qubits in these two processes. Test 2 of classifier β. The quantum circuit of Test 2 of classifier β for 2-step LED-128 is given in Supplementary Figure S7 of Supplementary B, which costs

$$\left\{\begin{array}{ll}\text{Toffoli depth}\quad 147\times(76\times 4+2\log_2 64+49)+5=53660 & \\ 147\times[1216\times 8+2\times(64-1)+49]+13=1455754 & \text{Toffoli gates}\\ 147\times(1472\times 8+64\times 10+1)=1825299 & \text{CNOT gates}\ ,\\ 147\times(256\times 8+64\times 2)+8=319880 & \text{NOT gates}\\ 64\times 2+63+6+8+1=206 & \text{qubits}\end{array}\right.$$

since $t=1,2,\ldots,147\,(\text{i.e.},\frac{3n+n\ell}{n})$ [24] in Supplementary Figure S7. Here $|i\rangle$ and the candidate period $|s'\rangle$ are not included in the qubits. The quantum circuit of Test 2 of classifier β for AES^2 is provided in Supplementary Figure S8 of Supplementary B, which requires

$$\left\{\begin{array}{ll}\text{Toffoli depth}\quad 282\times(11008\times 4+2\log_2 128+64)+7=12439027 & \\ 282\times[16508\times 8+2\times(128-1)+64]+15=37331739 & \text{Toffoli gates}\\ 282\times(81908\times 8+128\times 10+1)=185145690 & \text{CNOT gates}\ ,\\ 282\times(816\times 8+128\times 2)+10=1913098 & \text{NOT gates}\\ 128\times 10+127+9+7+1=1424 & \text{qubits}\end{array}\right.$$

where $t=1,2,\ldots,282$ in Supplementary Figure S8. Here $|i\rangle$ and $|s'\rangle$ are not included in the qubits.

Hence, the classifier β for 2-step LED-128 costs

$$\left\{\begin{array}{ll}\text{Toffoli depth}\quad 2\times(2007+6+2016)+53660+1=61719 & \\ 2\times(599040+63+2016)+1455754+1=2657993 & \text{Toffoli gates}\\ 2\times 64+1825299+1=1825428 & \text{CNOT gates}\ ,\\ 2\times 64+319880=320008 & \text{NOT gates}\\ 6256+64+206+1+1=6528 & \text{qubits}\end{array}\right.$$

where $|u_1\rangle, |u_2\rangle, \cdots, |u_\ell\rangle$ and $|i\rangle$ are not included in the qubits. The classifier β for AES^2 costs

$$\left\{\begin{array}{ll}\text{Toffoli depth}\quad 2\times(4339+7+8128)+12439027+1=12463976 & \\ 2\times(4606848+127+8128)+37331739+1=46561946 & \text{Toffoli gates}\\ 2\times 128+185145690+1=185145947 & \text{CNOT gates}\ .\\ 2\times 128+1913098=1913354 & \text{NOT gates}\\ 24791+128+1424+1+1=26345 & \text{qubits}\end{array}\right.$$

Altogether, the resource estimation for iterative oracle of GMS algorithm is summarized in Table 6.

In Supplementary Figure S6 of Supplementary B, the classifier oracle of OS algorithm consists of the computation of triangular basis and rank checking. Therefore, the classifier oracle costs Toffoli depth $2* \ [cn*(4+\lceil\log_2 n\rceil)+\ \sum_{i=2}^{n}(4+\lceil\log_2(n-i+1)\rceil)+\lceil\log_2 n\rceil]$, $2*[cn*n^2+cn*n+(n-1)]$ Toffoli gates, 1 CNOT gates, $2n+1$ NOT gates and $cn+n\ (n+1)/2+n\ (n-1)+(n-1)+1$ ancilla qubits, where $cn\simeq 2.5n$ [25]. Then, the corresponding resource estimation for iterative oracle of OS algorithm is listed in Table 6. Here, the resource estimation for iterative oracle of OS algorithm in Q1 model is same as the case of OS algorithm in Q2 model, except that the width in Q1 model should consider extra $(n-u)$ qubits.

Similarly, $\lceil\frac{\pi}{4}2^{n/2}\rceil$ iterations for the iterative operator of proposed quantum attacks are required. Here, we only consider the cost incurred by the iterative oracle and assume that the iterative oracle is applied in serial. Hence, the resources (except the number of qubits) in Table 6 are multiplied by $\lceil\frac{\pi}{4}2^{n/2}\rceil$ for estimating the resources of mounting presented quantum attacks on 2-step LED-128 and AES^2. The resource estimation is summarized in Table 7. From Table 7, it is obvious that the proposed quantum attacks based on GMS algorithm cost more than ones with OS algorithm in Q2 model. The main reason for this is caused by Test 2 of classifier β in GMS algorithm, which needs to check whether $f\ (i,\ z)=f\ (i,\ z\oplus s')$ for fixed i, the given t pairs of z and thus requires more resources. Note that the cost incurred by proposed quantum attacks with OS algorithm in Q1 model is more than the ones in Q2 model because guessing the value of j requires another $2^{(n-u)/2}$ iterations. Moreover, we also give the resource estimation for Grover algorithm on 2-step LED-128 and AES^2 in Supplementary C. Compared with the proposed quantum attacks on 2-step LED-128 and AES^2, the corresponding Grover algorithm costs much more since the Grover algorithm requires more iterations, except for the width.

Besides, it is worth noting that the resource estimation for OS algorithm in Q1 model should also consider the cost of preparing the quantum state $|\psi_g\rangle=\otimes^{cn}(\sum_{x\in\{0,1\}^n}|x\rangle|g(x)\rangle)$ with quantum read-only memory (QROM). According to Theorem 2 of Ref. [37], we can obtain that the transform

$$\sum_{x\in\{0,1\}^u}|x\rangle|0\rangle\mapsto\sum_{x\in\{0,1\}^u}|x\rangle|g(x)\rangle$$

costs Toffoli depth $\lceil 2^u/\omega\rceil+n(\omega-1)$, $\lceil 2^u/\omega\rceil+n(\omega-1)$ Toffoli gates and $n(\omega-1)+\lceil\log(2^u/\omega)\rceil$ ancilla qubits, where ω is a power of 2 such that $1<\omega<2^u$. Therefore, the preparing of the quantum state $|\psi_g\rangle$ in OS algorithm for 2-step LED-128 requires Toffoli depth 2^{46}, $2^{53.3}$ Toffoli gates and $2^{14.1}$ ancilla qubits when $\omega=2$. The preparing of the quantum state $|\psi_g\rangle$ in OS algorithm for AES^2 costs Toffoli depth 2^{88}, $2^{96.3}$ Toffoli gates and $2^{17.2}$ ancilla qubits when $\omega=4$. In such a case, we can easily prepare the quantum state $|\psi_g\rangle$ under the resources of the iteration in OS algorithm. Therefore, the cost incurred by preparing the quantum state $|\psi_g\rangle$ of OS algorithm in Q1 model can be ignored. Similarly, the cost imposed by recovering the period K_1 of GMS and OS algorithms can also be ignored since it is relatively small in terms of magnitude compared with the iteration in GMS and OS algorithms.

5 Conclusion

In this study, we consider the security of two-round Even-Mansour constructions in quantum setting. Compared with the classical attack with optimal query complexity, the presented quantum key-recovery attack on $2EM_1$ construction reduces the query complexity by a factor of $2^{n/6}$. For $2EM_2$ and $2EM_3$ constructions, we design quantum key-recovery attacks in Q1 and Q2 model respectively. The comparison in Table 2 shows that our attacks are more efficient than Grover search and QMITM attack no matter in Q1 or Q2 model. Furthermore, we also give the applications of proposed quantum attacks and analyze the corresponding resource estimation.

Data availability statement

The original contributions presented in the study are included in the article/Supplementary Material, further inquiries can be directed to the corresponding author.

Author contributions

These authors contributed equally to this work.

Funding

This work was supported by National Natural Science Foundation of China (Grant Numbers 61972048, 61976024), Henan Key Laboratory of Network Cryptography Technology (LNCT2021-A10), BUPT Excellent Ph.D. Students Foundation (Grant Number CX2019207) and China Scholarship Council (Grant Number 202006470082).

Conflict of interest

The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Publisher's note

All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers. Any product that may be evaluated in this article, or claim that may be made by its manufacturer, is not guaranteed or endorsed by the publisher.

Supplementary material

The Supplementary Material for this article can be found online at: https://www.frontiersin.org/articles/10.3389/fphy.2022.1028014/full#supplementary-material

References

1. Even S, Mansour Y. A construction of a cipher from a single pseudorandom permutation. *J Cryptology* (1997) 10(3):151–61. doi:10.1007/s001459900025

2. Orr D, Keller N, Shamir A. Minimalism in cryptography: The even-mansour scheme revisited. In: D Pointcheval T Johansson, editors. *Advances in cryptology - EUROCRYPT 2012 - 31st annual international conference on the theory and applications of cryptographic techniques*. Cambridge, UK: Springer (2012). p. 336–54. April 15-19, 2012. Proceedings, volume 7237 of Lecture Notes in Computer Science.

3. Bogdanov A, Knudsen LR, Leander G, Standaert F-X, Steinberger JP, Tischhauser E. Key-alternating ciphers in a provable setting: Encryption using a small number of public permutations - (extended abstract). In: D Pointcheval T Johansson, editors. *Advances in cryptology - EUROCRYPT 2012 - 31st annual international conference on the theory and applications of cryptographic techniques*. Cambridge, UK: Springer (2012). p. 45–62. April 15-19, 2012. Proceedings, volume 7237 of Lecture Notes in Computer Science.

4. Lampe R, Patarin J, Seurin Y. An asymptotically tight security analysis of the iterated even-mansour cipher. In: X Wang K Sako, editors. *Advances in cryptology - ASIACRYPT 2012 - 18th international conference on the theory and application of cryptology and information security*. Beijing, China: Springer (2012). p. 278–95. December 2-6, 2012. Proceedings, volume 7658 of Lecture Notes in Computer Science.

5. Chen S, Steinberger JP. Tight security bounds for key-alternating ciphers. In: PQ Nguyen E Oswald, editors. *Advances in cryptology - EUROCRYPT 2014 - 33rd annual international conference on the theory and applications of cryptographic techniques*. Copenhagen, Denmark: Springer (2014). p. 327–50. May 11-15, 2014. Proceedings, volume 8441 of Lecture Notes in Computer Science.

6. Jordan SP, Liu Y-K. Quantum cryptanalysis: Shor, grover, and beyond. *IEEE Secur Priv* (2018) 16(5):14–21. doi:10.1109/msp.2018.3761719

7. Bennett CH, Brassard G. *Quantum cryptography: Public key distribution and coin tossing* (2020). *arXiv preprint arXiv:2003.06557*.

8. Deng FG, Long GL. Bidirectional quantum key distribution protocol with practical faint laser pulses. *Phys Rev A* (2004) 70(1):012311. doi:10.1103/PhysRevA.70.012311

9. Ye T-Y, Li H-K, Hu J-L. Semi-quantum key distribution with single photons in both polarization and spatial-mode degrees of freedom. *Int J Theor Phys (Dordr)* (2020) 59(9):2807–15. doi:10.1007/s10773-020-04540-y

10. Ye T-Y, Geng M-J, Xu T-J, Chen Y. Efficient semiquantum key distribution based on single photons in both polarization and spatial-mode degrees of freedom. *Quan Inf Process* (2022) 21(4):123–1. doi:10.1007/s11128-022-03457-1

11. Zhandry M. How to construct quantum random functions. In: *53rd annual IEEE symposium on foundations of computer science*. New Brunswick, NJ, USA: FOCSIEEE Computer Society (2012). p. 679–87. October 20-23, 2012.

12. Kaplan M, Leurent G, Anthony L, Naya-Plasencia M. Breaking symmetric cryptosystems using quantum period finding. In: M Robshaw J Katz, editors. *Advances in cryptology - CRYPTO 2016 - 36th annual international cryptology conference*. Santa Barbara, CA, USA: Springer (2016). p. 207–37. August 14-18, 2016, Proceedings, Part II, volume 9815 of Lecture Notes in Computer Science.

13. Kuwakado H, Morii M. Security on the quantum-type even-mansour cipher. In: *Proceedings of the international symposium on information theory and its applications, ISITA 2012*. Honolulu, HI, USA: IEEE (2012). p. 312–6. October 28-31, 2012.

14. Alagic G, Chen B, Katz J, Majenz C. Post-quantum security of the even-mansour cipher. In: *Orr dunkelman and stefan DziembowskiAdvances in cryptology - EUROCRYPT 2022 - 41st annual international conference on the theory and applications of cryptographic techniques*. Trondheim, Norway: Springer (2022). p. 458–87. May 30 - June 3, 2022, Proceedings, Part III, volume 13277 of Lecture Notes in Computer Science.

15. Kaplan M. Quantum attacks against iterated block ciphers. *CoRR abs* (2014) 1410–34.

16. Brassard G, Høyer P, Tapp A. Quantum cryptanalysis of hash and claw-free functions. In: CL Lucchesi AV Moura, editors. *Latin '98: Theoretical informatics, third Latin American symposium*. Campinas, Brazil: Springer (1998). p. 163–9. April, 20-24, 1998, Proceedings, volume 1380 of Lecture Notes in Computer Science.

17. Nikolic I, Wang L, Wu S. Cryptanalysis of round-reduced LED. *IACR Cryptol Eprint Arch* (2015) 429.

18. Dinur I, Orr D, Keller N, Shamir A. Key recovery attacks on 3-round even-mansour, 8-step led-128, and full AES2. In: K Sako P Sarkar, editors. *Advances in cryptology - ASIACRYPT 2013 - 19th international Conference on the Theory and Application of Cryptology and information security*. Bengaluru, India: Springer (2013). p. 337–56. December 1-5, 2013, Proceedings, Part I, volume 8269 of Lecture Notes in Computer Science.

19. Dinur I, Orr D, Keller N, Shamir A. Key recovery attacks on iterated even-mansour encryption schemes. *J Cryptol* (2016) 29(4):697–728. doi:10.1007/s00145-015-9207-3

20. Isobe T, Shibutani K. New key recovery attacks on minimal two-round even-mansour ciphers. In: T Takagi T Peyrin, editors. *Advances in cryptology - ASIACRYPT 2017 - 23rd international Conference on the Theory and Applications of Cryptology and information security*. Hong Kong, China: Springer (2017). p. 244–63. December 3-7, 2017, Proceedings, Part I, volume 10624 of Lecture Notes in Computer Science.

21. Leurent G, Sibleyras F. Low-memory attacks against two-round even-mansour using the 3-xor problem. In: S Barbara, editor. *Alexandra boldyreva and daniele MicciancioAdvances in cryptology - CRYPTO 2019 - 39th annual international cryptology conference*. CA, USA: Springer (2019). p. 210–35. August 18-22, 2019, Proceedings, Part II, volume 11693 of Lecture Notes in Computer Science.

22. Hosoyamada A, Aoki K. On quantum related-key attacks on iterated even-mansour ciphers. *IEICE Trans Fundamentals* (2019) 102(1):27–34. doi:10.1587/transfun.e102.a.27

23. Grover LK. A fast quantum mechanical algorithm for database search. In: GL Miller, editor. *Proceedings of the twenty-eighth annual ACM symposium on the theory of computing*. Philadelphia, Pennsylvania, USA: ACM (1996). p. 212–9. May 22-24, 1996.

24. Leander G, May A. Grover meets simon - quantumly attacking the fx-construction. In: T Takagi T Peyrin, editors. *Advances in cryptology - ASIACRYPT 2017 - 23rd international Conference on the Theory and Applications of Cryptology and information security*. Hong Kong, China: Springer (2017). p. 161–78. December 3-7, 2017, Proceedings, Part II, volume 10625 of Lecture Notes in Computer Science.

25. Bonnetain X, Hosoyamada A, Naya-Plasencia M, Sasaki Y, Schrottenloher A. Quantum attacks without superposition queries: The offline simon's algorithm. In: SD Galbraith S Moriai, editors. *Advances in cryptology - ASIACRYPT 2019 - 25th international Conference on the Theory and Application of Cryptology and information security*. Kobe, Japan: Springer (2019). p. 552–83. December 8-12, 2019, Proceedings, Part I, volume 11921 of Lecture Notes in Computer Science.

26. Brassard G, Hoyer P, Mosca M, Tapp A. Quantum amplitude amplification and estimation. *Contemp Math* (2002) 305:53–74. doi:10.1090/conm/305/05215

27. Simon DR. On the power of quantum computation. *SIAM J Comput* (1997) 26(5):1474–83. doi:10.1137/s0097539796298637

28. Kilian J, Rogaway P. How to protect DES against exhaustive key search. In: K Neal, editor. *Advances in cryptology - CRYPTO '96, 16th annual international cryptology conference*. Santa Barbara, California, USA: Springer (1996). p. 252–67. August 18-22, 1996, Proceedings, volume 1109 of Lecture Notes in Computer Science.

29. Guo J, Peyrin T, Poschmann A, Matthew JB. Robshaw. The LED block cipher. In: *Bart preneel and tsuyoshi TakagiCryptographic hardware and embedded systems - CHES 2011 - 13th international workshop*. Nara, Japan: Springer (2011). p. 326–41. September 28 - October 1, 2011, Proceedings, volume 6917 of Lecture Notes in Computer Science.

30. Bogdanov A, Knudsen LR, Leander G, Paar C, Poschmann A, Matthew J, et al. Present: An ultra-lightweight block cipher. In: *Pascal paillier and ingrid VerbauwhedeCryptographic hardware and embedded systems - CHES 2007, 9th international workshop*. Vienna, Austria: Springer (2007). p. 450–66. September 10-13, 2007, Proceedings, volume 4727 of Lecture Notes in Computer Science.

31. Rahman M, Paul G. Grover on present: Quantum resource estimation. In: *IACR cryptol. ePrint arch.* (2021). p. 1655.

32. Stein W. *Sage mathematics software* (2007). Available at: http://www.sagemath//org.

33. Zou J, Wei Z, Sun S, Liu X, Wu W. Quantum circuit implementations of AES with fewer qubits. In: S Moriai H Wang, editors. *Advances in cryptology - ASIACRYPT 2020 - 26th international Conference on the Theory and Application of Cryptology and information security, daejeon*. South Korea: Springer (2020). p. 697–726. December 7-11, 2020, Proceedings, Part II, volume 12492 of Lecture Notes in Computer Science.

34. Jaques S, Naehrig M, Roetteler M, Virdia F. Implementing grover oracles for quantum key search on AES and lowmc. In: A Canteaut Y Ishai, editors. *Advances in cryptology - EUROCRYPT 2020 - 39th annual international conference on the theory and applications of cryptographic techniques*. Zagreb, Croatia: Springer (2020). p. 280–310. May 10-14, 2020, Proceedings, Part II, volume 12106 of Lecture Notes in Computer Science.

35. Li ZQ, Cai BB, Sun HW, Liu HL, Wan LC, Qin SJ, et al. Novel quantum circuit implementation of advanced encryption standard with low costs. *Sci China Phys Mech Astron* (2022) 65(9):290311–6. doi:10.1007/s11433-022-1921-y

36. Bonnetain X, Jaques S. Quantum period finding against symmetric primitives in practice. *IACR Trans Cryptogr Hardw Embed Syst* (2022) 2022(1):1–27. doi:10.46586/tches.v2022.i1.1-27

37. Berry DW, Craig G, Motta M, McClean JR, Ryan B. Qubitization of arbitrary basis quantum chemistry leveraging sparsity and low rank factorization. *Quantum* (2019) 3:208. doi:10.22331/q-2019-12-02-208

frontiers | Frontiers in Physics

TYPE Original Research
PUBLISHED 20 October 2022
DOI 10.3389/fphy.2022.1029262

Semi-quantum key distribution with two classical users

Wan Qing Wu[1,2] and Chen Yang Sun[1,2]*

[1]School of Cyber Security and Computers, Hebei University, Baoding, China, [2]Key Laboratory on High Trusted Information System in Hebei Province, Hebei University, Baoding, China

Check for updates

OPEN ACCESS

EDITED BY
Tianyu Ye,
Zhejiang Gongshang University, China

REVIEWED BY
Xiaoping Lou,
Hunan Normal University, China
Hong Lai,
Southwest University, China

*CORRESPONDENCE
Chen Yang Sun,
sevin6@126.com

SPECIALTY SECTION
This article was submitted to Quantum Engineering and Technology, a section of the journal Frontiers in Physics

RECEIVED 27 August 2022
ACCEPTED 28 September 2022
PUBLISHED 20 October 2022

CITATION
Wu WQ and Sun CY (2022), Semi-quantum key distribution with two classical users.
Front. Phys. 10:1029262.
doi: 10.3389/fphy.2022.1029262

Semi-quantum key distribution (SQKD) is an important research issue which allows one quantum participant equipped with advanced quantum devices to distribute a shared secret key securely with one classical user who has restricted capabilities. In this paper, we propose a SQKD protocol which allows one quantum user to distribute two different private secret keys to two classical users respectively at the same time. Alice distributes two particle sequences from Bell states to Bob and Charlie respectively. Once the particles have been processed and returned, Alice can simultaneously detect reflected particles by Bob and Charlie based on Bell-state measurement and generate two different raw keys. To enable more participants in sharing keys, this protocol can be extended to the $m + 1$ party communication scheme by employing m-particle GHZ state. In large-scale communication networks, this extended model significantly reduces the complexity of communication compared to the traditional SQKD scheme. Security analyses show that the presented protocol is free from several general attacks, such as the entangle-measure attack, the modification attack, the double CNOT attack, and so on.

KEYWORDS

semi-quantum cryptography, semi-quantum key distribution, classical party, bell states, security analysis

1 Introduction

It is known that the first quantum key distribution (QKD) protocol [1] was put forward by Bennett and Brassard in 1984, which allow two quantum participants to distribute a session key with unconditional security [2, 3]. Since then, many kinds of QKD protocols have been proposed [4–14]. However, these QKD protocols assumed that the participants possess unlimited quantum capabilities. Nowadays, most advanced quantum devices (e.g., quantum state generators and quantum storage) remain expensive and difficult to implement.

To improve the practicality of these protocols, Boyer et al. proposed a novel idea of quantum key distribution [15], where one of the player Alice has full quantum capabilities, while the other player Bob is classical. The “classical” Bob either measures the qubits Alice sent in classical basis (Z-basis) and resends it in the same state he found, or reflects the qubits without any change. They called the protocol as “quantum key distribution with classical Bob” or “semi-quantum key distribution(SQKD).” The idea was further extended in Ref . [16], where two similar protocols were presented based on measurement-resend and randomization-based environment. The "classical" users are restricted to perform the following operations: 1) generate Z-basis qubits, $\{|0\rangle, |1\rangle\}$, 2) measure the quantum state in the Z-basis, 3) reflect the qubits without disturbance, and 4) reorder the qubits *via* different delay lines. Due to the different operation types of classical users, two variants of SQKD environment was proposed. In the randomization-based SQKD protocol, the classical users can only to implement operations 2), 3) and 4), whereas in the measure-resend SQKD protocol, the classical participants are limited to perform 1), 2) and 3). In this regard, the idea of semi-quantum relieves users of the burden of quantum state generation and measurement, making it more convenient to participate in quantum key distribution.

Based on Boyer et al.'s study, various semi-quantum protocols have been proposed. Lu and Cai presented a SQKD protocol with classical Alice [17]. In 2009, Zou et al. [18] presented five SQKD protocols by employing less than four quantum states with complete robustness. Later, Wang et al. [19] proposed a SQKD protocol using entangle states. In 2014 and 2016, Yu et al. [20] and Li et al. [21] respectively proposed two authenticated semi-quantum key distribution (ASQKD) protocols. The ASQKD exploit the mechanism of a pre-shared key to transmit secret key without classical channels. In 2015, the mediated semi-quantum key distribution (MSQKD) protocol was first proposed by Krawec [22], which allows two classical participants to generate a secret key with the help of a quantum server. In 2018, Liu et al. [23] also proposed a MSQKD protocol without invoking quantum measurement for the classical users. Since then, Lin et al. [24] proposed a MSQKD protocol using single photons. Zhu et al. [25] devised two SQKD protocols with GHZ states involving a quantum server. One of these two protocols is to distribute keys between quantum users and classical users, and the other is to communicate between two classical users with the assistance of the quantum third party. Soon after, Chen et al. [26] also proposed two analogous SQKD protocols based on GHZ-like states. In 2020 and 2022, Ye et al. [27, 28] presented two SQKD protocols based on single photons in both polarization and spatial-mode degrees of freedom. Besides, security proofs, attack strategies, and improvement methods of SQKD protocols have been developed from information theory aspect in Refs [29–36].

However, under the above-mentioned protocols, the quantum user Alice can only share a private key with one classical user at a time or two classical parties distribute a session key with the help of a fully quantum server. Suppose a quantum server receives multiple distribution requests at the same time, the presented protocol is used to deal with this situation. In this paper, we are going to devise a semi-quantum key distribution protocol with two classical users. The presented protocol allows one quantum server to distribute two raw keys to these two classical users simultaneously. The proposed scheme greatly enhances the key distribution capability of the quantum server. Moreover, the proposed scheme can be expanded to $m + 1$ party SQKD.

The rest of this paper is organized as follows: Section 2 presents a SQKD protocol. The detailed security analyses are described in Section 3. Section 4 generalizes the proposed SQKD protocol to $m + 1$ party. An efficiency analysis and the comparison of our protocol to other SQKD protocols are provided in Section 5. This work is concluded in Section 6.

2 The designed semi-quantum key distribution protocol

Suppose that quantum user Alice wants to distribute two different secret keys to classical user Bob and classical user Charlie separately at the same time. The following semi-quantum key distribution (SQKD) protocol is designed to make it possible. Here, the SIFT operation refers to measuring the received qubits in the Z-basis, $\{|0\rangle, |1\rangle\}$, and resending it in the same state as found; the CTRL operation refers to reflecting the received qubits back without any disturbance. The steps of the presented SQKD protocol are described as follows (as shown in Figure 1):

Step 1: Alice generates $N = 8n(1 + \delta)$ Bell states in $|\phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, where n is the desired length of INFO bits and δ is a fixed positive parameter. Then Alice respectively picks out the first particle, the second particle from every Bell state to construct two sequences

$$S_b = \{S_b^1, S_b^2, \ldots, S_b^N\},$$
$$S_c = \{S_c^1, S_c^2, \ldots, S_c^N\}.$$

Step 2: Alice sends S_b to Bob and sends S_c to Charlie.

Step 3: For each coming qubits, Bob (Charlie) randomly chooses to SIFT or CTRL. For convenience, we denote the qubits reflected by Bob (Charlie) with CTRL-B (CTRL-C) qubits and the qubits resended by Bob (Charlie) with SIFT-B (SIFT-C) qubits.

Step 4: Alice stores the received qubits in two N-qubit quantum registers and informs Bob and Charlie.

Step 5: Bob and Charlie publish which particles they choose to SIFT.

Step 6: According to the published information by Bob and Charlie and Table 1, they check out the security of the quantum channel and produce INFO bits.

Case 1. Both Bob and Charlie perform the CTRL on some particles with the same superscript i, ($i = 1, \ldots, N$). Alice performs the Bell-state measurement on the received quantum qubits. Alice checks the error rate on the Bell measurement

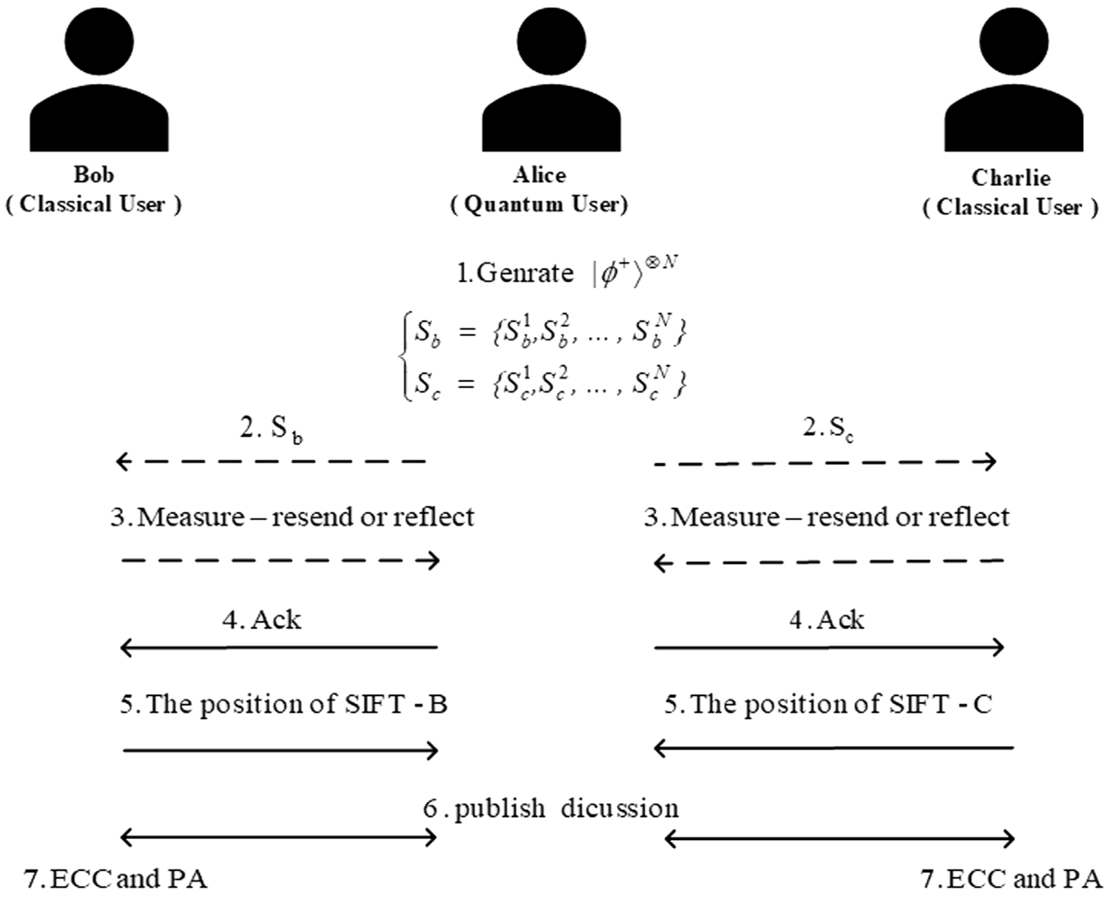

Bob
(Classical User)
Alice
(Quantum User)
Charlie
(Classical User)
1.Genrate $|\phi^{+}\rangle^{\otimes N}$
$\begin{cases} S_b = \{S_b^1, S_b^2, \ldots, S_b^N\} \\ S_c = \{S_c^1, S_c^2, \ldots, S_c^N\} \end{cases}$
2. S_b
2. S_c
3.Measure – resend or reflect
3.Measure – resend or reflect
4. Ack
4. Ack
5.The position of SIFT - B
5.The position of SIFT - C
6.publish dicussion
7.ECC and PA
7.ECC and PA

FIGURE 1
The proposed SQKD protocol.

TABLE 1 Alice's operation.

Bob's operation	Charlie's operation	Alice's operation
CTRL-B	CTRL-C	perform Bell-state measurement on CTRL-B qubit and CTRL-C qubit
SIFT-B	CTRL-C	measure SIFT-B qubit and CTRL-C qubit with Z-basis respectively
CTRL-B	SIFT-C	measure CTRL-B qubit and SIFT-C qubit with Z-basis respectively
SIFT-B	SIFT-C	measure SIFT-B qubit and SIFT-C qubit with Z-basis respectively

results. If it is higher than predefined threshold P_{CTRL} (the threshold depends on the noise level of the quantum channel), they abort the protocol.

Case 2. Bob performs the SIFT on some particles S_b^i and Charlie applies the operation CTRL on some particles S_c^i with the same i in Step 3. Alice measures S_b^i and S_c^i with Z-basis respectively and examines whether the two corresponding measurement results are equal. If the error rate is less than P_{TEST} (the threshold depends on the noise level of the quantum channel), the protocol continues. Otherwise it is terminated. In this case, Alice will obtain $2n$ SIFT-B bits. Alice chooses at random n SIFT-B bits to be TEST-B bits and announces what are the chosen bits and the value of these TEST-B bits by the classical channel. Alice's measurement results must be the states sent by Bob. Bob checks the error rate on the TEST bits. If it is higher than some predefined threshold P_{TEST}, Alice and Bob abort the protocol.

Case 3. Bob performs the operation CTRL on some particles S_b^i and Charlie applies the operation SIFT on some particles S_c^i with

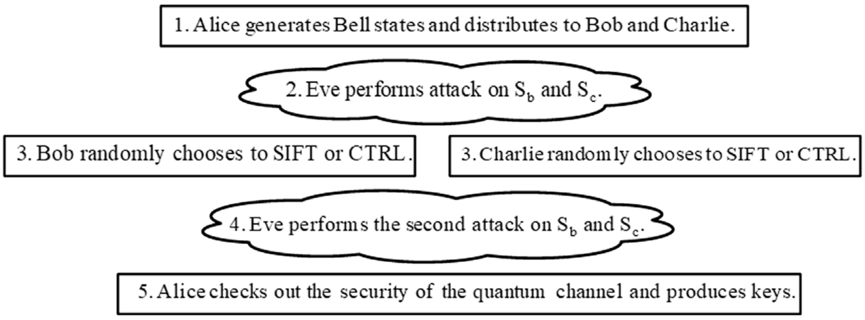

1. Alice generates Bell states and distributes to Bob and Charlie.
2. Eve performs attack on S$_b$ and S$_c$.
3. Bob randomly chooses to SIFT or CTRL.
3. Charlie randomly chooses to SIFT or CTRL.
4. Eve performs the second attack on S$_b$ and S$_c$.
5. Alice checks out the security of the quantum channel and produces keys.

FIGURE 2
Eve's attack.

the same i in Step 3. Alice measures S_b^i and S_c^i with Z-basis respectively and examines whether the two corresponding measurement results are equal. If the error rate is less than P_{TEST}, the protocol continues. Otherwise it is terminated. In this case, Alice will capture $2n$ SIFT-C bits. Alice selects random n SIFT-C bits as the TEST-C bits and announces the positions of the TEST-C bits and the value of these bits to Charlie. Charlie compares his measurement results with TEST-C bits, if it is higher than some predefined threshold P_{TEST}, Alice and Charlie abort the protocol.

Case 4. Both Bob and Charlie perform the operation SIFT on some particles with the same superscript i, ($i = 1, \ldots, N$). Alice measures S_b^i and S_c^i with Z-basis respectively and examines whether the two corresponding measurement results are equal. Alice aborts the protocol as the error rate is higher than the predefined threshold P_{TEST}. Alice requests measurement results from Bob and Charlie, and checks the error rate among these bits, if it is higher than the predefined threshold P_{TEST}, they abort the protocol.

Step 7: Alice and Bob select the n remaining SIFT-B bits in Case 2 to be used as INFO bits. Likewise, Alice and Charlie select the n remaining SIFT-C bits in Case 3 to be used as INFO bits. They abort the protocol as the number of remaining SIFT-B (SIFT-C) bits is less than n. Alice announces publicly the error correction code (ECC) and privacy amplification data [37–40]; Alice and Bob (Alice and Charlie) use them to extract the final key from the n-bit INFO string.

3 Security analysis

Basically, all existing SQKD protocols that adopt two-way quantum communication are suffer from the Trojan-horse attacks [41, 42]. To resist this kind of attacks, the photon number splitter device and the optical wavelength filter device could be equipped [43, 44]. Besides, identification should be employed to resist man-in-the-middle attack [45–47].

In this section, the security of the proposed protocol will be analyzed. Here, Eve is an outside attack and will try to perform the following possible attacks to reveal the secret key of the participants (as shown in Figure 2). Hence, the following five well-known attacks will be discussed.

3.1 Entangle-measure attack

Assume Eve possesses full quantum computational power and takes control of the quantum channel, Eve will prepare an ancillary quantum state $|E\rangle$ and performs an unitary operations, U_E, on the composite system $|\rho\rangle \otimes |E\rangle$, where $|\rho\rangle$ represents the transmitting qubit between participants. The effect of Eve's unitary operation U_E on the $|0\rangle$ or the $|1\rangle$ can be expressed as

$$U_E|0\rangle|E\rangle = a|0\rangle|e_0\rangle + b|1\rangle|e_1\rangle \tag{1}$$

$$U_E|1\rangle|E\rangle = c|0\rangle|e_2\rangle + d|1\rangle|e_3\rangle \tag{2}$$

where $|a|^2 + |b|^2 = 1$, $|c|^2 + |d|^2 = 1$, $\langle e_i|e_i\rangle = 1$ ($i = 0, 1, 2, 3$) and $\langle e_0|e_1\rangle = \langle e_2|e_3\rangle = 0$. When Eve captures the transit qubit on its return, Eve will implement another operation U_F. The following states are produced by implementing operation U_F on the states in Eqs 1, 2.

$$U_F U_E|0\rangle|E\rangle = |0\rangle\left(a_1|f_0\rangle + b_1|f_1\rangle\right) + |1\rangle\left(c_1|f_2\rangle + d_1|f_3\rangle\right) \tag{3}$$

$$U_F U_E|1\rangle|E\rangle = |0\rangle\left(a_2|f_4\rangle + b_2|f_5\rangle\right) + |1\rangle\left(c_2|f_6\rangle + d_2|f_7\rangle\right) \tag{4}$$

where $|a_i|^2 + |b_i|^2 + |c_i|^2 + |d_i|^2 = 1$ ($i = 1, 2$), and $\langle f_i|f_i\rangle = 1$ ($i = 0, 1, \ldots, 7$). At some point, Eve will measure the ancillary states to infer the private information based on the measurement of $|E\rangle$. We will now prove security against entangle-measure attack, that is, there is no unitary operations that allows Eve to obtain information about the participant's secret key without being detected.

When Alice prepares the Bell state and sends it through the quantum channel, Eve intercepts the particles sent by Alice and implements an unitary operation U_E on transmitted quantum state. The original Bell state will be transformed as

$$U_E|\phi^+\rangle|E\rangle = \frac{1}{\sqrt{2}}(a|00\rangle|e_0\rangle + b|01\rangle|e_1\rangle + c|10\rangle|e_2\rangle + d|11\rangle|e_3\rangle) \tag{5}$$

Then Eve distributes the contaminated quantum states to Bob and Charlie. If both Bob and Charlie perform SIFT, the participants will take the public discussion to check their measurement result in Step 6. Specifically, they will calculate the error rate on the TEST bits. If the error rate is lower than predefined threshold P_{TEST}, the process continues. Thus, in order to pass the detection on TEST qubits, Eve must modify the U_E to satisfy the following conditions

$$b|e_1\rangle = c|e_2\rangle = \vec{0} \tag{6}$$

Therefore, Eq. 5 becomes

$$U_E|\phi^+\rangle|E\rangle = \frac{1}{\sqrt{2}}(a|00\rangle|e_0\rangle + d|11\rangle|e_3\rangle) \tag{7}$$

When Eve intercepts the returned qubits sent by Bob and Charlie, Eve will perform the second unitary operation U_F on the transmitted quantum state. The Eq. 7 will be disturbed as follows

$$\begin{aligned} U_FU_E|\phi^+\rangle|E\rangle = \frac{1}{\sqrt{2}}[&|00\rangle(a_1|f_0\rangle + b_1|f_1\rangle) + |01\rangle(c_1|f_2\rangle + d_1|f_3\rangle) \\ &+|10\rangle(a_2|f_4\rangle + b_2|f_5\rangle) + |11\rangle(c_2|f_6\rangle + d_2|f_7\rangle)] \end{aligned} \tag{8}$$

Then Eve sends the polluted quantum states to Alice. Eve can infer the participants' measurement results through measuring his ancillary qubit. However, Alice will perform the Bell-state measurement on CTRL qubits in Step 6, and detect the presence of Eve if the error rate of CTRL qubits is higher than predefined threshold P_{CTRL}. Thus, Eve must set $a_2|f_4\rangle + b_2|f_5\rangle = c_1|f_2\rangle + d_1|f_3\rangle = 0$, and $a_1|f_0\rangle + b_1|f_1\rangle = c_2|f_6\rangle + d_2|f_7\rangle$. According to the abovementioned setting, the transmission of quantum states is turned into

$$\begin{aligned} U_FU_E|\phi^+\rangle|E\rangle &= \frac{1}{\sqrt{2}}[|00\rangle(a_1|f_0\rangle + b_1|f_1\rangle) + |11\rangle(c_2|f_6\rangle + d_2|f_7\rangle)] \\ &= |\phi^+\rangle(a_1|f_0\rangle + b_1|f_1\rangle) \end{aligned} \tag{9}$$

Based on the analysis of the above, the final quantum state of Eve's probe $|E\rangle$ is independent of the transmission of quantum entangled system, Eve can not obtain any information regarding INFO bits. In contrast, if Eve wishes to obtain useful information regarding the classical participants's INFO bits, so the Eve's attack will induce a detectable disturbance that increases the error rate P_{TEST} and P_{CTRL}. This gives participants a nonzero probability of detecting the Eve's attack.

3.2 Modification attack

In the modification attack, the purpose of Eve is to enable the communicating parties to obtain inconsistent keys by using the unitary operation. For example, Eve can implement the unitary operation σ_x to flip the qubit, where

$$\sigma_x = |0\rangle\langle 1| + |1\rangle\langle 0|. \tag{10}$$

To completely analyze modification attack, we discuss the following three situations: 1) Eve would perform the unitary operation σ_x on the quantum channel between Alice and Bob, Alice and Charlie, simultaneously; 2) Eve would randomly perform the unitary operation σ_x on the channel only between Alice and Bob; 3) Eve would randomly perform the unitary operation σ_x on the channel only between Alice and Charlie. All the situations of Modification Attack are shown below.

- Eve intends to flip S_b^i and S_c^i simultaneously, the $|\phi^+\rangle$ will be disturbed as follows

$$\sigma_x \otimes |\phi^+\rangle = \frac{1}{\sqrt{2}}(|11\rangle + |00\rangle) \tag{11}$$

The above quantum state is the same as the primitive Bell state, so it has no effect on the conduct of the protocol.

- Eve merely flips S_b^i, the Bell state will be changed to

$$\sigma_x \otimes |\phi^+\rangle = \frac{1}{\sqrt{2}}(|10\rangle + |01\rangle) \tag{12}$$

Although Eve successfully changed the state, his sneaky action will be detected in Step 6. In case both Bob and Charlie select to CTRL, Alice will check the error rate on the CTRL qubits, if the error rate is higher than predefined threshold P_{CTRL}, Alice aborts the protocol. Besides, both Bob and Charlie select to SIFT, they will calculate the error rate on the TEST bits. Likewise, the presence of Eve can be detected. There is the probability of $P_1 = 1 - 0.5^n$ to detect Eve's attack. It implies that if n is large enough, the detection probability will approach 1.

- Eve only flips S_c^i, the original Bell state will be transformed as

$$\sigma_x \otimes |\phi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) \tag{13}$$

Similar to the previous case, Eve's operation will be detected in Step 6. Alice will find errors with a $P_2 = 1 - 0.5^n$ probability. When n is large enough, the probability of an eavesdropper being detected will approach 1.

In summary, the proposed scheme can successfully resist modification attack through detecting SIFT and CTRL qubits.

TABLE 2 Comparison results with other SQKD protocols.

	Reference [18]	Reference [28]	Reference [26] - A	Reference [26] - B
Function	One quantum party share a secret key with a classical party	One quantum party share a secret key with a classical party	One quantum party share a secret key with a classical party	Two classical users share a secret key with the help of a third party
Quantum capability of classical participant	1) Generation	1) Generation	1) Generation	1) Generation
	2) Measurement	2) Measurement	2) Measurement	2) Measurement
	3) Reflection	3) Reflection	3) Reflection	3) Reflection
Quantum resource	Single photons	Single photons in both polarization and spatial-mode degrees of freedom	GHZ-like states	GHZ-like states
Pre-shared coding rules	No	No	No	Yes
Number of total participants	2	2	2	3
Number of secret keys	1	1	1	1
Quantum efficiency	$\frac{1}{12}$	$\frac{1}{9}$	$\frac{1}{8}$	$\frac{3}{32}$

3.3 Intercept-resend attack

Eve attempts to implement an intercept-resend attack on the traveling particles in S_b, to obtain what Bob's operation is. Firstly, Eve intercepts and saves the particle sequence S_b. Secondly, Eve sends the fake single photons randomly chosen from two different states (*i.e.*, $|+\rangle$, $|-\rangle$). Finally, Eve tries to infer Bob's operations through intercepting and measuring the returned particles by Bob in X-basis. That is, if the measurement result is different from the original state, the Bob's operation is SIFT. Unfortunately, if the measurement result is the same as the initial state, Eve dan not distinguish Bob's operation between SIFT and CTRL. Analogously, it is also useless for attacking S_c.

3.4 Measure-resend attack

In order to obtain SIFT-B bits and SIFT-C bits, Eve may intercept each traveling qubit of S_b and S_c and measure it with Z-basis. After Eve has performed the measurement operation on S_b and S_c, the initial Bell state generated by Alice is turned into $|00\rangle$, $|11\rangle$ with the same probability. Without loss of generality, assume that the original Bell state is collapsed into $|00\rangle$. Once Eve measures the qubits which Bob or Charlie measures, he will acquire SIFT-B bits and SIFT-C bits. However, Eve measures the qubits which both Bob and Charlie reflect, this attack will destroy the entanglement of Bell state. Thus, Eve must measure the corresponding position in which measured by Bob or Charlie. However, Eve does not have any information about their operation. In Step 6, Alice implements the Bell measurement on qubits consist of CTRL-B qubits and CTRL-C qubits in Case 1. The measurement results may be $|\phi^+\rangle$ or $|\phi^-\rangle$ with the same probability. The probability that Bob and Charlie both reflect is $\frac{1}{4}$, hence, the probability of discover Eve's fraudulent behavior is $\frac{1}{4}*\frac{1}{2}=\frac{1}{8}$. The reason Eve's measure-resend attack can be detected lies in two aspects: on one hand, the entanglement correlation among different particles of the initial state is destroyed by Eve's measurement; on the other hand, Bob and Charlie's operations are random to Eve.

3.5 Double CNOT attack

Assume that Eve performs the Double CNOT attack to the proposed protocol trying to get the secret key. For example, Eve performs CNOT operation, $U_{CNOT}=(|00\rangle\langle 00|+|01\rangle\langle 01|+|10\rangle\langle 10|+|11\rangle\langle 11|)$, with the particles sent to participants in Step 2 as the control bits the Eve's ancillary particles as the target bits. Then, Eve perform the second CNOT operation with the particles sent from the participants in Step 3 as the control bits and Eve's ancillary particles as the target bits. Eve tries to reveal Bob's (Charlie's) operation from the ancillary particles and then gets the secret key without being detected.

Alice's quantum state is $|\phi^+\rangle=\frac{1}{\sqrt{2}}(|00\rangle+|11\rangle)$, suppose Eve attacks the quantum channel between Alice and Bob. Eve generates a qubit $|0\rangle_E$ and performs a CNOT operation on Bell state and $|0\rangle_E$, the qubit systems become the following:

$$U_{CNOT}|\phi^+\rangle|0\rangle_E=\frac{1}{\sqrt{2}}(|00\rangle|0\rangle_E+|11\rangle|1\rangle_E) \tag{14}$$

After the operation, Eve send's the dirty qubits to Bob. According to the protocol, Bob either reflects it or resends a new one. Then, Eve intercepts each qubit send from Bob to Alice in Step 3 and performs the other CNOT operation on Bob's qubits and the corresponding qubit kept by Eve. If Bob chose to CTRL in Step 3, the qubit systems become the following:

$$\begin{aligned} U_{CNOT}\frac{1}{\sqrt{2}}(|00\rangle|0\rangle_E+|11\rangle|1\rangle_E) &= \frac{1}{\sqrt{2}}(|00\rangle|0\rangle_E+|11\rangle|0\rangle_E) \\ &= |\phi^+\rangle|0\rangle_E \end{aligned} \tag{15}$$

TABLE 3 Comparison results with other SQKD protocols.

	Reference [23]	Reference [24]	Proposed three-party SQKD	Extended m + 1 party SQKD
Function	Two classical users share a secret key with the help of a third party	Two classical users share a secret key with the help of a third party	One quantum party share two secret keys with two classical parties respectively	One quantum party share m secret keys with m classical parties respectively
Quantum capability of classical participant	1) Generation	1) Generation	1) Generation	1) Generation
	2) Reflection	2) Measurement	2) Measurement	2) Measurement
	3) Reorder	3) Reflection	3) Reflection	3) Reflection
Quantum resource	Bell states and Z-basis single photons	X-basis single photons	Bell states	m-particle GHZ states
Pre-shared coding rules	No	No	No	No
Number of total participants	3	3	3	3
Number of secret keys	1	1	2	m
Quantum efficiency	$\frac{1}{8}$	$\frac{1}{24}$	$\frac{1}{12}$	$\frac{1}{3m^2}$

If Bob chose to SIFT in Step 3, the qubits systems become the following:

$$\begin{aligned} U_{CNOT}|0\rangle_B|0\rangle_E) = |0\rangle_B|0\rangle_E \\ U_{CNOT}|1\rangle_B|1\rangle_E) = |1\rangle_B|0\rangle_E \end{aligned} \tag{16}$$

The subscript B means the new qubit generated by Bob. According to Eqs 15, 16, whether Bob performs CTRL or SIFT operation, Eve measures his qubit in Z-bais, he will always get the measurement result $|0\rangle$. That is, Eve cannot distinguish the current qubit is a reflected one or one generated by Bob. The analysis between Alice and Charlie is similar.

3.6 Key leakage problem

Assume Eve tries to eavesdrop on the Bob's raw key from the traveling qubits. Eve may perform Z-basis measurement on the photon sequence sent by Alice, S_b. Eve obtains the measurement results of S_b (i.e., $|0\rangle$, $|1\rangle$). Suppose Shannon entropy is defined as $E = -\sum_i \rho_i \log_2 \rho_i$, where ρ_i denotes probability distribution. The entropy E_1 can be computed as $E_1 = -2 \times \frac{1}{2}\log_2 \frac{1}{2} = 1$ bit. However, the protocol provides an eavesdropping check, which limits the possibility of the measurement S_b being used as the raw key, hence the probability is $\frac{1}{8}$.(i.e., Bob receives S_b and performs SIFT operation or CTRL operation. Charlie receives S_c and performs SIFT operation or CTRL operation. Alice and Bob obtain raw key in case that Bob performs SIFT operation and Charlie implements CTRL operation. Alice and Bob select half of the transmitted photons as eavesdropping check. Eventually, the probability of Eve eavesdrops the raw key from the measurement results of S_b is $\frac{1}{2} \times \frac{1}{2} \times \frac{1}{2} = \frac{1}{8}$). Hence, the entire entropy denotes $\frac{1}{8} \times E_1 = 0.125$ bit. Even though Eve can obtain 0.125 bit by performing eavesdropping, eventually the attack will be detected by an eavesdropping check in Step 6. Even if Eve passes the eavesdropping check, one can still perform the privacy amplification process on the transmitted information to distill the private key, avoiding the key leakage problem. Thus, Eve cannot obtain any private key under an eavesdropping attack.

4 Extension of the proposed semi-quantum key distribution protocol

4.1 Extended m + 1 party semi-quantum key distribution protocol

In this subsection, we extend the proposed scheme to construct a semi-quantum key distribution network that involves one quantum user Alice and m classical participants P_i (i = 1, 2, . . ., m). The detailed process of the extended SQKD protocol is shown as follows:

Step 1: Alice generates $N = 2n(m^2 + \delta)$ m-particle GHZ states in $|\Psi\rangle = \frac{1}{\sqrt{2}}(\underbrace{|00\ldots00\rangle}_{m} + \underbrace{|11\ldots11\rangle}_{m})$ and divides the m-particle GHZ states into m sequences

$$\begin{aligned} S_1 &= \{S_1^1, S_1^2, \ldots, S_1^N\}, \\ S_2 &= \{S_2^1, S_2^2, \ldots, S_2^N\}, \\ &\vdots \\ S_m &= \{S_m^1, S_m^2, \ldots, S_m^N\}. \end{aligned}$$

Step 2: Alice sends S_i to P_i (i = 1, 2, . . ., m) respectively.

Step 3: For each coming qubits, every classical user P_i randomly chooses to SIFT or CTRL. For convenience, we denote the qubits resended by P_i with SIFT - P$_i$ qubits.

Step 4: Alice stores the received qubits in m N-qubit quantum registers and informs all classical participants.

Step 5: All P_i publish which particles they choose to SIFT.

Step 6: According to the published information by all classical users, they check out the security of the quantum channel and produce INFO bits.

1) If all classical participants implement the operation CTRL on the kth m-particle GHZ state (k = 1, 2, . . ., N), Alice will perform m-particle GHZ measurement on the kth m-particle GHZ state. Alice checks the error rate on these measurement results. If it is higher than predefined threshold P_{CTRL}, they abort the protocol.

2) Only one classical participant P_i perform the operation SIFT, the others P_j apply the operation CTRL on kth m-particle GHZ state (k = 1, 2, . . ., N). Alice will measure these m particles with Z-basis respectively and examines whether these measurement results are equal. If the error rate is less than P_{TEST}, the protocol continues. Otherwise it is terminated. In this case, Alice will obtain $2n$ SIFT - P_i bits. Alice chooses at random n SIFT - P_i bits to be TEST - P_i bits and announces what are the chosen bits and the value of these TEST - P_i bits by the classical channel. P_i checks the error rate on the TEST bits. If it is higher than some predefined threshold P_{TEST}, Alice and P_i abort the protocol.

3) If all classical participants implement the operation SIFT on kth m-particle GHZ state (k = 1, 2, . . ., N), Alice will measure these m particles with Z-basis respectively and examines whether these measurement results are equal. Alice aborts the protocol as the error rate is higher than the predefined threshold P_{TEST}. Alice requests measurement results from all classical participants, and checks the error rate among these bits, if it is higher than the predefined threshold P_{TEST}, they abort the protocol.

4) Alice discards particles from other cases.

Step 7: Alice and P_i select the n remaining SIFT - P_i bits in above case 2 to be used as INFO bits. They abort the protocol as the number of INFO bits is less than n. Alice announces publicly the error correction code (ECC) and privacy amplification data, Alice and P_i use them to extract the final key from the n-bit INFO string.

4.2 Security analysis

4.2.1 Outside attack

In this part, we explain why an outside eavesdropper cannot learn the secrets in the extended scheme. In Step 2, qubits are transmitted and some usual attacks such as entangle-measure attack, intercept-resend attack and measure-resend attack may be launched by an outside eavesdropper. In Step 6, Alice will check the correctness of the returned particles from all classical participants. That is, an outside eavesdropper can be detected. Specifically, if Alice performs m-particle GHZ measurement on the kth m-particle GHZ state in case 1, her measurement result will be same as the initial entangle state. Once Eve has measured some reflected particles in case 1, he will be detected. Besides, Eve's destructive operations will also be found in case 2 and case 3. The specific analysis is similar to the presented three-party protocol since the idea is the same.

4.1.2 Participant attack.

Participant attack, which was put forward in Ref. [48], is a kind of powerful attack by either one dishonest participant or more dishonest participants who conspire together. We will discuss these two cases separately.

First, we discuss the case that one dishonest classical participant, without loss of generality, P_1, wants to steal other participants' secret. In our protocol, P_i's secret is generated from case 2, that is, only P_i performed operation SIFT, other $P_j(i \neq j)$ applied operation CTRL. P_1 cannot steal other participant's secrets since he performed operation CTRL. In step 5, P_1 can announce the erroneous information. For example, he declares a portion of SIFT as CTRL. He can obtain other participants' measurement results by implementing operation SIFT. However, it will be detected in case 1 since Alice's measurement result is different from original quantum state.

Second, we explain the more classical participants colluding together also cannot obtain others' secret. Without of generality, we consider the extreme case in which there are $m - 1$ classical participants P_1, P_2, . . ., P_{m-1} who collude together to steal the secret of classical user P_m. P_1, P_2, . . ., P_{m-1} cannot obtain which particles P_m performs operation SIFT, the conspiring participants cannot obtain P_m's key. If they publish misleading messages in step 5, Alice will find errors in case 1. Even though they can intercept the qubits from P_m, the conspiring participants can be put in light just like external attackers.

5 Comparison

In a quantum cryptographic protocol, we usually use the qubit efficiency to evaluate its performance of the communication protocol, which is defined as [49]

$$\eta = \frac{b_s}{q_t} \tag{17}$$

where b_s represents the sum of the shared secret bits between the participants and q_t denotes the total number of generated qubits in the protocol. In the presented three-party protocol, Alice expects to share n bits secret messages to Bob and Charlie at the same time. Alice prepares $8n(1 + \delta)$ Bell states and every Bell state have 2 particles, under the ideal conditions, $\delta = 0$; Bob and Charlie generate $4n$ single photons in Z-basis respectively, hence, the efficiency η of the proposed three-party SQKD is $\frac{1}{12}$. Likewise, we can compute the efficiency of the extended $m + 1$ party SQKD is $\frac{1}{3m^2}$.

We will compare the proposed protocol with typical SQKD protocols in Tables 2, 3. Here, Ref. [26] - A refers to the two-party protocol in Ref. [26], and Ref. [26] - B refers to the three-party protocol in Ref. [26]. In the Ref. [18], quantum user Alice can only share a secret key with classical user Bob by employing single photons. Refs. [18, 28] and Ref. [26] - A can only distribute one secret message at a time, but Alice can distribute two different raw keys in our three-party protocol. Reference [26] - B additionally use the pre-shared coding rules, which increases the complexity of operations between participants and thus, decreases the time efficiency. In the protocol of Ref. [23], although the classical participants do not need quantum measurement devices, quantum memory or quantum delay line is required for reordering qubits. The Refs. [23, 24] allows two limited semi-quantum users to establish a shared secret key with the help of a fully quantum server. However, the proposed three-party protocol accomplishes one quantum server to share two different secret keys with two classical users respectively at a time. Furthermore, our scheme can be extended to multi-user key distribution. If there are n users who want to distribute keys to each other in quantum network, typical SQKD needs $\frac{n(n-1)}{2}$ times to achieve key distribution, such as Refs. [18, 23, 24, 26, 28]. But our extended $m + 1$ party protocol only needs n times.

6 Conclusion

As above, different from other SQKD protocols, the proposed protocol allows one quantum participant to distribute two different session keys to two classical participants respectively. This scheme is expanded to simultaneously distribute m keys. It provides a good idea for building quantum key distribution network. For example, we can build a key distribution center which is quantum, but the users only have classical capabilities. The quantum server can process up to m distribution requests at a time, greatly reducing distribution time. We validate that the proposed SQKD protocol can overcome the entangle-measurement attack, the modification attack, and the other typical attacks.

Data availability statement

The raw data supporting the conclusion of this article will be made available by the authors, without undue reservation.

Author contributions

All authors listed have made a substantial, direct, and intellectual contribution to the work and approved it for publication.

Conflict of interest

The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Publisher's note

All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers. Any product that may be evaluated in this article, or claim that may be made by its manufacturer, is not guaranteed or endorsed by the publisher.

References

1. Bennett CH, Brassard G. *Quantum cryptography: Public key distribution and coin tossing* (2020). *arXiv preprint arXiv:2003.06557.*

2. Lo HK, Chau HF. Unconditional security of quantum key distribution over arbitrarily long distances. *science* (1999) 283(5410):2050–6. doi:10.1126/science.283.5410.2050

3. Shor PW, Preskill J. Simple proof of security of the bb84 quantum key distribution protocol. *Phys Rev Lett* (2000) 85(2):441–4. doi:10.1103/physrevlett.85.441

4. Wang XB. Fault tolerant quantum key distribution protocol with collective random unitary noise. *Phys Rev A (Coll Park)* (2005) 72(5):050304. doi:10.1103/physreva.72.050304

5. Lo HK, Curty M, Qi B. Measurement-device-independent quantum key distribution. *Phys Rev Lett* (2012) 108(13):130503. doi:10.1103/physrevlett.108.130503

6. Sasaki T, Yamamoto Y, Koashi M. Practical quantum key distribution protocol without monitoring signal disturbance. *Nature* (2014) 509(7501):475–8. doi:10.1038/nature13303

7. Yang CW. New probabilistic quantum key distribution protocol. *Int J Theor Phys (Dordr)* (2018) 57(12):3651–7. doi:10.1007/s10773-018-3878-0

8. Bunandar D, Anthony L, Lee C, Cai H, Long CM, Boynton N, et al. Metropolitan quantum key distribution with silicon photonics. *Phys Rev X* (2018) 8(2):021009. doi:10.1103/physrevx.8.021009

9. Aguado A, Lopez V, Lopez D, Peev M, Poppe A, Pastor A, et al. The engineering of software-defined quantum key distribution networks. *IEEE Commun Mag* (2019) 57(7):20–6. doi:10.1109/mcom.2019.1800763

10. Kumar A, Dadheech P, Singh V, Poonia RC, Raja L. An improved quantum key distribution protocol for verification. *J Discrete Math Sci Cryptography* (2019) 22(4):491–8. doi:10.1080/09720529.2019.1637153

11. Wu JZ, Yan L. Quantum key distribution protocol based on ghz like state and bell state. In: International Conference on Artificial Intelligence and Security. Berlin, Germany: Springer (2020). p. 298–306.

12. Wang Y, Lou X, Zhou F, Wang S, Huang G. (t, n) Threshold Quantum Secret Sharing Using Rotation Operation n) threshold quantum secret sharing based on

quantum walk. *Int J Theor Phys (Dordr)* (2022) 61(2):166–17. doi:10.1007/s10773-022-05121-x

13. Tian-Yu Y, Jia-Li H. Quantum secure multiparty summation based on the phase shifting operation of d-level quantum system and its application. *International Journal of Theoretical Physics* (2021) 60(3):819–827.

14. Tian-Yu Y, Hong-Kun L, Jia-Li H. Information leakage resistant quantum dialogue with single photons in both polarization and spatial-mode degrees of freedom. *Quantum Information Processing* (2021) 20(6):209

15. Boyer M, Dan K, Mor T. Quantum key distribution with classical bob. In: 2007 First International Conference on Quantum, Nano, and Micro Technologies (ICQNM'07). Guadeloupe, French Caribbean: IEEE (2007). p. 10.

16. Boyer M, Gelles R, Dan K, Mor T. Semiquantum key distribution. *Phys Rev A (Coll Park)* (2009) 79(3):032341. doi:10.1103/physreva.79.032341

17. Lu H, Cai QY. Quantum key distribution with classical alice. *Int J Quan Inform* (2008) 6(06):1195–202. doi:10.1142/s0219749908004353

18. Zou X, Qiu D, Li L, Wu L, Li L. Reply to "Comment on 'Semiquantum-key distribution using less than four quantum states' ". *Phys Rev A (Coll Park)* (2009) 79(5):046302. doi:10.1103/physreva.83.046302

19. Wang J, Zhang S, Zhang Q, Tang CJ. Semiquantum key distribution using entangled states. *Chin Phys Lett* (2011) 28(10):100301. doi:10.1088/0256-307x/28/10/100301

20. Yu KF, Yang CW, Liao CH, Hwang T. Authenticated semi-quantum key distribution protocol using bell states. *Quan Inf Process* (2014) 13(6):1457–65. doi:10.1007/s11128-014-0740-z

21. Li CM, Kun-Fei Y, Kao SH, Hwang T. Authenticated semi-quantum key distributions without classical channel. *Quan Inf Process* (2016) 15(7):2881–93. doi:10.1007/s11128-016-1307-y

22. Krawec WO. Mediated semiquantum key distribution. *Phys Rev A (Coll Park)* (2015) 91(3):032323. doi:10.1103/physreva.91.032323

23. Liu ZR, Hwang T. Mediated semi-quantum key distribution without invoking quantum measurement. *Annalen der Physik* (2018) 530(4):1700206. doi:10.1002/andp.201700206

24. Lin PH, Tsai CW, Hwang T. Mediated semi-quantum key distribution using single photons. *Annalen der Physik* (2019) 531(8):1800347. doi:10.1002/andp.201800347

25. Zhu KN, Zhou NR, Wang YQ, Wen XJ. Semi-quantum key distribution protocols with ghz states. *Int J Theor Phys (Dordr)* (2018) 57(12):3621–31. doi:10.1007/s10773-018-3875-3

26. Chen LY, Gong LH, Zhou NR. Two semi-quantum key distribution protocols with g-like states. *Int J Theor Phys (Dordr)* (2020) 59(6):1884–96. doi:10.1007/s10773-020-04456-7

27. Ye TY, Li HK, Hu JL. Semi-quantum key distribution with single photons in both polarization and spatial-mode degrees of freedom. *Int J Theor Phys (Dordr)* (2020) 59(9):2807–15. doi:10.1007/s10773-020-04540-y

28. Ye TY, Geng MJ, Xu TJ, Chen Y. Efficient semiquantum key distribution based on single photons in both polarization and spatial-mode degrees of freedom. *Quan Inf Process* (2022) 21(4):123–1. doi:10.1007/s11128-022-03457-1

29. Zhang W, Qiu D, Mateus P. Security of a single-state semi-quantum key distribution protocol. *Quan Inf Process* (2018) 17(6):135–21. doi:10.1007/s11128-018-1904-z

30. Krawec WO. Security proof of a semi-quantum key distribution protocol. In: 2015 IEEE International Symposium on Information Theory (ISIT). Hong Kong, China: IEEE (2015). p. 686–90.

31. Krawec WO. Restricted attacks on semi-quantum key distribution protocols. *Quan Inf Process* (2014) 13(11):2417–36. doi:10.1007/s11128-014-0802-2

32. Tsai CL, Hwang T. Semi-quantum key distribution robust against combined collective noise. *Int J Theor Phys (Dordr)* (2018) 57(11):3410–8. doi:10.1007/s10773-018-3854-8

33. Tsai CW, Yang CW. Cryptanalysis and improvement of the semi-quantum key distribution robust against combined collective noise. *Int J Theor Phys (Dordr)* (2019) 58(7):2244–50. doi:10.1007/s10773-019-04116-5

34. Meslouhi A, Hassouni Y. Cryptanalysis on authenticated semi-quantum key distribution protocol using bell states. *Quan Inf Process* (2017) 16(1):18–7. doi:10.1007/s11128-016-1468-8

35. Zhang W, Qiu D, Mateus P. Single-state semi-quantum key distribution protocol and its security proof. *Int J Quan Inform* (2020) 18(04):2050013. doi:10.1142/s0219749920500136

36. Krawec WO. Security of a semi-quantum protocol where reflections contribute to the secret key. *Quan Inf Process* (2016) 15(5):2067–90. doi:10.1007/s11128-016-1266-3

37. Reed IS, Solomon G. Polynomial codes over certain finite fields. *J Soc Ind Appl Math* (1960) 8(2):300–4. doi:10.1137/0108018

38. Gallager R. Low-density parity-check codes. *IEEE Trans Inf Theor* (1962) 8(1):21–8. doi:10.1109/tit.1962.1057683

39. Bennett CH, Brassard G, Claude C, Maurer UM. Generalized privacy amplification. *IEEE Trans Inf Theor* (1995) 41(6):1915–23. doi:10.1109/18.476316

40. Bennett CH, Brassard G, Robert JM. Privacy amplification by public discussion. *SIAM J Comput* (1988) 17(2):210–29. doi:10.1137/0217014

41. Deng FG, Zhou P, Li XH, Li CY, Zhou HY. *Robustness of two-way quantum communication protocols against trojan horse attack* (2005). *arXiv preprint quant-ph/0508168*.

42. Cai QY. Eavesdropping on the two-way quantum communication protocols with invisible photons. *Phys Lett A* (2006) 351(1-2):23–5. doi:10.1016/j.physleta.2005.10.050

43. Deng FG, Li XH, Zhou HY, Zhang ZJ. Improving the security of multiparty quantum secret sharing against trojan horse attack. *Phys Rev A (Coll Park)* (2005) 72(4):044302. doi:10.1103/physreva.72.044302

44. Li XH, Deng FG, Zhou HY. Improving the security of secure direct communication based on the secret transmitting order of particles. *Phys Rev A (Coll Park)* (2006) 74(5):054302. doi:10.1103/physreva.74.054302

45. Zhang Z, Zeng G, Zhou N, Jin X. Quantum identity authentication based on ping-pong technique for photons. *Phys Lett A* (2006) 356(3):199–205. doi:10.1016/j.physleta.2006.03.048

46. Shi WM, Zhang JB, Zhou YH, Yang YG. A novel quantum deniable authentication protocol without entanglement. *Quan Inf Process* (2015) 14(6):2183–93. doi:10.1007/s11128-015-0994-0

47. Zhou NR, Zhu KN, Bi W, Gong LH. Semi-quantum identification. *Quan Inf Process* (2019) 18(6):197–17. doi:10.1007/s11128-019-2308-4

48. Gao F, Qin SJ, Wen QY, Zhu FC. A simple participant attack on the brádler-dušek protocol. *Quan Inf Comput* (2007) 7(4):329–34. doi:10.26421/qic7.4-4

49. Cabello A. Quantum key distribution in the holevo limit. *Phys Rev Lett* (2000) 85(26):5635–8. doi:10.1103/physrevlett.85.5635

frontiers | Frontiers in Physics

TYPE Original Research
PUBLISHED 21 October 2022
DOI 10.3389/fphy.2022.1047466

Check for updates

OPEN ACCESS

EDITED BY
Xiubo Chen,
Beijing University of Posts and Telecommunications, China

REVIEWED BY
Guang-Bao Xu,
Shandong University of Science and Technology, China
Lihua Gong,
Nanchang University, China
Bin Liu,
Chongqing University, China

*CORRESPONDENCE
Chun-Yue Lu,
lu_chyue66@163.com
Gong-De Guo,
ggd@fjnu.edu.cn
Song Lin,
lins95@gmail.com

SPECIALTY SECTION
This article was submitted to Quantum Engineering and Technology, a section of the journal Frontiers in Physics

RECEIVED 18 September 2022
ACCEPTED 06 October 2022
PUBLISHED 21 October 2022

CITATION
Gao L-Z, Lu C-Y, Guo G-D, Zhang X and Lin S (2022), Quantum K-nearest neighbors classification algorithm based on Mahalanobis distance.
Front. Phys. 10:1047466.
doi: 10.3389/fphy.2022.1047466

Quantum *K*-nearest neighbors classification algorithm based on Mahalanobis distance

Li-Zhen Gao[1,2], Chun-Yue Lu[3]*, Gong-De Guo[3]*, Xin Zhang[4] and Song Lin[5]*

[1]College of Computer Science and Information Engineering, Xiamen Institute of Technology, Xiamen, China, [2]Higher Educational Key Laboratory for Flexible Manufacturing Equipment Integration of Fujian Province, Xiamen Institute of Technology, Xiamen, China, [3]College of Computer and Cyber Security, Fujian Normal University, Fuzhou, China, [4]College of Mathematics and Statistics, Fujian Normal University, Fuzhou, China, [5]Digital Fujian Internet-of-Things Laboratory of Environmental Monitoring, Fujian Normal University, Fuzhou, China

Mahalanobis distance is a distance measure that takes into account the relationship between features. In this paper, we proposed a quantum *K*NN classification algorithm based on the Mahalanobis distance, which combines the classical *K*NN algorithm with quantum computing to solve supervised classification problem in machine learning. Firstly, a quantum sub-algorithm for searching the minimum of disordered data set is utilized to find out *K* nearest neighbors of the testing sample. Finally, its category can be obtained by counting the categories of *K* nearest neighbors. Moreover, it is shown that the proposed quantum algorithm has the effect of squared acceleration compared with the classical counterpart.

KEYWORDS
quantum computing, quantum machine learning, k-nearest neighbor classification, Mahalanobis distance, quantum algorithm

1 Introduction

With the development of era, the amount of global data is increasing exponentially every year. People often use machine learning to extract valid information from large amounts of data. However, with the increase of the amount of data, classical machine learning algorithms need a lot of time. How to design an efficient learning algorithm has become a major difficulty in the field of machine learning. At this point, the speed advantage of quantum computing over classical computing in solving certain specific problems has led more and more scholars to think about how to use quantum computing to solve the problem more efficiently and has given rise to a new field of research – quantum machine learning (QML). Quantum machine learning uses quantum superposition, quantum entanglement and other basic principles of quantum mechanics to realize computing tasks [1]. That is to say, QML is a quantum version of machine learning algorithms, which can achieve an exponential or squared quantum acceleration effect.

In recent years, researchers have studied quantum machine learning algorithms in depth and have achieved outstanding works in many branches of research, such as quantum *K*-nearest neighbor (Q*K*NN) algorithm [2–4], quantum support vector machine (QSVM) [5, 6], quantum neural network (QNN) [7–9] and so on [10, 11]. These algorithms take full advantage of quantum superposition and entanglement properties, allowing them to achieve quantum acceleration compared to classical algorithms.

Q*K*NN algorithms is a combination of quantum computing and classical algorithm. In 2013, Lloyd proposed a distance-based supervised learning quantum algorithm [12], which has exponential acceleration effect compared with classical algorithms. In 2014, Wiebe raised a Q*K*NN algorithm based on inner product distance [2] with squared acceleration effect. In 2017, Ruan realized a Q*K*NN algorithm based on Hamming distance [3], which has a time complexity of $O((log_2 M)^3)$ in the case of an optimal threshold. These algorithms measure the similarity between samples according to different distance metrics and achieve quantum acceleration. However, none of these distance measures consider the connection between individual attributes in the samples, which leads to many limitations in practical applications.

In this paper, we propose an efficient quantum version of *K*NN algorithm based on Mahalanobis distance. The algorithm architecture is similar to the classical algorithm. Similarly, we also notice two key points in designing the *K*NN algorithm. One is to efficiently compute the distance between *M* training samples and test sample, and the other is to find the smallest *K* number of samples. However, compared with the existing algorithms, the proposed algorithm takes fully account of the sample correlations and uses Mahalanobis distance to eliminate the interference of correlations between variables. Finally, the test samples are successfully classified using the algorithm of searching for *K*-nearest neighbor samples and the calculated Mahalanobis distance. The algorithm achieves a quadratic speedup in terms of time complexity.

2 Preliminaries

In this section, we briefly review the main process of the classical *K*NN classification and the Mahalanobis distance.

2.1 *K*-nearest neighbors classification algorithm

*K*NN algorithm is a common supervised classification algorithm, which works as follows: given a test sample and a training sample set, where the training sample set contains *M* training samples. Then, we compute the distances between the test sample and the *M* training samples, and find the *K* nearest training samples by comparing these distances. If the majority of the *K* nearest neighbor training samples of the test sample belong to a class, then the class of the test sample is that class [13, 14]. In the *K*NN algorithm, the most complex step is to compute the distance between the test sample and all training samples. Moreover, the computational complexity increases with the number and dimensionality of the training samples. In order to classify the test samples with dimension *N* and perform the distance metric with *M* *N*-dimensional training samples, we need to perform $O(MN)$ operations.

The general process of classical *K*NN classification can be summarized in the following points.

1) Choose an appropriate distance metric and calculate the distance between the test sample with *M* training samples.
2) Find the *K* training samples with closest distance to the test sample.
3) Count the class with the highest frequency among these *K* training samples, and that class is the class of the sample to be classified.

Although the *K*-nearest neighbor algorithm has better performance and accuracy, we should note that the choice of the distance metric is extremely important [15]. In general, we use the Euclidean distance as the metric. In fact, the Euclidean distance is just an integration of the two samples' deviations on each variable by treating all variables equally, which has some limitations in terms of data relevance. Instead, we use a generalization of the Euclidean distance: the Mahalanobis distance, which calculates the distance between two points by covariance and is an effective method to calculate the similarity of two unknown samples. Unlike the Euclidean distance, it takes into account the correlation between various variables. The difference between Euclidean distance and Mahalanobis distance is shown in Figure 1.

As shown above, we can easily find that the Mahalanobis distance is better than the Euclidean distance. The Mahalanobis distance can be used to reasonably unify the data between different features, since its computation takes into account the fact that the scale units are different in different directions.

2.2 The Mahalanobis distance

Mahalanobis distance is an effective metric to calculate the distance between two samples, which considers the different feature attributes. It also has two advantages as follows. 1) It is independent of the magnitude and the distance between two points is independent of the measurement units of the original data. 2) The Mahalanobis distance can also eliminate the interference of correlation between variables.

In this paper, the training samples and the test sample are combined into a data set $\{x_1, x_2, x_3, \cdots x_M, v\}$, which can be described as a column vector composed of N characteristic attributes $\{z_1, z_2, z_3 \cdots z_N\}^T$ μ_i is the expected value of i th element, $\mu_i = E(z_i)$. The correlation between the dimensions of these samples is expressed by the covariance matrix Σ, i.e.,

$$\Sigma = \begin{bmatrix} E[(z_1-\mu_1)(z_1-\mu_1)] & \cdots & E[(z_1-\mu_1)(z_N-\mu_N)] \\ E[(z_2-\mu_2)(z_1-\mu_1)] & \cdots & E[(z_2-\mu_2)(z_N-\mu_N)] \\ \vdots & \ddots & \vdots \\ E[(z_N-\mu_N)(z_1-\mu_1)] & \cdots & E[(z_N-\mu_N)(z_N-\mu_N)] \end{bmatrix} \tag{1}$$

where, the ij term in the covariance matrix (the ij term is a covariance) is

$$\Sigma_{ij} = cov(z_i, z_j) = E[(z_i-\mu_i)(z_j-\mu_j)]. \tag{2}$$

The Mahalanobis distance between data points x and y is

$$D = \sqrt{(x-y)^T \Sigma^{-1}(x-y)}, \tag{3}$$

where Σ is the covariance matrix of x and y. By multiplying the inverse of the covariance matrix based on Euclidean distance, the effect of correlation between the data can be eliminated.

As description above all, it is not difficult to find approaches to calculate the Mahalanobis distances between M training samples and the test sample

$$\sum_{i=1}^{M} d_i = \sum_{i=1}^{M} \sqrt{(x_i - v)\Sigma^{-1}(x_i - v)}. \tag{4}$$

Σ represents the covariance matrix of X and v. The covariance matrix is a semi-positive definite symmetric matrix that allows for eigenvalue decomposition. $\Sigma = \sum_{j=1}^{N} \lambda_j |\mu_j\rangle\langle\mu_j|$, where λ_j is the eigenvalue, and μ_j is the corresponding feature vectors. Then, Eq. 4 can be redescribed as

$$\sum_{i=1}^{M} d_i = \sum_{i=1}^{M} \sqrt{\langle x_i - v| \sum_{j=1}^{N} \lambda_j^{-1} |\mu_j\rangle\langle\mu_j|\ |x_i - v\rangle}. \tag{5}$$

While we need to get the K minimum distance of them, thus we just need to get

$$\sum_{i=1}^{M} d_i = \sum_{i=1}^{M} \sum_{j=1}^{N} \lambda_j^{-1} \langle\mu_j|x_i - v.\rangle \tag{6}$$

3 The proposed quantum *K*-nearest neighbor classification algorithm

In this section, we mainly describe the significant steps of the proposed quantum *K*NN classification algorithm.

3.1 Calculating the Mahalanobis distance

Computing similarity is an important subprogram in classification algorithms. For the classification of *non-numerical* data, Mahalanobis distance is one of the popular ways to calculate similarity. Here, we describe a quantum method to calculate Mahalanobis distance between x_i and v in parallel.

A1: *Prepare the superposition state*

According to Eq. 6, we need to prepare the required quantum states $\frac{1}{\sqrt{M}}\sum_{i=1}^{M}|i\rangle|x_i - v\rangle$ and the covariance matrix Σ. For simple description, $x_i - v$ is preprocessed on the basis of classical data to make it normalized data.

Here, we firstly introduce the preparation process of $\frac{1}{\sqrt{M}}\sum_{i=1}^{M}|i\rangle|x_i - v\rangle$. The process can be briefly divided into two steps. First, prepare the superposition type $\frac{1}{\sqrt{M}}\sum_{i=1}^{M}|i\rangle$,

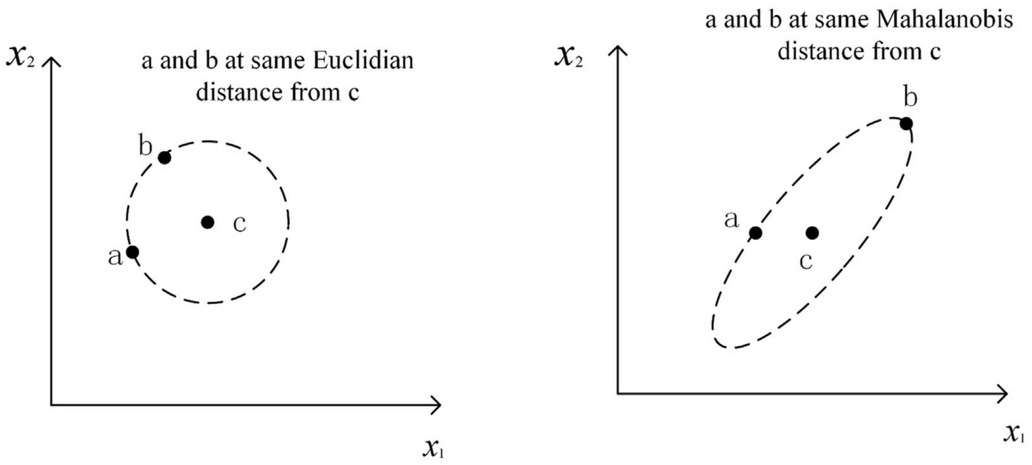

x_2
a and b at same Euclidian distance from c
b
c
a
x_1
x_2
a and b at same Mahalanobis distance from c
b
a
c
x_1

FIGURE 1
The difference between Euclidean distance and Mahalanobis distance.

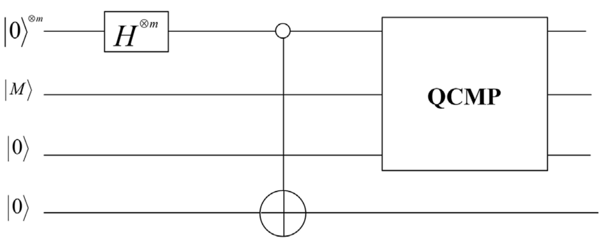


FIGURE 2
Prepare the quantum state $|\alpha\rangle$.

and then the data $x_i - v$ is accessed through quantum random access memory [16]. Next, we will explain these two steps in detail.

At first, we prepare $m = log_2(M+1)$ quantum qubit in the state of $|000\cdots000\rangle(|0\rangle^{\otimes m})$, and then a Hadamard gate operation is performed once for each qubit to get the state:

$$H^{\otimes m}|000\cdots000\rangle = \frac{1}{\sqrt{2^m}}\sum_{i=0}^{2^m-1}|i\rangle \tag{7}$$

However, our aim is to get the initial superposition qubits $|\alpha\rangle = \frac{1}{\sqrt{M}}\sum_{i=1}^{M}|i\rangle$. Since M may not be a power of 2, the state is obtained with the help of a quantum comparator [17], as show in Figure 2.

With the help of two auxiliary particles $|0\rangle|0\rangle$, we can judge the value space of index i through the quantum comparator. The details are shown as follows:

$$U_1\left(|0\rangle^{\otimes m}|0\rangle|0\rangle\right) \rightarrow \frac{1}{\sqrt{2^m}}\sum_{i=0}|i\rangle|0\rangle|1\rangle + \frac{1}{\sqrt{2^m}}\sum_{0<i\leq M}|i\rangle|0\rangle|0\rangle + \frac{1}{\sqrt{2^m}}\sum_{i>M}|i\rangle|1\rangle|0\rangle \tag{8}$$

Then we measure the auxiliary particles to obtain the target state. When the result is $|0\rangle|0\rangle$ and the probability of measuring success is $\frac{M}{2^m}$, the require quantum state $|\alpha\rangle = \frac{1}{\sqrt{M}}\sum_{i=1}^{M}|i\rangle$ will be obtained after $O\left(\frac{M}{2^m}\right) = O(1)$ times.

Finally, we access the classical data based on the quantum random access memory theory. It is assumed that there exists a quantum channel that can access the data stored in quantum random access memory, and the data $x_i - v$ is stored in the form of classical data in M storage units in QRAM. So, we can access $x_i - v$ efficiently through a black box O_x in $O(log_2 MN)$. The specific operation is as follows:

$$\frac{\sum_{i=1}^{M}|i\rangle|0\rangle}{\sqrt{M}} \xrightarrow{O_x} \frac{\sum_{i=1}^{M}|i\rangle|x_i - v\rangle}{\sqrt{M}} \tag{9}$$

Next, we show how to get the covariance matrix. Since the covariance matrix Σ is semi-positive definite, we can implement it by Hamiltonian simulation [18]. Assuming that $\Sigma = \sum_{j=1}^{N}\lambda_j|\mu_j\rangle\langle\mu_j|$ [19]. Prepare a quantum black box given access to Hermitian matrix Σ, any time t, and errors ϵ, operate with approximate unitary precision ϵ through a quantum circuit U_2. Then the state $e^{i\Sigma t}$ can be obtained.

$$\left\|U_2 - e^{i\Sigma t}\right\| \leq \epsilon \tag{10}$$

Compared with the classical algorithm, the state $e^{i\Sigma t}$ obtained by the quantum circuit has exponential acceleration effect. Its time complexity is $O(polylogN)$.

A2: *Compute distances*

In the following, we talk about how to compute the Mahalanobis distances between the test sample and the training samples, i.e., Eq. 6. Obviously, by performing the steps of A1, we have obtained the state $\frac{\sum_{i=1}^{M}|i\rangle|x_i-v\rangle}{\sqrt{M}}$. To obtain the form of Eq. 6, we need to perform the phase estimation and controlled rotation. Specifically, it can be divided into two sub-processes.

Step 2.1 Adding one register in the state $|0\rangle$ to get the state $\frac{\sum_{i=1}^{M}|i\rangle|0\rangle|x_i-v\rangle}{\sqrt{M}}$. Then, we perform an unitary operation on the second and the third registers controlled by U_2 to achieve the phase estimation. At this point, we obtain the quantum state $|\Psi_1\rangle$,

$$|\Psi_1\rangle = \frac{\sum_{i=1}^{M}\left[\sum_{j=1}^{N}\langle u_j|x_i - v\rangle|i\rangle\left|\frac{\widetilde{\lambda_j t_0}}{2\pi}\right\rangle|u_j\rangle\right]}{\sqrt{M}}. \tag{11}$$

In phase estimation, $\frac{\widetilde{\lambda_j t_0}}{2\pi} \in [0,1)$, which is a period that numerical values outside the range are projected into the range. So that we should limit the scope of $\frac{\lambda_j t_0}{2\pi}$ belong to $[-\frac{1}{2},\frac{1}{2})$. To ensure the accuracy of results, some algorithmic assumptions are made here, assuming that $|\lambda_j| \in [\frac{1}{k}, 1]$. Due to $\lambda_j \geq 0$, $t_0 > 0$ (t_0 is the minimum time for simulating the covariance matrix $e^{i\Sigma t}$), when $t_0 \leq \pi$, it can ensure $\frac{\lambda_j t_0}{2\pi} \in [-\frac{1}{2},\frac{1}{2})$. Usually, we take $t_0 = \pi$ to make the results obtained from the phase estimation more accurate.

Step 2.2 Adding an auxiliary qubit $|0\rangle$, and performing a controlled rotation operation (CR) on the second register of $|\Psi_1\rangle$, which can effectively extract the information in the quantum register to the amplitude of the quantum state. The process is as follows.

Suppose that $\theta \in R$, $\tilde{\theta}$ is a d-bit finite precision representation of θ. The controlled rotation U_θ can make:

$$|\tilde{\theta}\rangle|0\rangle \rightarrow |\tilde{\theta}\rangle\left(f(\tilde{\theta})|0\rangle + \sqrt{1 - f(\tilde{\theta})^2}|1\rangle\right). \tag{12}$$

So, the following operation can be achieved by setting the relevant parameters.

$$\left|\frac{\widetilde{\lambda_j t_0}}{2\pi}\right\rangle|0\rangle \rightarrow \left|\frac{\widetilde{\lambda_j t_0}}{2\pi}\right\rangle\left(f\left(\frac{\widetilde{\lambda_j t_0}}{2\pi}\right)|0\rangle + \sqrt{1 - f\left(\frac{\widetilde{\lambda_j t_0}}{2\pi}\right)^2}|1\rangle\right). \tag{13}$$

Apparently, if $f(x) = \frac{2\pi}{t_0}x$, we can obtain $|\Psi_2\rangle$.

$$|\Psi_2\rangle = \frac{\sum\limits_{i=1}^{M}|i\rangle\sum\limits_{j=1}^{N}\langle u_j|x_i - v\rangle\left|\frac{\tilde{\lambda}_j t_0}{2\pi}\right\rangle|u_j\rangle\left(\frac{c}{\tilde{\lambda}_j}|0\rangle + \sqrt{1-\left(\frac{c}{\tilde{\lambda}_j}\right)^2}|1\rangle\right)}{\sqrt{M}} \tag{14}$$

From the preceding information, we know that the Mahalanobis distance is $d_i = \sum_{j=1}^{N}\lambda_j^{-1}\langle\mu_j|x_i - v\rangle$, so $|\Psi_2\rangle$ can be rewrite to

$$|\Psi_2\rangle = \frac{\sum\limits_{i=1}^{M}|i\rangle d_i\left|\frac{\tilde{\lambda}_j t_0}{2\pi}\right\rangle|u_j\rangle|0\rangle}{\sqrt{M}} + \frac{\sum\limits_{i=1}^{M}|i\rangle\sum\limits_{j=1}^{N}\sqrt{1-\left(\frac{c}{\tilde{\lambda}_j}\right)^2}\langle u_j|x_i - v\rangle\left|\frac{\tilde{\lambda}_j t_0}{2\pi}\right\rangle|u_j\rangle|1\rangle}{\sqrt{M}} \tag{15}$$

For applying the Mahalanobis distance calculated by the above process to the classification algorithm, we have to use the amplitude estimation (AE) algorithm to transfer the distance information to qubits [20]. Then, we get the state about distance information $|\Psi_3\rangle = \frac{\sum_{i=1}^{M}|i\rangle|d_i\rangle}{\sqrt{M}}$. This process uses R iterations of Grover operators and the error is less than δ, where R and δ satisfy $R \geq \frac{\pi(\pi+1)}{\delta}$.

3.2 Searching *K* minimum distances

In this section, we use the state $|\Psi_3\rangle$ acquired by previous chapter to search the K minimum distances through quantum minimum search algorithm [21, 22].

Step 1. The set $D = \{D_1, D_2 \cdots D_K\}$ represents K training sample closest to test sample $v = \{v_1, v_2, v_3 \cdots v_N\}$ in the training sample. The initialization D is a random selection of K samples from the training samples.

Step 2. By Grover's algorithm, we get one point x_i at a time from the quantum state $|\Psi_3\rangle$. If that point is closer to the test sample than some points in D_k, i.e., $d(v, x_i) < d(v, D_k)\,(k \in [1, K])$, the ith point is used to replace the point D_k in D, and k is the $max\{d(v, D_k)\}\,(k \in [1, K])$.

Step 3. In order to get the k points with the smallest distance, repeat Step 2 to make q smaller and smaller (q is the number of remaining points in the set Q) until $q = 0$. That is, we find the k points that are closest to the test sample.

To analyze the time complexity of the above process more easily, we introduce a set Q, which is a subset of X beyond of D and smaller than some points in set D from the test sample. q is the number of points in set Q. In the following, we will use the size of q to analyze the performance of the algorithm after each operation. Repeating Step 2 k times can decrease q to $\frac{3}{4}q$. When $q > 2K$, it can be reduced to $\frac{1}{2}q$ by calling Oracle operation $O(\sqrt{\frac{KM}{q}})$ times. When q is decreased to $q \leq 2K$, the calling time of Oracle is $K\sqrt{\frac{M}{K} + \frac{M}{2K} + \frac{M}{4K} + \cdots}$. Then, if q is decreased to 0, the total time is $O\sqrt{KM}$. At this time, the points in set D are the K training samples closest to the test sample.

TABLE 1 The time complexity of the algorithm.

Step	Running time
A1	$O(logMN + polylogN)$
A2	$O(\frac{R \cdot polylogN}{\epsilon})$
A3	$O(\sqrt{KM})$
totally	$O(logMN + \frac{R \cdot polylogN}{\epsilon} + \sqrt{KM})$

4 Complexity analysis

Let us start with discussing the time complexity of the whole algorithm. As mentioned above, the algorithm contains three steps:

A1. Preparation of the initial state.
A2. Parallel computation of the martingale distance.
A3. Search for K nearest neighbor samples.

An overview of the time complexity of each step is shown in Table 1. A detailed analysis of each step of this algorithm is depicted as follows.

In step A1, $\frac{1}{\sqrt{M}}\sum_{i=1}^{M}|i\rangle|x_i - v\rangle$ can be generated in time $O(logMN)$ with the help of quantum comparator and QRAM. Then, the Hamiltonian simulation has been performed to make the covariance matrix Σ. So, the time complexity of A1 is $O(logMN + polylogN)$. In part of A2, we utilize phase estimation and controlled rotation to compute the distance, and then translate the information into quantum state. According to Ref. [1], the time complexity of phase estimation is $O(\frac{T_u}{\epsilon})$, where T_u is the time of preparing the unitary operator $e^{i\Sigma t}$ and $\frac{1}{\epsilon} = 2^{-m}\ e^{i\Sigma t}$ is obtained by Hamiltonian simulation, therefore, the time complexity is $O(polylogN)$. In a word, the time complexity is $O(\frac{polylogN}{\epsilon})$. Afterwards, in order to transfer the distance information to qubits, we have to perform the AE algorithm R times (discussed in step A2.2). Hence, the total time complexity of the quantum algorithm for computing the Mahalanobis distance is $O(logMN + \frac{R \cdot polylogN}{\epsilon})$. In Step A3, the time complexity of searching is analyzed in Section 3.2, that is $O(\sqrt{KM})$.

Therefore, the time complexity of the whole algorithm is $O(logMN + \frac{R \cdot polylogN}{\epsilon} + \sqrt{KM})$. Compared with the classical *KNN* classification algorithm with $O(MN)$ time complexity, it has quadratic acceleration.

5 Conclusion

In this paper, we combine the ideology of quantum computation with classical *KNN* classification algorithm to propose a quantum *KNN* classification algorithm based on Mahalanobis distance. First, we quantified the similarity measure algorithm based on the Mahalanobis distance. Then, K nearest neighbor samples are filtered using the quantum minimum search algorithm.

Compared with other quantum *K*NN classification algorithms based on Hamming distance or Euclidean distance, the Mahalanobis distance used in this paper overcomes the drawback that individual feature attributes with different degrees of variation play the same role in calculating the distance metric and excludes the interference of different degrees of correlation between variables. When the training sample is very large, the time complexity of the algorithm is $O[logMN + \frac{R\cdot polylogN}{\epsilon} + \sqrt{KM}]$, which has a quadratic acceleration effect. In conclusion, we give a complete quantum classification algorithm. By executing the proposed algorithm, the classification classes of the test samples can be obtained. Moreover, our work gives the sub-algorithm to calculate the Mahalanobis distance, which can be directly applied to the designing of other quantum machine learning algorithms, such as clustering.

Data availability statement

The raw data supporting the conclusions of this article will be made available by the authors, without undue reservation.

Author contributions

All authors listed have made a substantial, direct, and intellectual contribution to the work and approved it for publication.

Funding

This work was supported by the National Natural Science Foundation of China (Grants Nos. 61,772,134, 61,976,053 and 62,171,131), the Higher Educational Key Laboratory for Flexible Manufacturing Equipment Integration of Fujian Province (Xiamen Institute of Technology), the research innovation team of Embedded Artificial Intelligence Computing and Application at Xiamen Institute of Technology (KYTD202003), and the research innovation team of Intelligent Image Processing and Application at Xiamen Institute of Technology (KYTD202101).

Conflict of interest

The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Publisher's note

All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers. Any product that may be evaluated in this article, or claim that may be made by its manufacturer, is not guaranteed or endorsed by the publisher.

References

1. Nielsen MA, Chuang IL. Quantum computation and quantum information. *Math Structures Comput Sci* (2002) 17(6):1115.

2. Nathan W, Kapoor A, Svore K. Quantum algorithms for nearest-neighbor methods for supervised and unsupervised learning. *Quan Inf Comput* (2014) 15(3): 316–56. doi:10.26421/qic15.3-4-7

3. Yue R, Xue X, Liu H, Tan J, Li X. Quantum algorithm for k-nearest neighbors classification based on the metric of hamming distance. *Int J Theor Phys (Dordr)* (2017) 56(11):3496–507. doi:10.1007/s10773-017-3514-4

4. Hai VT, Chuong PH, Bao PT. New approach of knn algorithm in quantum computing based on new design of quantum circuits. *Informatica* (2022) 46(5): 2022. doi:10.31449/inf.v46i5.3608

5. Rebentrost P, Mohseni M, Lloyd S. Quantum support vector machine for big data classification. *Phys Rev Lett* (2014) 113(13):130503. doi:10.1103/physrevlett.113.130503

6. Zhang R, Wang J, Jiang N, Hong L, Wang Z. Quantum support vector machine based on regularized Newton method. *Neural Networks* (2022) 151:376–84. doi:10.1016/j.neunet.2022.03.043

7. Farhi E, Neven H. *Classification with quantum neural networks on near term processors* (2018). *arXiv preprint arXiv:1802.06002.*

8. Nathan K, Bromley TR, Arrazola JM, Schuld M, Quesada N, Lloyd S. Continuous-variable quantum neural networks. *Phys Rev Res* (2019) 1:033063. doi:10.1103/physrevresearch.1.033063

9. Cong I, Choi S, Lukin MD. Quantum convolutional neural networks. *Nat Phys* (2019) 15(12):1273–8. doi:10.1038/s41567-019-0648-8

10. Wu C, Huang F, Dai J, Zhou N. Quantum susan edge detection based on double chains quantum genetic algorithm. *Physica A: Stat Mech its Appl* (2022) 605: 128017. doi:10.1016/j.physa.2022.128017

11. Zhou N, Xia S, Ma Y, Zhang Y. Quantum particle swarm optimization algorithm with the truncated mean stabilization strategy. *Quan Inf Process* (2022) 21(2):42–23. doi:10.1007/s11128-021-03380-x

12. Lloyd S, Mohseni M, Rebentrost P. *Quantum algorithms for supervised and unsupervised machine learning* (2013). *arXiv preprint arXiv: 1307.0411.*

13. Dang Y, Jiang N, Hu H, Ji Z, Zhang W. Image classification based on quantum k-nearest-neighbor algorithm. *Quan Inf Process* (2018) 17(9):239–18. doi:10.1007/s11128-018-2004-9

14. Zhou N, Liu X, Chen Y, Du N. Quantum k-nearest-neighbor image classification algorithm based on k-l transform. *Int J Theor Phys (Dordr)* (2021) 60(3):1209–24. doi:10.1007/s10773-021-04747-7

15. Yu K, Guo G, Jing L, Lin S. Quantum algorithms for similarity measurement based on Euclidean distance. *Int J Theor Phys (Dordr)* (2020) 59(10):3134–44. doi:10.1007/s10773-020-04567-1

16. Giovannetti V, Lloyd S, Maccone L. Quantum random access memory. *Phys Rev Lett* (2008) 100(16):160501. doi:10.1103/physrevlett.100.160501

17. Wang D, Liu Z, Zhu W, Li S. Design of quantum comparator based on extended general toffoli gates with multiple targets. *Comput Sci* (2012) 39(9): 302–6.

18. Rebentrost P, Steffens A, Marvian I, Lloyd S. Quantum singular-value decomposition of nonsparse low-rank matrices. *Phys Rev A (Coll Park)* (2018) 97(1):012327. doi:10.1103/physreva.97.012327

19. He X, Sun L, Lyu C, Wang X. Quantum locally linear embedding for nonlinear dimensionality reduction. *Quan Inf Process* (2020) 19(9):309–21. doi:10.1007/s11128-020-02818-y

20. Brassard G, Høyer P, Mosca M, Tapp A. *Quantum amplitude amplification and estimation* (2000). *arXiv preprint arXiv:quant-ph/0005055.*

21. Gavinsky D, Ito T. *A quantum query algorithm for the graph collision problem* (2012). *arXiv preprint arXiv:1204.1527.*

22. Durr C, Høyer P. *A quantum algorithm for finding the minimum* (1996). *arXiv preprint quant-ph/9607014.*

frontiers | Frontiers in Physics

TYPE Original Research
PUBLISHED 24 October 2022
DOI 10.3389/fphy.2022.1021113

OPEN ACCESS

EDITED BY
Xiubo Chen,
Beijing University of Posts and Telecommunications (BUPT), China

REVIEWED BY
Mahmoud Abdel-Aty,
Sohag University, Egypt
Song Lin,
Fujian Normal University, China
Cai Zhang,
South China Agricultural University, China

*CORRESPONDENCE
Ke-Jia Zhang,
zhangkejia@hlju.edu.cn
Long Zhang,
lzhang@hlju.edu.cn

†These authors contributed equally to this work

SPECIALTY SECTION
This article was submitted to Quantum Engineering and Technology,
a section of the journal
Frontiers in Physics

RECEIVED 17 August 2022
ACCEPTED 30 September 2022
PUBLISHED 24 October 2022

CITATION
Fu S-J, Zhang K-J, Zhang L and Hou K-C (2022), A new non-entangled quantum secret sharing protocol among different nodes in further quantum networks.
Front. Phys. 10:1021113.
doi: 10.3389/fphy.2022.1021113

A new non-entangled quantum secret sharing protocol among different nodes in further quantum networks

Si-Jia Fu[1,2], Ke-Jia Zhang[1,2*†], Long Zhang[1,2*†] and Kun-Chi Hou[1,2]

[1]School of Mathematical Science, Heilongjiang University, Harbin, China, [2]Institute for Cryptology and Network Security, Heilongjiang University, Harbin, China

As an important branch of quantum secure multi-party computation, quantum secret sharing (QSS) can distribute secret information among dishonest network nodes without revealing the secrets. In this study, a new four-party QSS protocol based on locally indistinguishable orthogonal product (LIOP) states is first proposed for quantum network communication. Then, the general multiparty QSS model based on LIOP states will be expanded. Combined with the property of LIOP states and obfuscating operation, the source node can send the secrets to different destination nodes in the quantum network. Accordingly, it is proven that the destination nodes have to work together to recover the shared secrets against some existing attacks. Furthermore, no entangled resources and complicated operations are required in the presented protocol. We hope the results could make positive effects to the development of quantum secure communication in the future.

KEYWORDS

quantum secret sharing, quantum network, quantum secure communication, orthogonal product states, quantum cryptography

1 Introduction

With the rapid development of the Internet, the security of information is becoming more and more important. Cryptography, as one of the fastest developing fields in modern science, is the basic theory to guarantee information security. Due to the development of quantum algorithms [1, 2], classical cryptographic protocols based on computational complexity are facing great security threats. Applying quantum theory to the research of cryptography, quantum cryptography has made a scientific breakthrough in cryptography. In 2002, Long et al. first discussed the quantum secure direct communication idea and analyzed its application in further quantum networks [3]. In 2008, Ma et al. proposed a group quantum communication network based on quantum secret sharing (QSS) among multiple nodes [4]. Afterward, QSS is becoming an important application in the quantum network [5–12].

QSS is the use of quantum technology to distribute secrets to a group of sharers. In QSS, a secret can only be recovered by all authorized sharers working together. As an important branch of quantum secure multi-party computation, QSS has attracted much attention. In 1999, Hillery et al. proposed the first QSS protocol [13]. On this basis, Karlsson et al. designed a Bell state secret sharing protocol [14]. In 2004, Xiao et al. generalized Hillery's protocol to arbitrary multi-parties, effectively solving the limitation to secret sharing among multiple parties [15]. In 2017, Qin et al. proposed a QSS protocol using the n-qudit GHZ states [16]. In 2019, Zhang et al. gave an n-party QSS model based on multiparty entangled states [17]. In 2020, Mansour et al. presented a QSS protocol using maximally entangled multi-qudit states [18]. In 2021, Hu et al. proposed a novel dynamic QSS protocol in the high-dimensional quantum system based on transmitted particles and local unitary operations [19].

During the study, it can be seen that most of the existing QSS protocols are achieved by entangled states. As we know, the preparation of entangled states is difficult. It is necessary to propose more practical QSS protocols. The local indistinguishability of orthogonal product states is one of the hot topics in quantum information field recently. In 2015, Yu et al. constructed a set of orthogonal product states which cannot be perfectly distinguished by local operations and classical communication (LOCC) [20]. The indistinguishable orthogonal product (LIOP) states are easier to prepare than the entangled ones. It exhibits the overall non-locality of a wide range of applications in quantum cryptographic protocols. For example, Guo et al. proposed a quantum key distribution (QKD) protocol based on LIOP states in 2001 [21]. In 2007, Yang et al. presented a QSS protocol based on LIOP states [22]. In 2019, Jiang et al. proposed a quantum voting protocol based on LIOP states [23]. In 2020, Jiang et al. implemented a trusted third-party e-payment protocol on LIOP states [24].

In this study, we proposed a practical new four-party QSS protocol for LIOP states in quantum networks. First, the source node encodes the secret information into LIOP states. Second, the source node safely obfuscates the particles in the sequence and sends the corresponding particles to different destination nodes. Finally, all destination nodes work together to recover the secrets. Then, we generalize the protocol to any number of parties. According to the property of LIOP states, even if an attacker obtains $n - 1$ ($n \geq 3$) particles of orthogonal product states, it is impossible to determine the shared messages.

The rest of the study is organized as follows. In Section 2, we introduce two LIOP states: X-LIOP states and F-LIOP states. With the introduced LIOP states, a new specific four-party QSS protocol and an extended multi-party QSS protocol are presented in Section 3 and Section 4. The security of the protocol is discussed in Section 5. A brief conclusion is given in Section 6.

2 Preliminaries

Here, we introduce the following specific form and properties of LIOP states, which will be used in the following protocols. It is well known that a set of orthogonal states is locally indistinguishable if it cannot be completely distinguished by LOCC [25].

Definition 1. In a $2 \otimes 2 \otimes \cdots \otimes 2$ quantum system, the product basis that contains the following $2n$ orthogonal product states

$$\begin{aligned}
|\phi_1\rangle &= \frac{1}{\sqrt{2}}|0\rangle_1|1\rangle_2|1\rangle_3\cdots|1\rangle_{n-1}(|0\rangle+|1\rangle)_n,\\
|\phi_2\rangle &= \frac{1}{\sqrt{2}}|1\rangle_1|1\rangle_2|1\rangle_3\cdots(|0\rangle+|1\rangle)_{n-1}|0\rangle_n,\\
&\cdots\\
|\phi_n\rangle &= \frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)_1|0\rangle_2|1\rangle_3\cdots|1\rangle_{n-1}|1\rangle_n,\\
|\phi_{n+1}\rangle &= \frac{1}{\sqrt{2}}|0\rangle_1|1\rangle_2|1\rangle_3\cdots|1\rangle_{n-1}(|0\rangle-|1\rangle)_n,\\
|\phi_{n+2}\rangle &= \frac{1}{\sqrt{2}}|1\rangle_1|1\rangle_2|1\rangle_3\cdots(|0\rangle-|1\rangle)_{n-1}|0\rangle_n,\\
&\cdots\\
|\phi_{2n}\rangle &= \frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)_1|0\rangle_2|1\rangle_3\cdots|1\rangle_{n-1}|1\rangle_n
\end{aligned} \tag{1}$$

cannot be perfectly distinguished by LOCC, where $n \geq 3$, and the subscript i of the state $\frac{1}{\sqrt{2}}|0\rangle_1|1\rangle_2|1\rangle_3\cdots|1\rangle_{n-1}(|0\rangle+|1\rangle)_n$ denotes that the corresponding subsystem belong to the i-th party. In order to simplify the following protocol, the states aforementioned are named X-LIOP states.

We can get the special case of $n = 3$, i.e., the following Definition 2.

Definition 2. In a $2 \otimes 2 \otimes 2$ quantum system, the product basis that contains the following six orthogonal product states

$$\begin{aligned}
|\phi_1\rangle &= \frac{1}{\sqrt{2}}|0\rangle_1|1\rangle_2(|0\rangle+|1\rangle)_3,\\
|\phi_2\rangle &= \frac{1}{\sqrt{2}}|1\rangle_1(|0\rangle+|1\rangle)_2|0\rangle_3,\\
|\phi_3\rangle &= \frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)_1|0\rangle_2|1\rangle_3,\\
|\phi_4\rangle &= \frac{1}{\sqrt{2}}|0\rangle_1|1\rangle_2(|0\rangle-|1\rangle)_3,\\
|\phi_5\rangle &= \frac{1}{\sqrt{2}}|1\rangle_1(|0\rangle-|1\rangle)_2|0\rangle_3,\\
|\phi_6\rangle &= \frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)_1|0\rangle_2|1\rangle_3
\end{aligned} \tag{2}$$

cannot be perfectly distinguished by LOCC. In order to simplify the subsequent protocol, the states aforementioned are named F-LIOP states.

In Refs. [26, 27], these states are proven not to be perfectly distinguished by LOCC. We can find some properties of them.

Property 1. Even if $n - 1$ ($n \geq 3$) particles of orthogonal product states are obtained, the exact form cannot be determined.

Property 2. Each particle can be transmitted independently.

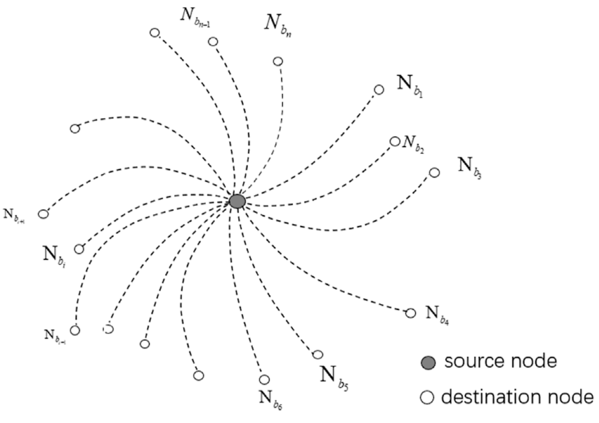


FIGURE 1
Communication in N_a and N_{b_i}.

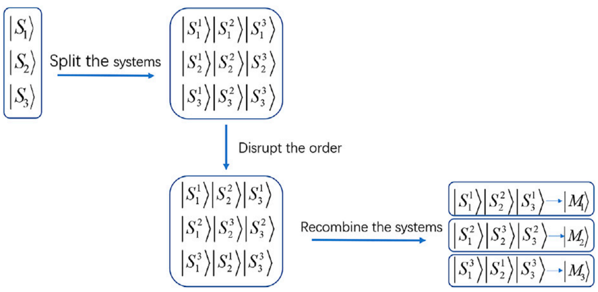

$|S_1\rangle$
$|S_2\rangle$
$|S_3\rangle$
Split the systems
$|S_1^1\rangle|S_1^2\rangle|S_1^3\rangle$
$|S_2^1\rangle|S_2^2\rangle|S_2^3\rangle$
$|S_3^1\rangle|S_3^2\rangle|S_3^3\rangle$
Disrupt the order
$|S_1^1\rangle|S_2^2\rangle|S_3^1\rangle$
$|S_1^2\rangle|S_2^3\rangle|S_3^2\rangle$
$|S_1^3\rangle|S_2^1\rangle|S_3^3\rangle$
Recombine the systems
$|S_1^1\rangle|S_2^2\rangle|S_3^1\rangle \rightarrow |M_1\rangle$
$|S_1^2\rangle|S_2^3\rangle|S_3^2\rangle \rightarrow |M_2\rangle$
$|S_1^3\rangle|S_2^1\rangle|S_3^3\rangle \rightarrow |M_3\rangle$

FIGURE 2
Generation process of the $|M\rangle$ sequence.

Property 3. An operation on one of the particles does not affect the other particles.

3 Four-party quantum secret sharing protocol based on F-LIOP states

3.1 Proposed protocol

In this section, a four-party QSS protocol applied in the quantum network based on F-LIOP states is proposed. The network graph has two types of nodes (Figure 1): the source node (N_a) wants to distribute secrets, and destination nodes ($N_{b_1}, N_{b_2}, N_{b_3}$) receive secrets. The secrets can only be recovered if all destination nodes collaborate. The specific description is as follows:

Step 1) N_a divides the secret message X into n groups, i.e., $x_1, \ldots, x_n$, where $x_i \in \{00, 01, 10, 11\}$, $i = 1, 2, \ldots, n$.

Step 2) N_a encodes the secret message X to a quantum sequence $|S\rangle$, and according to the following rules, it should be accepted by all the nodes:

$$\begin{aligned} 00 &\mapsto |\phi_1\rangle, & 01 &\mapsto |\phi_2\rangle \\ 10 &\mapsto |\phi_3\rangle, & 11 &\mapsto |\phi_4\rangle. \end{aligned} \tag{3}$$

Step 3) N_a generates three identical sequences $|S\rangle$, where the i-th sequence is denoted by $|S_i\rangle$, $i = 1, 2, 3$. N_a splits $|S_i\rangle$ into three subsystems, i.e., $|S_i^1\rangle, |S_i^2\rangle, |S_i^3\rangle$. Then, N_a generates three sequences $|M_1\rangle$, $|M_2\rangle$, and $|M_3\rangle$, where $|M_1\rangle = \{|S_1^1\rangle, |S_2^2\rangle, |S_3^1\rangle\}$, $|M_2\rangle = \{|S_1^2\rangle, |S_2^3\rangle, |S_3^2\rangle\}$, and $|M_3\rangle = \{|S_1^3\rangle, |S_2^1\rangle, |S_3^3\rangle\}$. The distribution of the particles is shown in Figure 2.

Step 4) N_a takes the left states composed of $|\phi_5\rangle, |\phi_6\rangle$ as decoy states to randomly insert the quantum sequence $|M_t\rangle$ to form $|M_t\rangle'$, where $t = 1, 2, 3$. Finally, $|M_t\rangle'$ is sent to N_{b_l} randomly, where $l = 1, 2, 3$. In this case, N_{b_l} does not know which particle they receive.

Step 5) After receiving the sequence $|M_t\rangle'$ from N_a, N_{b_l} sends an acknowledgment to N_a. Then, N_a announces both the basis and the positions of the decoy photons in $|M_t\rangle'$. N_{b_l} measures the decoy states. According to the measurement results of N_{b_l}, N_a performs eavesdropping detection. If no eavesdropping is detected, the protocol will continue to the next step. Otherwise, it will be aborted and will restart from Step 1.

Step 6) After the eavesdropping check, N_{b_l} has the sequence $|M_t\rangle$. Then, N_{b_l} sends the j-th group of particles $|M_t\rangle$ with the decoy states to N_{b_j}, where the decoy states are chosen from $\{|+\rangle, |-\rangle, |0\rangle, |1\rangle\}$, and where $j = 1, 2, 3$.

Step 7) After receiving the sequences from N_{b_l}, N_{b_j} sends him a confirmation. N_{b_l} announces both the basis and the positions of the decoy photons. According to the measurement results of N_{b_j} $(j \neq l)$, N_{b_l} performs eavesdropping detection. If no eavesdropping is detected, the protocol will continue to the next step; otherwise, it will be aborted.

Step 8) After the eavesdropping check, N_{b_l} has $|S_l^1\rangle, |S_l^2\rangle, |S_l^3\rangle$, i.e., $|S_l\rangle$. Then, the quantum sequence $|S_l\rangle$ is measured under the basis of Eq. 2, and $\bar{X}_l$ is recovered. N_a announces the measurement basis and order of all sequences.

Step 9) N_{b_1}, N_{b_2} and N_{b_3} hold the same particles and perform the same operations. Therefore, if the protocol is valid, $\bar{X}_1, \bar{X}_2, \bar{X}_3$ and the secret X must be the same. Intuitively, if $\bar{X}_1 = \bar{X}_2 = \bar{X}_3 = X$, the protocol will be valid; otherwise, the protocol fails.

TABLE 1 N_{b_l} received the sequence $|M_t\rangle$.

N_{b_1}	N_{b_2}	N_{b_3}
$\|M_1\rangle$	$\|M_2\rangle$	$\|M_3\rangle$
$\|M_1\rangle$	$\|M_3\rangle$	$\|M_2\rangle$
$\|M_2\rangle$	$\|M_1\rangle$	$\|M_3\rangle$
$\|M_2\rangle$	$\|M_3\rangle$	$\|M_1\rangle$
$\|M_3\rangle$	$\|M_1\rangle$	$\|M_2\rangle$
$\|M_3\rangle$	$\|M_2\rangle$	$\|M_1\rangle$

3.2 Example

To illustrate our protocol more clearly, the following example is proposed. For convenience, eavesdropping detection is ignored. Suppose $N_a's$ secret is 10010111, it can been encoded as $|\phi_3\rangle$, $|\phi_2\rangle$, $|\phi_2\rangle$, $|\phi_4\rangle$.

Therefore,

$|S_1^1\rangle = \{|+\rangle, |1\rangle, |1\rangle, |0\rangle\} = |S_2^1\rangle = |S_3^1\rangle$,

$|S_1^2\rangle = \{|0\rangle, |+\rangle, |+\rangle, |1\rangle\} = |S_2^2\rangle = |S_3^2\rangle$, and

$|S_1^3\rangle = \{|1\rangle, |0\rangle, |0\rangle, |-\rangle\} = |S_2^3\rangle = |S_3^3\rangle$.

Then, we get

$|M_1\rangle = \{|S_1^1\rangle, |S_2^2\rangle, |S_3^1\rangle\} = \{|+\rangle, |1\rangle, |1\rangle, |0\rangle; |0\rangle, |+\rangle, |+\rangle, |1\rangle; |+\rangle, |1\rangle, |1\rangle, |0\rangle\}$,

$|M_2\rangle = \{|S_1^2\rangle, |S_2^3\rangle, |S_3^2\rangle\} = \{|0\rangle, |+\rangle, |+\rangle, |1\rangle; |1\rangle, |0\rangle, |0\rangle, |-\rangle; |0\rangle, |+\rangle, |+\rangle, |1\rangle\}$, and

$|M_3\rangle = \{|S_1^3\rangle, |S_2^1\rangle, |S_3^3\rangle\} = \{|1\rangle, |0\rangle, |0\rangle, |-\rangle; |+\rangle, |1\rangle, |1\rangle, |0\rangle; |1\rangle, |0\rangle, |0\rangle, |-\rangle\}$.

Here, we assume that N_a sends $|M_1\rangle$, $|M_2\rangle$, $|M_3\rangle$ to $N_{b_1}, N_{b_2}, N_{b_3}$, respectively (This is just one of the cases; see Table 1).

Then, N_{b_1} (N_{b_2}, N_{b_3}) sends $|S_2^2\rangle$ $(|S_1^2\rangle, |S_1^3\rangle)$ to $N_{b_2}(N_{b_1}, N_{b_1})$. In the same way, N_{b_1} (N_{b_2}, N_{b_3}) sends $|S_3^1\rangle$ $(|S_3^2\rangle, |S_2^1\rangle)$ to N_{b_3} (N_{b_3}, N_{b_2}). N_{b_1} (N_{b_2}, N_{b_3}) holds $|S_1^1\rangle(|S_2^3\rangle, |S_3^3\rangle)$ on its own. Then, N_{b_1} gets$(|S_1^1\rangle, |S_1^2\rangle, |S_1^3\rangle) = |S_1\rangle$, N_{b_2} gets $|S_2\rangle$, and N_{b_3} gets $|S_3\rangle$. N_{b_1} (N_{b_2}, N_{b_3}) measures the quantum sequence $|S_1\rangle(|S_2\rangle$, $|S_3\rangle)$. According to the measurement basis and order of all sequences announced by N_a, the secret can be obtained. The specific procedures can be seen in Figure 3.

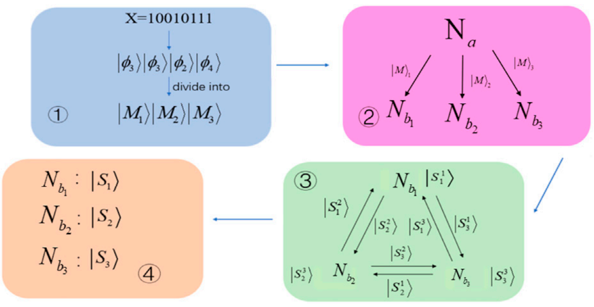


FIGURE 3
Process of quantum secret sharing.

4 Multi-party quantum secret sharing protocol based on X-LIOP states

In this section, we generalize the QSS protocol to any multi-party based on X-LIOP states applied in the quantum network. There are source node (N_a) and n destination nodes $(N_{b_1}, N_{b_2}, \ldots, N_{b_n})$. The secrets can be recovered only when the destination nodes cooperate together. The protocol can be described as follows. Here, we denote different m-bit sequences as $a_1 = 000\cdots000, a_2 = 000\cdots001,$ $a_3 = 000\cdots011, \ldots, a_{2^m-2} = 111\cdots101, a_{2^m-1} = 111\cdots110, a_{2^m} =$ $111\ \cdots\ 111$, where $m = \lfloor \log_2 n \rfloor$.

Step 1) N_a divides the secret message X into n groups, i.e., x_1, . . ., x_n, where $x_i \in \{a_1, a_2, a_3, \ldots, a_{2^m-2}, a_{2^m-1}, a_{2^m}\}$, $i = 1, 2, \ldots, n$.

Step 2) N_a encodes the secret message X to a quantum sequence $|S\rangle$ according to the following rules accepted by all the nodes:

$$a_i \mapsto |\phi_i\rangle\,(i = 1, 2, \ldots, 2^m). \tag{4}$$

Step 3) N_a creates n identical sequences $|S\rangle$, where the i-th sequence is denoted by $|S_i\rangle$ and i = 1, 2, . . ., n. N_a splits $|S_i\rangle$ into n systems, i.e., $|S_i^1\rangle, |S_i^2\rangle, \ldots, |S_i^n\rangle$. N_a generates n sequences $|M_1\rangle$, $|M_2\rangle$, . . ., $|M_n\rangle$, where $|M_1\rangle = \{|S_1^1\rangle, |S_2^2\rangle, \ldots, |S_{n-1}^{n-1}\rangle, |S_n^1\rangle\}$, $|M_2\rangle = \{|S_1^2\rangle, |S_2^3\rangle, \ldots, |S_{n-1}^n\rangle, |S_n^2\rangle\}$, . . ., and $|M_n\rangle = \{|S_1^n\rangle, |S_2^1\rangle, \ldots, |S_{n-1}^{n-2}\rangle, |S_n^n\rangle\}$ (Figure 4).

Step 4) N_a randomly inserts n unencoded orthogonal products into the quantum sequence as the decoy states and generates $|M_t\rangle'$, where t = 1, 2, 3, . . ., n. Finally, $|M_t\rangle'$ is given to N_{b_l} randomly, where l = 1, 2, 3, . . ., n. Therefore, N_{b_l} does not know which particle it gains.

Step 5) After getting the sequence $|M_t\rangle'$ from N_a, N_{b_l} sends an acknowledgment to the sender. N_a announces the basis and the positions of the decoy photons in $|M_t\rangle'$, and N_{b_l} measures these decoy states. According to the measurement results of N_{b_l}, N_a checks eavesdropping. If N_a does not detect eavesdropping, the protocol will continue to perform the next step. Otherwise, it will stop and restart from Step 1.

Step 6) After detecting eavesdropping, N_{b_l} gets sequence $|M_t\rangle$, and N_{b_l} generates n decoy states that are selected from $\{|+\rangle, |-\rangle, |0\rangle, |1\rangle\}$. Then, decoy states are randomly inserted into the sequence $|M_t\rangle$, and then, the j-th group of particles is sent to N_{b_j}, where j = 1, 2 . . ., n.

Step 7) After receiving the sequences from N_{b_l}, N_{b_j} sends N_{b_l} a confirmation. Then, N_{b_l} announces the basis and the positions of the decoy photons. According to the measurement results of N_{b_j}, N_{b_l} performs eavesdropping detection. If no eavesdropping is

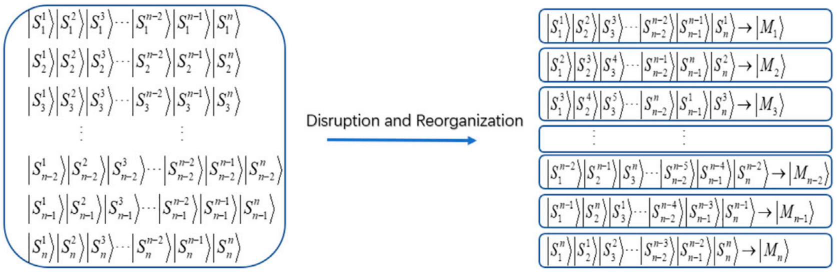


FIGURE 4
Generation process of the $|M\rangle$ sequence.

detected, the protocol will continue to the next step; otherwise, it will stop.

Step 8) After the eavesdropping check, N_{b_l} gets $|S_l^1\rangle, |S_l^2\rangle, |S_l^3\rangle, \ldots, |S_l^n\rangle$, i.e., $|S_l\rangle$. Then, the quantum sequence $|S_l\rangle$ is measured under the basis of Eq. 1, and $\bar{X}_l$ is recovered. N_a announces the measurement basis and order of all sequences.

Step 9) $N_{b_1}, N_{b_2}, \ldots, N_{b_n}$ keep the same particles and perform the same operations. Therefore, if the protocol is effective, $\bar{X}_1, \bar{X}_2, \bar{X}_3, \ldots, \bar{X}_n$ and the secret X must be the same. Intuitively, if $\bar{X}_1 = \bar{X}_2 = \bar{X}_3 = \cdots = \bar{X}_n = X$, the protocol will be effective; otherwise, the protocol fails.

5 Security analysis

In this section, we analyze the attack performed by the internal and external malicious nodes.

5.1 Internal attack

Since the internal nodes directly take part in the process of the protocol, the malicious internal nodes can perform more strong attacks than the external ones. Here, we analyzed two types of participant attacks: information leak attacks and forgery attacks.

5.1.1 Information leak attack

Here, we consider information leak attacks and assume that malicious nodes can guess the secret messages together. In order to show that the following three cases are analyzed, without loss of generality, we assume that r nodes are malicious.

Case 1: Since r malicious nodes conspire, they will send the corresponding particles according to the normal process. Hence, the r particles of r malicious nodes are correctly arranged, and the left $(n - r)$ correct particles are required. As the states of each part come from $\{|+\rangle, |-\rangle, |0\rangle, |1\rangle\}$, the probability of the malicious nodes intuitively guessing one particle is $\frac{1}{4}$, and the probability of guessing $n - r$ particles is

$$P_1 = \left(\frac{1}{4}\right)^{n-r}. \tag{5}$$

For the malicious nodes, the successful probability to obtain the secrets is shown in Figure 5.

Case 2: In the same case, the r malicious nodes can also use other methods to guess the remaining particles. It is observed that the malicious nodes have a total of $r \times (n - r)$ particles left in their hands. If malicious nodes want to guess the secrets, they will arrange the remaining $r \times (n - r)$ particles correctly, and only one arrangement of particles is correct. Therefore, the successful probability to obtain the secrets is

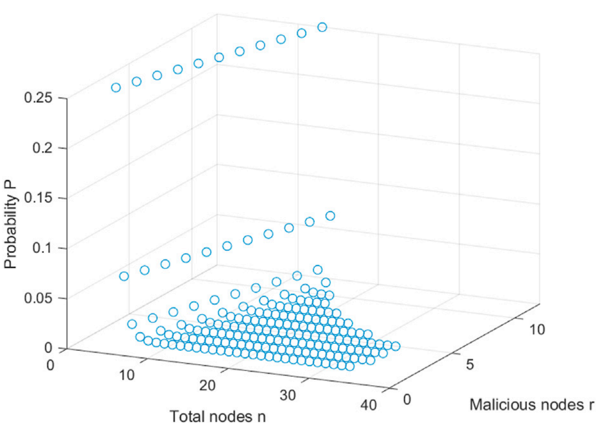


FIGURE 5
Successful probability to obtain the secrets in Case 1.

TABLE 2 Comparison among some different QSS protocols.

Protocol	Participant	Local measurement	Operation
Hsu et al. [30]	Three-party	Yes	*R*, *H*
Yang et al. [22]	Three-party	Yes	*R*
Xu et al. [31]	Three-party	Yes	*R*, *H*
Our protocol	Multi-party	No	*R*

$$P_2 = \frac{1}{(r \times (n-r))!}. \tag{6}$$

For malicious nodes, the successful probability to obtain the secrets is shown in Figure 6.

Case 3: Moreover, the r malicious nodes can perform the following different attacks as they give all the particles in their hands to one malicious node. In this sense, the malicious node independently guesses the secrets with the successful probability of

$$P_3 = \frac{C_{r+1}^1 \times \left(C_r^1\right)^{n-2} \times C_{r-1}^1}{C_{r\times n}^n} = \frac{(r+1) \times \left(r^{n-2}\right) \times (r-1) \times (n!)}{(r \times n) \times (r \times n - 1) \times \cdots \times (r \times n - n + 1)}. \tag{7}$$

For malicious nodes, the successful probability to obtain the secrets is shown in Figure 7.

Above all, the probability of malicious nodes guessing the secrets successfully can be shown as

$$P = max\{P_1, P_2, P_3\}. \tag{8}$$

From the analysis mentioned previously, it can be seen for all malicious nodes without all the particles, and the probability to guessing the secrets tends to be 0. According to the property of the LIOP states, our protocol can resist information leak attacks.

5.1.2 Forgery attack

A forgery attack is an easily overlooked but important attack in the QSS protocol. Forgery attack means that malicious nodes can obtain secret messages and successfully forge secret messages so that other nodes get the wrong secret messages. This attack was proposed by Zhang et al. in 2013 [28] and was also mentioned by Sutradhar et al. in 2020 [29]. In the protocol, a forgery attack is also considered. The secrets are encoded as LIOP states, and particles are transmitted between all destination nodes. Therefore, it is possible for malicious nodes to complete the forgery attack.

When malicious nodes change $|+\rangle$ ($|-\rangle$) to $|-\rangle$ ($|+\rangle$), they have a certain probability to complete the forgery attack. So, the secrets encoded as $|\phi_1\rangle$ ($|\phi_4\rangle$) are forged and are encoded as $|\phi_4\rangle$ ($|\phi_1\rangle$) in Eq. 3. In the multi-party QSS protocol, the secrets are encoded most in the first n states in Eq. 1. The secrets are not encoded in LIOP states with $|-\rangle$ states. Therefore, this attack is only possible in the four-party QSS protocol.

5.1.2.1 Individual attack

Here, we assume that the malicious node can only perform a forgery attack on its own. When a malicious node gets all $|S_i^3\rangle$ and $N_a's$, secret messages encoded as $|\phi_1\rangle or|\phi_4\rangle$, it can successfully forge secrets 00 to secrets 11 or secrets 11 to secrets 00, as in Eq. 3, i = 1, 2, 3. The probability that the secret messages are encoded as $|\phi_1\rangle or|\phi_4\rangle$

$$P_a = \frac{1}{2}. \tag{9}$$

Next, we analyze the probability that the malicious node gets all $|S_i^3\rangle$. When we assume that N_{b_1} or N_{b_3} is a malicious node, we will find that it is impossible for them to get all sequences $|S_i^3\rangle$. Only when it is assumed that N_{b_2} is a malicious node and obtains sequence $|M_3\rangle$, the individual has a certain probability to acquire

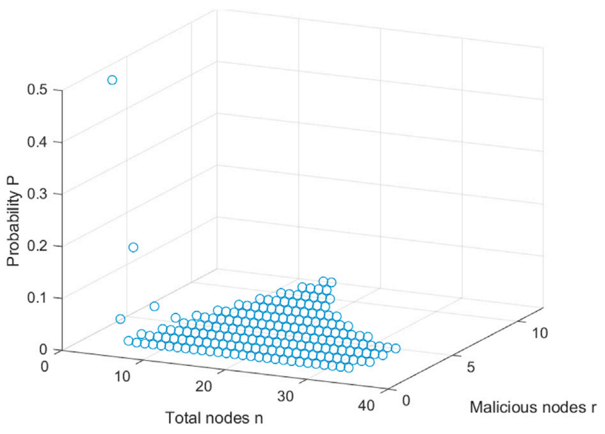


FIGURE 6
Successful probability to obtain the secrets in Case 2.

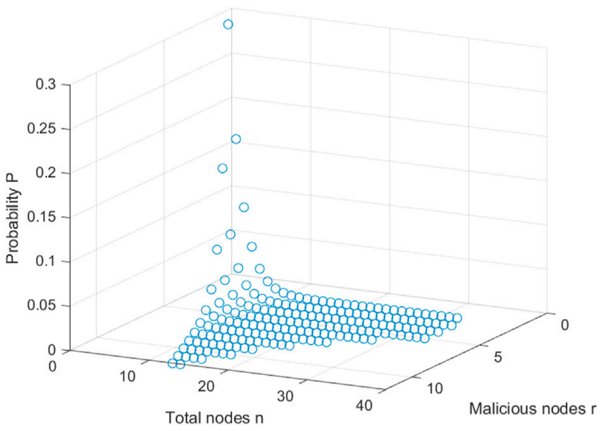


FIGURE 7
Successful probability to obtain the secrets in Case 3.

all sequences $|S_i^3\rangle$. Therefore, the probability that N_{b_2} obtains all $|S_i^3\rangle$ is

$$P_b = \frac{1}{3}. \tag{10}$$

So, the probability that the individual wants to successfully forge the secrets is

$$P = P_a \times P_b = \frac{1}{2} \times \frac{1}{3} = \frac{1}{6}. \tag{11}$$

For the n length of the quantum sequences, it is not difficult to see that the probability of the malicious node successfully forging secrets P' tends to be zero with the increase in n in Eq. 12.

$$P' = P^n = \left(\frac{1}{6}\right)^n. \tag{12}$$

5.1.2.2 Collusion attack

A more serious threat than an individual attack is that some attackers cooperate to forge secrets. Since this attack in this study only exists in the four-party QSS protocol, there are at most two malicious nodes here. When the malicious nodes obtain the secret messages of all sequences $|S_i^3\rangle$ and $N_a's$ secret messages encoded as $|\phi_1\rangle$ or $|\phi_4\rangle$, the malicious nodes can successfully forge secret messages 00 to secret messages 11 or forge secret messages 11 to secret messages 00. The secret messages are encoded as $|\phi_1\rangle or|\phi_4\rangle$ with the probability

$$P_a = \frac{1}{2}. \tag{13}$$

We analyze the probability of malicious nodes obtaining all sequences $|S_i^3\rangle$. A total of three cases were found to be possible to get $|S_i^3\rangle$.

Case 1: N_{b_1} and N_{b_2} are malicious nodes.
Case 2: N_{b_2} and N_{b_3} are malicious nodes.
Case 3: N_{b_1} and N_{b_3} are malicious nodes.

First, we analyze Case 1, and when they get sequence $|M_3\rangle$, they can obtain sequences $|S_i^3\rangle$. The probability of Case 1 is

$$P_{b_1} = \frac{1}{3}. \tag{14}$$

Next, we see Case 2; when they obtain sequence $|M_3\rangle$, the success probability is

$$P_{b_2} = \frac{1}{3}. \tag{15}$$

Finally, during Case 3, when they receive sequence $|M_2\rangle$, the successful probability is

$$P_{b_3} = \frac{1}{3}. \tag{16}$$

Therefore, the successful probability of malicious nodes forging messages is

$$P_1 = P_a \times P_{b_1} = \frac{1}{6}, \quad P_2 = P_a \times P_{b_2} = \frac{1}{6}, \quad P_3 = P_a \times P_{b_3} = \frac{1}{6}. \tag{17}$$

For the length of n of the quantum sequences, it is not difficult to see that in Eq. 18, as n increases, the probability P_i' of malicious nodes successfully forging secrets tends to be zero, where $i = 1, 2, 3$.

$$P_1' = P_1^n = \left(\frac{1}{6}\right)^n, \quad P_2' = P_2^n = \left(\frac{1}{6}\right)^n, \quad P_3' = P_3^n = \left(\frac{1}{6}\right)^n. \tag{18}$$

They want to successfully forge the secret without being discovered is almost impossible. Therefore, the protocol is safe against internal attacks.

5.2 External attack

Unlike internal attackers, external attackers are illegal eavesdroppers from outside. We analyze intercept-replay attacks, intercept-measure-replay attacks, and entangle-measure attacks in the following sections.

5.2.1 Intercept-resend (IR) attack

Eve is an eavesdropper who wants to obtain the secrets of the source node. In order to obtain secrets, he can intercept secrets in Step 4 and Step 6 and complete the attack. *Eve* prepares large quantities of $\{| + \rangle, | - \rangle, |0\rangle, |1\rangle\}$. *Eve* intercepts the sequences $|M_t\rangle$ and sends the sequences prepared on his own to N_{b_l} at the same time. The probability of *Eve* guessing one particle is $\frac{1}{4}$, and the probability of guessing n particles is $(\frac{1}{4})^n$; the probability approximates to zero. Therefore, when N_a and N_{b_l} perform eavesdropping detection, N_{b_l} has a high probability of getting wrong measurements, and N_a will find that it has eavesdropped. N_a will give up sharing secrets, so *Eve* will not get any secret messages.

5.2.2 Intercept-measure-resend (IMR) attack

Eve receives the sequences $|M_t\rangle$ and measures them in the computational basis. After the measurement, the sequences are resent to N_{b_l}. Considering one of the particles in the measured sequence, if N_{b_l} measurement basis is the same as $Eve's$ selection, *Eve* will get N_{b_l} measurement basis, which means *Eve* will get secrets. However, *Eve* does not distinguish between secret particles and decoy particles, so they do not get useful secret messages.

Similar to the IR attack and IMR attack, *Eve* is an external attacker, while in the entanglement and measurement attack, *Eve* has less information than an internal attacker and, therefore, has a higher probability of failure.

6 Discussion and conclusion

We compare and summarize the QSS protocols based on LIOP states in Table 2. *R* denotes a rearrangement operation, and *H* denotes a random three-level Hadamard transform.

Compared with the existing QSS protocols based on LIOP states, our protocol can be extended to the arbitrary multi-party. In addition, we only use the characteristics of the states themselves to perform arrangement operations and do not require local measurement. In this case, two new QSS protocols based on LIOP states are proposed and may be applied in further quantum networks. The four-party QSS protocol is a special case of the multi-party QSS protocol. However, the secrets are encoded into different forms and attack strategies are different. To improve the efficiency, two more states are introduced in the four-party QSS protocol for encoding. Hence, the necessary forgery attack is discussed. For the multi-party QSS protocol, it is not difficult to see that the forgery attack can be naturally resisted.

In conclusion, combining with the property of LIOP states and obfuscating operation, the source nodes and destination nodes can complete the secret sharing in the quantum network. The destination nodes work together to recover the secrets. Since the LIOP states are more convenient to prepare than the entangled ones, the protocol is easily realized. Moreover, with regard to the property of LIOP states, it is proven that our protocol can be secure against the existing attacks. We hope this can be helpful to the further development of quantum networks.

Data availability statement

The original contributions presented in the study are included in the article/Supplementary Material; further inquiries can be directed to the corresponding authors.

Author contributions

Conceptualization, S-JF and K-JZ; methodology, S-JF; software, S-JF; validation, S-JF, K-JZ, LZ, and K-CH; writing—original draft preparation, S-JF; writing—review and editing, S-JF and K-JZ. All authors have read and agreed to the published version of the manuscript.

Funding

This work was supported by the National Natural Science Foundation of China under Grant 61802118 and Natural Science Foundation of Heilongjiang Province under Grant YQ2020F013, LH2019F031. The work of K-JZ was supported by the Advanced Programs of Heilongjiang Province for the overseas scholars and the Outstanding Youth Fund of Heilongjiang University. This research is supported by the Heilongjiang Provincial Key Laboratory of the Theory and Computation of Complex Systems.

Conflict of interest

The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Publisher's note

All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors, and the reviewers. Any product that may be evaluated in this article, or claim that may be made by its manufacturer, is not guaranteed or endorsed by the publisher.

References

1. Shor PW. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Rev Soc Ind Appl Math* (1999) 41(2): 303–32. doi:10.1137/S0036144598347011

2. Grover LK. A fast quantum mechanical algorithm for database search. In: Proceedings of the twenty-eighth annual ACM symposium on Theory of computing (1996). p. 212–9. doi:10.1145/237814.237866

3. Long GL, Liu XS. Theoretically efficient high-capacity quantum-key-distribution scheme. *Phys Rev A (Coll Park)* (2002) 65(3):032302. doi:10.1103/PhysRevA.65.032302

4. Ma H, Guo Z. A group quantum communication network using quantum secret sharing. In: 2008 IFIP International Conference on Network and Parallel Computing; 2008 October 18–21; Shanghai, China (2008). p. 549–52. IEEE. doi:10.1109/NPC.2008.42

5. Zidan M, Abdel-Aty A-H, El-Sadek A, Zanaty EA, Abdel-Aty M. Low-cost autonomous perceptron neural network inspired by quantum computation. *AIP Conf Proc* (2017) 1905:020005. doi:10.1063/1.5012145

6. Noor KI, Noor MA, Mohamed HM. Quantum approach to starlike functions. *Appl Math Inf Sci* (2021) 15(4):437–41. doi:10.18576/amis/150405

7. Bogolyubov NN, Jr., Soldatov AV. Time-convolutionless master equation for multi-level open quantum systems with initial system-environment correlations. *Appl Math Inf Sci* (2020) 14(5):771–80. doi:10.18576/amis/140504

8. Said T, Chouikh A, Bennai M. N two-transmon-qubit quantum logic gates realized in a circuit QED system. *Appl Math Inf Sci* (2019) 13(5):839–46. doi:10.18576/amis/130518

9. Zidan M, Abdel-Aty A-H, Younes A, El-khayat I, Abdel-Aty M. A novel algorithm based on entanglement measurement for improving speed of quantum algorithms. *Appl Math Inf Sci* (2018) 12(1):265–9. doi:10.18576/amis/120127

10. Abdel-Aty A-H, Kadry H, Zidan M, Zanaty EA, Abdel-Aty M. A quantum classification algorithm for classification incomplete patterns based on entanglement measure. *J Intell Fuzzy Syst* (2020) 38(3):2809–16. doi:10.3233/JIFS-179566

11. Ye TY, Li HK, Hu JL. Semi-quantum key distribution with single photons in both polarization and spatial-mode degrees of freedom. *Int J Theor Phys (Dordr)* (2020) 59(9):2807–15. doi:10.1007/s10773-020-04540-y

12. Ye TY, Geng MJ, Xu TJ, Chen Y. Efficient semiquantum key distribution based on single photons in both polarization and spatial-mode degrees of freedom. *Quan Inf Process* (2022) 21(4):123. doi:10.1007/s11128-022-03457-1

13. Hillery M, Buvek V, Berthiaume A. Quantum secret sharing. *Phys Rev A (Coll Park)* (1999) 59(3):1829–34. doi:10.1103/PhysRevA.59.1829

14. Karlsson A, Koashi M, Imoto N. Quantum entanglement for secret sharing and secret splitting. *Phys Rev A (Coll Park)* (1999) 59(1):162–8. doi:10.1103/PhysRevA.59.162

15. Xiao L, Long GL, Deng FG, Pan JW. Efficient multiparty quantum-secret-sharing schemes. *Phys Rev A (Coll Park)* (2004) 69(5):052307. doi:10.1103/PhysRevA.69.052307

16. Qin H, Dai Y. Dynamic quantum secret sharing by using d-dimensional GHZ state. *Quan Inf Process* (2017) 16(3):64–13. doi:10.1007/s11128-017-1525-y

17. Zhang KJ, Zhang X, Jia HY, Zhang L. A new n-party quantum secret sharing model based on multiparty entangled states. *Quan Inf Process* (2019) 18(3):81–15. doi:10.1007/s11128-019-2201-1

18. Mansour M, Dahbi Z. Quantum secret sharing protocol using maximally entangled multi-qudit states. *Int J Theor Phys (Dordr)* (2020) 59(12):3876–87. doi:10.1007/s10773-020-04639-2

19. Hu W, Zhou RG, Li X, Fan P, Tan C. A novel dynamic quantum secret sharing in high-dimensional quantum system. *Quan Inf Process* (2021) 20(5):159–28. doi:10.1007/s11128-021-03103-2

20. Yu S, Oh CH. Detecting the local indistinguishability of maximally entangled states (2015). arXiv preprint arXiv:1502.01274. Available at: https://arxiv.org/abs/1502.01274 (Accessed Feb 4, 2015).doi:10.48550/arXiv.1502.01274

21. Guo GP, Li CF, Shi BS, Li J, Guo GC. Quantum key distribution scheme with orthogonal product states. *Phys Rev A (Coll Park)* (2001) 64(4):042301. doi:10.1103/PhysRevA.64.042301

22. Yang Y, Wen Q, Zhu F. An efficient quantum secret sharing protocol with orthogonal product states. *Sci China Ser G: Phys Mech Astron* (2007) 50(3):331–8. doi:10.1007/s11433-007-0028-8

23. Jiang DH, Wang J, Liang XQ, Xu GB, Qi HF. Quantum voting scheme based on locally indistinguishable orthogonal product states. *Int J Theor Phys (Dordr)* (2020) 59(2):436–44. doi:10.1007/s10773-019-04337-8

24. Jiang DH, Hu QZ, Liang XQ, Xu GB. A trusted third-party E-payment protocol based on locally indistinguishable orthogonal product states. *Int J Theor Phys (Dordr)* (2020) 59(5):1442–50. doi:10.1007/s10773-020-04413-4

25. Walgate J, Hardy L. Nonlocality, asymmetry, and distinguishing bipartite states. *Phys Rev Lett* (2002) 89(14):147901. doi:10.1103/PhysRevLett.89.147901

26. Xu GB, Wen QY, Qin SJ, Yang YH, Gao F. Quantum nonlocality of multipartite orthogonal product states. *Phys Rev A (Coll Park)* (2016) 93(3): 032341. doi:10.1103/PhysRevA.93.032341

27. Feng Y, Shi Y. Characterizing locally indistinguishable orthogonal product states. *IEEE Trans Inf Theor* (2009) 55(6):2799–806. doi:10.1109/TIT.2009.2018330

28. Zhang K, Qin S. The Cryptanalysis of Yuan et al.'s Multiparty Quantum Secret Sharing Protocol. *Int J Theor Phys (Dordr)* (2013) 52(11):3953–9. doi:10.1007/s10773-013-1706-0

29. Sutradhar K, Om H. Efficient quantum secret sharing without a trusted player. *Quan Inf Process* (2020) 19(2):73–15. doi:10.1007/s11128-019-2571-4

30. Hsu LY, Li CM. Quantum secret sharing using product states. *Phys Rev A (Coll Park)* (2005) 71(2):022321. doi:10.1103/PhysRevA.71.022321

31. Xu J, Chen HW, Liu WJ, Liu ZH. An efficient quantum secret sharing scheme based on orthogonal product states. In: IEEE Congress on Evolutionary Computation; 2010 July 18–23; Barcelona, Spain (2010). p. 1–4. IEEE. doi:10.1109/CEC.2010.5586410

TYPE Original Research
PUBLISHED 03 November 2022
DOI 10.3389/fphy.2022.1046314

OPEN ACCESS

EDITED BY
Tianyu Ye,
Zhejiang Gongshang University, China

REVIEWED BY
Suzhen Yuan,
Chongqing University of Posts and Telecommunications, China
H. Z. Shen,
Northeast Normal University, China

*CORRESPONDENCE
Yumin Dong,
dym@cqnu.edu.cn

SPECIALTY SECTION
This article was submitted to Quantum Engineering and Technology, a section of the journal Frontiers in Physics

RECEIVED 16 September 2022
ACCEPTED 19 October 2022
PUBLISHED 03 November 2022

CITATION
Li Z, Chen Z, Che X, Wu Y, Huang D, Ma H and Dong Y (2022), A classification method for multi-class skin damage images combining quantum computing and Inception-ResNet-V1.
Front. Phys. 10:1046314.
doi: 10.3389/fphy.2022.1046314

A classification method for multi-class skin damage images combining quantum computing and Inception-ResNet-V1

Ziyi Li[1], Zhengquan Chen [1], Xuanxuan Che [1], Yaguang Wu [2], Dong Huang [3,4], Hongyang Ma [5] and Yumin Dong[1]*

[1]College of Computer and Information Science, Chongqing Normal University, Chongqing, China, [2]Department of Dermatology, First Affiliated Hospital of Army Medical University, Chongqing, China, [3]School of Computer and Software Engineering, Xihua University, Chengdu, Sichuan, China, [4]Key Laboratory of Advanced Manufacturing Technology, Ministry of Education Guizhou University, Guiyang, Guizhou, China, [5]School of Science, Qingdao University of Technology, Qingdao, Shandong, China

Melanoma is a high-grade malignant tumor. Melanoma and mole lesions are highly similar and have a very high mortality rate. Early diagnosis and treatment have an important impact on the patient's condition. The results of dermoscopy are usually judged visually by doctors through long-term clinical experience, and the diagnostic results may be different under different visual conditions. Computer-aided examinations can help doctors improve efficiency and diagnostic accuracy. The purpose of this paper is to use an improved quantum Inception-ResNet-V1 model to classify multiple types of skin lesion images and improve the accuracy of melanoma identification. In this study, the FC layer of Inception-ResNet-V1 is removed, the average pooling layer is the last, SVM is used as the classifier, and the convolutional layer is quantized. The performance of the model was tested experimentally on the ISIC 2019 dataset. To prevent the imbalance of the sample data set from affecting the experiment, the sample data is sampled with weight. Experiments show that the method used shows excellent performance, and the classification accuracy rate reaches 98%, which provides effective help for the clinical diagnosis of melanoma.

KEYWORDS
melanoma, deep learning, CNN, quantum computing, skin cancer, ISIC 2019

Introduction

Melanoma is one of the most harmful skin cancers, and it is a deadly malignant tumor [1–3]. There are many risk factors leading to the formation of melanoma, such as ultraviolet radiation, drug treatment, gene, family history, skin color, race, age, gender, etc. Although melanoma is not common, it is more lethal, and the incidence rate is still rising in the world. And the average diagnosis and treatment cost of melanoma is 10 times that of non-melanoma skin cancer [4–6]. Melanoma is cancer with the highest mortality among skin cancers. If melanoma is diagnosed at an early stage, a small operation can increase the chance of recovery and reduce the mortality rate of cancer. But without early detection and treatment, it can spread to other parts of the body [7]. Early and correct diagnosis is the key to ensuring the best prognosis for patients [8]. However, melanoma is misdiagnosed more than any cancer except breast cancer. Dermatoscopy is one of the most commonly used imaging techniques for dermatologists. It enlarges the surface of skin lesions, and its structure becomes more obvious to dermatologists [9,10]. The diagnosis of melanoma is usually carried out by using the vision of experienced doctors, first visually inspecting the skin lesions (usually using the ABCD rule and the seven-point inspection method) [11,12], analyzing the results of dermatoscopy and matching them with medical science [13]. The weakness of manual detection is greatly affected by human subjectivity, which makes it inconsistent under certain conditions because it is completely based on doctors' vision and experience. Although the accuracy of suspicious cases can be further improved by using special high-resolution cameras and magnifying glasses to capture dermoscopic images for visual examination [14]. However, recent studies have shown that the classification method based on CNN has become the best choice for melanoma detection. The high accuracy of CNN based classifier for skin cancer image classification is equivalent to an experienced dermatologist [15].

[16] proposed a deep learning system for detecting melanoma lesions. They first performed illumination correction on the input image, and cut, scaled, and rotate the image. Then, they fed back the enhanced image to the pre-trained CNN for a large number of sample training and obtained an accuracy rate of 81%. [17] also preprocessed the skin image data set, segmented the region of interest (ROI) of the lesion area, extracted the features of the segmented image using the gray level co-occurrence matrix, and combined with the ABCD rule to identify and classify malignant tumors, achieving an accuracy rate of 92.1%. [18] used GoogLeNet to train the ISIC 2016 dataset and processed the samples of the ISIC 2016 dataset through the traditional data enhancement method to reduce the impact of the unbalanced training dataset on the CNN performance, with the maximum accuracy of 83.6%. [19] used the ResNet-152 model to classify clinical images of 12 skin diseases, fine-tuned the model using the training part of the Asan dataset, the MED-NODE dataset, and atlas site images, and the trained model passed Asan, Hallym and Edinburgh datasets for validation. Experiments demonstrate that the algorithm performance, tested with 480 Asan and Edinburgh images, is comparable to the results of 16 dermatologists. [20] used CNN to extract features from images, used SVM, RF, and NN to train and classify features, and processed the datasets ISIC 2017 and PH2 using data augmentation to avoid overfitting in accuracy. Due to the influence of the integration problem, the experiment obtained an accuracy of 89.2%. [21] used the improved Inception V4 model to classify skin cancer diseases, pre-trained the model on the ImageNet dataset, fused the low-level and high-level features of the image, and used the ISIC 2018 dataset to achieve 94.7% classification accuracy. [22] proposed an enhanced encoder-decoder network to overcome the limitations of uneven skin image features and blurred boundaries, which made the semantic level of the encoder feature map closer to the decoder feature map, and The model was tested on the ISIC 2017 and PH2 datasets for melanoma recognition and achieved 95% accuracy. [23] pre-trained Alex Net with the Softmax layer as the classification layer, and the model achieved 97% accuracy for skin cancer classification on three datasets: MED-NODE, Derm (IS & Quest), and ISIC. [24] analyzed ISIC images using a fully convolutional residual network (FCRN) and CNN to check for anomalies in the skin, a residual network was used to segment the images in the dataset, and a neural network was used for classification. [25] firstly preprocess the input color skin image to segment the region of interest (ROI); secondly, use traditional transformation to enhance the segmented ROI image. They evaluated the performance of the proposed method on three different datasets (MED-NODE, DermIS & DermQuest, and ISIC 2017) using the improved AlexNet, ResNet101, and GoogLeNet network structures, and achieved 99% accuracy on the MED-NODE dataset. [26] used a hybrid quantum mechanical system to encode and process image information to classify cancerous and noncancerous pigmented skin lesions in the HAM10000 dataset. [27] proposed a high-precision skin lesion classification model, using transfer learning and GoogLeNet pre-training model, to classify eight different categories of skin lesions in the dataset ISIC 2019, with an accuracy rate of 94%.

In this study, the trained model is applied to images of skin lesions, the classification layer is replaced with SVM, and the convolutional layer is quantized to improve the classification process. One of the difficulties in image classification is that the amount of computation in the classification process is very large, resulting in a relatively slow classification speed and consuming a lot of computing resources. [28, 29] Due to the characteristics of quantum parallel computing, the quantum image classification algorithm can still quickly complete the classification task in the case of a large amount of image data. [28] The contributions of the proposed method are as follows:

- This study quantizes the convolutional layers of Inception-ResNet-V1 to enhance the performance of the network.
- In this study, the FC layer of the network was removed, and SVM was used as the classifier because SVM also showed excellent performance in melanoma classification, which can be compared with the original model.
- This study adopts data augmentation and weighted sampling methods to alleviate the impact of data imbalance.

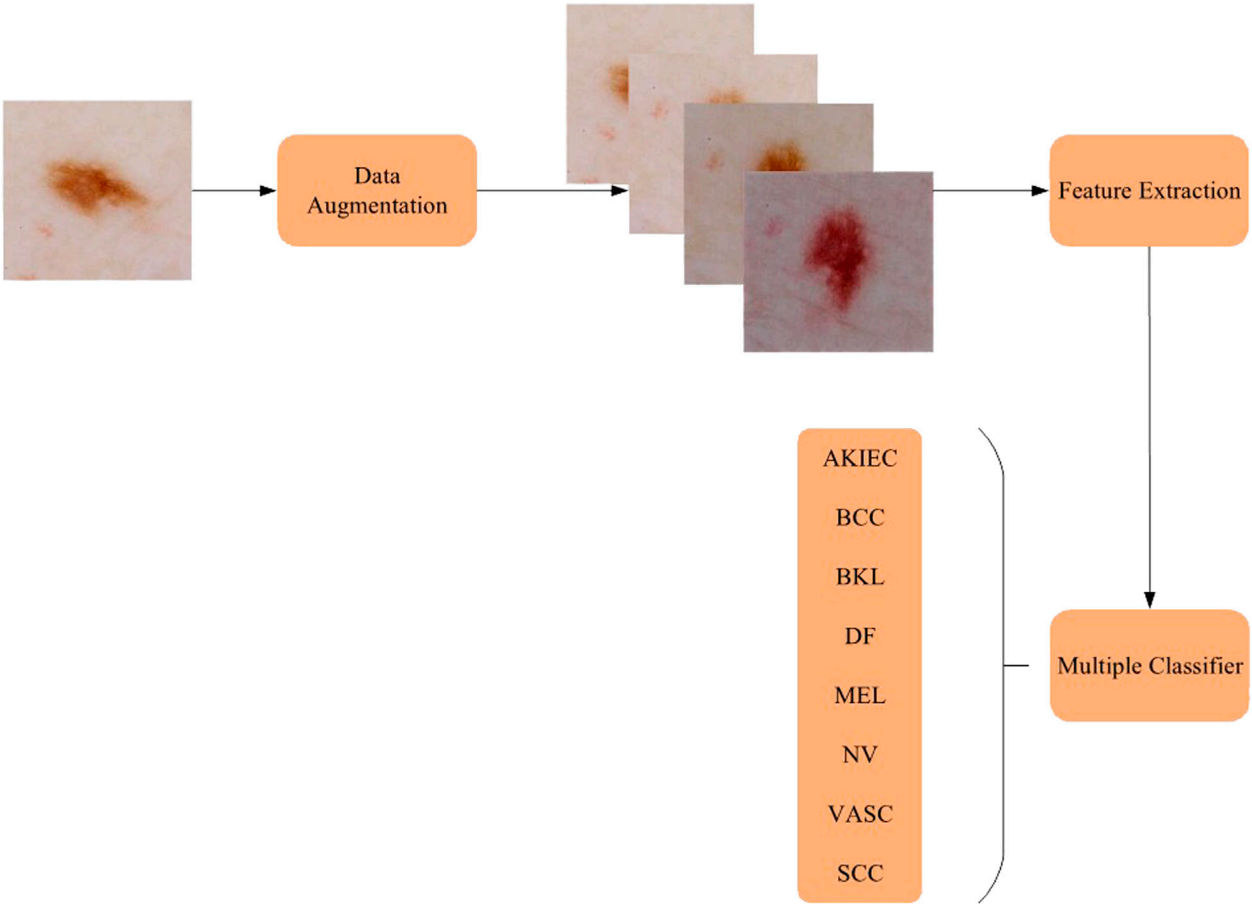


FIGURE 1
Method structure.

- The model exhibits a high accuracy classification rate.

Proposed method

The proposed method is elaborated in this section, and the method structure is shown in Figure 1. The proposed method first augments and normalizes the image data, and then feeds the proposed model for training. The following is a detailed description of the proposed method.

Data augmentation and weighted sampling

ISIC 2019 dataset is an imbalanced dataset, which may make the model biased toward classes with a large number of samples during training. For example, the number of the most NV class is 50 times more than that of the least VASC class, which is likely to lead to the model being biased toward NV during training, thus affecting the accuracy of the model. To reduce the imbalance in the given dataset, this study uses the data augmentation method to expand the images of minority classes through rotation, cutting, flipping, and other ways [30,31], to reduce the image quantity gap between the majority class and the model, to reduce the influence of unbalanced data sets on the model. However, using traditional data augmentation alone has defects, because repeated samples lead to over-sampling, which will easily lead to overfitting of the learning algorithm. To solve this problem, this study applies the weighted random sampling method to the overlapping of repeated samples, that is, the weight of each instance is defined by the number of instances in the class [32], and this weight represents the probability of the instance being randomly sampled [32], which can offset the oversampling effect of the class with a small number of samples. The weighted sampling method is based on weight

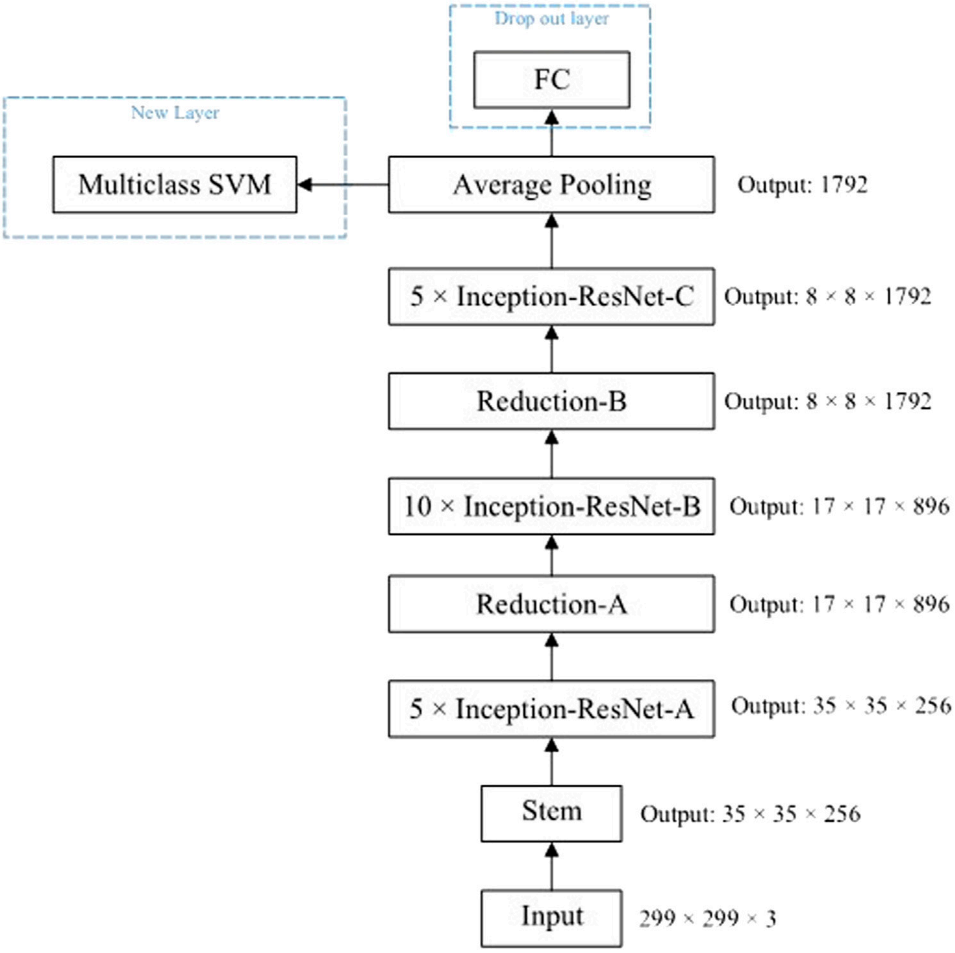


FIGURE 2
Model architecture.

sampling, which can reserve more labels and meet the diversity. Although there are changes, they are still constrained by the relative weight size of labels [33].

Image normalization

For image data, the pixel value of the image is an integer between 0 and 255. When training a deep neural network for fitting, a small weight value is generally used. If the value of the training data is large, the model training process may be slowed down. Therefore, pixel normalization of image data is necessary. In this paper, Min-Max normalization is used to remove the pixel unit of image data and convert the data into dimensionless pure values. Specifically, after pixel normalization, the image pixel value is scaled to [0,1] [34].

Improved quantum Inception-ResNet-V1 model

The research uses residual connections to join the filter connection stage in the Inception architecture, which will allow the Inception architecture to retain its computational efficiency while gaining the benefits of the residual connection method. The residual version of the Inception network uses a more simplified Inception module than the source Inception uses. Each Inception module is followed by a filter expansion layer (i.e., a 1 × 1 convolutional layer without an activation function) that enlarges the dimension of the filter bank before adding it to match the input. This compensates for the dimensionality reduction in the Inception block. The research removes the FC of the Inception-ResNet-V1 model and uses the SVM as a classifier to test the performance. The architecture is shown in Figure 2.

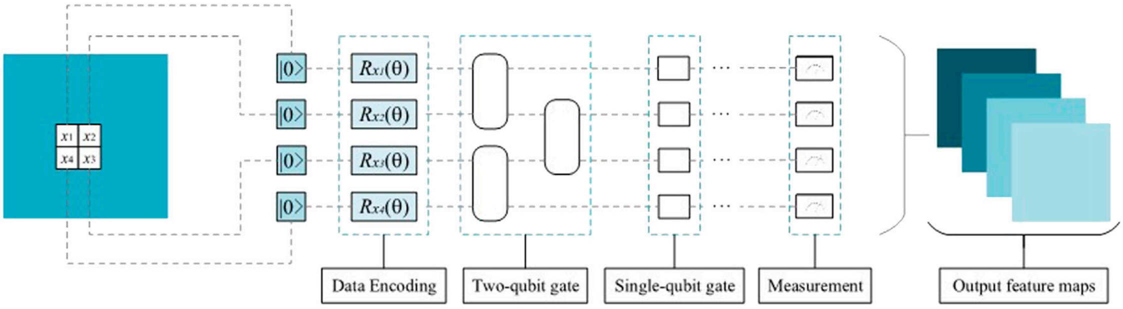


FIGURE 3
Quantum convolution layer.

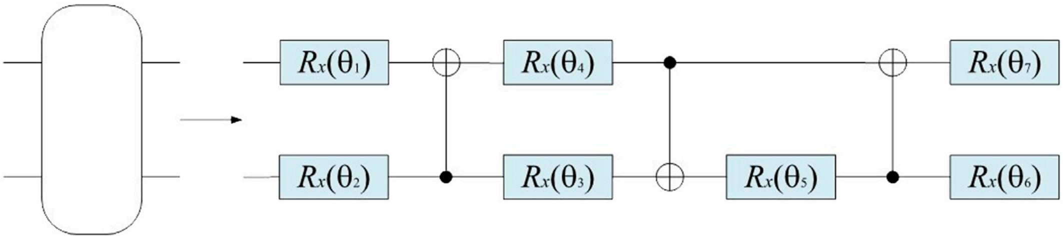


FIGURE 4
Two-qubit gate.

The backbone network Stem in Figure 2 uses a quantum convolution layer for feature extraction, which is composed of multiple parameterized quantum filters. Similar to the convolution kernel in the classical convolution layer, it uses a parameterized quantum filter to extract the characteristic information of all quantum bits in the local space of the data. The quantum filter includes many types of quantum bit gates, including single-bit gate and double-bit gate, which can perform unitary conversion of corresponding quantum bit, and impose a double-bit gate on adjacent quantum bits, thus causing quantum entanglement of adjacent quantum bits. In this paper, the quantum rotation gate R(θ) is used to transform the pixel value information of the image into quantum state information by quantum state encoding. On this basis, the obtained image feature information is converted into the angle of the quantum rotary gate. Each pixel value provides the corresponding parameters for the quantum rotary gate. Different quantum rotary gates act on the corresponding initial state $|0\rangle$ of the quantum bit, and the feature information is stored in the quantum state, which can be used as the model input to the quantum convolution neural network [35]. For example, for n ×n, the quantum feature extraction function first encodes it into a quantum state through quantum bit coding, then evolves the quantum state through the parameterized quantum circuit, and finally outputs a real number through the expected value measurement. This method not only has the unique properties of quantum mechanics but also can keep the weight sharing of the convolutional kernel. In this study, we introduce a quantum circuit with parameters to enhance the performance of the network. The quantum convolution layer is shown in Figure 3.

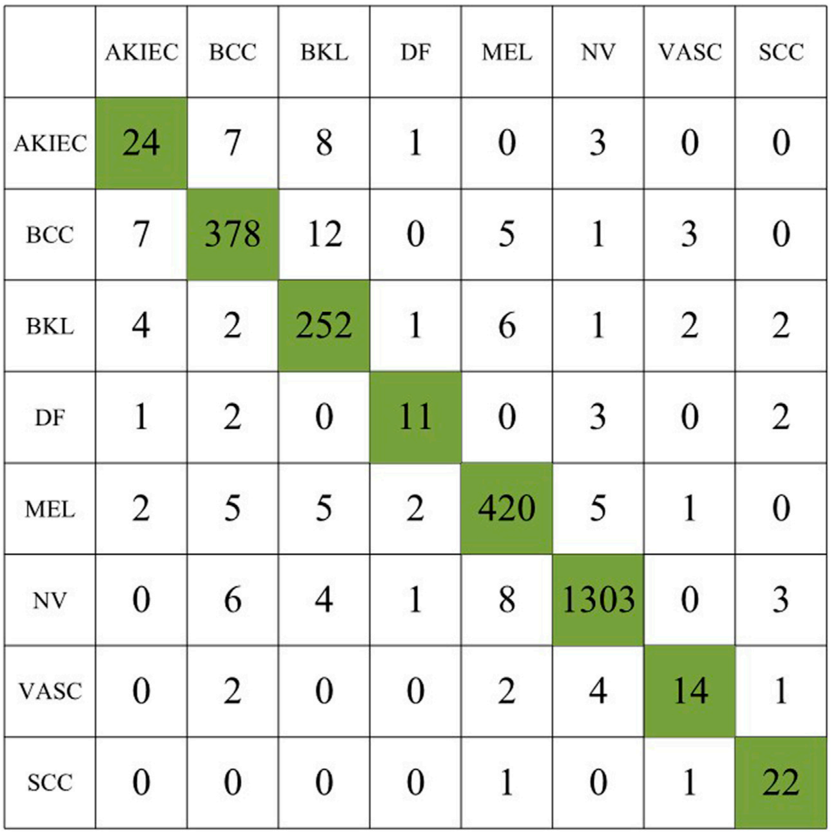
TABLE 1 ISIC 2019 dataset.

AKIEC	BCC	BKL	DF	MEL	NV	VASC	SCC
867	3,323	2,624	239	4,522	12,875	253	628

The quantum filter used in this study consists of CNOT gate and rotary gate $R_x(\theta)$. The quantum circuit diagram is shown in Figure 4.

TABLE 2 Results of the first experiment.

Accuracy (%)	Precision (%)	Sensitivity (%)	Specificity (%)
95.05	80.8	81.16	99.22



	AKIEC	BCC	BKL	DF	MEL	NV	VASC	SCC
AKIEC	24	7	8	1	0	3	0	0
BCC	7	378	12	0	5	1	3	0
BKL	4	2	252	1	6	1	2	2
DF	1	2	0	11	0	3	0	2
MEL	2	5	5	2	420	5	1	0
NV	0	6	4	1	8	1303	0	3
VASC	0	2	0	0	2	4	14	1
SCC	0	0	0	0	1	0	1	22

FIGURE 5
Confusion matrix for the first experiment.

Experiments and results

Dataset description

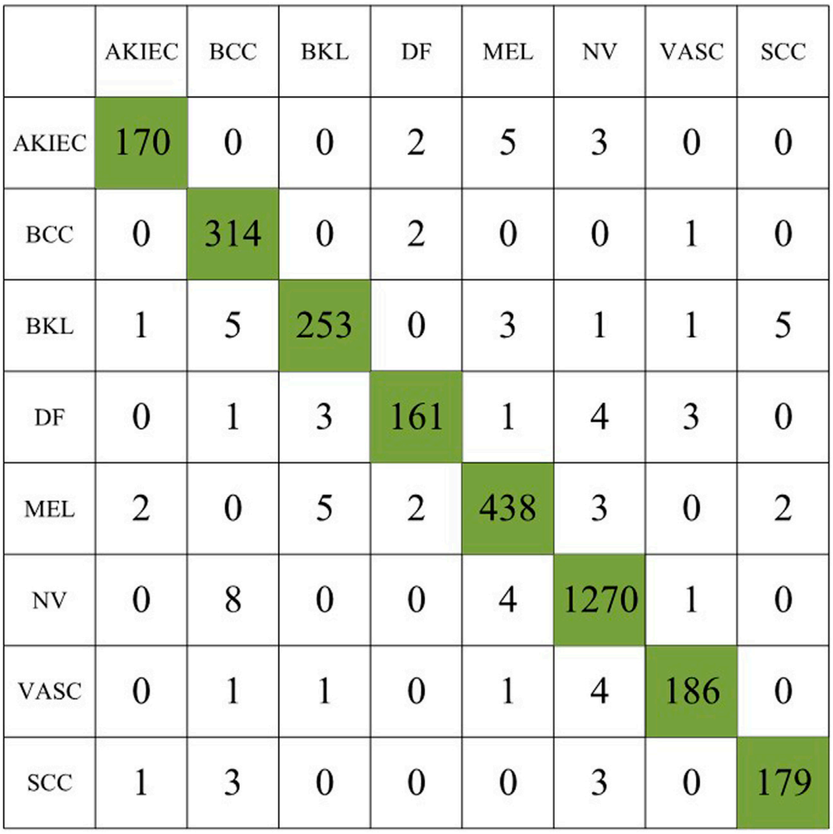
The data in this article comes from the ISIC 2019 [36] challenge (Skin Lesion Analysis Towards Melanoma Detection). The ISIC 2019 dataset contains 25,331 dermoscopy images in 8 categories, namely actinic keratosis (AKIEC): 867, basal cell carcinoma (BCC): 3,323, benign keratosis (BKL): 2,624, skin fibers Tumor (DF): 239, Melanoma (MEL): 4,522, Melanocytic nevus (NV): 12,875, Angiosarcoma (VASC): 253, Squamous cell carcinoma (SCC): 628, as shown in Table 1. In the experiments, we randomly 80% of images (about 20,231 images) of the dataset for training, 10% images (about 2,550 images) for testing, and 10% images (about 2,550 images) for validation.

Experiment

The study conducted three experiments using the ISIC 2019 dataset. The first is to evaluate the proposed method using the original dataset without image augmentation. The second approach is to augment the dataset and re-evaluate the proposed method. The third is to use the processed dataset to evaluate the proposed method after processing the dataset using image augmentation and weighted sampling. All experiments are performed with fixed values, i.e. batch size 10, number of training

TABLE 3 Results of the second experiment.

Accuracy (%)	Precision (%)	Sensitivity (%)	Specificity (%)
97.31	96.14	96.73	99.6



	AKIEC	BCC	BKL	DF	MEL	NV	VASC	SCC
AKIEC	170	0	0	2	5	3	0	0
BCC	0	314	0	2	0	0	1	0
BKL	1	5	253	0	3	1	1	5
DF	0	1	3	161	1	4	3	0
MEL	2	0	5	2	438	3	0	2
NV	0	8	0	0	4	1270	1	0
VASC	0	1	1	0	1	4	186	0
SCC	1	3	0	0	0	3	0	179

FIGURE 6
Confusion matrix for the second experiment.

32, and initial learning rate 0.001. The proposed model was evaluated using four performance metrics [37]: accuracy, precision, sensitivity, and specificity.

$$Accuracy = \frac{t_p + t_n}{t_p + f_p + f_n + t_n} \tag{1}$$

$$Precision = \frac{t_p}{t_p + f_p} \tag{2}$$

$$Sensitivity = \frac{t_p}{t_p + f_n} \tag{3}$$

$$Specificity = \frac{t_n}{f_p + t_n} \tag{4}$$

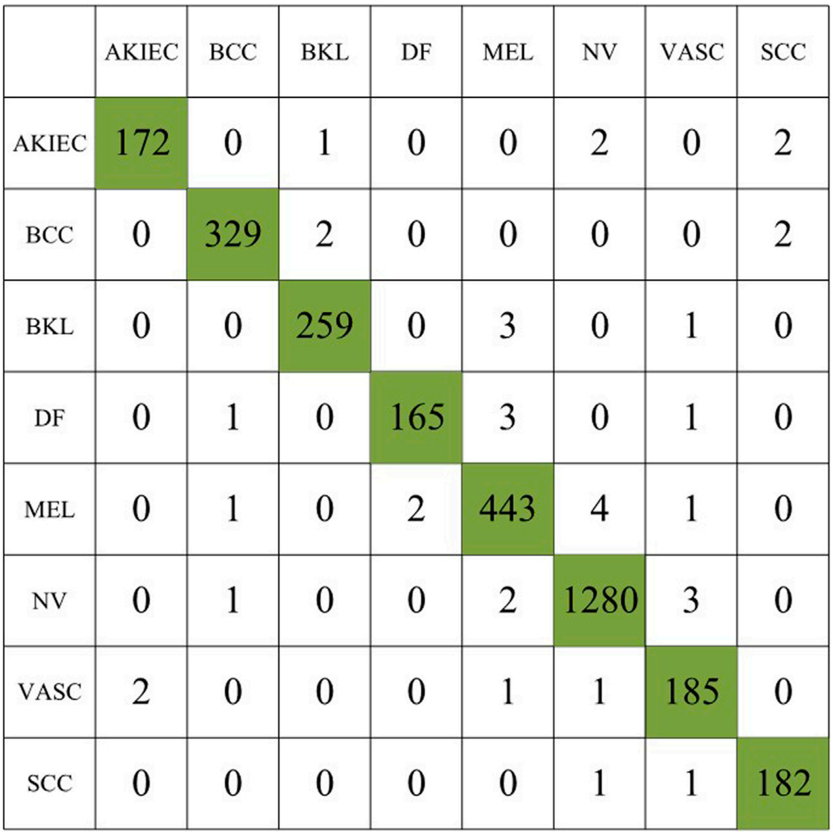
where t_p, f_p, t_n, and f_n refer to true positives, false positives, true negatives, and false negatives, respectively.

In the first experiment, we use the original dataset to evaluate the proposed method, the experimental results are summarized in Table 2, and the confusion matrix of the first experiment is shown in Figure 5.

In the second experiment, we augment the number of images for the minority classes AKIEC, DF, VASC, and SCC to 1743, 1,667, 1920, and 1856, respectively, resulting in a total of 3,053 images. Table 3 summarizes the experimental results, and the confusion matrix for the second experiment is shown in Figure 6.

TABLE 4 Results of the third experiment.

Accuracy (%)	Precision (%)	Sensitivity (%)	Specificity (%)
98.76	98.26	98.4	99.81



	AKIEC	BCC	BKL	DF	MEL	NV	VASC	SCC
AKIEC	172	0	1	0	0	2	0	2
BCC	0	329	2	0	0	0	0	2
BKL	0	0	259	0	3	0	1	0
DF	0	1	0	165	3	0	1	0
MEL	0	1	0	2	443	4	1	0
NV	0	1	0	0	2	1280	3	0
VASC	2	0	0	0	1	1	185	0
SCC	0	0	0	0	0	1	1	182

FIGURE 7
Confusion matrix for the third experiment.

Compared to the first experiment, we observed a significant increase in sensitivity and precision. The imbalance gap in the number of minority class images is reduced. The accuracy of the model also increases to 97.31%, indicating that data augmentation plays an important role in model performance.

In the third experiment, we augmented the images of the minority classes AKIEC, DF, VASC, and SCC to 1743, 1,667, 1920, and 1856, respectively, and used the weighted sampling method for the augmented class images to prevent duplicate samples affect the experimental accuracy. Table 4 summarizes the experimental results, and the confusion matrix for the second experiment is shown inFigure 7.

The accuracy of the model after using the weighted sampling method is increased to 98.76%. Compared with the first two experiments, each index has been improved to varying degrees. The performance comparison of the three experiments is shown in Figure 8.

Experimental results show the lowest performance when using the original dataset in the first experiment. In the second experiment, the obtained results were improved. The third experiment shows the best value for the performance metric. The accuracy of the model increased from 95.05% to 98.765%, the Precision increased from 80.8% to 98.26%, the Sensitivity increased from 81.16% to 98.45%, and the Specificity increased from 99.22% to 99.81%.

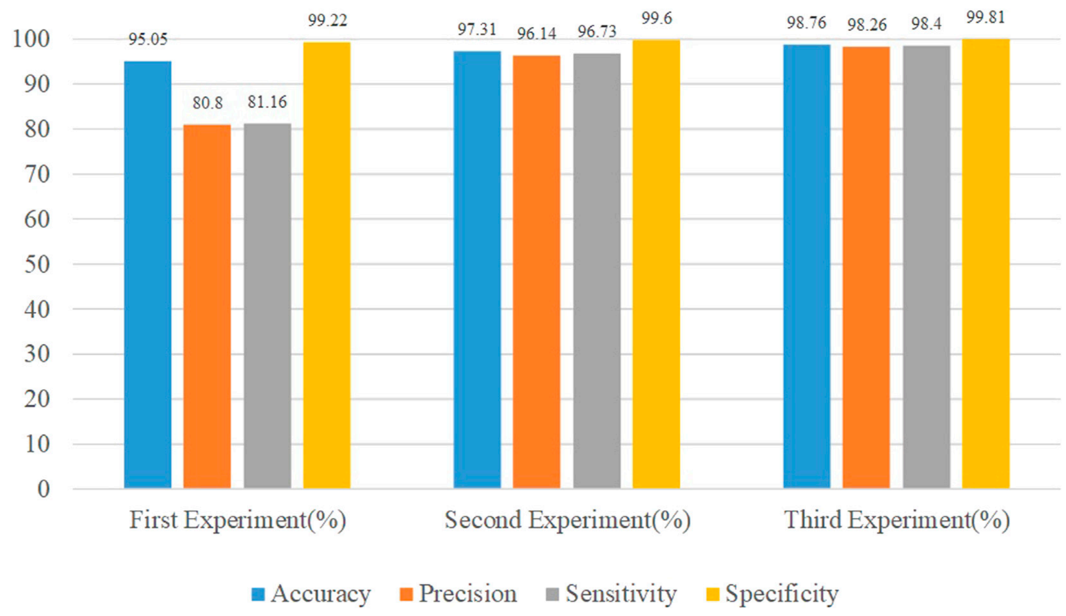


FIGURE 8
Performance comparison.

TABLE 5 Results of the third experiment.

	Year	Method	Dataset	Accuracy (%)
[38]	2019	An ensemble composed of 13 CNN SENet architecture	ISIC 2019	91
[39]	2020	One-dimensional fractal feature method based on texture feature	ISIC 2019	97.35
[40]	2020	A multi-classifier based on neural network and feature	ISIC 2019	95
[25]	2020	ABCD and GLCM are used to extract statistical features and texture features, and SVM is used for classification	ISIC 2019	96.25
[41]	2021	Weighted average ensemble learning model	ISIC 2019	93
[42]	2021	CNN is based on transfer learning	ISIC 2019	81.2
[43]	2021	CNN is based on transfer learning	ISIC 2019	81.2
[44]	2021	Using deep learning models with image and metadata features	ISIC 2019	80

The sampling process can be combined with the memorylessness of the Markovian effect, that is, the system does not remember the previous state of the current state, and only decides what state to transition to at the next moment based on the current state. Markov Decision Processes (MDPs) maximize returns by using methods such as dynamic programming, random sampling, etc.

The performance of this method is compared with that of existing skin cancer classification methods, and Table 5 summarizes the data image types, used models, and accuracy rates of existing methods. Table 5 clearly shows that this method outperforms the literature methods listed in the table.

Conclusion

In this study, the improved quantum Inception-ResNet-V1 network was used, and after data augmentation and weighted sampling of the ISIC 2019 dataset, the skin damage images were classified, and the classification accuracy was as high as 98.76%. Inception with residuals makes the network need to learn less knowledge and the data distribution of each layer is close, making it easy to learn. The feature extraction function of quantum convolution can extract features in a larger space and achieve higher learning accuracy. In the quantum convolution layer, a single quantum gate applies operations to adjacent qubits, and the same quantum convolution is performed. Within the layers, all quantum gates have tunable parameters, preserving the properties of local connections and weight sharing in convolutional neural networks. These two characteristics enable the quantum convolutional neural network to effectively extract image features, reduce the complexity of the network model, and significantly improve the computational efficiency of the model.

Data availability statement

The original contributions presented in the study are included in the article/Supplementary Material, further inquiries can be directed to the corresponding author.

Author contributions

ZL proposed the content and methods of the research and organized the database to conduct experiments, and wrote the first draft. XC and ZC performed statistical analysis. YW and HM provides direction for dissertation medical content. DH and YD participated in the revision and reading of the manuscript.

Funding

The National Natural Science Foundation of China (No. 61772295, 61572270). The Science and Technology Research Program of Chongqing Municipal Education Commission (Grant No. KJZD-M202000501). Chongqing Technology Innovation and application development special general project (cstc2020jscxlyjsAX0002). Chongqing Technology Foresight and Institutional Innovation Project (cstc2021jsyj-yzysbAX0011).

Acknowledgments

Thanks for the important technical help given by colleagues in the laboratory, and the fund support.

Conflict of interest

The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Publisher’s note

All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers. Any product that may be evaluated in this article, or claim that may be made by its manufacturer, is not guaranteed or endorsed by the publisher.

References

1. Vuković P, Lugović-Mihić L, Ćesić D, Novak-Bilić G, Šitum M, Spoljar S. Melanoma development: Current knowledge on melanoma pathogenesis. *Acta Dermatovenerologica Croatica* (2020) 28:163.

2. Amaria RN, Menzies AM, Burton EM, Scolyer RA, Tetzlaff MT, Antdbacka R, et al. Neoadjuvant systemic therapy in melanoma: Recommendations of the international neoadjuvant melanoma consortium. *Lancet Oncol* (2019) 20: e378–89. doi:10.1016/S1470-2045(19)30332-8

3. Saginala K, Barsouk A, Aluru JS, Rawla P, Barsouk A. Epidemiology of melanoma. *Med Sci* (2021) 9:63. doi:10.3390/medsci9040063

4. Carr S, Smith C, Wernberg J. Epidemiology and risk factors of melanoma. *Surg Clin North Am* (2020) 100:1–12. doi:10.1016/j.suc.2019.09.005

5. Hartman RI, Lin JY. Cutaneous melanoma—A review in detection, staging, and management. *Hematol Oncol Clin North Am* (2019) 33:25–38. doi:10.1016/j.hoc.2018.09.005

6. Pérez E, Reyes O, Ventura S. Convolutional neural networks for the automatic diagnosis of melanoma: An extensive experimental study. *Med image Anal* (2021) 67:101858. doi:10.1016/j.media.2020.101858

7. Naeem A, Farooq MS, Khelifi A, Abid A. Malignant melanoma classification using deep learning: Datasets, performance measurements, challenges and opportunities. *IEEE Access* (2020) 8:110575–97. doi:10.1109/access.2020.3001507

8. Marconcini R, Spagnolo F, Stucci LS, Ribero S, Marra E, De Rosa F, et al. Current status and perspectives in immunotherapy for metastatic melanoma. *Oncotarget* (2018) 9:12452–70. doi:10.18632/oncotarget.23746

9. Jenkins RW, Fisher DE. Treatment of advanced melanoma in 2020 and beyond. *J Invest Dermatol* (2021) 141:23–31. doi:10.1016/j.jid.2020.03.943

10. Chin R, Chen K, Abraham C, Jr, Robinson C, Perkins S, Johanns T, et al. Brain metastases in metastatic cutaneous melanoma: Patterns of care and clinical outcomes in the era of immunotherapy and targeted therapy. *Int J Radiat Oncology*Biology*Physics* (2021) 111:e565–6. doi:10.1016/j.ijrobp.2021.07.1528

11. Nachbar F, Stolz W, Merkle T, Cognetta AB, Vogt T, Landthaler M, et al. The abcd rule of dermatoscopy: High prospective value in the diagnosis of doubtful melanocytic skin lesions. *J Am Acad Dermatol* (1994) 30:551–9. doi:10.1016/s0190-9622(94)70061-3

12. Argenziano G, Fabbrocini G, Carli P, De Giorgi V, Sammarco E, Delfino M. Epiluminescence microscopy for the diagnosis of doubtful melanocytic skin lesions: Comparison of the abcd rule of dermatoscopy and a new 7-point checklist based on pattern analysis. *Arch Dermatol* (1998) 134:1563–70. doi:10.1001/archderm.134.12.1563

13. Vuković P, Lugović-Mihić L, Ćesić D, Novak-Bilić G, Šitum M, Spoljar S. Melanoma development: Current knowledge on melanoma pathogenesis. *Acta Dermatovenerologica Croatica* (2020) 28:163.

14. Atkins MB, Curiel-Lewandrowski C, Fisher DE, Swetter SM, Tsao H, Aguirre-Ghiso JA, et al. The state of melanoma: Emergent challenges and opportunities. *Clin Cancer Res* (2021) 27:2678–97. doi:10.1158/1078-0432.ccr-20-4092

15. Wouters J, Kalender-Atak Z, Minnoye L, Spanier KI, De Waegeneer M, Bravo González-Blas C, et al. Robust gene expression programs underlie recurrent cell states and phenotype switching in melanoma. *Nat Cel Biol* (2020) 22:986–98. doi:10.1038/s41556-020-0547-3

16. Nasr-Esfahani E, Samavi S, Karimi N, Soroushmehr SMR, Jafari MH, Ward K, et al. (2016). Melanoma detection by analysis of clinical images using convolutional neural network. In 2016 38th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC IEEE), 1373–6.

17. Alquran H, Qasmieh IA, Alqudah AM, Alhammouri S, Alawneh E, Abughazaleh A, et al. (2017). The melanoma skin cancer detection and classification using support vector machine. In 2017 IEEE Jordan Conference on Applied Electrical Engineering and Computing Technologies (AEECT). 1–5. doi:10.1109/AEECT.2017.8257738

18. Vasconcelos CN, Vasconcelos BN. Experiments using deep learning for dermoscopy image analysis. *Pattern Recognition Lett* (2020) 139:95–103. doi:10.1016/j.patrec.2017.11.005

19. Han SS, Kim MS, Lim W, Park GH, Park I, Chang SE. Classification of the clinical images for benign and malignant cutaneous tumors using a deep learning algorithm. *J Invest Dermatol* (2018) 138:1529–38. doi:10.1016/j.jid.2018.01.028

20. Pham T-C, Luong C-M, Visani M, Hoang V-D (2018). Deep cnn and data augmentation for skin lesion classification. In Asian Conference on Intelligent Information and Database Systems (Springer), 573–82.

21. Emara T, Afify HM, Ismail FH, Hassanien AE (2019). A modified inception-v4 for imbalanced skin cancer classification dataset. In 2019 14th International Conference on Computer Engineering and Systems *(ICCES) (IEEE)*, 28–33.

22. Adegun AA, Viriri S. Deep learning-based system for automatic melanoma detection. *IEEE Access* (2019) 8:7160–72. doi:10.1109/access.2019.2962812

23. Hosny KM, Kassem MA, Foaud MM. Classification of skin lesions using transfer learning and augmentation with alex-net. *PloS one* (2019) 14:e0217293. doi:10.1371/journal.pone.0217293

24. Yu L, Chen H, Dou Q, Qin J, Heng P-A. Automated melanoma recognition in dermoscopy images via very deep residual networks. *IEEE Trans Med Imaging* (2017) 36 (4):994–1004. doi:10.1109/TMI.2016.2642839

25. Hosny KM, Kassem MA, Foaud MM. Skin melanoma classification using roi and data augmentation with deep convolutional neural networks. *Multimed Tools Appl* (2020) 79:24029–55. doi:10.1007/s11042-020-09067-2

26. Iyer V, Ganti B, Hima Vyshnavi A, Krishnan Namboori P, Iyer S. Hybrid quantum computing based early detection of skin cancer. *J Interdiscip Math* (2020) 23:347–55. doi:10.1080/09720502.2020.1731948

27. Kassem MA, Hosny KM, Fouad MM. Skin lesions classification into eight classes for isic 2019 using deep convolutional neural network and transfer learning. *IEEE Access* (2020) 8:114822–32. doi:10.1109/access.2020.3003890

28. Zhou N-R, Liu X-X, Chen Y-L, Du N-S. Quantum K-nearest-neighbor image classification algorithm based on KL transform. *Int J Theor Phys*. Springer (2021) 60 (3):1209–1224.

29. Gong L-H, Xiang L-Z, Liu S-H, Zhou N-R. Born machine model based on matrix product state quantum circuit. *Phys A: Stat Mech Appl*. Elsevier (2022) 593: 126907.

30. Abdelhalim ISA, Mohamed MF, Mahdy YB. Data augmentation for skin lesion using self-attention based progressive generative adversarial network. *Expert Syst Appl* (2021) 165:113922. doi:10.1016/j.eswa.2020.113922

31. Bissoto A, Perez F, Valle E, Avila S. Skin lesion synthesis with generative adversarial networks. In: *OR 2.0 context-aware operating theaters, computer assisted robotic endoscopy, clinical image-based procedures, and skin image analysis*. Springer (2018). p. 294–302.

32. Ren J, Yang Q, Zhu Y, Zhu X, Tian H, Wang W, et al. Complex social contagions on weighted networks considering adoption threshold heterogeneity. *IEEE Access* (2020) 8:61905–14. doi:10.1109/access.2020.2984615

33. Athey S, Imbens GW. Design-based analysis in difference-in-differences settings with staggered adoption. *J Econom* (2022) 226:62–79. doi:10.1016/j.jeconom.2020.10.012

34. Marsh-Armstrong B, Migacz J, Jonnal R, Werner JS. Automated quantification of choriocapillaris anatomical features in ultrahigh-speed optical coherence tomography angiograms. *Biomed Opt Express* (2019) 10:5337–50. doi:10.1364/boe.10.005337

35. Ye T-Y, Li H-K, Hu J-L. Semi-quantum key distribution with single photons in both polarization and spatial-mode degrees of freedom. *Int J Theor Phys (Dordr)* (2020) 59:2807–15. doi:10.1007/s10773-020-04540-y

36. Combalia M, Codella NC, Rotemberg V, Helba B, Vilaplana V, Reiter O, et al. *Bcn20000: Dermoscopic lesions in the wild* (2019). *arXiv preprint arXiv:1908.02288*.

37. Fawcett T. An introduction to roc analysis. *Pattern recognition Lett* (2006) 27: 861–74. doi:10.1016/j.patrec.2005.10.010

38. Pacheco AG, Ali A-R, Trappenberg T. *Skin cancer detection based on deep learning and entropy to detect outlier samples* (2019). *arXiv preprint arXiv: 1909.04525*.

39. Molina-Molina EO, Solorza-Calderón S, Álvarez-Borrego J. Classification of dermoscopy skin lesion color-images using fractal-deep learning features. *Appl Sci* (2020) 10:5954. doi:10.3390/app10175954

40. El-Khatib H, Popescu D, Ichim L. Deep learning–based methods for automatic diagnosis of skin lesions. *Sensors* (2020) 20:1753. doi:10.3390/s20061753

41. Monika MK, Vignesh NA, Kumari CU, Kumar M, Lydia EL. Skin cancer detection and classification using machine learning. *Mater Today Proc* (2020) 33: 4266–70. doi:10.1016/j.matpr.2020.07.366

42. Rahman Z, Hossain MS, Islam MR, Hasan MM, Hridhee RA. An approach for multiclass skin lesion classification based on ensemble learning. *Inform Med Unlocked* (2021) 25:100659. doi:10.1016/j.imu.2021.100659

43. Cauvery K, Siddalingaswamy P, Pathan S, D'souza N (2021). A multiclass skin lesion classification approach using transfer learning based convolutional neural network. In 2021 Seventh International conference on Bio Signals, *Images, and Instrumentation (ICBSII) (IEEE)*, 1–6.

44. Pacheco AG, Krohling RA. An attention-based mechanism to combine images and metadata in deep learning models applied to skin cancer classification. *IEEE J Biomed Health Inform* (2021) 25:3554–63. doi:10.1109/jbhi.2021.3062002

TYPE Original Research
PUBLISHED 03 November 2022
DOI 10.3389/fphy.2022.1029552

Check for updates

OPEN ACCESS

EDITED BY
Mingxing Luo,
Southwest Jiaotong University, China

REVIEWED BY
Hong Lai,
Southwest University, China
H. Z. Shen,
Northeast Normal University, China

*CORRESPONDENCE
Jindong Wang,
Wangjindong@m.scnu.edu.cn

SPECIALTY SECTION
This article was submitted to Quantum Engineering and Technology,
a section of the journal
Frontiers in Physics

RECEIVED 27 August 2022
ACCEPTED 23 September 2022
PUBLISHED 03 November 2022

CITATION
Mi S, Dong S, Hou Q, Wang J, Yu Y, Wei Z and Zhang Z (2022), Joint photon-number splitting attack on semi-quantum key distribution.
Front. Phys. 10:1029552.
doi: 10.3389/fphy.2022.1029552

Joint photon-number splitting attack on semi-quantum key distribution

Shang Mi[1], Shuang Dong[1], Qincheng Hou[1], Jindong Wang[1]*, Yafei Yu[2], Zhengjun Wei[1] and Zhiming Zhang[2]

[1]Guangdong Provincial Key Laboratory of Quantum Engineering and Quantum Materials, School of Information and Optoelectronic Science and Engineering, South China Normal University, Guangzhou, China, [2]Guangdong Provincial Key Laboratory of Nanophotonic Functional Materials and Devices, School of Information and Optoelectronic Science and Engineering, South China Normal University, Guangzhou, China

Semi-quantum key distribution is based on the basic principle of quantum mechanics, which allows a classical user and quantum user to use information theory to have a secure shared key. In 2021, our research group proved the first proof-of-principle experimental demonstration of semi-quantum key distribution and verified its feasibility. Due to the limitations of existing science and technology, the experimental system still features a combination of multiphoton signal source and loss in the transmission line. This makes semi-quantum key distribution as susceptible to a photon-number splitting attack as quantum key distribution, leading to limitations of secure transmission distance. It seems that practical single-state semi-quantum key distribution can overcome photon-number splitting attack due to the SIRT bits (also known as the “sifted key”). However, its dual-channel feature still opens up an observation window to Eve. We present two joint photon-number splitting attacks suitable for a single-state semi-quantum key distribution system and show that through the joint photon-number splitting attack, Eve can obtain key information without being detected by Alice or Bob.

KEYWORDS

quantum key distribution, semi-quantum key distribution, practical security, weak coherent pulses, photon-number splitting attack

1 Introduction

In recent years, with the rapid development of quantum computing, the security of the original classical secure communication has been greatly compromised. Compared with classical communication, whose security depends on the complexity of mathematical computation, quantum communication, whose security is based on quantum theory [1], is not threatened by the quantum computer, which theoretically guarantees the absolute security of the communication. The field of quantum communication includes quantum key distribution (QKD) [2–7], quantum secret sharing (QSS) [8–10], quantum secure direct communication (QSDC) [11–13], quantum teleportation (QT) [14–16], quantum dense coding (QDC) [17–19], and quantum digital signature (QDS) [20]. After more than

30 years of efforts by scientists, QKD, the most mature quantum communication technology, has made breakthrough progress in both theory and experiment and has become an indispensable component in the development of information security field. It is worth mentioning that measurement-device-independent quantum key distribution (MDI-QKD) [21, 22] can be immune to all detector side-channel attacks. Moreover, it can be easily implemented in combination with the matured decoy-state methods under current technology. In 2021, Yi-Peng Chen et al. implemented the double-scanning method into MDI-QKD for the first time and carried out corresponding experimental demonstration [5]. In 2022, Pei Zeng et al. proposed a mode-pairing measurement-device-independent quantum key distribution scheme in which the encoded key bits and bases are determined during data post processing [23].

Based on the consideration of reducing quantum resources in the process of key distribution, the concept of semi-quantum key distribution (SQKD) [24] has been proposed and extended into semi-quantum cryptography, such as semi-quantum secret sharing (SQSS) [25, 26], semi-quantum secure direct communication (SQSDC) [27–29], semi-quantum digital signature (SQDS) [30], semi-quantum private comparison (SQPC) [31–35], and semi-quantum key agreement (SQKA) [36, 37]. In 2007, Boyer et al. proposed the first SQKD protocols: BKM07 [24], which place a further restriction on the classical user. The classical user just can access a segment of the channel, whenever a qubit passes through that segment Bob can either let it go undisturbed (Ctrl) or measure the qubit in the classical basis and resend a fresh qubit (Sift); in 2009, the second SQKD protocol BGKM09 [38] was proposed. This protocol utilized the Permute operation as opposed to the Measure and Resend operations. The same year, Zou et al. proposed five new protocols based on the consideration of whether quantum resources can be further reduced on the part of the two users [39], among which the single-state protocol attracted the most attention. It was show for the first time that fully quantum users can also reduce their resource requirements. In 2014, Reflection-based SQKD was proposed [40], it was similar to B92-protocol, and was shown that a key can be distilled from B's action. In 2017, Boyer et al. extended the operation of Bob side to cleverly avoid the problem of reproducing new photons, and proposed a mirror protocol [41] that could overcome "tagged" attack. To some extent, this is also a single-state protocol, and only two SQKD experiments have been based on it. Subsequently, other important SQKD protocols have also been proposed, such as the high-efficiency SQKD protocol [42, 43], which can improve efficiency by biasing choices to improve their overall efficiency; the authenticated SQKD protocol [44–47], which does not utilize an authenticated channel (instead relying on a pre-shared key); and the high-dimensional SQKD protocol [48, 49], which has been shown to tolerate high levels of noise as the dimension of the quantum state increases.

The security of idealized SQKD has been reported against individual [50, 51] and very sophisticated collective [40, 52–54] attacks. A lower bound has been derived for the key rate as a function of the noise of the quantum channel in high dimension semi-quantum key distribution [55]. In 2021, our research group performed the first proof-of-principle demonstration [56] of semi-quantum key distribution based on the Mirror protocol, which contributed to the further application of SQKD. The experiments are also based on weak coherent pulses as signal states with a low probability of containing more than one photon. This SQKD experiment, like the QKD experiment, is also based on weak coherent pulses (WCP) as signal states with a low probability of containing more than one photon. Whether the multiphoton problem of such non-ideal light source will lead to security vulnerabilities of the SQKD system is an urgent issue to be discussed. The most powerful tool at the disposition of an eavesdropper, as we know, is the photon-number splitting attack [57–59]. This multiphoton problem in semi-quantum contexts was discussed as early as 2009 [38], but the examination of the protocol against PNS attacks was left to future research. In Gurevich's experiment [60], some operations in SQKD protocol were realized with the use of a time-coding scheme, and it was mentioned that a pulse power level that is too high, which is a security hole that enables various attacks. In 2018, Chrysoula presented a short discussion [48] of possible attacks and countermeasures for the case of optical implementations. He proposed that while the PNS attack is applicable to most of the protocols that use imperfect photon sources, the above description of its particular implementation is given on the example of a standard QKD one-way scheme, thus, it should be re-examined when applied to different protocols. Some other reports [37, 61–63] have mentioned Bob should set up a photon number splitter (PNS) to protect against a Trojan horse attack. In Ref. [64], the author mentioned that due to the two-way channel and the use of the Measure-Resend operation, Eve is afforded even more attack opportunities, such as the photon-tagging attack and PNS attack, and it is an open question in the semi-quantum case. To our knowledge, we are the first to do further subject research in this issue. We prove that it is useless to implement single-channel PNS attack in SQKD. Does this mean that a single-state SQKD system with multiphoton sources has unconditional security? The answer is no, because due to SQKD's requirement of a two-way quantum channel, Eve has the opportunity to implement joint PNS attack through the forward channel and reverse channel. Based on this, we propose two kinds of joint PNS attack for a single-state SQKD system, as long as there is loss in the channel, Eve can get the key information. With a large enough loss, Eve can obtain all key information without being detected by Alice and Bob.

The remainder of this study is organized as follows. In Section 2, a brief background on PNS attacks and the SQKD model is provided. In Section 3, two joint PNS attack were designed for single-state SQKD. In Section 4, an evaluation of

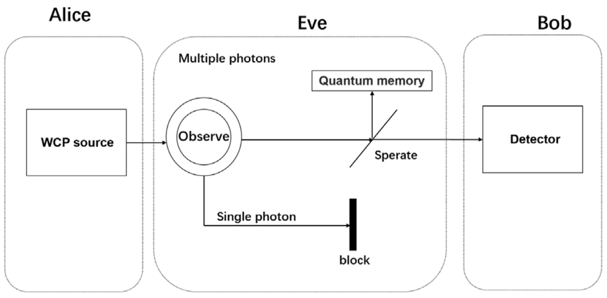


FIGURE 1
Schematic of a PNS attack. Eve learns the number of photons in the pulse through nondestructive measurements. For single photons, Eve blocks them with a certain probability, and she separates one photon from multiphotons.

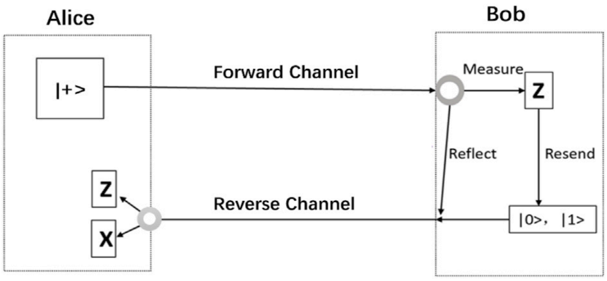


FIGURE 2
The typical setup of a single-state SQKD protocol. Reflect is Ctrl, meaning that Bob reflects the qubit back to Alice undisturbed. Measure and Resend is Sift, meaning that Bob measures it in the Z basis and resends it to Alice in the same state that he found it. For the returned qubit, Alice chooses to measure it on the Z or the X basis randomly.

a joint PNS attack is given, and the conclusion is given in Section 5.

2 Single-channel attack in single-state SQKD

2.1 Review of PNS attack

In a quantum optical implementation, single-photon states are ideally suited for quantum key distribution. However, such states have not been practically implemented for QKD and SQKD. The experiments attenuate the weakly coherent light generated by the laser light source to the order of single photon to replace the single-photon light source. The realistic signal sources with a certain probability of containing multiple photons. For the practical system, consisting of the actual signal source, lossy channel, and threshold detector, Eve can implement PNS attack [57, 58]. In a PNS attack, eavesdropper Eve needs to have three abilities: 1) ability to replace the noisy and lossy transmission line by a superior one, 2) ability to use quantum nondestructive (QND) measurement technology to measure the number of photons contained in the pulse and block or separate the photons without modifying the polarization of the photons, and 3) and possession of a quantum register, can keep photon. When receiving the data regarding the basis, Eve measures her photon and obtains qubit information.

In this study, we assume the model where any non-accessible loss [58] of the quantum channel is considered to be part of detection apparatus, which allows us to conduct our research without loss of generality. Moreover, a PNS attack that keeps the photon number distribution constant in the detector is not considered. When there is available loss in the channel, for the case of a single-photon state, Eve directly blocks the photon. For the multiphoton pulse with the number of photons greater than or equal to 2, Eve extracts a photon from the pulse and puts it into quantum memory, sending the remaining photons to Bob, so that Eve can replace the lossy quantum channel by an ideal one, block a fraction b of the single-photon signals or even use only a multiphoton signal to match the detector's expectation of non-vacuum pulses. The general process of this protocol is shown in Figure 1.

2.2 Review of single-state SQKD

The quantum communication process of single-state SQKD [39, 65] operates by repeating the following (Alice is a quantum user and Bob is a classical user):

Step 1. Alice prepares a single qubit in the state |+> and sends it to Bob. Alice's photon source emits signals with a Poisson photon number distribution that has a mean value of ν. The quantum channel is described by a single-photon transmission efficiency η. We can find at Bob's end of the quantum channel a Poisson photon number distribution with mean photon number $\eta\nu$.
Step 2. Bob will choose to either Measure and Resend or to Reflect the incoming qubit.

a. Bob's Ctrl operation uses a fully reflective instrument (that is, no optical loss), the average number of photons of the pulse entering the reverse channel after the Ctrl operation is still $\eta\nu$.
b. Bob selects the measurement but gets no information and sends an empty pulse to the reverse channel, which we call Sift-0.
c. Bob subjects the incoming qubit to a Z basis measurement and then resend the result back to A as a Z basis qubit with a Poisson photon number distribution with mean value μ, which we call Sift-1.

Step 3. Alice chooses to measure the returning qubit in the Z or the X basis randomly.

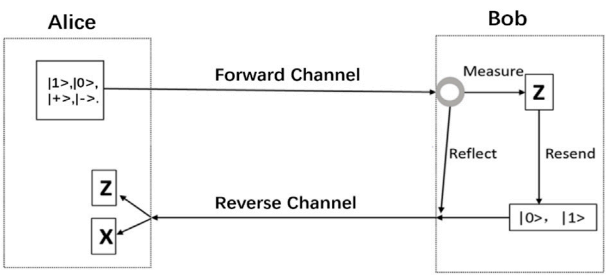


FIGURE 3
The typical setup of a four-state SQKD protocol. The figure is from [61], Alice prepares and sends one of the four states with uniform probability, and Bob chooses either to Measure and Resend or to Reflect the incoming qubit, and Alice measures the returning qubit on the same basis she initially used to prepare it (Z or X).

Step 4. Users Alice and Bob disclose their choices. If Bob has chosen Sift-1 and if Alice has chosen to measure in the Z basis, they should share a correlated bit to be used for their raw key. If Bob has chosen Ctrl and if Alice has chosen to measure in the X basis, she should observe outcome $|+>$, and any other outcome is considered an error.

The general process of this protocol is shown in Figure 2.

2.3 Why single-state SQKD can overcome single-channel PNS attack

By implementing the attack procedure described in Section 2.1 in the forward channel, Eve can take away the qubit information in the forward channel, but Eve's qubit information $|+>$ is not valid information and is public information, so the PNS attack in the forward channel is meaningless.

According to the analysis in 2.2, Ctrl's bits (Bob has chosen Ctrl and Alice has chosen to measure in the X basis) are not only used as Text bits but are also equivalent to inserts of a Ctrl state pulse into the Sift state pulse and sends it together with the signal state pulse to Bob. We can confirm that there are two kinds of pulses with different average photon number (when $\eta\nu \neq \mu$) in the reverse channel after Bob's operation, the proportion of single and multiple photons in them is very different. At the same time, the modes of these two pulses are completely consistent. The eavesdropper Eve cannot effectively distinguish between the two states of the intercepted optical pulse, and can only carry out PNS attack, which will lead to abnormal attenuation of the Sift pulse, and thus be discovered by Alice and Bob. Thus, SQKD can naturally overcome the single-channel PNS attack in the reverse channel.

It is worth mentioning that the first proposed SQKD protocol is BKM07. In this article, we call this the four-state protocol. The general process of this protocol is shown in Figure 3 [65]. There are two differences between these two protocols. First, the states sent by Alice are different. In the four-state protocol, Alice prepares and sends one of the four states $|0>, |1>, |+>$, or $|->$ with uniform probability. In the single-state protocol, Alice just prepares and sends the state $|+>$. Second, for qubit that are returned to Alice after Bob's operation, Alice measures the returning qubit in the same basis she initially used to prepare it in four-state protocol, but in single-state, Alice chooses to measure it on the Z or the X basis randomly. Therefore, some of the states $|0>, |1>$ will be used directly to be raw key in the forward channel of the four-state protocol. Eve can take away the effective qubit information by implementing attack procedure described in Section 2.1 in the forward channel. Furthermore, both the forward channel and reverse channel leak qubit information independently, and the single-channel PNS attack described in Section 2.1 can make the four-state protocol insecure. By comparing these two protocols, we can also see that, while the PNS attack is applicable to most of the standard QKD one-way schemes using imperfect photon sources, analysis of PNS attacks of the SQKD two-way schemes are even more challenging. The single-channel PNS analysis of SQKD protocol with different states and coding rules is different.

3 Two joint PNS attack methods for single-state SQKD

Let's take Eve's perspective and model the experimental process of single-state SQKD as follows:

Step 1: Alice prepares and sends signals with a Poisson photon number distribution with mean value ν(n is the number of photons in the forward channel pulse).

$$P_\nu(n) = e^{-\nu}\frac{\nu^n}{n!} \tag{1}$$

Step 2: The quantum channel is described by a single-photon transmission efficiency η. The photon number distribution at Bob's end of the quantum channel forms a Poissonian distribution with a mean photon number of $\eta\nu$.

$$P_B(\mathbf{n}) = e^{-\eta\nu}\frac{(\eta\nu)^n}{n!} \tag{2}$$

Step 3: Bob's action:

a. Bob has a probability of $\frac{1}{2}$ to perform Ctrl, in this case, Bob reflects a Poisson-distributed pulse with mean photon number $\eta\nu$ into the reverse channel (m is the number of photons in the reverse channel pulse).

$$P_{\eta\nu}(\mathrm{m}) = e^{-\eta\nu}\frac{(\eta\nu)^m}{m!} \tag{3}$$

b. Bob has a probability of $\frac{1}{2}P_B(0)$ to perform Sift-0; in this case, Bob sends an empty pulse to the reverse channel.

c. Bob has a probability of $\frac{1}{2}[1 - P_B(0)]$ to perform Sift-1; in this case, Bob sends a Poisson-distributed pulse with mean photon number μ into the reverse channel.

$$P_\mu(m) = e^{-\mu}\frac{\mu^m}{m!} \tag{4}$$

Step 4: The distribution of the pulse reaching Alice's detector after the loss of reverse channel:

d. Ctrl:

$$P_{ctrl}(m) = \frac{1}{2}P_{\eta^2\nu}(m) = \frac{1}{2}e^{-\eta^2\nu}\frac{(\eta^2\nu)^m}{m!} \tag{5}$$

e. Sift-0:

$$P_{sift-0}(0) = \frac{1}{2}P_B(0) \tag{6}$$

f. Sift-1:

$$P_{sift-1}(m) = \frac{1}{2}[1 - P_B(0)]P_{\eta\mu}(m) = \frac{1}{2}[1 - P_B(0)]e^{-\eta\mu}\frac{\eta\mu^m}{m!} \tag{7}$$

Step 5: The vacuum signals are expected at the entrance to Alice's apparatus of the lossy channel:

$$P_A(0) = P_{ctrl}(0) + P_{sift-0}(0) + P_{sift-1}(0) \tag{8}$$

3.1 The first joint PNS attack mode

In the forward channel, Eve blocks single-photon signal with a probability f but does not split the signal, which consists of two or more photons (multiphoton signal). In the reverse channel, Eve blocks a single-photon signal with probability b and deterministically splits one photon off each multiphoton signal. When receiving the data regarding the basis, Eve measures her photon and obtains qubit information.

We model the first joint PNS attack process as follows:

Step 1: Alice prepares and sends signals with a Poisson photon number distribution with mean value ν.

Step 2: Eve replaces the original channel with a lossless channel and blocks single photon with probability f, do nothing on multiphoton pulses. The photon number distribution at Bob's end of the quantum channel after Eve's attack, as follows.

$$P_B^{'}(n) = \begin{cases} (1+f\nu)e^{-\nu} & n = 0 \\ (1-f)\nu e^{-\nu} & n = 1 \\ \frac{\nu^n}{n!}e^{-\nu} & n > 1 \end{cases} \tag{9}$$

Step 3: Bob's action.

a. Bob has a probability of $\frac{1}{2}$ to perform Ctrl, in this case, Bob reflects the forward channel pulse distributed into the reverse channel.

b. Bob has a probability of $\frac{1}{2}P_B^{'}(0)$ to perform Sift-0, in this case, Bob sends an empty pulse into the reserve channel.

c. Bob has a probability of $\frac{1}{2}[1 - P_B^{'}(0)]$ to perform Sift-1, in this case, Bob sends a Poisson-distributed pulse with a mean photon number μ into the reserve channel.

Step 4: Eve replaces the original channel with a lossless channel and blocks a single photon with probability b and splits a photon from multiphoton pulses into the reverse channel.

d. Ctrl:

$$P_{ctrl}^{\prime}(\mathrm{m}) = \frac{1}{2}\begin{cases} P_B^{'}(0) + bP_B^{'}(1) & m = 0 \\ (1-b)P_B^{'}(1) + P_B^{'}(2) & m = 1 \\ P_B^{'}(m+1) & m > 1 \end{cases} \tag{10}$$

e. Sift-0:

$$P_{sift-0}^{\prime}(0) = \frac{1}{2}P_B^{'}(0) \tag{11}$$

f. Sift-1:

$$P_{sift-1}^{\prime}(m) = \frac{1}{2}\left[1 - P_B^{'}(0)\right]\begin{cases} (1+b\mu)e^{-\mu} & m = 0 \\ \left((1-b)\mu + \frac{\mu^2}{2}\right)e^{-\mu} & m = 1 \\ \frac{\mu^{m+1}}{(m+1)!}e^{-\mu} & m > 1 \end{cases} \tag{12}$$

Step 5: Vacuum signals are expected at the entrance to Alice's apparatus of the first joint PNS attack.

$$P_A^{'}(0) = P_{ctrl}^{\prime}(0) + P_{sift-0}^{\prime}(0) + P_{sift-1}^{\prime}(0) \tag{13}$$

First, to remain undetected, Eve adjusts f to match the number of vacuum signals arriving at Bob's detector of the PNS attack to that of the lossy channel, $P_B^{'}(0) = P_B(0)$. This leads to the following expression:

$$f = \frac{1}{\nu}\left(e^{\nu(1-\eta)} - 1\right) \tag{14}$$

Second, to remain undetected, Eve adjusts b to match the number of vacuum signals arriving at Alice's detector of the PNS attack to that of the lossy channel, $P_A^{'}(0) = P_A(0)$. This leads to the following expression:

$$\boldsymbol{b} = \frac{e^{-\eta^2 \nu} + e^{-\eta\mu}(1 - e^{-\eta\nu}) - e^{-\eta\nu} - e^{-\mu}(1 - e^{-\eta\nu})}{e^{-\nu}\left[\nu + 1 - e^{\nu(1-\eta)}\right] + \mu e^{-\mu}(1 - e^{-\eta\nu})} \tag{15}$$

It is possible to fulfill this matching condition if $f, b > 0$. Based on the analysis of b and f, we can draw the following conclusions:

We find, for $\eta = 1, f = 0, b = 0$, which expresses the fact that for a lossless channel the joint PNS attack cannot (and need not) be accompanied by the blocking of single-photon signals in forward channel and reverse channel.

We find that all single-photon signals can be blocked if there are exactly as many multiphoton signals leaving the source as non-vacuum signals are arriving at the receiver of Alice and Bob, that is $f = 1$, $b = 1$. Meaning in this case the complete information falls into Eve's hands.

Assuming that $\nu = 0.1$, for $1 - \frac{\ln(\nu+1)}{\nu} < \eta < 1$, f takes on values in the interval [1, 0].

When $\mu \geq 0.93$, as long as $0.05 \ll \eta$, Eve can always adjust f, to let $b > 0$, meaning that she can carry out joint PNS attacks. Such as $\mu = 0.93, \nu = 0.1, \eta = 0.05, f = 0.996589, b = 0.993804$.

When $0.93 > \mu > 0$, as long as $0.05 \ll \eta \ll 0.18$, there is always $1 > f > 0, b > 1$. Eve can always adjust f so that b is greater than 1, Meaning Eve can carry out joint PNS attacks, Eve needs to suppress not only single-photon signals, but also multiphoton signals in reverse. Here, $\mu = 0.01, \nu = 0.1, \eta = 0.05, f = 0.997, b = 12.16$.

Assuming that $\nu = 0.1$, for $0 < \eta < 1 - \frac{\ln\ (\nu+1)}{\nu}$, $f > 1$.

When $b > 0$, at this time, a PNS attack can be implemented, which means that when the loss is large enough and the average photon number μ sent by Bob's sender is large, Eve can block multiple photons with certain probability in both the forward channel and the reverse channel to complete the joint PNS attack Here, $\mu = 0.99, \nu = 0.1, \eta = 0.04, f = 1.0075, b = 1.25$.

When $b < 0$, It means that even if the loss is small, Eve cannot block multiple photons, otherwise Eve needs to add photons in the reverse channel, which is impossible. Here, $\mu = 0.93, \nu = 0.1, \eta = 0.02, f = 1.02, b = -1.78$.

3.2 The second joint PNS attack mode

Eve does not operate the photons in the forward channel and only observes the number of photons in the forward channel pulse. The single photon in the reverse channel (a single photon cannot be distinguished from Ctrl or Sift-1) is blocked with probability p. On the multiphoton pulse that Bob performs Sift-1 operation in the reverse channel, Eve blocks the m-photon pulse that she can distinguish with probability k_m. For the remaining multiphoton pulses in the reverse channel, Eve separates a single photon. When receiving data regarding the basis, Eve measures her photon and obtains qubit information.

Eve performs nondestructive measurements on the number of photons in the forward and reverse pulses. When the number of photons in the reverse channel of the same pulse is larger than that in the forward channel, Eve can determine that the pulse in this reverse channel is from the Sift-1 operation. The probability of all m-photon pulses for Bob to perform the Sift-1 operation is:

$$\boldsymbol{P_{sift-1} = \frac{1}{2}[1 - P_B(0)]\, P_\mu(m)} \tag{16}$$

In the reverse channel, the m-photon pulse probability of Sift-1 that Eve can distinguish is:

$$\boldsymbol{P'_{sift-1} = \frac{1}{2}[1 - P_B(0)] \sum\nolimits_{n=1}^{m-1} P_\nu(n) P_\mu(m)} \tag{17}$$

Then, the probability that the Sift-1 operation m-photon pulse that Eve can distinguish accounted for all the Sift-1 photons is:

$$\boldsymbol{j_m = \frac{\frac{1}{2}[1 - P_B(0)] \sum_{n=1}^{m-1} P_\nu(n) P_\mu(m)}{\frac{1}{2}[1 - P_B(0)]\, P_\mu(m)} = \sum\nolimits_{n=1}^{m-1} P_\nu(n)} \tag{18}$$

In the second joint PNS attack, Eve only operates in reverse channel after Bob's operation:

g. Ctrl:

$$\boldsymbol{P''_{ctrl}\ (m) = \frac{1}{2}\begin{cases} (1 + p\eta\nu)e^{-\eta\nu} & m = 0 \\ (1 - p)\eta\nu e^{-\eta\nu} + \dfrac{(\eta\nu)^2}{2} e^{-\eta\nu} & m = 1 \\ \dfrac{\nu^m}{m!} e^{-\nu} & m > 1 \end{cases}} \tag{19}$$

h. Sift-0:

$$\boldsymbol{P''_{sift-0}\ (0) = \frac{1}{2} P_B(0)} \tag{20}$$

i. Sift-1:

$$\boldsymbol{P''_{sift-1}\ (m) = \frac{1}{2}[1 - P_B(0)] \times \begin{cases} (1 + p\mu)e^{-\mu} + \sum_{m=2}^{\infty} j_m K_m P_\mu(m) & m = 0 \\ (1 - p)\mu e^{-\mu} + (1 - j_2 K_2) P_\mu(2) & m = 1 \\ (1 - j_{m+1} K_{m+1}) P_\mu(m + 1) & m > 1 \end{cases}} \tag{21}$$

Vacuum signals are expected at the entrance to Alice's apparatus of the second joint PNS attack:

$$\boldsymbol{P''_A(0) = P''_{ctrl}\ (0) + P''_{sift-0}\ (0) + P''_{sift-1}\ (0)} \tag{22}$$

Eve adjusts b, K_m to match the number of vacuum signals arriving at Alice's detector of the PNS attack to that of the lossy channel.

As a first step for remaining undetected, we let $P''_{ctrl}\ (0) = P_{ctrl}(0)$ and obtain:

$$p = \frac{1}{\eta\nu}\left(e^{\eta\nu(1-\eta)} - 1\right) \tag{23}$$

Assuming Eve only blocks distinguishable two-photon pulses from Bob's SIFT-1 operation, combined with the condition that $P''_{sift-1}(0) = P_{sift-1}(0)$ we have:

$$\frac{1}{2}[1 - P_B(0)]e^{-\eta\mu} = \frac{1}{2}[1 - P_B(0)]\left[(1 + P\mu)e^{-\mu} + j_2K_2P_\mu(2)\right] \tag{24}$$

Substituting $j_2 = P_\nu(1)$ into Eq. 24:

$$K_2 = \frac{e^{\mu(1-\eta)} - 1 - \frac{\mu}{\eta\nu}\left(e^{\eta\nu(1-\eta)} - 1\right)}{\frac{\mu^2}{2}\nu e^{-\nu}} \tag{25}$$

It is possible to fulfill this matching condition if $p, K_2 > 0$. On this basis, the analysis of p and K_2 shows that:

We find, for $\eta = 1$, $p = 0$, $K_2 = 0$, which expresses the fact that for a lossless channel the second joint PNS attack cannot (and need not) be accompanied by the blocking of signals in reverse channel.

When $\eta < 1$, Eve can always block part of single photon and discriminable two-photon for PNS attack. Here, $\mu = 0.7, \nu = 0.1, \eta = 0.75, p = 0.252358, k_2 = 0.65667$.

When $\mu \geq 0.02$, as long as $\eta \leq 0.17$, the existence of $K_2 > 1$, means that Eve should block not only the distinguishable two-photon but also other distinguishable multiphoton pulses in the reverse channel. Here, $\mu = 0.02, \nu = 0.1, \eta = 0.01, p = 0.99049, k_2 = 1.036$.

4 Results of the two joint PNS attack

From the analysis in Section 2, we know that PNS is found in the reverse channel because Eve is unable to distinguish whether the photons in the pulse originate from Ctrl or Sift-1 (the average number of photons is different). It is easy to come up with two possible solutions.

The inspiration of the first attack is that Eve does not distinguish between the pulse after Bob performs Ctrl operation (the average number of photons is $\eta\nu$) and the pulse after the Sift operation (the average number of photons is μ) in the backward channel. For these two pulses, Eve blocks the single-photon signal with probability b indiscriminately and separates one photon from each multiphoton signal. Eve blocks the single-photon signal with probability b in reverse to match Alice's expectation of the Sift non-vacuum pulses. For Alice's expectation of Ctrl's non-vacuum pulses, Eve needs to block single-photon signal with probability f in the forward channel. Only when $\eta\nu > \mu$, Eve can block a single photon in both the forward channel and the reverse channel. Otherwise, $f < 0$, which means that it is necessary to add photons in the forward channel, which is impossible.

TABLE 1 Example for the first joint PNS attack.

η	μ	ν	f	b
0.2	0.02	0.1	0.843709	0.980309
0.16	0.13	0.1	0.876289	0.938026
0.15	0.2	0.1	0.887171	0.902605
0.2	0.4	0.1	0.832871	0.667241
0.35	0.45	0.1	0.67159	0.494493

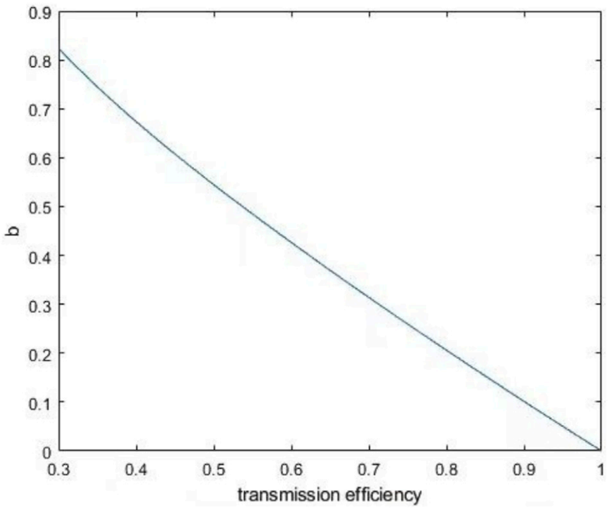


FIGURE 4
When μ = 0.03 and ν = 0.01, the relation image between b and η is obtained according to Eq. 15. The stronger the loss in the channel, the higher the value of *b* (the probability that Eve can block a single photon).

For different values of μ, ν, and η, the values of b and f obtained by the Eq. 14 and Eq. 15 are listed in Table 1.

For the first joint PNS attack, when $\nu = 0.1$, $\mu = 0.03$, we can get the diagram of b and η and show it in Figure 4.

Based on the second idea, the Sift and Ctrl bits are distinguished to carry out PNS attack by the change of photon number in the same pulse in the forward and reverse channels, respectively. We can identify Eve without changing the intercepted pulse under the condition that a quantum nondestructive measurement technique is used to measure whether the pulse contains the number of photons, but only for the same pulse; the reverse channel of the photon number is greater than the former channel of the photon number that we can distinguish. The inspiration of the second attack is that Eve can distinguish between the pulse after Bob performs Ctrl operation (the average number of photons is $\eta\nu$) and the pulse after the Sift operation (the average number of photons is μ) in the backward channel. We found that the number of photons in the

TABLE 2 Example for the second joint PNS attack.

η	μ	v	f	b
0.01	0.01	0.1	0.99049	0.978408
0.04	0.06	0.1	0.961846	0.970377
0.3	0.06	0.1	0.707402	0.276523
0.4	0.4	0.1	0.607258	0.391589
0.84	0.45	0.1	0.16108	0.023679

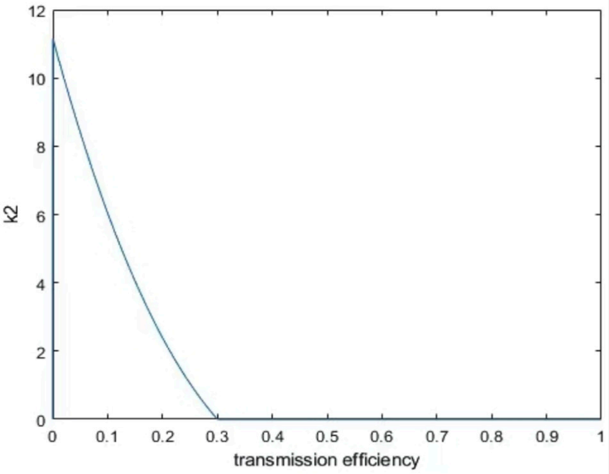


FIGURE 5
When μ = 0.03 and ν = 0.01, the relation image between K_2 and η is obtained according to Eq. 25. We can see that the stronger the loss in the channel, the higher the value of K_2 (the probability that Eve can block a single photon), which is the same as in Figure 4. We can also see that the second method requires more loss.

pulse may vary due to Bob's Sift operation in the reverse channel, and Eve can distinguish a small number of Sift pulses by her technology of quantum-nondestructive (QND) measurement. For indistinguishable pulses, Eve blocks the single-photon signal with probability p. For distinguishable Sift pulses, Eve blocks the signal with probability k.This means more blocking of the Sift pulses, which needs to satisfy $\eta v < \mu$. Otherwise, $k < 0$, means that it is necessary to add photons in the distinguishable Sift pulses, which is impossible.

For different values of μ, v, and η, the values of p and $k_2$obtained by the Eq. 23 and Eq. 25 are listed in Table 2.

For the first joint PNS attack, when $v = 0.1$, $\mu = 0.03$, we can get the diagram of k_2 and η, and show it in Figure 5.

Here we also discuss the joint PNS attack in four-state SQKD, and the two joint PNS attack methods mentioned above are also applicable to four-state SQKD and other Measure and Resend SQKD. Because both the forward channel and reverse channel of four-state SQKD can leak information, Eve can get more information when implementing joint PNS attack on four-state SQKD compared with single-state SQKD.

5 Conclusion

SQKD was proposed by scientists based on the consideration of reducing quantum resources, and it has shown that even though semi-quantum protocols are limited in their quantum capabilities, they hold similar security properties to that of fully quantum protocols, at least in ideal qubit channels. However, it is not clear whether SQKD has an advantage in practical application scenarios. With the continuous improvement of SQKD experimental implementation, we can gradually clarify the application potential and application value of SQKD in real scenes.

Of course, SQKD also faces the multiphoton problem due to the limitation of experimental conditions. We are the first to consider the multiphoton problem in a single-state SQKD system. Through analysis, we find that the single-state SQKD system can overcome the PNS attack in a one-way channel by making the average photon number of the pulse distribution different. Even so, the SQKD of the actual system is also not secure. We propose two models of joint PNS attack, through which Eve can take away information without being detected.

As a reminder, in the second joint PNS attack, we only blocked off the distinguishable two-photon signal, and we can also block out three photons and even block all distinguishable multiphotons. The probability of blocking off $\boldsymbol{k_m}$ can be calculated by Eq. 28. However the Sift-1 pulse is used to form the final key, so to obtain more information, we want to block pulses of Sift-1 as little as possible. As mentioned in the second method, Eve can distinguish Sift-1 operated photons by observing the number of photons. This ability, combined with other attacks, may cause more trouble to the security of SQKD.

In this study, we do not consider this type of PNS which can preserve the Poisson photon number distribution of the combination of the signal source and the lossy channel. We will address this issue in future work.

Data availability statement

The original contributions presented in the study are included in the article and in the Supplementary Material. Further inquiries can be directed to the corresponding author.

Author contributions

SM: conceptualization, methodology, investigation, formal analysis, writing—original draft; SD: resources, supervision; QH: resources, supervision; JW: conceptualization, funding acquisition, resources, supervision, writing–review and editing resources, supervision; YY: resources, supervision; ZW: resources, supervision; ZZ: resources, supervision.

Funding

National Science Foundation of China (62071186, 61771205); National Science Foundation of Guangdong Province (2015A030313388).

Acknowledgments

The authors thank the Guangdong Provincial Key Laboratory of Quantum Engineering and Quantum Materials for provision of experimental platform.

Conflict of interest

The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Publisher's note

All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors, and the reviewers. Any product that may be evaluated in this article, or claim that may be made by its manufacturer, is not guaranteed or endorsed by the publisher.

References

1. Bennett CH, Brassard G. Quantum cryptography: Public key distribution and coin tossing. *Quan Phys* (2020) 560:7–11. doi:10.48550/arXiv.2003.06557

2. Bennett CH. Quantum cryptography using any two nonorthogonal states. *Phys Rev Lett* (1992) 68:683121–4. doi:10.1103/PhysRevLett.68.3121

3. Bruß D. Optimal eavesdropping in quantum cryptography with six states. *Phys Rev Lett* (1998) 8114:3018–21. doi:10.1103/PhysRevLett.81.3018

4. Buzek V, Hillery M. Quantum copying: Beyond the no-cloning theorem. *Phys Rev A (Coll Park)* (1996) 546:1844–52. doi:10.1103/physreva.54.1844

5. Chen Y-P, Liu J-Y, Sun M-S, Zhou X-X, Zhang C-H, Li J, et al. Experimental measurement-device-independent quantum key distribution with the double-scanning method. *Opt Lett* (2021) 4615:3729–32. doi:10.1364/ol.431061

6. Liu J-Y, Ding H-J, Zhang C-M, Xie S-P, Wang Q. Practical phase-modulation stabilization in quantum key distribution via machine learning. *Phys Rev Appl* (2019) 121:014059. doi:10.1103/PhysRevApplied.12.014059

7. Zhou X-Y, Zhang C-H, Zhang C-M, Wang Q. Asymmetric sending or not sending twin-field quantum key distribution in practice. *Phys Rev A (Coll Park)* (2019) 996:062316. doi:10.1103/PhysRevA.99.062316

8. Hillery M, Bužek V, Berthiaume A. Quantum secret sharing. *Phys Rev A (Coll Park)* (1999) 593:1829–34. doi:10.1103/PhysRevA.59.1829

9. Deng FG, Zhou HY, Long GL. Circular quantum secret sharing. *J Phys A: Math Gen* (2006) 3945:14089–99. doi:10.1088/0305-4470/39/45/018

10. Wei KJ, Ma HQ, Yang JH. Experimental circular quantum secret sharing over telecom fiber network. *Opt Express* (2013) 2114:16663–9. doi:10.1364/OE.21.016663

11. Long GL, Liu XS. Theoretically efficient high-capacity quantum-key-distribution scheme. *Phys Rev A (Coll Park)* (2002) 653:032302. doi:10.1103/PhysRevA.65.032302

12. Zhang W, Ding DS, Sheng YB, Zhou L, Shi BS, Guo GC. Quantum secure direct communication with quantum memory. *Phys Rev Lett* (2017) 11822:220501. doi:10.1103/PhysRevLett.118.220501

13. Zhu F, Zhang W, Sheng YB, Huang YD. Experimental long-distance quantum secure direct communication. *Sci Bull* (2017) 6222:1519–24. doi:10.1016/j.scib.2017.10.023

14. Bennett CH, Brassard G, Crepeau C, Jozsa R, Peres A, Wootters WK. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. *Phys Rev Lett* (1993) 7013:1895–9. doi:10.1103/PhysRevLett.70.1895

15. Bouwmeester D, Pan JW, Mattle K, Eibl M, Weinfurter H, Zeilinger A. Experimental quantum teleportation. *Nature* (1997) 3906660:575–9. doi:10.1038/37539

16. Furusawa A, Sorensen JL, Braunstein SL, Fuchs CA, Kimble HJ, Polzik ES. Unconditional quantum teleportation. *Science* (1998) 2825389:706–9. doi:10.1126/science.282.5389.706

17. Bennett CH, Wiesner SJ. Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states. *Phys Rev Lett* (1992) 6920:2881–4. doi:10.1103/PhysRevLett.69.2881

18. Mattle K, Weinfurter H, Kwiat PG, Zeilinger A. Dense coding in experimental quantum communication. *Phys Rev Lett* (1996) 7625:4656–9. doi:10.1103/PhysRevLett.76.4656

19. Chen Y, Liu S, Lou Y, Jing J. Orbital angular momentum multiplexed quantum dense coding. *Phys Rev Lett* (2021) 1279:093601. doi:10.1103/PhysRevLett.127.093601

20. Zhang C-H, Zhou X-Y, Ding H-J, Zhang C-M, Guo G-C, Wang QJ. Proof-of-principle demonstration of passive decoy-state quantum digital signatures over 200 km. *Phys Rev Appl* (2018) 103:034033. doi:10.1103/physrevapplied.10.034033

21. Ranu SK, Prabhakar A, Mandayam P. Differential phase encoded measurement-device-independent quantum key distribution. *Quan Inf Process* (2021) 202:67–37. doi:10.1007/s11128-021-03006-2

22. Tang GZ, Li CY, Wang MJ. Polarization discriminated time-bin phase-encoding measurement-device-independent quantum key distribution. *Quan Eng* (2021) 34:e79. doi:10.1002/que2.79

23. Zeng P, Zhou H, Wu W, Ma X. Quantum key distribution surpassing the repeaterless rate-transmittance bound without global phase locking. *Quan Physice*(2022) 2201:04300. doi:10.48550/arXiv.2201.04300

24. Boyer M, Kenigsberg D, Mor T. Quantum key distribution with classical Bob. *Phys Rev Lett* (2007) 99:99140501. doi:10.1103/PhysRevLett.99.140501

25. Li Q, Chan WH, Long DY. Semiquantum secret sharing using entangled states. *Phys Rev A (Coll Park)* (2010) 822:022303. doi:10.1103/PhysRevA.82.022303

26. Wang J, Zhang S, Zhang Q, Tang CJ. Semiquantum secret sharing using two-particle entangled state. *Int J Quan Inform* (2012) 105:1250050. doi:10.1142/S0219749912500505

27. Zou XF, Qiu DW. Three-step semiquantum secure direct communication protocol. *Sci China Phys Mech Astron* (2014) 579:1696–702. doi:10.1007/s11433-014-5542-x

28. Zhang MH, Li HF, Xia ZQ, Feng XY, Peng JY. Semiquantum secure direct communication using EPR pairs. *Quan Inf Process* (2017) 165:117–4. doi:10.1007/s11128-017-1573-3

29. Li-Hua G, Zhen-Yong C, Liang-Chao X, Nan-Run Z. *Bi-Directional semi-quantum secure direct communication protocol based on high-dimensional single-particle states* (2022). doi:10.7498/aps.71.20211702

30. Xia C, Li H, Hu J. Semi-quantum digital signature protocol based on Einstein–Podolsky–Rosen steering. *J Phys A: Math Theor* (2022) 5532:325302. doi:10.1088/1751-8121/ac7f6d

31. Thapliyal K, Sharma RD, Pathak A. Orthogonal-state-based and semi-quantum protocols for quantum private comparison in noisy environment. *Int J Quan Inform* (2018) 165:1850047. doi:10.1142/S0219749918500478

32. Zhou NR, Xu QD, Du NS, Gong LH. Semi-quantum private comparison protocol of size relation with d-dimensional Bell states. *Quan Inf Process* (2021) 203: 124–15. doi:10.1007/s11128-021-03056-6

33. Luo Q-b., Li X-y., Yang G-w., Lin C. A mediated semi-quantum protocol for millionaire problem based on high-dimensional Bell states. *Quan Inf Process* (2022) 217:257–15. doi:10.1007/s11128-022-03590-x

34. Tian Y, Li J, Ye C, Chen X-B, Li C. W-state-based semi-quantum private comparison. *Int J Theor Phys (Dordr)* (2022) 612:18–6. doi:10.1007/s10773-022-05005-0

35. Tang Y-H, Jia H-Y, Wu X, Chen H-M, Zhang Y-M. Robust semi-quantum private comparison protocols against collective noises with decoherence-free states. *Quan Inf Process* (2022) 213:97–24. doi:10.1007/s11128-022-03444-6

36. Xu T-J, Chen Y, Geng M-J, Ye T-Y. Single-state multi-party semiquantum key agreement protocol based on multi-particle GHZ entangled states. *Quan Inf Process* (2022) 217:266–18. doi:10.1007/s11128-022-03615-5

37. Lili Y, Shibin Z, Yan C, Zhiwei S, Xiangmei L. Mutual weak quantum users key agreement protocol based on semi-honest quantum server. *Int J Theor Phys (Dordr)* (2022) 617:198–11. doi:10.1007/s10773-022-05161-3

38. Boyer M, Gelles R, Kenigsberg D, Mor T. Semiquantum key distribution. *Phys Rev A (Coll Park)* (2009) 793:032341. doi:10.1103/PhysRevA.79.032341

39. Zou XF, Qiu DW, Li LZ, Wu LH, Li LJ. Semiquantum-key distribution using less than four quantum states. *Phys Rev A (Coll Park)* (2009) 795:052312. doi:10.1103/PhysRevA.79.052312

40. Krawec WO. Restricted attacks on semi-quantum key distribution protocols. *Quan Inf Process* (2014) 1311:2417–36. doi:10.1007/s11128-014-0802-2

41. Boyer M, Katz M, Liss R, Mor T. Experimentally feasible protocol for semiquantum key distribution. *Phys Rev A (Coll Park)* (2017) 966:062335. doi:10.1103/PhysRevA.96.062335

42. Liu W, Zhou H. A new semi-quantum key distribution protocol with high efficiency. In: Proceeding of the 2018 IEEE 3rd Advanced Information Technology, Electronic and Automation Control Conference (IAEAC); October 2018; Chongqing, China. IEEE (2018). p. 2424–7. doi:10.1109/IAEAC.2018.8577673

43. Wang MM, Gong LM, Shao LH. Efficient semiquantum key distribution without entanglement. *Quan Inf Process* (2019) 189:260–10. doi:10.1007/s11128-019-2378-3

44. Yu KF, Yang CW, Liao CH, Hwang T. Authenticated semi-quantum key distribution protocol using Bell states. *Quan Inf Process* (2014) 136:1457–65. doi:10.1007/s11128-014-0740-z

45. Li CM, Yu KF, Kao SH, Hwang T. Authenticated semi-quantum key distributions without classical channel. *Quan Inf Process* (2016) 157:2881–93. doi:10.1007/s11128-016-1307-y

46. Meslouhi A, Hassouni Y. Cryptanalysis on authenticated semi-quantum key distribution protocol using Bell states. *Quan Inf Process* (2017) 161:18–7. doi:10.1007/s11128-016-1468-8

47. Wang H-W, Tsai C-W, Lin J, Yang C-W. Authenticated semi-quantum key distribution protocol based on W states. *sensors* (2022) 2213:4998. doi:10.3390/s22134998

48. Vlachou C, Krawec W, Mateus P, Paunkovic N, Souto A. Quantum key distribution with quantum walks. *Quan Inf Process* (2018) 1711:288–37. doi:10.1007/s11128-018-2055-y

49. Iqbal H, Krawec WOJa.QP. *High-dimensional semi-quantum cryptography* (2019).

50. Sun ZW, Du RG, Long DY. Quantum key distribution with limited classical Bob. *Int J Quan Inform* (2013) 111:1350005. doi:10.1142/S0219749913500056

51. Miyadera T. Relation between information and disturbance in quantum key distribution protocol with classical Alice. *Int J Quan Inform* (2011) 96:1427–35. doi:10.1142/S0219749911008118

52. Krawec WO. Key-rate bound of a semi-quantum protocol using an entropic uncertainty relation. In: Proceeding of the 2018 IEEE International Symposium on Information Theory (ISIT); June 2018; Vail, CO, USA. IEEE (2018). p. 2669–73.

53. Krawec WO. Security proof of a semi-quantum key distribution protocol. In: Proceeding of the 2015 IEEE International Symposium on Information Theory (ISIT); June 2015; Hong Kong, China. IEEE (2015). p. 686–90. doi:10.1109/ISIT.2015.7282542

54. Krawec WO. Quantum key distribution with mismatched measurements over arbitrary channels. *Quan Phys* (2016) 17:209–241. doi:10.48550/arXiv.1608.07728

55. Hajji H, El Baz M. Mutually unbiased bases in 3 and 4 dimensions semi-quantum key distribution protocol. *Phys Lett A* (2022) 426:127884. doi:10.1016/j.physleta.2021.127884

56. Han SY, Huang YT, Mi S, Qin XJ, Wang JD, Yu YF, et al. Proof-of-principle demonstration of semi-quantum key distribution based on the Mirror protocol. *EPJ Quan Technol* (2021) 81:28–10. doi:10.1140/epjqt/s40507-021-00117-8

57. Brassard G, Lutkenhaus N, Mor T, Sanders BC. Limitations on practical quantum cryptography. *Phys Rev Lett* (2000) 856:1330–3. doi:10.1103/PhysRevLett.85.1330

58. Lütkenhaus N, Jahma M. Quantum key distribution with realistic states: Photon-number statistics in the photon-number splitting attack. *New J Phys* (2002) 41:344. doi:10.1088/1367-2630/4/1/344

59. Lütkenhaus N. Security against individual attacks for realistic quantum key distribution. *Phys Rev A (Coll Park)* (2000) 615:052304. doi:10.1103/PhysRevA.61.052304

60. Gurevish P. *Experimental quantum key distribution with classical Alice*. Mastersthesis (2013). doi:10.3390/e20070536

61. Chen L-Y, Gong L-H, Zhou N-R. Two semi-quantum key distribution protocols with G-like states. *Int J Theor Phys (Dordr)* (2020) 596:1884–96. doi:10.1007/s10773-020-04456-7

62. Ye T-Y, Li H-K, Hu J-L. Semi-quantum key distribution with single photons in both polarization and spatial-mode degrees of freedom. *Int J Theor Phys (Dordr)* (2020) 599:2807–15. doi:10.1007/s10773-020-04540-y

63. Zhou Y-H, Qin S-F, Shi W-M, Yang Y-G. Measurement-device-independent continuous variable semi-quantum key distribution protocol. *Quan Inf Process* (2022) 218:303–21. doi:10.1007/s11128-022-03626-2

64. Guskind J, Krawec WO. Mediated semi-quantum key distribution with improved efficiency. *Quan Sci Technol* (2022) 73:035019. doi:10.1088/2058-9565/ac7412

65. Iqbal H, Krawec WO. Semi-quantum cryptography. *Quan Inf Process* (2020) 193:97–52. doi:10.1007/s11128-020-2595-9

TYPE Original Research
PUBLISHED 11 November 2022
DOI 10.3389/fphy.2022.1042806

Check for updates

OPEN ACCESS

EDITED BY
Tianyu Ye,
Zhejiang Gongshang University, China

REVIEWED BY
Tingting Song,
Jinan University, China
Mahmoud Abdel-Aty,
Sohag University, Egypt

*CORRESPONDENCE
Yumin Dong,
dym@cqnu.edu.cn

SPECIALTY SECTION
This article was submitted to Quantum Engineering and Technology, a section of the journal Frontiers in Physics

RECEIVED 13 September 2022
ACCEPTED 04 October 2022
PUBLISHED 11 November 2022

CITATION
Dong Y, Xu Q, Fu Y, Jia F and Nian Z (2022), An improved quantum artificial fish swarm algorithm for resource allocation in multi-user system.
Front. Phys. 10:1042806.
doi: 10.3389/fphy.2022.1042806

An improved quantum artificial fish swarm algorithm for resource allocation in multi-user system

Yumin Dong[1]*, Qian Xu[1], Yanying Fu[1], Fanghua Jia[2] and Zheng Nian[3]

[1]College of Computer and Information Science, Chongqing Normal University, Chongqing, China, [2]School of Information and Control Engineering, Qingdao University of Technology, Qingdao, Shandong, China, [3]School of Big Data and Computer Science, Chongqing College of Mobile Communication, Chongqing, China

Through in-depth research and application, it is found that with the increasing number of artificial fish, the required storage space is also increasing, which finally leads to the increasing difficulty of calculation, and the ability to obtain accurate solutions is seriously insufficient, and only satisfactory solution domains can be obtained for the system. Since the development of multi-user systems, there are still some problems in resource allocation, such as poor user fairness, low system throughput, and low system security. In view of the appeal problem, we can design a multi-user system resource allocation scheme based on quantum artificial fish swarm algorithm. Firstly, it is necessary to analyze the working principle of resource allocation in multi-user system, and establish a mathematical model according to its working principle; Furthermore, through the research and in-depth research on the artificial fish swarm algorithm, we integrate the quantum phase concept fish artificial fish swarm algorithm, introduce quantum evolutionary algorithm into the algorithm, and use quantum phase to code and improve it; Then, through simulation experiments, we compare other types of resource allocation schemes in the market, and process and analyze the experimental results; Finally, according to the experimental data, the conclusion is drawn that the improved quantum artificial fish school algorithm can accurately and quickly obtain the optimal allocation scheme, and to a certain extent, ensure user fairness, improve the communication ability of the multi-user system. Compared with other multi-user system resource allocation schemes, its overall performance is also more outstanding.

KEYWORDS

quantity resource allocation method, multi user system, user fairness, quantum artificial fish swarm algorithm, system capacity

1 Wireless network communication system

1.1 Resource allocation in wireless communication

In a wireless network, it is possible to allocate and schedule the resources which are available for allocation and scheduling, such as the transmission rate, the time slot, and the antenna. The wireless resource allocation problem is how to optimize the preset parameters and maximize the resource utilization efficiency by allocating wireless resources reasonably in terms of physical conditions and QOL requirements [1]. Mathematically, this is an optimization problem. Therefore, we have to build a model for the wireless communication system [2], write restrictions on the wireless resources, and make the optimized targets based on the demand of the users. Based on the above results, we can find an appropriate resource distribution approach to optimize the resource utilization of wireless systems [3, 7].

Resource allocation involves wireless channel, multi-user diversity, user quality of service and fairness among users [8]. Among them, wireless channel has its fading phenomenon: due to the small-scale effects of multi-path fading, as well as the large-scale effects such as path loss due to distance attenuation and noise caused by obstacles, the channel has time-varying properties. It is very challenging to combat fading and interference in wireless communication [9]; The root of multi-user diversity is the independence of user channels, which is manifested in three aspects: time, frequency and space. Through effective channel allocation and multi-user scheduling, this potential gain can be used to effectively improve the system transmission efficiency; To optimize the resource allocation strategy is to improve the service quality of users; Because the resources are limited, it is impossible to fully meet the needs of users, which requires effective division of network resources and fair allocation of resources to users in the network.

1.2 Resource allocation principle of wireless network communication system

The multi-user system adopts the multi carrier modulation technology, which divides the channel into multiple orthogonal sub channels, decomposes the high-speed serial data stream into several low-speed parallel sub data blocks, transmits on multiple mutually orthogonal sub channels at the same time, and performs narrowband modulation on each sub channel. This operation reduces the mutual interference of the sub channel time, and improves the spectrum utilization. The bandwidth of the signal on each sub-channel is less than the correlation bandwidth of the channel, so the frequency selective fading on each sub-channel is flat, effectively eliminating the inter-symbol interference. In order to further improve the spectral efficiency of multi-user systems, we can obtain stronger performance in asymmetric services, and we can introduce adaptive resource allocation. The principle of adaptive resource allocation is to obtain the diversity of the system in each domain through the adaptation of bandwidth, power and rate. The main reasons for diversity [1, 10] are channel time variation, frequency selective fading, channel fading independence between multi-users, parallel sub-channels between space and frequency domain, and randomness of signal arrival. Link adaptation is the application of diversity. Its basic idea is to adaptively select the modulation order, coding method, transmission power of sub carriers, *etc.* according to the channel conditions of the system. The ultimate purpose of link adaptation is to improve the spectral efficiency and reliability of the system.

Three elements of mobile communication system operation: resources and resource allocation, network architecture, and information interaction. The quality of communication services often depends on the amount of allocable resources, the efficiency of resource allocation, the quality of network architecture, and the effect of information interaction. Radio resource allocation Objective: to ensure various QoS requirements of users, ensure fairness of users, and improve resource utilization efficiency of the system. The wireless network communication system uses orthogonal frequency division multiplexing technology for data communication and processing. Because the relationship between sub-channels is called positive correlation, its channels can be divided into multiple sub-channels, and each sub-channel will not interfere with each other Khan et al. [11]. Each sub-channel uses a separate and independent sub-carrier for modulation communication to achieve parallel communicatio [12]. The resource allocation principle of the wireless network communication system is shown in Figure 1, where: *FFT* means fast Fourier transform; *IFFT* represents inverse fast Fourier transform.

With the deepening of research, the problems that need to be solved by wireless resource allocation algorithms become diverse, and the strategies and methods adopted are also different. According to different standards, the algorithm classification of wireless communication network system allocation is shown in the following Figure 2:

1.3 Mathematical model of multi-purpose resource allocation in wireless network communication system

When building a mathematical model of resource allocation, It is essential to know what components are required in order to build a complete wireless communication system. In a wireless network communication system, n subcarriers exist for k users. Every user is aware of the state of the channel in the system. A subcontractor may also be assigned only to one user at a given time [13]. Then, the power assigned to the n sub carrier by the k user is Pk,n and then there is the equation for calculating the k-user's power on the n sub channel:

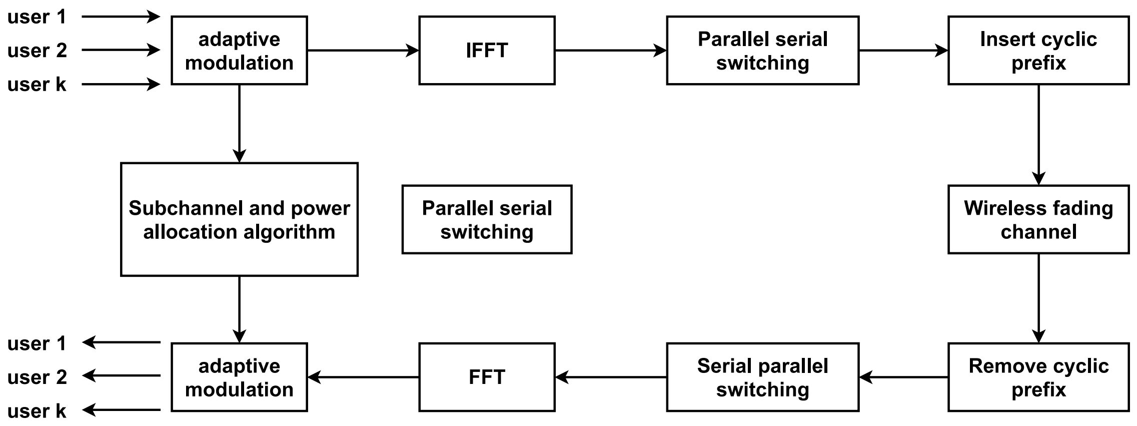


FIGURE 1
Resource allocation principle of wireless network communication system.

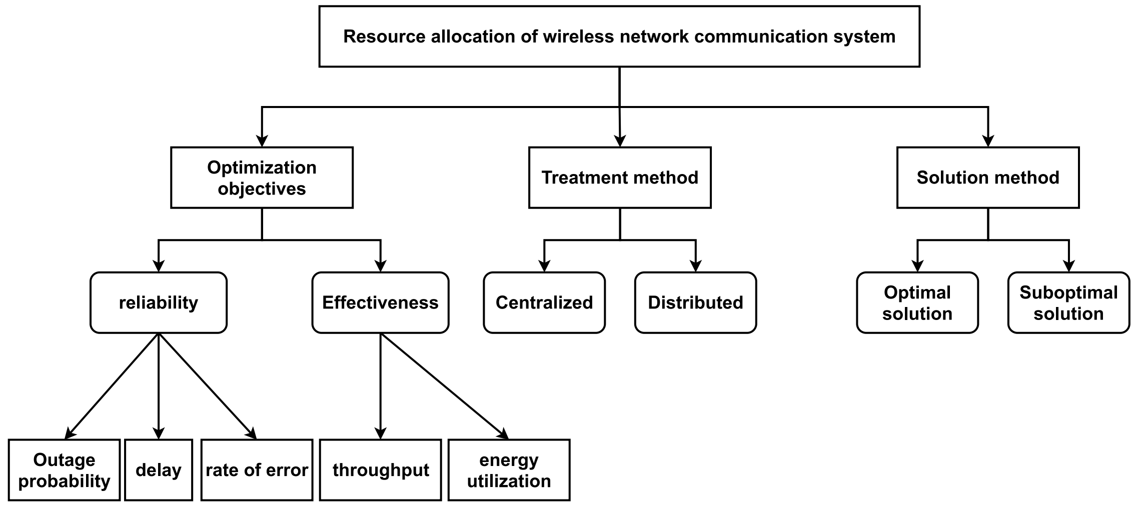


FIGURE 2
Classification of wireless network communication resource allocation.

$$\gamma_{k,n} = \log_2\left(1 + p_{k,n}\cdot\frac{H_{k,n}}{\Gamma}\right) \tag{1}$$

$H_{k,n}$, n is the signal to noise ratio in the nth subcarrier, $\Gamma = -Ln\ (4\ BER)*1.4$.

Reasonable allocation of sub-carriers [14] and power is the multi-user resource allocation goal of the wireless network communication system. To maximize the throughput of the wireless network communication system, the sub-carrier allocation index coefficient is defined as follows:

$$C_{k,n} = \begin{cases} 1, \text{ Subcarrier allocation to user } k \\ 0, \text{ Subcarrier are not allocated to user} \end{cases} \tag{2}$$

The multi-user resource allocation mathematical model of wireless network communication system is:

$$\begin{cases} \max\limits_{C_{k,n}P_{k,n}} \dfrac{B}{N} \sum\limits_{k=1}^{K} \sum\limits_{n=1}^{N} \sum_{n=1}^{N} c_{k,n} \log_2\left(1 + P_{k,n} \cdot \dfrac{H_{k,n}}{\Gamma}\right), \\ C_1\colon\ C_{k,n} \in \{0,1\}, \forall k, n, \\ C_2\colon\ \sum\limits_{k=1}^{K} C_{k,n} = 1, \forall n, \\ C_3\colon\ p_{k,n} \geq 0, \forall k, n, \\ C_4\colon\ \sum_{k=1}^{k} \sum_{n=1}^{N} C_{k,n} Pk, n \\ C_5\colon\ R_i\colon\ R_j = \varphi_i\colon\ \varphi_j; \forall i, j \in \{1, 2, \ldots, k\} \end{cases} \tag{3}$$

In the above equation: C_1 is whether the sub-carrier is allocated or not; C_2 is a sub-carrier, which can only be assigned to a unique user; C_3 denotes that the power must be positiv; C_4 indicates that the sub-carrier power cannot be greater than the maximum power; φ_i represents the user scale constraint condition; P_{tot} is the maximum power; R_i represents the total transmission rate of the k user, and the calculation formula is:

$$R_k = \frac{B}{N}\sum_{n=1}^{N} C_{k,n} r_{k,n} \tag{4}$$

Where B in the formula is the bandwidth of fading channel.

2 Artificial fish swarm algorithm

2.1 Standard artificial fish swarm algorithm

The artificial fish swarm algorithm mainly shows the activity of artificial fish in the environment by simulating the four behaviors of fish-foraging behavior, crowding behavior, tail chasing behavior and random behavior. The basic activities of artificial fish are described as follows [15]:

1) Feeding behavior: Generally, fish swim freely and randomly in the water. When they find food, they will swim quickly in the direction of gradually increasing food.
2) Crowding behavior: In order to ensure their survival and avoid hazards, fish will naturally gather in groups during swimming. There are three rules for fish to follow when gathering: separation rules: try to avoid overcrowding with nearby partners; Alignment rules: try to be consistent with the average direction of neighboring partners; Cohesion rule: try to move towards the center of nearby partners.
3) Chasing behavior: When one or several fish in the school find food, their nearby partners will follow them to the food point quickly.
4) Random behavior: Individual fish usually swim randomly in the water, which is to find food points or partners in a wider range.

In this paper, a new method based on PSO is proposed in this paper, which is based on PSO, and it is used in the resource allocation. When the artificial fish in the school find food, the fish in the school can continuously adjust their location, focus on the food, and finish the location update [16]. By using this approach, we can deal with the quantity and priority of the distribution of user resources. The algorithm is made up of a parameter system and a perceptual system. The state of the artificial fish can be represented by the vector $x = (x_1, x_2, \ldots, x_n)$, in which $I = (1, 2, \ldots, n)$ is to be optimized [17], and the amount of food at the present location of the artificial fish is represented by $y = f(x)$, with y being an objective function;

The distance between artificial fish individuals is expressed as $d_{i,j} = \|x_i - x_j\|$; In its perception system, the perception of artificial fish is realized by vision [18]. Through this method, the number and priority of user resource allocation can be well handled, The change of the position of the $\Delta x_i\,(t+1)$ data list at $t+1$ and t is, $x_i(t)$ represents the spatial position of the i fish, then:

$$\Delta x_i = Rand\,()*Step*[x_i\,(t+1) - x_i\,(t)] \tag{5}$$

Where $Rand()$ is random data, and $Step$ is the step of fish school position update operation.

Given that the current spatial coordinate of the i-fish is x_i, the expression of the spatial coordinate x_j obtained by the random movement of the fish is:

$$x_i\,(t+1) = x_i\,(t) + \Delta\,(t+1) \tag{6}$$

$$x_j = x_i + Visual*Rand\,() \tag{7}$$

Where $Visual$ is the visual field range value of artificial fish.

Let the food concentration in the spatial coordinates be a function of $f(x)$, the food coordinate concentration be $F_{\max}$, the food concentration at x_i be $f\,(x_i)$, and the food concentration at the center point x_c of the fish school be $f\,(x_c)$. Within the range of fish movement, according to the position x_j randomly assigned by $Rand()$, if the fish group has not found the food point, it will continue to search for food according to Eq. 6.

$$x_{t+1i} = x_{ti} + x_j - x_{ti}\|x_j - x_{ti}\|*Step*Rand\,() \tag{8}$$

The current position of the i fish is X_i. According to the maximum value of $f(x)$ within the visual range of the fish, it is determined whether the position of the food is within the visual range of the fish. If the current position x_o is within the visual range of the fish, there is Eq. 9:

$$x_{t+1i} = x_{ti} + x_o - x_{ti}\|x_o - x_{ti}\|*Step*Rand\,() \tag{9}$$

The current position of the i fish is x_i. According to the maximum value of $f(x)$ in the visual range, it is determined whether there are multiple food points in the visual range of the current fish. If multiple food points are visible in the current position $x's$ max, the fish position is updated as follows:

$$\mathrm{x}_{t+1i} = x_{ti} + x_{max} - x_{ti}\|x_{max} - x_{ti}\|*Step*Rand\,() \tag{10}$$

If $|f\,(x_c - f_{\max})|$ reach a parameter originally designed, the operation is terminated.

The above equation theory relates to the four kinds of fish groups in the AI: foraging, cluster, tail, and stochastic. These four behaviors will transform each other at different times, and this transformation is usually realized by fish from the main through their perception of the environment. All these behaviors have close relationship with the feeding and survival of the fish, and also have close relationship with solving the optimal problem.

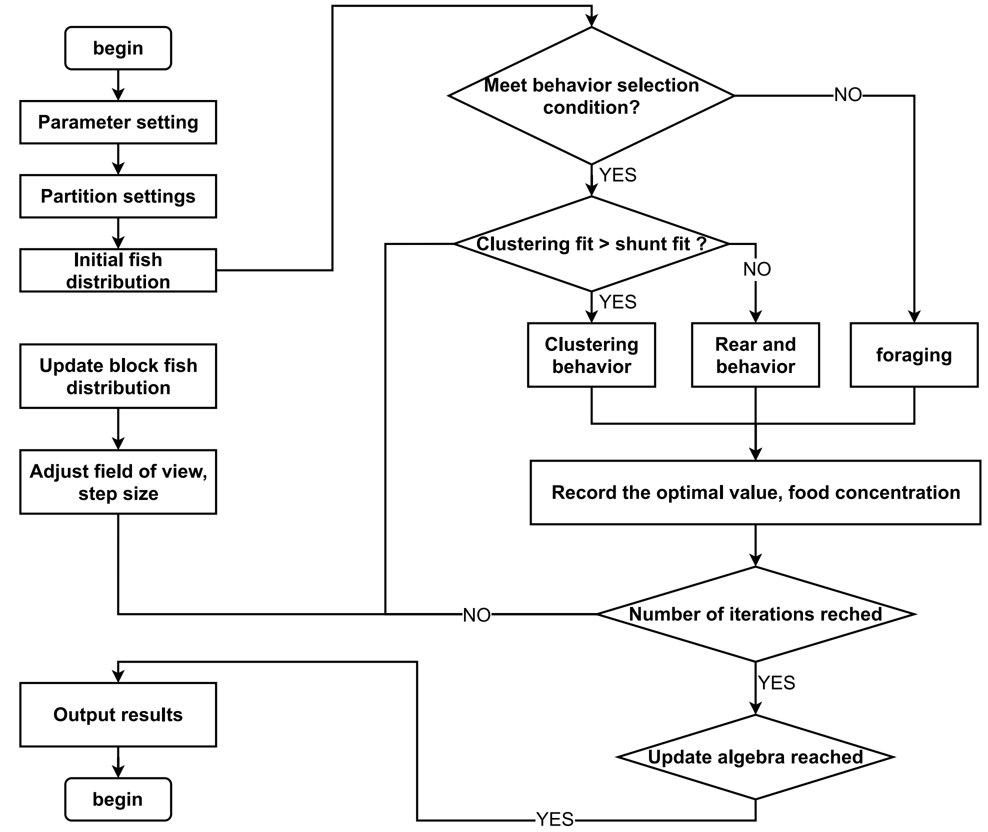

begin
Parameter setting
Partition settings
Initial fish distribution
Update block fish distribution
Adjust field of view, step size
Output results
begin
Meet behavior selection condition?
NO
YES
Clustering fit > shunt fit ?
NO
YES
Clustering behavior
Rear and behavior
foraging
Record the optimal value, food concentration
Number of iterations reched
NO
YES
Update algebra reached
YES

FIGURE 3
Flow chart of artificial fish swarm algorithm.

2.2 Steps and flow chart of artificial fish swarm algorithm

The basic principle of the AI is that in the water zone, the most fish population is the one with the most nutrients in the water. Based on this property, it can simulate the behavior of the fish group, including foraging, clustering, tail chasing, randomizing, and so on, so as to realize global optimization. In the optimization process, the artificial fish may choose a few local optimum solutions, which will cause the fish to jump out of the local optimal solution, and then influence the overall optimization. Therefore, it is important to pay attention to the number of repeats in the foraging process, and to select a suitable random step, and to restrict the size of the clustering and the behavior of clustering. In order to use the AI, we first need to assign values to different types of discards, which include the population size n, the starting location of each man-made fish, the visual field of the artificial fish, the step size, the crowding factor δ, and the repetition times the trial number; The second is to calculate the fitness of the individual at the beginning of the fish colony, choose the best condition of the fish, and send the value to the bulletinship; In the course of the implementation, every person must be assessed, and the actions to be executed are chosen carefully, such as foraging prayer, swarm, tail chase, and random behavioral behavior. Then, after the artificial fish makes a choice, it will choose its location to create a new group of fish. Moreover, if the algorithm scores all the different actions, the notice board will be updated to that person; At the end, if the optimum solution on the bulletin board reaches the satisfactory error border or reaches the upper limit of the prescribed number of iterations, the algorithm terminates; otherwise, an individual assessment is made, and an appeal is executed. The detailed flow chart is shown in Figure 3.

2.3 Quantization of artificial fish swarm algorithm

A kind of quantum particle swarm optimization algorithm [19] based on the truncated mean stabilization strategy has improved the search performance of the algorithm to a certain extent, and has also improved the convergence efficiency to a certain extent. According to the salient points of its algorithm, the fish swarm algorithm studied in this study also uses its ideas on a certain basis, and has obtained good results in practical operation. In the process of quantum bit coding, fewer quantum bits are used to solve the problem of large data sets. The Born machine model [20] effectively solves this problem.

The quantizing of artificial fish is represented by the quantum phase coding, and the location of the artificial fish can be expressed more efficiently by quantum operations [21].

$$|\varphi\rangle \geq \alpha|0\rangle + \beta|1\rangle \tag{11}$$

In the above equations, they all belong to complex numbers and exist at the same time $|\alpha|^2 + |\beta|^2 = 1$, $|\alpha|^2$ is the probability of quantum collapse to 0 state, $|\beta|^2$ is the probability of quantum collapse to 1 state. To make it easier to calculate the machine, the above equation is formed to get the corresponding matrix formula, that is:

$$|\varphi\rangle = [\alpha, \beta]^T \tag{12}$$

If the matrix U conforms to the relation of $U(U^*)T = I$, transform the above matrix to obtain:

$$U|\varphi\rangle = U(\alpha|0\rangle + \beta|1\rangle) \tag{13}$$

The position of the artificial fish is described by quantum bits, so that $\alpha = \cos(\theta)$, $\beta = \sin(\theta)$. Then Eq. 13 can be expressed as:

$$|\varphi\rangle = \cos(\theta)|0\rangle + \sin(\theta)|1\rangle = [\cos(\theta), \ \sin(\theta)]^T \tag{14}$$

According to Eq. 14, the spatial position of the artificial fish is effectively quantized and encoded in the following way:

$$P_i = \begin{bmatrix} \begin{vmatrix} \cos(\theta_{i1}) \\ \sin(\theta_{i1}) \end{vmatrix} & \begin{vmatrix} \cos(\theta_{i2}) \\ \sin(\theta_{i2}) \end{vmatrix} \cdots \\ \begin{vmatrix} \cos(\theta_{ij}) \\ \sin(\theta_{ij}) \end{vmatrix} & \begin{vmatrix} \cos(\theta_{im}) \\ \sin(\theta_{im}) \end{vmatrix} \end{bmatrix} \tag{15}$$

Of which $\theta_{i\,j} = 2\pi \cdot rand\,()$, $rand\,() \in (0, 1)$, $i \in \{1, 2, \ldots, n\}$, $\in \{1, 2, \ldots, m\}$, n represents artificial fish total quantity, M represents the dimension decomposition number of the location of an artificial fish school in the spatial coordinate system [22]. In order to describe the location of an artificial fish colony in a multidimensional spatial coordinate system, we can get a quantum representation of the location of an artificial fish colony by a combination of Eq. 16:

$$\begin{cases} P_{ic} = (\cos(\theta_{i1}), \cos(\theta_{i2}), \cdots \cos(\theta_{im})) \\ P_{is} = (\sin(\theta_{i1}), \sin(\theta_{i2}), \cdots \sin(\theta_{im})) \end{cases} \tag{16}$$

Decree θ is $[\alpha, \beta]$. For the phase of t relative to $|0\rangle = [1, 0]^T$, Eq. 16 is expressed in polar coordinates as follows:

$$\begin{cases} |\varphi\rangle = \cos(\theta) + i\sin(\theta) = e^{i\theta} = r(\theta) \\ \cos^2\theta = |\alpha|^2, \ \sin^2\theta = |\beta|^2 \end{cases} \tag{17}$$

θ meet $1 < \theta \leq 2\pi$. Compared with Eq. 11, the artificial fish coordinate position of Eq. 13 is only θ.

A mathematical description of the location update of the artificial fish is given. In combination with Eq. 7, the update method is as follows:

$$\begin{bmatrix} \cos\big(\theta_{ij}(t+1)\big) \\ \sin\big(\theta_{ij}(t+1)\big) \end{bmatrix} = \begin{bmatrix} \cos\big(\Delta\theta_{ij}(t+1)\big) - \sin\big(\Delta\theta_{ij}(t+1)\big) \\ \sin\big(\Delta\theta_{ij}(t+1)\big) - \cos\big(\Delta\theta_{ij}(t+1)\big) \end{bmatrix} \tag{18}$$

$$\begin{bmatrix} \cos\big(\theta_{ij}(t+1)\big) \\ \sin\big(\theta_{ij}(t+1)\big) \end{bmatrix} = \begin{bmatrix} \cos\big(\theta_{ij}(t) + \Delta\theta_{ij}(t+1)\big) \\ \sin\big(\theta_{ij}(t) + \Delta\theta_{ij}(t+1)\big) \end{bmatrix} \tag{19}$$

In the above equation, a and B are the quintile of the i artificial fish in the j dimension at t and $t + 1$, and C is the position change between t and $t + 1$.

In order to better solve the problem of fish school position update accuracy and prevent the problem of operation time caused by too large or [23], it is necessary to adopt the dynamic phase-shift update method. At the beginning of the iteration, the phase-shift update angle is large. As the number of iterations increases, the update angle gradually decreases. The phase-shift update method for the T iteration is:

$$\Delta\theta_{ij}(t+1) = 0.1\pi\left(1 - k\frac{t}{Iter}\right) \tag{20}$$

Represents a constant, and its value meets $K \in (0, 1)$ the requirements. *ITER* represents the maximum number of iterations.

3 System resource allocation policy process

Firstly, it analyses the process of resource allocation policy, and then proposes a multi-user system resource assignment strategy based on QSAR [24]. The workflow is illustrated in Figure 4: Firstly, the topology of the system is established, and then the mathematical model of the system is established. Secondly, the parameters of the AI are set up, including the effective search area size, δ, P_{fb}, θ step, and max iterate [25]. In the third step, the initialization of N man-made fish is randomly formed and assembled into an group, and the location of each of the artificial fish represents a multi-user resource assignment scheme of the radio network communication system [18]. In the fourth step, the artificial fish group is quantum encoded for the sub-layer, and the four behaviors of the AI are also quantum verified. In the seventh step, the four actions of the artificial fish are realized, so that each of the artificial fish is free to pursue, feed and cluster, and the optimum location is determined. In the eighth step, a random number is generated at random, and if $r < P_{fb}$ is met, a random search is performed; Otherwise, a

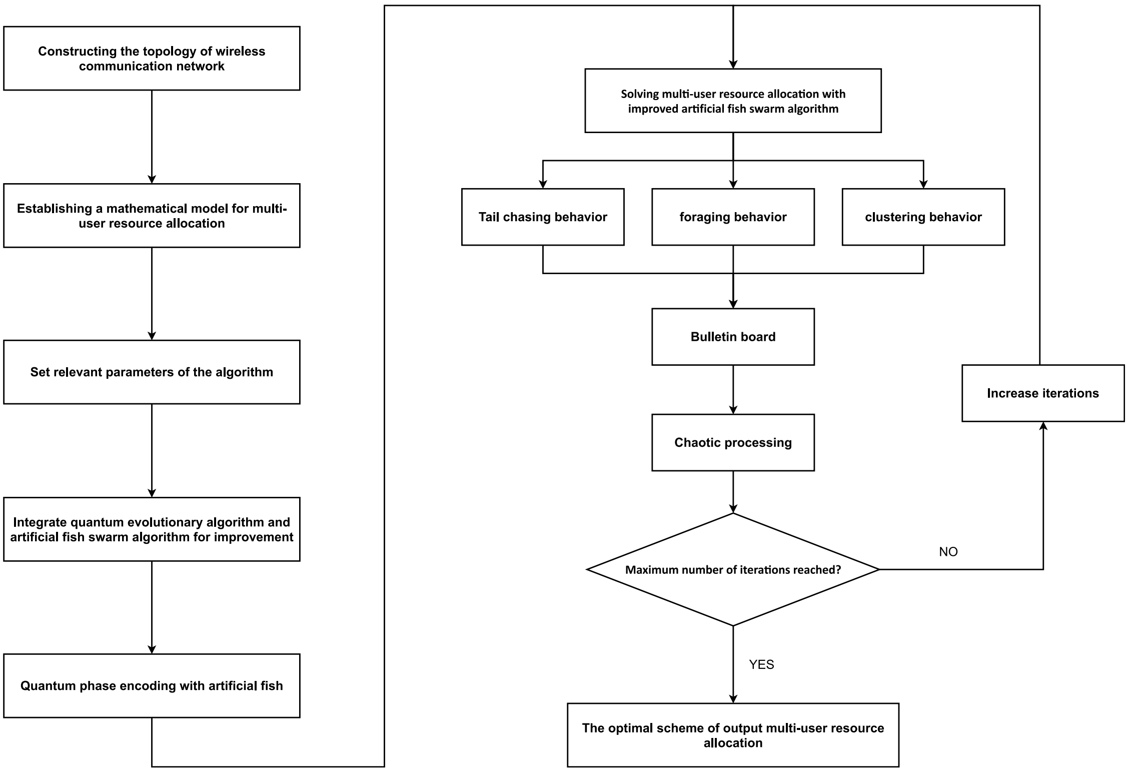

Constructing the topology of wireless communication network
Establishing a mathematical model for multi-user resource allocation
Set relevant parameters of the algorithm
Integrate quantum evolutionary algorithm and artificial fish swarm algorithm for improvement
Quantum phase encoding with artificial fish
Solving multi-user resource allocation with improved artificial fish swarm algorithm
Tail chasing behavior
foraging behavior
clustering behavior
Bulletin board
Increase iterations
Chaotic processing
Maximum number of iterations reached?
NO
YES
The optimal scheme of output multi-user resource allocation

FIGURE 4
Flow chart of artificial fish swarm algorithm.

TABLE 1 Test environment parameters of wireless network communication system.

Serial number	Project type and unit	Value
1	Total bandwidth/MHZ	10
2	Total transmit power/W	1
3	Number of users/prep	2 ~ 20
4	Update cycle of channel status information/ms	0.5
5	Channel average SNR/dB	40
6	Total number of sub-carriers	64
7	System bit error rate	10^{-3}
8	Channel fading model	Rayleigh model

feedback search is performed, and all fish move to the optimum location on the bulletin board; in the ninth step, the position of the currently optimum man-made fish is confused to locate the optimum location within the valid search zone. In the 10th step: save the current state of the best man-made fish on the notice board, and update the feedback search probability [24]; In the 11th step, the number of iterations is $iterate = iterate + 1$; Otherwise, go back to step 5 and proceed.

4 Testing of resource allocation strategy for multi-user system

4.1 Testing environment

In this paper, a comparison is made between the multi-user system resource allocation strategy and the multi-user system resource allocation strategy of GA, and the multi-user system resource allocation strategy. Table 1 shows the test

TABLE 2 Relevant parameters of quantum artificial fish swarm algorithm.

Serial number	Project type and unit	Value
1	Maximum number of iterations	100
2	Feedback search probability	0.5
3	Valid search area/m^2	100 × 100
4	Artificial fish Visual	20
5	Crowding degree of artificial fish	0.35
6	Attenuation factor of feedback probability	0.01
7	Move step/step	5

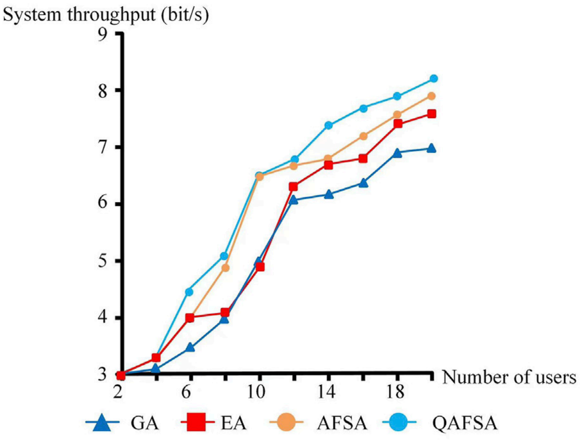


FIGURE 5
Throughput change curve of wireless network communication system.

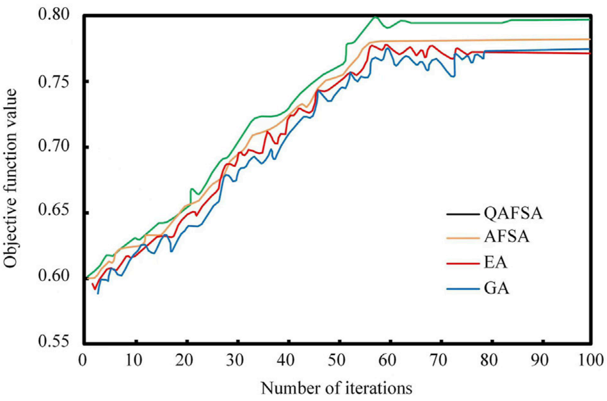


FIGURE 6
Convergence performance of multi-user system resource allocation strategy.

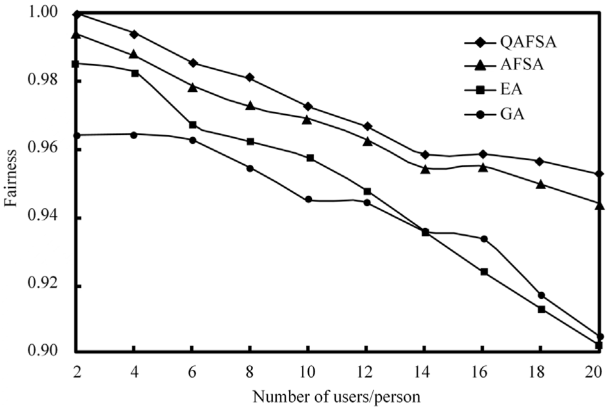


FIGURE 7
Fairness change curve of multi-user system resource allocation strategy.

environment parameters of the wireless network communication system, and the related parameters of the QSAR are given in Table 2.

4.2 Comparison and analysis of experimental data

For different numbers of users, the throughput change curve of wireless network communication system based on the multi-user system resource allocation strategy of quantum artificial fish swarm algorithm [26], in Figure 5, we can conclude from the data in Figure 5 that the amount of data which needs to be handled by the wireless network communication system also keeps increasing as the number of users increases. This is due to the fact that the data transfer rate of the wireless network communication system continues to increase as the amount of data processed by customers increases. The throughput of QRS is superior to that of artificial fish, GA, *etc.* This further demonstrates the superiority of QSAR in system throughput. The convergence curves of all the algorithms searching for multiuser system resources are shown in Figure 6. Compared with AI, GA, QSAR, etc, which makes it faster to solve the resource allocation scheme of multi-user system and increase the search accuracy of QGA.

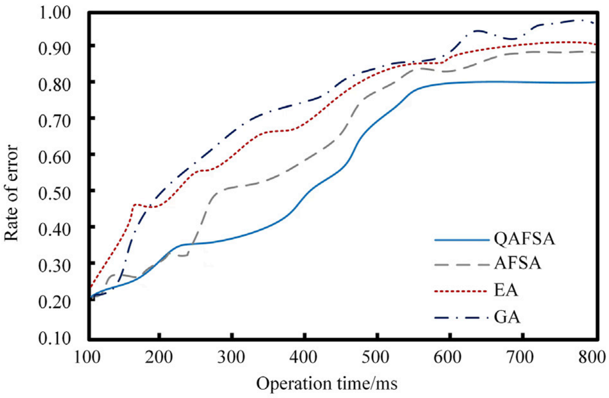


FIGURE 8
Fairness change curve of multi-user system resource allocation strategy.

In Figure 7, the fairness change curves of the distribution policies of multi-user systems are illustrated in Figure 7. The experimental data in Figure 7 show that the fairness of the wireless network communication system is reduced to varying degrees as the number of users continues to increase [27]. This is due to the fact that the average number of allocated subcarriers in the system is steadily declining as the number of users increases, which also makes it more difficult to achieve a fair distribution; However, it can be seen from the experimental data that QMI has less variation scope and better fairness than the others [13]. Compared with QSAR, the AI is less superior to QSAR in terms of fairness and the fairness of GA is the next. It also indicates that QPSO can resolve the conflict between throughput and equity, significantly increase the usage of MIMO system, satisfy the needs of users, and enhance the communication efficiency of the system.

It is well known that as time goes on, anything is going to be more and more apparent. In Figure 8, the QSAR, AI, GA, *etc.* As shown in Figure 8, the error rate of multi-user resource allocation continues to increase with time. As time passes, there will be some mistakes in the channel. Finally, the competition between the users gets stronger and stronger, which causes the error rate to evolve in an upward direction. It is shown that QSAR, AIS, GA will have different levels as time goes by, but QSAR is more slow than the other QSAR, GA. Based on the graph, the algorithm of the Quantum Artificial Fish Swarm is roughly equal to 0.8. The QSAR algorithm is not an optimal multiuser resource allocation algorithm, so it is necessary to study it further.

To sum up, aiming at the problems of poor user fairness and small system capacity of the current multi-user system resource allocation strategy, in this paper, we present a new strategy for multi-user system resource allocation based on QSAR. First, this paper analyses the working principle of the multi-user system resource distribution, builds up the mathematical model, and then carries on the quantizing and coding of the artificial fish Swarm algorithm to compute the resource distribution model. Based on the test results, we find that the multi-user system resource allocation strategy based on this approach is fairly fair, improves the throughput of the multi-user system, speeds up the data transmission speed, reduces the error rate of the multi-user system resource allocation, and is better than other multi-user system resource allocation strategies, it has broad application prospects.

5 Expectation

The arrival of the Internet era has accelerated a new round of social revolution. It has made people change a lot in society and changed human beings completely. With the progress of society and the constant updating of the times, the resource allocation strategy of multi-user system will develop in a better and better direction, and will play a vital role in the future computer field. In the future, the computer field will develop towards the goal of faster, higher and better. It is essential to pursue efficient data transmission. Therefore, the application of quantum is the trend of future development. Quantum will be applied to different computer technology research, and play a huge role in a small body. In order to solve the problem that the system is not fair and the system capacity is small, a new kind of multiuser resource allocation scheme is proposed in this paper. With the existence of this method, it has better fairness, improves the throughput of multi-user system, accelerates the data transmission speed, and has a good development prospect in the future. However, at present, scientists' research on quantum is not very in-depth, and the estimation of the role of quantum in the future is unknown. Therefore, in future research, it is hoped that more and more scholars can contact this field and make corresponding achievements in this field.

Data availability statement

The raw data supporting the conclusions of this article will be made available by the authors, without undue reservation.

Author contributions

All authors have the same contribution in participating in research article and work support.

Funding

The National Natural Science Foundation of China (Nos. 61772295, 61572270, and 61173056). The PHD foundation of Chongqing Normal University (No. 19XLB003). The Science and Technology Research Program of Chongqing Municipal Education Commission (Grant No. KJZD-M202000501). Chongqing Technology Innovation and application development special general project (cstc2020jscx-lyjsAX0002).

Acknowledgments

Upon the completion of this thesis, I could not stop expressing my heartfelt appreciation and great gratitude to those who have contributed to the thesis.

Conflict of interest

The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Publisher's note

All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers. Any product that may be evaluated in this article, or claim that may be made by its manufacturer, is not guaranteed or endorsed by the publisher.

References

1. Cao H, Tang L, Li J, Fang X. *Resource allocation algorithm for the downlink of multi-user ofdm system based on fairness*. ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering (2015).

2. Yang G, Hu F, Hou J. The multi-user detection for the mimo-ofdm system based on the genetic simulated annealing algorithm. In: *Proceedings. The 2009 international workshop on information security and application (IWISA 2009) (citeseer)* (2009). p. 334.

3. Zidan M, Abdel-Aty A-H, El-Sadek A, Zanaty E, Abdel-Aty M. Low-cost autonomous perceptron neural network inspired by quantum computation. In: AIP conference proceedings. AIP Publishing LLC (2017). Vol. 1905: 020005.

4. Zidan M., Abdel-Aty A, Younes A, Zanaty E, El-Khayat I, Abdel-Aty M. A novel algorithm based on entanglement measurement for improving speed of quantum algorithms. *Appl Math Inf Sci* (2018) 12:265–9. doi:10.18576/amis/120127

5. Said T, Chouikh A, Bennai M. N two-transmon-qubit quantum logic gates realized in a circuit qed system. *Appl Math Inf Sci* (2019) 13:839–46. doi:10.18576/amis/130518

6. Abdel-Aty A-H, Kadry H, Zidan M, Al-Sbou Y, Zanaty E, Abdel-Aty M. A quantum classification algorithm for classification incomplete patterns based on entanglement measure. *J Intell Fuzzy Syst* (2020) 38:2809–16. doi:10.3233/jifs-179566

7. Zidan M, Aldulaimi S, Eleuch H. Analysis of the quantum algorithm based on entanglement measure for classifying boolean multivariate function into novel hidden classes: Revisited. *App Mat Inf Sci* (2021) 15:643–7. doi:10.18576/amis/150513

8. Yang Y, Luan Y. *Performance comparison of user detections for mc-cdma system*. Electronic Science and Technology (2010).

9. Luo B, Sun Z. Enabling end-to-end communication between wireless sensor networks and the internet based on 6lowpan. *Chin J Electron* (2016) 24:633–8. doi:10.1049/cje.2015.07.033

10. Teng Z, Xie L, Xian Y, Xu Z, Chu Y, University ND. Resource allocation strategy for multi-user ofdm systems based on genetic algorithm. *J Hunan Univ Sci Technology(Natural Sci Edition)* (2018).

11. Khan HZ, Ali M, Rashid I, Ghafoor A, Naeem M, Khan AA, et al. Resource allocation for energy efficiency optimization in uplink-downlink decoupled 5g heterogeneous networks. *Int J Commun Syst* (2021) 34. doi:10.1002/dac.4925

12. Zhang J, Zhang J, Dong JP, Zhao SI. A genetic algorithm based subcarrier and antennaallocation in multiuser mimo-ofdm system. *J Shanghai Norm Univ (Natural Sciences)* (2009).

13. Liu M, Zhang F, Ma Y, Pota HR, Shen W. Evacuation path optimization based on quantum ant colony algorithm. *Adv Eng Inform* (2016) 30:259–67. doi:10.1016/j.aei.2016.04.005

14. Chen B, Li Y, Tao G, Peng L, Liu X. A resource allocation algorithm based on subcarrier pairing in multi-user cooperative relay communication. *Telecommunications Sci* (2014) 2011:691–702.

15. D T, J W. *Pmsm parameter identification based on artificial fish swarm algorithm*. Journal of Hangzhou University of Electronic Science and Technology (Natural Science Edition (2021).

16. Neshat M, Sepidnam G, Sargolzaei M, Toosi AN. Artificial fish swarm algorithm: A survey of the state-of-the-art, hybridization, combinatorial and indicative applications. *Artif Intell Rev* (2014) 42:965–97. doi:10.1007/s10462-012-9342-2

17. Wu Y, Gao X-Z, Zenger K. Knowledge-based artificial fish-swarm algorithm. *IFAC Proc volumes* (2011) 44:14705–10. doi:10.3182/20110828-6-it-1002.02813

18. Guobi L, Hongjun Y. Optimization of svr prediction model based on improved artificial fish swarm algorithm. *J Huaiyin Normal Univ (NATURAL SCIENCE EDITION)* (2020) 19:6.

19. Gong L-H, Xiang L-Z, Liu S-H, Zhou N-R. Born machine model based on matrix product state quantum circuit. *Physica A: Stat Mech its Appl* (2022) 593: 126907. doi:10.1016/j.physa.2022.126907

20. Zhou N-R, Liu X-X, Chen Y-L, Du N-S. Quantum k-nearest-neighbor image classification algorithm based on kl transform. *Int J Theor Phys* (2021) 60:1209–24. doi:10.1007/s10773-021-04747-7

21. Hongyang R. *Prediction of flotation concentrate grade and recovery based on improved artificial fish swarm algorithm*, 2. Liaoning University of science and Technology (2021).

22. Yang H, Du T, Wu J, Liu X, Wenwu LI. Solving high dimensional and complex non-convex programming based on improved quantum artificial fish algorithm. *Open Automation Control Syst J* (2014) 6:129–37. doi:10.2174/1874444301406010129

23. Du T, Hu Y, Ke X. Improved quantum artificial fish algorithm application to distributed network considering distributed generation. *Comput Intell Neurosci* (2015) 2015:1–13. doi:10.1155/2015/851863

24. Guo Y, Wu X, Huang W, Wang H. Adaptive minimum entropy blind equalization algorithm based on quantum artificial fish swarm optimization. *J Syst Simulation* (2016).

25. Ye T-Y, Geng M-J, Xu T-J, Chen Y. Efficient semiquantum key distribution based on single photons in both polarization and spatial-mode degrees of freedom. *Quan Inf Process* (2022) 21:123–1. doi:10.1007/s11128-022-03457-1

26. Ye T-Y, Li H-K, Hu J-L. Semi-quantum key distribution with single photons in both polarization and spatial-mode degree. *Int J Theor Phys* (2020) 59(9): 2807–15. doi:10.48550/arXiv.2205.06813

27. Chen C, Xu Y. An improved quantum ant colony optimization algorithm for solving complex function problems. *Int J Multimedia Ubiquitous Eng* (2015) 10: 193–204. doi:10.14257/ijmue.2015.10.11.19

TYPE Original Research
PUBLISHED 24 November 2022
DOI 10.3389/fphy.2022.1079624

Partial quantisation scheme for optimising the performance of hopfield network

Zhaoyang Song[1], Yingjie Qu[2], Ming Li[2], Junqing Liang[1]* and Hongyang Ma[2]*

[1]School of Information and Control Engineering, Qingdao University of Technology, Qingdao, China, [2]School of Science, Qingdao University of Technology, Qingdao, China

Check for updates

OPEN ACCESS

EDITED BY
Tianyu Ye,
Zhejiang Gongshang University, China

REVIEWED BY
Yumin Dong,
Chongqing Normal University, China
Lihua Gong,
Nanchang University, China

*CORRESPONDENCE
Junqing Liang,
liangjunqing@qut.edu.cn
Hongyang Ma,
hongyang_ma@aliyun.com

SPECIALTY SECTION
This article was submitted to Quantum Engineering and Technology, a section of the journal Frontiers in Physics

RECEIVED 25 October 2022
ACCEPTED 07 November 2022
PUBLISHED 24 November 2022

CITATION
Song Z, Qu Y, Li M, Liang J and Ma H (2022), Partial quantisation scheme for optimising the performance of hopfield network.
Front. Phys. 10:1079624.
doi: 10.3389/fphy.2022.1079624

The ideal Hopfield network would be able to remember information and recover the missing information based on what has been remembered. It is expected to have applications in areas such as associative memory, pattern recognition, optimisation computation, parallel implementation of VLSI and optical devices, but the lack of memory capacity and the tendency to generate pseudo-attractors make the network capable of handling only a very small amount of data. In order to make the network more widely used, we propose a scheme to optimise and improve its memory and resilience by introducing quantum perceptrons instead of Hebbian rules to complete its weight matrix design. Compared with the classical Hopfield network, our scheme increases the threshold of each node in the network while training the weights, and the memory space of the Hopfield network changes from being composed of the weight matrix only to being composed of the weight matrix and the threshold matrix together, resulting in a dimensional increase in the memory capacity of the network, which greatly solves the problem of the Hopfield network's memory The problem of insufficient memory capacity and the tendency to generate pseudo-attractors was solved to a great extent. To verify the feasibility of the proposed scheme, we compare it with the classical Hopfield network in four different dimensions, namely, non-orthogonal simple matrix recovery, incomplete data recovery, memory capacity and model convergence speed. These experiments demonstrate that the improved Hopfield network with quantum perceptron has significant advantages over the classical Hopfield network in terms of memory capacity and recovery ability, which provides a possibility for practical application of the network.

KEYWORDS
hopfield network, weight matrix, quantum perceptron, storage capacity, recovery capability

1 Introduction

Machine learning [1] is an important branch of artificial intelligence and a way to achieve artificial intelligence, i.e. machine learning is used as a means to solve problems in artificial intelligence. It is a multi-disciplinary discipline involving probability theory, statistics convex optimisation, complexity theory and many other disciplines. Machine learning algorithms are a class of algorithms that analyse existing data to obtain a certain pattern and use this pattern to make predictions about unknown data. It has been used with great success in very many fields, including medicine [2], biology [3], chemistry [4], physics [5–8] and mathematics [9]. Machine learning has proven to be one of the most successful ways to explore the field of artificial intelligence.

Perceptron [10] is a two-classification linear classification model, which aims to find the hyperplane that divides the training data linearly. Its biggest feature is that it is easy to implement. Suppose the training data set is $D = \left\{(\hat{x}_\varrho, \hat{y}_\varrho)\right\}_{\varrho=1}^{m}$, where $\hat{x}_\varrho \subseteq \mathbf{R}^m$, $\hat{y}_\varrho \in \{+1, -1\}$. The perceptron model is:

$$f(x) = \mathrm{sign}(\hat{w} \cdot \hat{x} + b) \tag{1}$$

Where $\hat{w}$ and $\hat{x}$ are the model parameters of the perceptron, $\hat{w} \in \mathrm{R}^{\mathrm{m}}$ is called weight or weight vector, and $\mathrm{b} \in \mathrm{R}$ is called bias. $\hat{w} \cdot \hat{x}$ represents the inner product of $\hat{w}$ and $\hat{x}$. The sign function is a symbolic function:

$$\mathrm{sign}(\hat{x}) = \begin{cases} +1, & \hat{x} \geq 0 \\ -1, & \hat{x} < 0 \end{cases} \tag{2}$$

The linear equation $\hat{w} \cdot \hat{x} + b = 0$ is a hyperplane in the characteristic space, where $\hat{w}$ is the normal vector of the hyperplane and b is the intercept of the hyperplane. The hyperplane can divide the feature space into two parts, and the point above the hyperplane conforms $\hat{w} \cdot \hat{x} + b \geqslant 0$, otherwise, it conforms $\hat{w} \cdot \hat{x} + b < 0$. The model of the classic perceptron and its application to classification is illustrated in Figure 1.

Quantum information is a new discipline developed based on quantum physics and information technology, which mainly includes two fields: quantum communication and quantum computing. Quantum communication focuses on quantum cryptography [11,12], quantum teleportation [13–16], and quantum direct communication [17], while quantum computing focuses on algorithms that fit quantum properties [18–23]. This is an extremely active field, as it has the potential to disrupt classical informatics, communication technologies, and computing methods.

Quantum perceptron belongs to quantum machine learning algorithms [24,25], which is the quantum counterpart of the classical perceptron model. Kapoor proved that quantum computation can provide significant improvements in the computational and statistical complexity of the perceptron model [26]; Schuld proposed a scalable quantum perceptron based on quantum Fourier transform [27], which can be used as a component of other more advanced networks [28]; Tacchino proposed a quantum perceptron model that can run on near-term quantum processing hardwar [29]. Currently, quantum perceptron models are in the exploratory stage and there is no absolute authority on them. In our work, the quantum perceptron model based on the quantum phase estimation algorithm [27] proposed by Schuld is used. The inverse quantum Fourier transform and the gradient descent algorithm on a classical computer are used to train the weight matrix of the perceptron.

Hopfield network (HNN) are single-layer full feedback network [30], which are characterised by the fact that the output x_i of any neuron is fed back to all neurons x_j as output by connecting the weights w_{ij}. The network usually uses Hebbian rule [31] for the design of the weight matrix. Hebbian rule is simpler but useful for the design of the weight matrix in HNN. However, sometimes the Hebbian rule cannot find an exact weight matrix, even though such a matrix exists [32]. This is because the rule does not incorporate the thresholds of the HNN into the training, which can result in attractors producing ranges of attraction domains that overlap each other or even appear to overwrite. And if the vectors to be stored are closer to each other, their probability of error is higher.

Considering that the weight matrix designed by the Hebbian rule is not enough to support the HNN to accomplish various practical tasks, we propose an improvement scheme, which will use the quantum perceptron instead of the Hebbian rule for the design of the HNN weights, Firstly, the weights and thresholds of the Hopfield network are mapped into the weight matrix of the quantum perceptron, and each node of the HNN is used as the input vector, and the weight matrix of the quantum perceptron is passed through the quantum The final weight matrix of the quantum perceptron is the weight matrix and threshold matrix of the HNN. The improved HNN has more memory storage space than the Hebbian rule because it has an additional threshold matrix to assist in storage, and can store the memorised information better. Moreover, due to the more accurate weight information, it is also easier to reach the steady state when iterating the HNN, thus the resilience and model convergence speed are significantly improved. Currently, the most widespread use of HNNs is for information recovery and information matching. Our improved HNN has been simulated and analysed to provide a huge improvement over the classical HNN in both information recovery and information matching, which makes the improved HNN more usable than the classical HNN, which is expected to provide more applications for HNNs in more fields, such as playing a greater role in virus information identification, human brain simulation, and error correction of quantum noise [33].

In Section 2, we describe in detail the HNN model, the Hebbian rule, the quantum Fourier transform and the quantum phase estimation algorithm used in this paper; Section 3 describes in detail the theory of our approach, including the

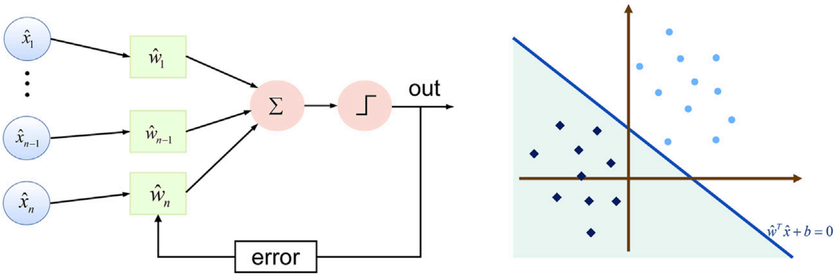


FIGURE 1
Models of classical perceptual machines (left) and applications to classification (right).

correspondence between the HNN and the perceptron model, the quantum perceptron model and how to use the quantum perceptron model for training the HNN weights and thresholds; Section 4 presents our simulation Section 4 presents our experimental analysis, in which we design experiments to verify the feasibility of our proposed scheme and its improvement and advantages over the classical scheme; Section 5 concludes the paper and provides predictions and analysis of the future of our proposed scheme.

2 Preliminaries

2.1 Hopfield network

HNN are multi-input, thresholded, binary nonlinear dynamic systems. The excitation function of the neuron is usually a step function, and the value of the neuron is −1, 1, or 0,1. When the value is 0 or −1, the current neuron is in the inhibited state, and when the value is 1, the current neuron is in the activated state. The HNN is a single layer neural network in which all neuron nodes are connected to other neuron nodes. There is no self-feedback between the nodes, forming a complete graph model. A neuron node in the inhibited state will enter the activated state when the stimulus exceeds a set threshold, i.e. it will jump from 0 or −1 to 1.

Each node in a HNN has the same function, and the output of a single node corresponds to the final state of that node, denoted by x_i, with the states of all nodes forming the state of the network $\boldsymbol{X} = [x_1, x_2, x_3, x_4 \ldots x_{n-1}, x_n]^T$. The topology and mode of operation is shown in Figure 2. The network enters a steady state and produces an output when the rate of change of the energy function of the network, $\Delta E = 0$ or when a preset upper limit of iterations is reached. The energy function and the rate of change of the energy function are as follows.

$$\begin{aligned} E(\epsilon) &= -\frac{1}{2}\boldsymbol{X}^T(\epsilon)\boldsymbol{W}\boldsymbol{X}(\epsilon) + \boldsymbol{X}^T(\epsilon)\boldsymbol{\theta} \\ \Delta E &= \Delta E(\epsilon+1) - \Delta E(\epsilon) \end{aligned} \tag{3}$$

where $\mathbf{W} = \{x_{ij}\}$ is the weight matrix, $\boldsymbol{X} = \{x_i\}$ is the network state and $\boldsymbol{\theta} = \{\theta_i\}$ is the threshold matrix.

2.2 Hebbian rule

The Hebbian rule describes the basic principle of synaptic plasticity, that is, continuous and repeated stimulation from presynaptic neurons to postsynaptic neurons can increase the efficiency of synaptic transmission.

The Hebbian rule is the oldest and simplest neuron learning rule. Here is the description equantion of the Hebbian rule:

$$w_{ij} = \frac{1}{p}\sum_{k=1}^{p} x_i^z x_j^z \tag{4}$$

Where w_{ij} is the connection weight from neuron j to neuron i, p is the number of training modes, and x_i^z is the i input of neuron k.

In the HNN, Hebbian rules can be used to design weight matrices:

$$\boldsymbol{W} = \sum_{p=1}^{P} \boldsymbol{X}^p(\boldsymbol{X}^p)^T \tag{5}$$

Here $w_{ii} = 0$, which means that there is no self-feedback between nodes. The equantion is rewritten as follows:

$$\boldsymbol{W} = \sum_{p=1}^{P}\left[\boldsymbol{X}^p(\boldsymbol{X}^p)^{\mathrm{T}} - \boldsymbol{I}\right] \tag{6}$$

Where $\boldsymbol{I}$ is the unit matrix and $\boldsymbol{X}$ is the system state of HNN.

2.3 HNN attractor and pseudo attractor

Considering that the Hopfield network has M samples of X^m, then:

$$(\boldsymbol{X}^m)^{\mathrm{T}}\boldsymbol{X}^z = \begin{cases} 0, & m \neq z \\ n, & m = z \end{cases} \tag{7}$$

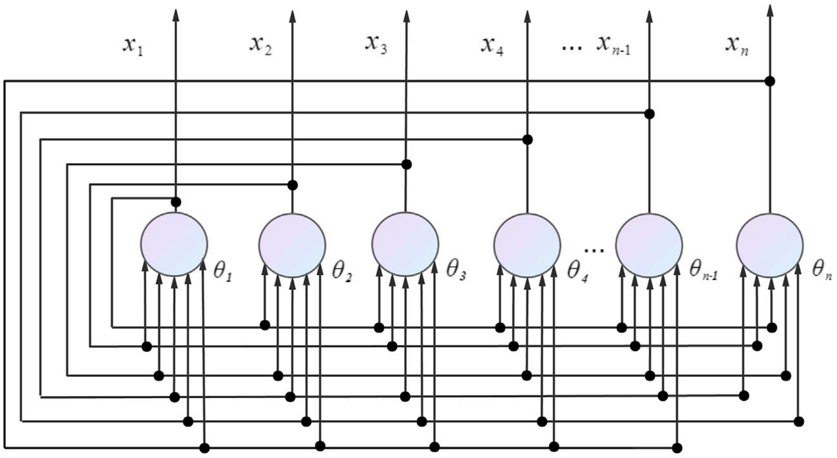


FIGURE 2
HNN topology operating structure and mode of operation.

$$\boldsymbol{W}\boldsymbol{X}^z = \sum_{m=1}^{m}\left[\boldsymbol{X}^m(\boldsymbol{X}^m)^{\mathrm{T}} - \boldsymbol{I}\right]\boldsymbol{X}^z = (n-M)\boldsymbol{X}^z \tag{8}$$

Because of n > M, therefore:

$$\begin{aligned} f(\boldsymbol{W}\boldsymbol{X}^m) &= f[(n-M)\boldsymbol{X}^m] \\ &= \mathrm{sgn}[(n-M)\boldsymbol{X}^{\mathrm{m}}] = \boldsymbol{X}^m \end{aligned} \tag{9}$$

According to Eq. 9: when a given sample, $\boldsymbol{X}^{\mathrm{m}}$ is the ideal attractor and produces a certain attractor domain around it, which will be "captured" by the attractor in the attractor domain. However, the condition that the given samples are orthogonal to each other is too harsh, which eventually leads to the attraction domain of some points outside the samples, which are regarded as pseudo attractors of the HNN.

2.4 Quantum Fourier transform

The quantum Fourier transform is an efficient quantum algorithm for the Fourier transform of quantum amplitudes. The quantum Fourier transform is not the classical counterpart of the Fourier transform and does not speed up the Fourier transform process on classical data, but it can perform an important task-phase estimation, i.e. estimating the eigenvalues of the You operator under certain conditions. The matrix representation of the quantum Fourier transform is as follows:

$$QFT_N = \frac{1}{\sqrt{N}}\begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \omega & \omega^2 & \cdots & \omega^{N-1} \\ 1 & \omega^2 & \omega^4 & \cdots & \omega^{2(N-1)} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \omega^{N-1} & \omega^{(N-1)2} & \cdots & \omega^{(N-1)(N-1)} \end{bmatrix} \tag{10}$$

Where, $\omega = e^{\frac{2\pi i}{N}} = \cos\frac{2\pi}{N} + i\sin\frac{2\pi}{N}$.

In the classical Fourier transform, the transformation takes the following form:

$$y_k = \frac{1}{\sqrt{N}}\sum_{j=0}^{N-1} x_j e^{2\pi jk/N} \tag{11}$$

The mathematical form of the quantum Fourier transform is similar to the mathematical representation of the discrete Fourier transform [34]. It is an operator defined on a set of standard orthogonal bases $|0\rangle$, $|1\rangle\cdots|N-1\rangle$ with the following action:

$$|j\rangle = \frac{1}{\sqrt{N}}\sum_{j=0}^{N-1} e^{2\pi jjk/N}|k\rangle \tag{12}$$

An arbitrary quantum state action can be expressed as:

$$\begin{aligned} |\psi\rangle &= \sum_j \tilde{x}_j|j\rangle \rightarrow \sum_{j=0}^{N-1}\tilde{x}_j QFT(|j\rangle) = \sum_{j=0}^{N-1}\tilde{x}_j\left(\frac{1}{\sqrt{N}}\sum_{k=0}^{N-1} e^{i\frac{2\pi}{N}jk}|k\rangle\right) \\ &= \sum_{k=0}^{N-1}\left(\sum_{j=0}^{N-1}\frac{\tilde{x}_j}{\sqrt{N}}e^{i\frac{2\pi}{N}jk}\right)|k\rangle = \sum_{k=0}^{N-1} y_k|k\rangle \end{aligned} \tag{13}$$

where the amplitude $y_k = \frac{1}{\sqrt{N}}\sum_{j=0}^{N-1}\tilde{x}_j e^{i\frac{2\pi}{N}jk}$ is the value of the discrete Fourier transform of the amplitude $\tilde{x}_j$.

The transform itself does not have much obvious value, but it is an important component subalgorithm of the quantum phase estimation algorithm. The quantum Fourier transform corresponds to the quantum line diagram (omitting the SWAP gate), where $R_k = \begin{pmatrix} 1 & 0 \\ 0 & e^{\frac{2\pi}{2^k}} \end{pmatrix}$. Figure 3 illustrates the quantum circuit of the quantum Fourier transform.

2.5 Qunamtum phase estimation algorithm

The quantum phase estimation algorithm is the key to many quantum algorithms [6,35], and its role is to estimate the phase in the eigenvalues of the eigenvectors corresponding to the You matrix. The quantum circuit for quantum phase estimation is shown in Figure 4. The algorithm uses two registers, the first of which contains τ quantum bits with initial state $|0\rangle$. The value of τ depends on the number of bits desired to be accurately estimated and the desired success rate. The second register has an initial state of $|\tilde{x}_n\rangle$. The essence of the process is the ability to perform the inverse Fourier transform:

$$\frac{1}{2^{\frac{\tau}{2}}}\sum_{j=0}^{2^{\tau}-1} e^{2\pi i\varphi j}|j\rangle|\tilde{x}_n\rangle \rightarrow |\tilde{\varphi}\rangle|\tilde{x}_n\rangle \tag{14}$$

where state $|\tilde{\varphi}\rangle$ is the estimated value of φ.

3 Methods

3.1 Correspondence between perceptron models and HNN

Firstly, we will discuss HNN with the range restricted to cells with non-zero thresholds and a step function as the threshold function, which is by far the most common form of HNN. Secondly two consensus needs to be established: 1) the units in this network are perceptrons. 2) The perceptron can determine the weights and thresholds of the network for the problem to be learned. Focus on consensus i): Based on the definitions of HNN and perceptual machines above, it is clear that the unit in a HNN is a perceptual machine.

Focus on consensus ii): Consider a HNN with n cells, where W is the weight matrix of $n \times n$, such that θ_i denotes the threshold of the cell i and the state of the network is $\boldsymbol{X}$. If one wants this network to reach a steady state, it means that the following n inequalities must be satisfied:

$$\begin{gathered}\operatorname{sign}(x_1)\,(x_2w_{12} + x_3w_{13} + \cdots + x_nw_{1n} - \theta_1) > 0\\ \operatorname{sign}(x_2)\,(x_1w_{21} + x_3w_{23} + \cdots + x_nw_{2n} - \theta_2) > 0\\ \vdots\\ \operatorname{sign}(x_n)\,(x_1w_{n1} + x_2w_{n2} + \cdots + x_{n-1}w_{mn-1} - \theta_n) > 0\end{gathered} \tag{15}$$

Since it has no self-feedback, only the $n\,(n-1)/2$ non-zero entries of the weight matrix $\boldsymbol{W}$ and the n thresholds of the cells appear in these inequalities. Let $\boldsymbol{u}$ denote the vector of $n + n\,(n + 1)/2$ dimension whose components are the non-diagonal elements of the weight matrix $w_{ij}\ (i < j)$ and the n threshold minus signs. The vector $\boldsymbol{u}$ is given by the following equation:

$$\boldsymbol{u} = (w_{12}, w_{13}, \ldots, w_{1n}, w_{23}, w_{24}, \ldots, w_{2n}, \ldots, w_{n-1n}, -\theta_1, \ldots, -\theta_n) \tag{16}$$

The vector x is transformed into n auxiliary vectors $\boldsymbol{v}_1, \boldsymbol{v}_2, \boldsymbol{v}_3, \ldots,$ $\boldsymbol{v}_n$ of dimension $n + n\,(n + 1)/2$ given by the expression:

$$\begin{aligned}\boldsymbol{v}_1 &= \left(\underbrace{x_2, x_3, \ldots, x_n}_{n-1}, 0, 0, \ldots, \underbrace{1, 0, \ldots, 0}_{n}\right)\\ \boldsymbol{v}_2 &= \left(\underbrace{x_1, 0, \ldots, 0}_{n-1}, \underbrace{x_3, \ldots, x_n}_{n-2}, 0, 0, \ldots, \underbrace{0, 1, \ldots, 0}_{n}\right)\\ \boldsymbol{v}_n &= \left(\underbrace{0, 0, \ldots, x_1}_{n-1}, \underbrace{0, 0, \ldots, x_2}_{n-2}, 0, 0, \ldots, \underbrace{0, 0, \ldots, 1}_{n}\right)\end{aligned} \tag{17}$$

Eq. 15 can be rewritten in the following form:

$$\operatorname{sign}(x_i)\boldsymbol{v}_i \cdot \boldsymbol{u} > 0 \tag{18}$$

Eq. 18 shows that the solution to the original problem is found by computing the linear separation of vectors z_i. The vectors belonging to the positive half-space are those with $\operatorname{sgn}(x_i) = 1$, and those belonging to the negative half-space are those with $\operatorname{sgn}(x_i) = -1$. This problem can be solved using perceptron learning, which allows us to calculate the weight vector $\boldsymbol{v}$ required for linear separation and from this to derive the weight matrix W with the threshold matrix θ. Figure 5 shows the correspondence between the HNN and the perceptron model.

3.2 Quantum perceptron model

First, t-qubit state$|0\rangle$ are passed through the Hadmard gate, to obtain the superposition state $|0\rangle^{\otimes\tau} \rightarrow \frac{1}{\sqrt{2^{\tau}}}\sum_{J=0}^{2^{\tau}-1}|J\rangle$, where J is the integer form of the bit string $|j_1, \ldots, j_\tau\rangle$, i.e. $J = j_1 2^{n-1} + j_2 2^{n-2} + \cdots + j_n 2^0$. Next, by an orcal operation $\mathcal{O}$:

$$\begin{gathered}\mathcal{O}\colon \frac{1}{\sqrt{2^{\tau}}}\sum_{J=0}^{2^{\tau}-1}|J\rangle|\psi_0\rangle \rightarrow \frac{1}{\sqrt{2^{\tau}}}\sum_{J=0}^{2^{t}-1}|J\rangle U^J|\psi_0\rangle\\ |J\rangle U^J|\psi_0\rangle = e^{2\pi i\Delta\phi h\,(w,\tilde{x})J}|J\rangle|\psi_0\rangle\end{gathered} \tag{19}$$

Where $U_0 = e^{i\pi}, U = e^{i\pi}\otimes_{k=1}^{n}U_k, U_k = \begin{pmatrix} e^{-2\pi w_k\Delta\phi} & 0\\ 0 & e^{2\pi i w_k\Delta\phi}\end{pmatrix}, \Delta\phi = 1/2n.$

From Eqs. 13–19:

$$\frac{1}{\sqrt{2^{\tau}}}\sum_{J=0}^{2^{\tau}-1}|J\rangle U^J|\psi_0\rangle = \frac{1}{\sqrt{2^{\tau}}}\sum_{J=0}^{2^{\tau}-1}e^{2\pi i J\varphi}|J\rangle|\psi_0\rangle \tag{20}$$

Finally the estimated phase can be obtained by inverse Fourier transform $|\tilde{\varphi}\rangle$:

$$\frac{1}{\sqrt{2^{\tau}}}\sum_{J=0}^{2^{\tau}-1}e^{2\pi i J\varphi}|J\rangle|\psi_0\rangle \overset{QFT^{-1}}{\rightarrow} |\tilde{\varphi}\rangle\otimes|\psi_0\rangle$$

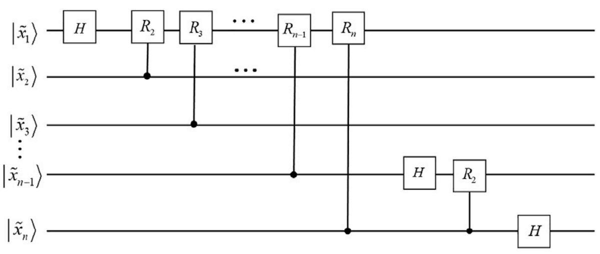


FIGURE 3
Quantum circuits for quantum Fourier transform.

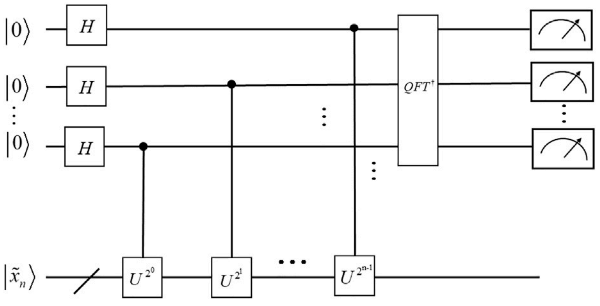


FIGURE 4
Quantum circuits for quantum phase estimation.

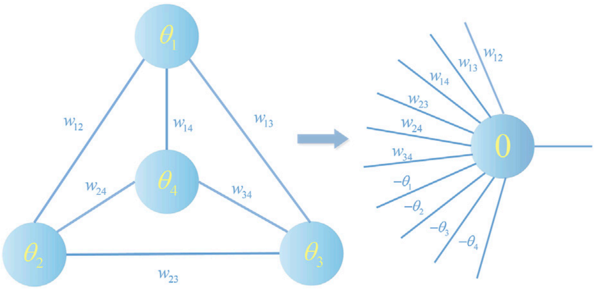


FIGURE 5
HNN and perceptual model transformation relationship.

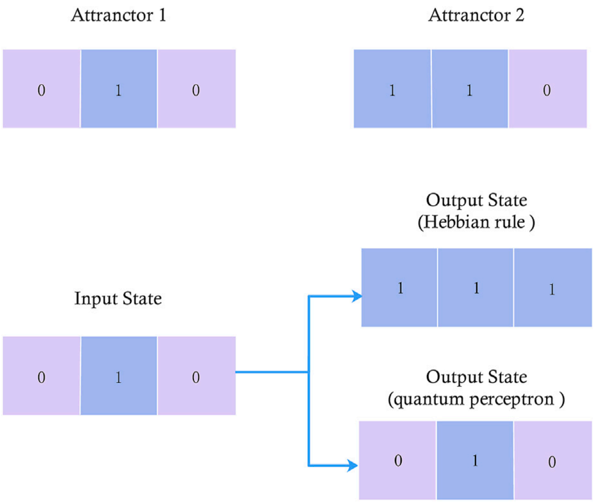


FIGURE 6
Non-orthogonal simple matrix memory test.

3.3 Obtaining parameter information using quantum perception

The connection between the HNN and the perceptron model was described above. It is now clarified how the design of the HNN weight matrix can be carried out using the quantum perceptron. Firstly, $\sigma = (\boldsymbol{v}, \boldsymbol{u})$ is input to the quantum perceptron model as an initial parameter and the model update rule for the quantum perceptron is as follows:

$$\begin{aligned} U|\sigma\rangle &= \otimes_{k=1}^{n} U_k |v_k\rangle = \otimes_{k=1}^{n} e^{2\pi i u_k v_k \Delta\phi} |v_k\rangle \\ &= e^{2\pi i \Delta\phi \sum_{k=1}^{n} u_k v_k} \otimes_{k=1}^{n} |v_k\rangle \\ &= e^{2\pi i \Delta\phi h(u,v)} \otimes_{k=1}^{n} |v_k\rangle \\ &= e^{2\pi i \Delta\phi h(u,v)} |\sigma\rangle \end{aligned} \tag{21}$$

From the above equation, it can be deduced that $|\sigma\rangle$ is an eigenvector of the matrix U and $e^{2\pi i \Delta\phi h(u,v)}$ is the corresponding eigenvalue. By picking the appropriate value of t in the quantum perceptron, the inverse Fourier transform by:

$$\frac{1}{\sqrt{2^{\tau'}}} \sum_{J'=0}^{2^{\tau}-1} e^{2\pi i J'\theta} |J'\rangle |\sigma\rangle \rightarrow |\tilde{\varphi}'\rangle \otimes |\sigma\rangle \tag{22}$$

It is possible to obtain a value of, which is very close to the true phase, and also becomes closer to the true phase as the value of t becomes larger. Combining Eq. 19 gives:

$$U|\psi_0\rangle = e^{2\pi i\theta}|\psi_0\rangle, \quad \theta = 0.5 + \Delta\phi h(u,v) \in [0,1] \tag{23}$$

Therefore the value of $\sigma = (\boldsymbol{v}, \boldsymbol{u})$ can be obtained by $\tilde{\varphi}'$.According to [], it can be known that in the perceptron model, its weight update rule:

$$u_{ij}(\xi+1) \coloneqq u_{ji}(\xi+1) \coloneqq u_{ij}(\xi) + \frac{\eta}{2}\left[(\sigma_i^q - Y_i^q)\sigma_j^q + \left(\sigma_j^q - Y_j^q\right)\sigma_i^q\right] \tag{24}$$

where $\boldsymbol{Y}^q = \mathrm{sgn}(\boldsymbol{u}(\xi)\boldsymbol{\sigma}^q), \eta$ is the learning rate. However, when training with a perceptron, it is difficult to guarantee the separability of the data. Therefore, our perceptron model is trained using the delta rule, i.e. a gradient descent algorithm to search the space of possible weight vectors in order to find the best-fitting sample weight vector. The process is implemented with the aid of a classical computer. Its weight update rule is expressed in the same form as (Eq. 25), except that $\boldsymbol{Y}^q = \boldsymbol{u}(\xi)\boldsymbol{\sigma}^q$.

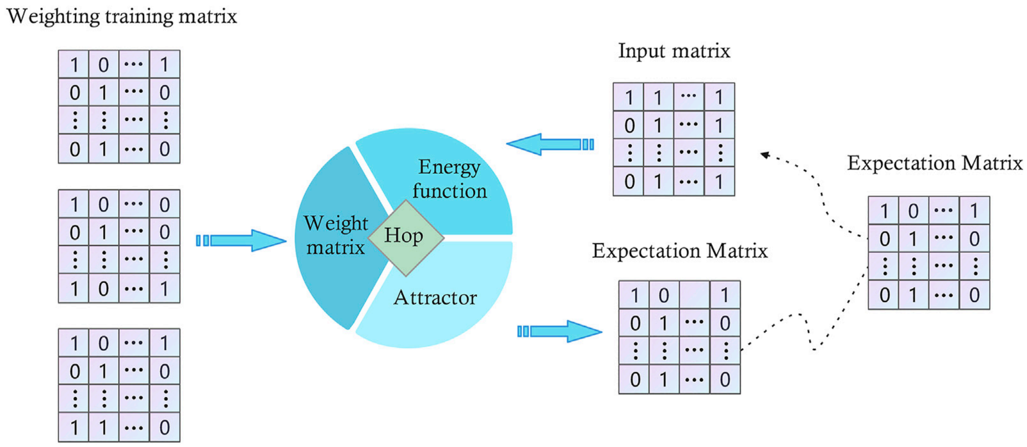


FIGURE 7
Example model of fragmented data recovery.

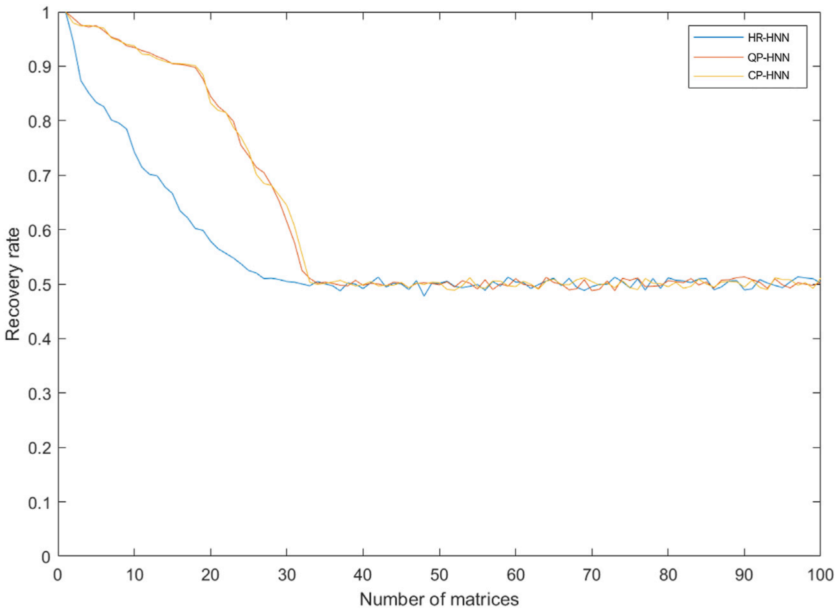


FIGURE 8
Diagram corresponding to the number of binary matrices and the recovery rate.

3.4 Computational complexity analysis

We analyze the computational complexity of the HNN in two steps. 1) Analysis of the lift rate of the data to be trained after conversion of the HNN to the perceptron model. 2) The computational complexity required to complete the weight parameters by means of the quantum phase estimation algorithm. First we analyse i), any HNN with n nodes satisfying the requirements of Section 3.1 can be converted into a perceptron model with $n\ (n-1)/2$ weight parameters. For ii), we analyze here two different algorithms for finding the weight parameters, namely the gradient descent-based algorithm and the Grover fast weight finding algorithm. The time complexity of the gradient descent-based algorithm is mainly

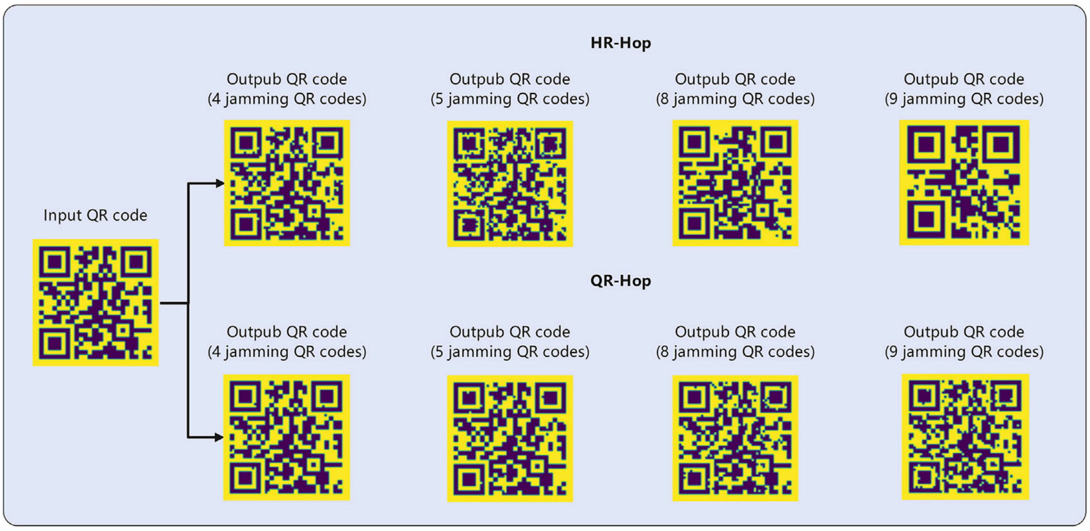

HR-Hop
Input QR code
Outpub QR code (4 jamming QR codes)
Outpub QR code (5 jamming QR codes)
Outpub QR code (8 jamming QR codes)
Outpub QR code (9 jamming QR codes)
QR-Hop
Outpub QR code (4 jamming QR codes)
Outpub QR code (5 jamming QR codes)
Outpub QR code (8 jamming QR codes)
Outpub QR code (9 jamming QR codes)

FIGURE 9
QP-HNN compared to HR-HNN memory capacity.

controlled by the number of steps ε accuracy, i.e. $O \propto \varepsilon^2$; the time complexity of finding the parameters using the Grover algorithm can reach $O(n)$ under certain conditions. It is clear from this analysis that the final computational complexity is $O(n^{\Upsilon})$, regardless of the algorithm used. However, quantum machine learning is able to process information using quantum effects, as in this paper, where we input the training set as a superposition of feature vectors into a quantum perceptron model that can be processed simultaneously, and this process is not affected by the size of the model. The value of this process is small when the model size is small, and becomes more apparent as the model size increases and becomes the most important part of determining the computational complexity.

4 Emulation analysis

The two most important applications of HNN are data matching and data recovery, which correspond to the accuracy of the HNN's weight matrix and memory capacity respectively. The convergence speed of the HNN model is extremely important in both data matching and data recovery. To this end, we designed three experiments, namely a non-orthogonal simple matrix recovery test, a Random binary-based incomplete matrix recovery test, and a memory capacity test based on the recognizability of QR codes, to compare the effectiveness of our proposed improved HNN with that of the classical HNN, and finally we added a model convergence speed comparison experiment to compare the performance differences between the models.

Our simulation analysis is based on the pennylane open source framework. The framework has embedded transition algorithms between quantum and classical algorithms as well as parameter optimisation algorithms, eliminating the need for us to package the parameters and design the optimisation algorithms separately. With this framework, the measured and calculated weight parameters are directly updated iteratively by means of a gradient descent algorithm, and the relevant information is fed back into the quantum algorithm to update the perceptron weights. Using this as a basis, we have designed the following simulation experiments.

4.1 Result

In the non-orthogonal simple matrix memory test, we demonstrated that our proposed solution can effectively cope with the memory confusion caused by non-orthogonal simple matrices; in the fragmented data recovery test, we demonstrated that our proposed QP-HNN has an average recovery rate improvement of 30.6% and a maximum of 49.1% in the effective interval compared with Hebbian rule-Hopfield network (HR-HNN), making it more practical. In the memory stress test based on QR code recognisability, our proposed QP-HNN is 2.25 times more effective than HR-HNN.

4.2 Non-orthogonal simple matrix memory test

The non-orthogonal simple matrix memory test is set up for the Hebbian rule in the classical HNN, as one of the prerequisites

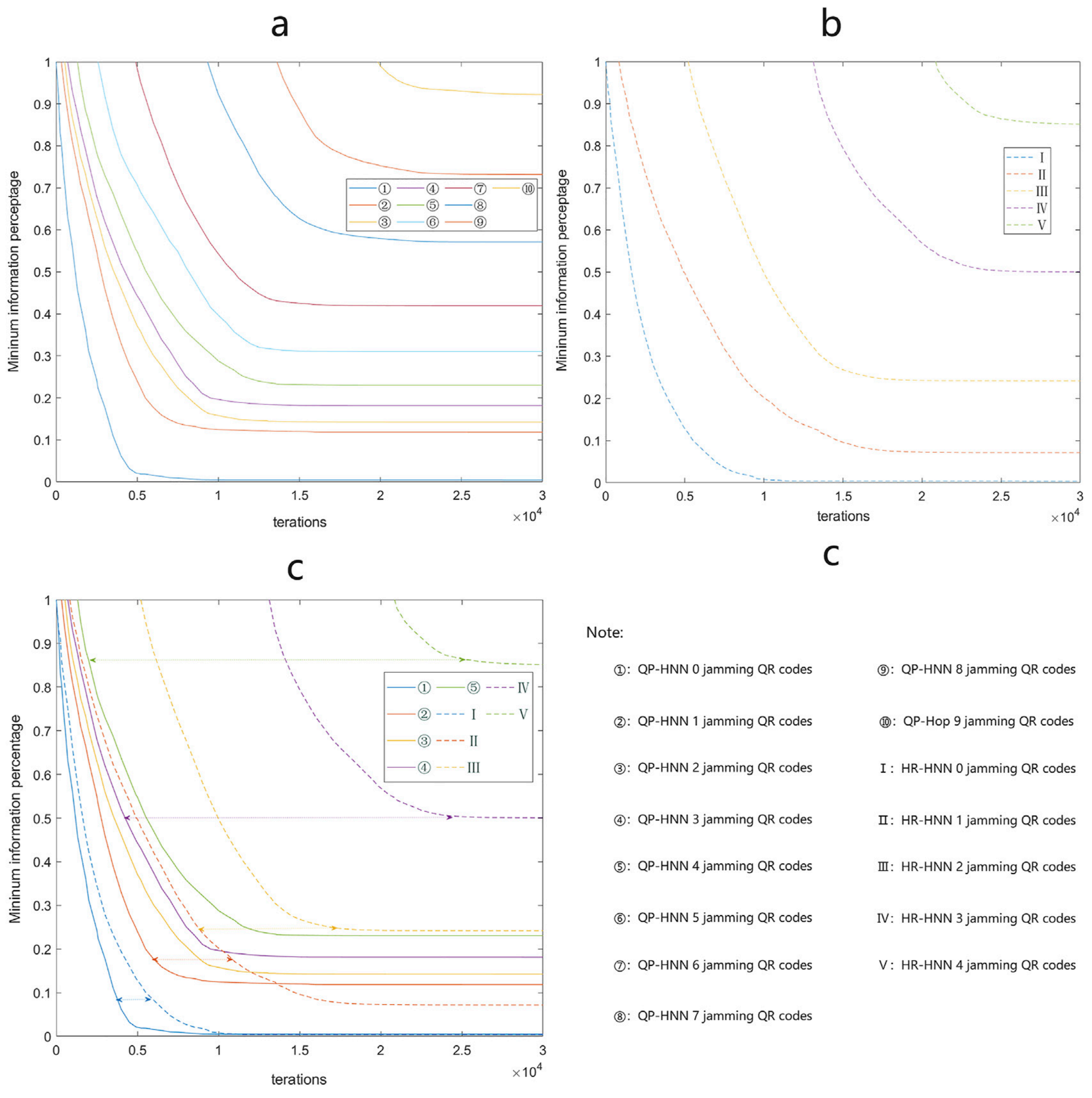


FIGURE 10
HR-HNN and QP-HNN convergence and resilience tests.

TABLE 1 Percentage of information required for recovery.

Number Type	1	2	3	4	5	6	7	8	9
HR-HNN	7%	24%	51%	86%	-	-	-	-	-
QP-HNN	12%	14%	18%	23%	31%	42%	57%	73%	92%

for the design of the weight matrix using the Hebbian rule is that the input vectors must be orthogonal to each other, and if they do not satisfy orthogonality, the designed weight matrix may be incorrect. We demonstrate the impact of this deficiency using two non-orthogonal 3D row vectors $X_{\nu} = [0, 1, 0]$ and $X_{9} = [1, 1, 1]$ as the input matrices for HR-HNN and QP-HNN, as shown in Figure 6 Where the trained weight matrix $\boldsymbol{W}_{HR} = [[0, 1, 1]\ [1, 0, 1]\ [1, 1, 0]]$ for HR-HNN, the weight matrix $\boldsymbol{W}_{QP} = [[0, 0.5, 0.3]\ [0.5, 0, 0]\ [0, 0, 0.2]]$ for QP – Hop and the threshold matrix $\boldsymbol{\theta}_{QP} = [0.6, -0.1, 0.2]$.

4.3 Random binary-based incomplete matrix recovery test

In this subsection, we test and compare the recoverability of three different HNN: ClassicalPerceptron-Hopfield (CP-HNN), QP-HNN, and HR-HNN. Firstly, a random number generator was used to generate 100 60 × 60 binary matrices $M = \{M_{br1}, M_{br2} \ldots M_{bri} \ldots M_{br99}, M_{br100}\}$, and a different number of binary matrices M_ι, $\iota \in \{1, 2 \ \ldots \ 100\}$ were randomly selected from M as the weight training matrices using QuantumPerceptron, ClassicalPerceptron, and HebbianRule to design the weight matrices respectively. A matrix M_{bri} was selected from M_ι and generated $M'_{bri} = M_{bri}.1/3$ of the data in M'_{bri} was inverted to simulate data residuals, and this matrix was used as the input matrix for the network to test the recovery rate of the above three HNN. The example model is shown in Figure 7, and its recovery rate with different numbers of binary matrices memorised is shown in Figure 8.

From Figure 8, it can be seen that the resilience of the HR-HNN network decreases rapidly as ι becomes larger ι means that the orthogonality between the matrices in M_ι decreases, and consequently, memory confusion ensues. The resilience of the network basically fails at $\iota = 20$ and is completely lost at $\iota = 30$; the ClassicalPerceptron-Hopfield (CP-HNN) network is highly similar to the QP-HNN network in terms of resilience and has excellent robustness in the first and middle stages of ι growth because the network also trains the threshold This is equivalent to increasing the error tolerance space and mitigating errors due to the non-orthogonality of the vectors in the matrix. As can be seen from the diagram, the network is still very resilient at $\iota = 20$. However, as ι increases, the fault tolerance space becomes saturated and the resilience decreases rapidly until it fails.

4.4 Memory capacity test based on the recognizability of QR codes

In order to visualise the memory capacity of the models, the differences between the models are presented using QR codes, which have different levels of fault tolerance and represent the number of error pixels that can be tolerated in the QR code. For our tests we have used the L level of fault tolerance, which allows for a maximum of 7% of incorrect pixels.

The QR code q_1 is generated and stored in the "Successful Identification", generating a QR code set $Q = \{q_n\}$, $n = 2, 3, 4, 5 \ldots$ the information in q_n is an irregular string of numbers generated by a random number generator, a randomly selected m - QR code from Q is used as the interfering QR code, and q_1 is involved in the design work of HR-HNN and QP-HNN weight matrices. After 100 tests and statistical processing, the output matrix of HR-HNN can be successfully recognised when $m \leq 4$; $\mathrm{QP-Hop}$ output matrix can be successfully recognised when, $m \leq 8$. In Figure 9 we show a comparison of these two HNNs in terms of memory capacity.

4.5 HNN recovery rate test

The usability of HNN is also affected by the number of iterations required for the model to converge, which in turn is affected by the completeness of the weights, threshold information and input data. Therefore, building on the previous subsection, we further investigate the number of iterations required for q' to recover to the state $\hat{q}$ where information can be correctly identified for different numbers of interfering QR codes, as shown in subplot a and subplot b in Figure 10. Subplot c shows the difference in the number of iterations required for q' to recover to $\hat{q}$ with the same amount of information. As can be seen from the figure, QP-HNN possesses a significant advantage over HR-HNN for the q' to $\hat{q}$ process, and this advantage becomes more pronounced as m grows.

Table 1 counts the recovery capacity limit of the HNN when the preset upper limit of 30,000 iterations is reached, where HR-HNN reaches the memory limit at $m = 4$, i.e. at $m = 5$, q' cannot recover to $\hat{q}$ even if the number of iterations is increased, while in QP-HNN, the memory limit occurs at $m = 8$.

5 Conclusion

We improve the original HNN weight design method by using a quantum perceptron instead of the Hebbian rule. The improved QP-HNN can better handle non-orthogonal matrices, and its information memory and recovery capabilities as well as model convergence speed are significantly improved compared to HR-HNN. It also opens up the possibility of further expanding the scope of applications in areas such as virus information recognition, human brain simulation, and error correction of quantum noise.

Our improved scheme is based on the quantum perceptron model proposed that we can input all the data to be processed into the model simultaneously by transforming and preparing them into quantum entangled states. The current model used is still the quantum-classical computing model, where the optimal weighting parameters are found by a classical computer, but Kapoor et al. have shown that the weighting parameters can be found much faster using the Grover algorithm, considerably increase the efficiency of finding the weight parameters to compensate for the extra time consumed in its determination of the weights compared to the Hebbian rule. Currently, corresponding quantum models of HNNs already exist, and the combination of quantum perceptrons and quantum HNNs is also destined to be more desirable in pure quantum computers than in classical HNNs.

Data availability statement

The raw data supporting the conclusions of this article will be made available by the authors, without undue reservation.

Author contributions

ZS: Conceptualization, Methodology, Software,Writing-Original draft preparation. YQ: Data curation, Writing-Original draft preparation. ML: Visualization, Investigation. JL:Supervision, Writing—Review and Editing. HM: Supervision, Writing—Review and Editing, Project administration, Funding acquisition.

Funding

Project supported by the National Natural Science Foundation of China (Grant Nos. 61772295), Natural Science Foundation of Shandong Province, China (Grant Nos. ZR2021MF049, ZR2019YQ01), Project of Shandong Provincial Natural Science Foundation Joint Fund Application (ZR202108020011).

Conflict of interest

The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Publisher's note

All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers. Any product that may be evaluated in this article, or claim that may be made by its manufacturer, is not guaranteed or endorsed by the publisher.

References

1. Carleo G, Cirac I, Cranmer K, Daudet L, Schuld M, Tishby N, et al. Machine learning and the physical sciences. *Rev Mod Phys* (2019) 91:045002. doi:10.1103/RevModPhys.91.045002

2. Liakos KG, Busato P, Moshou D, Pearson S, Bochtis D. Machine learning in agriculture: A review. *Sensors* (2018) 18:2674. doi:10.3390/s18082674

3. Pinter G, Felde I, Mosavi A, Ghamisi P, Gloaguen R. Covid-19 pandemic prediction for Hungary; a hybrid machine learning approach. *Mathematics* (2020) 8:890. doi:10.3390/math8060890

4. Dral PO. Quantum chemistry in the age of machine learning. *J Phys Chem Lett* (2020) 11:2336–47. doi:10.1021/acs.jpclett.9b03664

5. Radovic A, Williams M, Rousseau D, Kagan M, Bonacorsi D, Himmel A, et al. Machine learning at the energy and intensity frontiers of particle physics. *Nature* (2018) 560:41–8. doi:10.1038/s41586-018-0361-2

6. Haug T, Dumke R, Kwek L-C, Miniatura C, Amico L. Machine-learning engineering of quantum currents. *Phys Rev Res* (2021) 3:013034. doi:10.1103/PhysRevResearch.3.013034

7. Zhang L, Chen Z, Fei SM. Einstein-podolsky-rosen steering based on semisupervised machine learning. *Phys Rev A (Coll Park)* (2021) 104:052427. doi:10.1103/PhysRevA.104.052427

8. Jasinski A, Montaner J, Forrey RC, Yang BH, Stancil PC, Balakrishnan N, et al. Machine learning corrected quantum dynamics calculations. *Phys Rev Res* (2020) 2:032051. doi:10.1103/PhysRevResearch.2.032051

9. Jumper J, Evans R, Pritzel A, Green T, Figurnov M, Ronneberger O, et al. Highly accurate protein structure prediction with alphafold. *Nature* (2021) 596:583–9. doi:10.1038/s41586-021-03819-2

10. Rosenblatt F. The perceptron: A probabilistic model for information storage and organization in the brain. *Psychol Rev* (1958) 65:386–408. doi:10.1037/h0042519

11. Zhou N, Hu Y, Gong L, Li G. Quantum image encryption scheme with iterative generalized arnold transforms and quantum image cycle shift operations. *Quan Inf Process* (2017) 16:164–23. doi:10.1007/s11128-017-1612-0

12. Yi Nuo W, Zhao Yang S, Yu Lin M, Nan H, Hong Yang M. Color image encryption algorithm based on dna code and alternating quantum random walk. *Acta Phys Sin* (2021) 70:230302–23. doi:10.7498/aps.70.20211255

13. Ye TY, Geng MJ, Xu TJ, Chen Y. Efficient semiquantum key distribution based on single photons in both polarization and spatial-mode degrees of freedom. *Quan Inf Process* (2022) 21:123–1. doi:10.1007/s11128-022-03457-1

14. Ma HY, Guo ZW, Fan XK, Wang SM. The routing communication protocol for small quantum network based on quantum error correction code. *Acta Electonica Sinica* (2015) 43:171. doi:10.3969/j.issn.0372-2112.2015.01.027

15. Zhou NR, Zhu KN, Zou XF. Multi-party semi-quantum key distribution protocol with four-particle cluster states. *Annalen der Physik* (2019) 531:1800520. doi:10.1002/andp.201800520

16. Ye TY, Li HK, Hu JL. Semi-quantum key distribution with single photons in both polarization and spatial-mode degrees of freedom. *Int J Theor Phys (Dordr)* (2020) 59:2807–15. doi:10.1007/s10773-020-04540-y

17. Sheng YB, Zhou L, Long GL. One-step quantum secure direct communication. *Sci Bull* (2022) 67:367–74. doi:10.1016/j.scib.2021.11.002

18. Noiri A, Takeda K, Nakajima T, Kobayashi T, Sammak A, Scappucci G, et al. Fast universal quantum gate above the fault-tolerance threshold in silicon. *Nature* (2022) 601:338–42. doi:10.1038/s41586-021-04182-y

19. Lloyd S, Mohseni M, Rebentrost P. Quantum principal component analysis. *Nat Phys* (2014) 10:631–3. doi:10.1038/nphys3029

20. Li Z, Liu X, Xu N, Du J. Experimental realization of a quantum support vector machine. *Phys Rev Lett* (2015) 114:140504. doi:10.1103/PhysRevLett.114.140504

21. Low GH, Yoder TJ, Chuang IL. Quantum inference on bayesian networks. *Phys Rev A (Coll Park)* (2014) 89:062315. doi:10.1103/PhysRevA.89.062315

22. Dong D, Chen C, Li H, Tarn T-J. Quantum reinforcement learning. *IEEE Trans Syst Man Cybern B* (2008) 38:1207–20. doi:10.1109/TSMCB.2008.925743

23. Zhou N, Zhang TF, Xie XW, Wu JY. Hybrid quantum–classical generative adversarial networks for image generation via learning discrete distribution. *Signal Processing: Image Commun* (2022) 2022:116891. doi:10.1016/j.image.2022.116891

24. Biamonte J, Wittek P, Pancotti N, Rebentrost P, Wiebe N, Lloyd S. Quantum machine learning. *Nature* (2017) 549:195–202. doi:10.1038/nature23474

25. Harrow AW, Hassidim A, Lloyd S. Quantum algorithm for linear systems of equations. *Phys Rev Lett* (2009) 103:150502. doi:10.1103/PhysRevLett.103.150502

26. Kapoor A, Wiebe N, Svore K. Quantum perceptron models. *Adv Neural Inf Process Syst* (2016) 29.

27. Weinstein YS, Pravia M, Fortunato E, Lloyd S, Cory DG. Implementation of the quantum Fourier transform. *Phys Rev Lett* (2001) 86:1889–91. doi:10.1103/PhysRevLett.86.1889

28. Schuld M, Sinayskiy I, Petruccione F. Simulating a perceptron on a quantum computer. *Phys Lett A* (2015) 379:660–3. doi:10.1016/j.physleta.2014.11.061

29. Tacchino F, Macchiavello C, Gerace D, Bajoni D. An artificial neuron implemented on an actual quantum processor. *Npj Quan Inf* (2019) 5:26–8. doi:10.1038/s41534-019-0140-4

30. Hopfield JJ. Neural networks and physical systems with emergent collective computational abilities. *Proc Natl Acad Sci U S A* (1982) 79:2554–8. doi:10.1073/pnas.79.8.2554

31. Hebb DO. *The organization of behavior: A neuropsychological theory*. London: Psychology Press (2005). doi:10.4324/9781410612403

32. Wuensche A. Discrete dynamical networks and their attractor basins. *Complex Syst* (1998) 98:3–21.

33. Wang H, Song Z, Wang Y, Tian Y, Ma H. Target-generating quantum error correction coding scheme based on generative confrontation network. *Quan Inf Process* (2022) 21:280–17. doi:10.1007/s11128-022-03616-4

34. Harris FJ. On the use of windows for harmonic analysis with the discrete Fourier transform. *Proc IEEE* (1978) 66:51–83. doi:10.1109/PROC.1978.10837

35. Dorner U, Demkowicz-Dobrzanski R, Smith BJ, Lundeen JS, Wasilewski W, Banaszek K, et al. Optimal quantum phase estimation. *Phys Rev Lett* (2009) 102: 040403. doi:10.1103/PhysRevLett.102.040403

TYPE Original Research
PUBLISHED 09 December 2022
DOI 10.3389/fphy.2022.978220

Check for updates

OPEN ACCESS

EDITED BY
Tianyu Ye,
Zhejiang Gongshang University, China

REVIEWED BY
Farhad Sattari,
University of Mohaghegh Ardabili, Iran
Tingting Song,
Jinan University, China

*CORRESPONDENCE
Jie Shen,
shenjie74@163.com

†These authors contributed equally to this work

SPECIALTY SECTION
This article was submitted to Quantum Engineering and Technology, a section of the journal Frontiers in Physics

RECEIVED 25 June 2022
ACCEPTED 05 August 2022
PUBLISHED 09 December 2022

CITATION
Shen J, Dong WQ, Shi X, Wang J, Wang Y and Liu HM (2022), The model for non-Abelian field topology for the multilayer fractional quantum anomalous Hall device.
Front. Phys. 10:978220.
doi: 10.3389/fphy.2022.978220

The model for non-Abelian field topology for the multilayer fractional quantum anomalous Hall device

Jie Shen[1,2*†], Wen Qi Dong[1,3†], Xuewei Shi[1], Jing Wang[1,3], Yang Wang[1] and Han Min Liu[1]

[1]State Grid Jibei Zhangjiakou Wind and Solar Energy Storage and Transportation New Energy Co., Ltd., Beijing, China, [2]Beijing University of Posts and Telecommunications, Beijing, China, [3]Hebei Province Wind and Solar Energy Storage Combined Power Generation Technology Innovation Center, Beijing, China

From the recent empirical discovery of the quantum anomalous Hall effect (QAHE), the interaction of the particle with spin−orbit coupling (SOC) plays an essential role in the cause of the QAHE, which includes three terms: external, internal, and chiral symmetric terms. Then, the non-Abelian quantum field theory was adopted to analyze and prove the conjecture on the causes that can lead to the fractional quantum Hall effect (FQHE). The spontaneously topological chiral symmetry breaking is the main contribution to the FQHE, which also includes two terms: the hopping of sublattice and Coulomb energy by the interaction of many-body particles. More generally, this exciton possesses an intermediate characteristic between the Wannier regimes and displays a peculiar two-dimensional wavefunction in the three-dimensional FQHE states. Finally, a bilayer three-dimensional model is proposed to implement the FQHE on the lattice by incorporating ferromagnetic dopants into three-dimensional topological insulative thin films. This study theoretically predicts the FQHE on the basis of other reports that have experimentally verified the rationality of the proposed model in magnetic topological insulators.

KEYWORDS
FQHE (fractional quantum Hall effect), SOC (spin−orbit coupling), non-Abelian, chiral symmetry breaking, multilayer model, Berry curvature

1 Introduction

The quantum anomalous Hall effect (QAHE) has a totally different physical nature, with a semi-integer quantum Hall effect and a perfect quantum tunneling effect. It allows for resistance quantization and dissipationless edge states without the presence of any applied magnetic field. The materials and structures of the QAHE, where quantum effects are responsible for novel physical properties, reveal the important roles of symmetry, topology, and dimensionality. In 1988, according to Haldane, there might be no need to apply any external magnetic field for the quantum Hall effect, but it seemed impossible to implement such a particular material system of quantum effects in physical ways. In 2010, physicists achieved a breakthrough in the theory and design of materials, such that Cr/Fe magnetic ions could be doped into Bi_2Te_3 and Bi_2Se_3 and Sb_2Te_3 topological insulators. There are special V-Vleck ferromagnetic exchange mechanisms to ensure stability of ferromagnetic insulators, creating the best system to achieve the quantum anomalous Hall effect [1, 2]. The calculations show that the multilayer magnetic exchange of magnetic topological insulators takes place at a certain thickness and strength, that is, in the "QAHE" state. The breakthrough in theories and material design has given rise to the idea of looking for the QAHE.

The topological flat-band model is an extended version of the famous Haldane model. At least one energy band has non-trivial topological properties, that is, it has a non-zero Chern number, and the bandwidth of this energy band is very narrow. There is a wide energy gap between these energy bands. Recently, through the systematic numerical study of fermions and boson lattice systems with strong correlative interactions with topological flat bands, a novel class of Abelian and non-Abelian FQHEs has been discovered. The newly discovered FQHE is distinct from the continuous FQHE on the traditional Landau energy level. Without requiring any external magnetic field, it has a relatively wide characteristic energy gap and can exist at higher temperatures without requiring a single-particle Landau. The energy level cannot be described by conventional Laughlin wavefunctions. These fractional phenomena with no external magnetic field and no Landau energy levels define a new class of fractional topological phases, which are also called fractional insulators. The FQHE is also called the fractional quantum anomalous Hall effect (FQAHE) [3].

This paper is organized into five sections: Section 1 discusses the spin–orbit coupling theory for the QAHE in Section 2. Section 3 shifts the attention to an explanation of the intrinsic non-Abelian gauge field for properties of QHE and the cause of the QAHE. The next two sections expand the circumstance to the three-dimensional topology insulator and a conjecture on the existence of the FQAHE. Conclusions are drawn in Section 6.

2 Mathematical theory foundation of the quantum anomalous Hall effect

The difference between the QAHE and QAH lies in the absence of an external magnetic field, with homogeneous magnetization M. Their measurements in the magnetic field can be presented as follows:

$$\rho_{xy} = R_0 B + 4\pi R_s M. \tag{1}$$

There are three causes for QHE: The first, the extrinsic mechanism, views QHE as related to material impurities and spin–orbit (SO) interaction, such as skew scattering and side-jump of the lattice; the second, the intrinsic mechanism, points out that crystal potential is periodic and SO is interactive; the third, the chirality mechanism, suggests in noncollinear ferromagnets the spin–orbit interaction causes the effect [4]. The spin–orbit interaction can be expressed as follows:

$$H_{SO,vac} = \lambda_{vac} \cdot \sigma \cdot \left(k \times \nabla\tilde{V}\right), \tag{2}$$

where subscripts SO and vac signify the spin–orbit interaction and vacuum holes, respectively; the random Rashba coupling parameter λ has the zero mean and a Gaussian correlator; the other parameters are $\mathbf{k}$ for the wave vector, V for the voltage, and σ for the current conductivity.

Also, in a 2D high-symmetry system, anomalous Hall effect Hamiltonian has three forms:

$$\begin{aligned} H_{eff} &= \varepsilon_k + V + H_{\text{int}} + H_{ext} \\ H_{int} &= \frac{1}{2}\mathbf{b}(\mathbf{k}) \cdot \sigma \\ H_{ext} &= \lambda \cdot \sigma \cdot (\mathrm{k} \times \nabla V). \end{aligned} \tag{3}$$

The QAHE has the following characteristics: magnetization, spin-polarized and transverse carriers, Hall voltage on spin current, and spin accumulation. On the other hand, the pure spin Hall effect (SHE) is different, without applying any external magnetic field. The spin–orbit interaction causes electrons to carry opposite spins to move in opposite directions at the 2D insulator boundary with metal boundaries. The electric field provided generates a spin current that fails to create a charge flow.

The linear response of non-conserved spin current to the applied electric field can be calculated by the Kubo formula.

$$\sigma = \frac{e^2}{\omega^2} Tr \int \frac{d\varepsilon}{2\pi} \langle \hat{v}_i \hat{G}(\varepsilon + \omega) \hat{v}_j \hat{G}(\varepsilon) \rangle. \tag{4}$$

Taking the static limit, we get the Streda formula as follows:

$$\begin{aligned} \sigma^I_{ij} &= \frac{e^2}{2} Tr \int \frac{d\varepsilon}{2\pi} \left(-\frac{\partial f(\varepsilon)}{\partial\varepsilon}\right) \langle \hat{v}_i \left[\hat{G}^R(\varepsilon) - \hat{G}^A(\varepsilon)\right]; \\ & v_j \hat{G}^A(\varepsilon) - \hat{v}_i \hat{G}^R(\varepsilon) \hat{v}_j \left[\hat{G}^R(\varepsilon) - \hat{G}^A(\varepsilon)\right] \rangle \\ \sigma^{II}_{ij} &= \frac{e^2}{2} Tr \int \frac{d\varepsilon}{2\pi} f(\varepsilon) \langle \hat{v}_i \frac{\partial \hat{G}^A(\varepsilon)}{\partial\varepsilon} \hat{v}_j \hat{G}^A(\varepsilon) - \hat{v}_i \hat{G}^A(\varepsilon) \hat{v}_j \\ & \frac{\partial \hat{G}^A(\varepsilon)}{\partial\varepsilon} + \hat{v}_i \hat{G}^R(\varepsilon) \hat{v}_j \frac{\partial \hat{G}^R(\varepsilon)}{\partial\varepsilon} - \hat{v}_i \frac{\partial \hat{G}^R(\varepsilon)}{\partial\varepsilon} \hat{v}_j \hat{G}^R(\varepsilon) \rangle, \end{aligned} \tag{5}$$

where $\hat{G}^A$ and $\hat{G}^R$ are the advanced and retarded Green functions, respectively. The off-diagonal conductivity presents the contribution from all occupied states. The limit as $\omega \rightarrow 0$ implies $\omega \rightarrow \hbar/\tau$.

The difference in cleanliness of the current and the possible disappearance of Gaussian disorder can be explained by asymmetric dispersion. Impurities have no effect on the side view current [5].

The single-particle energy band system is dispersive and does not support fractional excitation and cannot implement the

FQHE. A series of topological flat-band lattice models are expected to overcome the abovementioned difficulties and implement the FQHE. The tight-binding model of the two-dimensional triangular lattice model is expressed in the Hamiltonian. Hall conductivity is calculated by the Kubo formula:

$$\begin{aligned}&\sigma_{xy}(\omega) = \frac{\mathrm{e}^2}{\omega}\int_{-\infty}^{\infty}\frac{\mathrm{d}\varepsilon}{2\pi}\sum_{mm}\sum_{k}(v_x)_{nm}\\ &G_{kam}(\varepsilon + w)\left(v_y\right)_{mm}G_{knn}(\varepsilon)\end{aligned}, \tag{6}$$

where the velocity operator $\mathbf{v} = \partial H/\partial \mathbf{k}$.

Hence, we have

$$\sigma_{xy} = e^2\sum_{n}\sum_{\mathbf{k}}\tilde{f}(E_{\mathbf{k}n})\left(\frac{\partial A_y(\mathbf{k}n)}{\partial k_x} - \frac{\partial A_x(\mathbf{k}n)}{\partial k_y}\right),$$

where $\tilde{f}$ is the Femi statistic function with gauge potential

$$A_\alpha(\mathbf{k}n) = -i\langle\mathbf{k}n\left|\frac{\partial}{\partial k_\alpha}\right|\mathbf{k}n\rangle.$$

Based on the 2D Rashba model, we obtain the magnetization Rashba Hamiltonian:

$$H = \varepsilon_k + \alpha\left(k_y\sigma_x - k_x\sigma_y\right) - M\sigma_z,$$

where $\varepsilon_k = k^2/2m$. Then, the Hall conductivity is

$$\sigma_{xy}(\omega) = \frac{e^2}{\omega}Tr\int_{-\infty}^{\infty}\frac{d\varepsilon}{2\pi}\frac{d^2\mathbf{k}}{(2\pi)^2}v_x G_{\mathbf{k}}(\varepsilon + \omega)v_y G_{\mathbf{k}}(\varepsilon), \tag{7}$$

with $v_x = \frac{k_m}{m} - \alpha\sigma_y, v_y = \frac{k_m}{m} - \alpha\sigma_x$, and the energy spectrum is

$$E_{k\uparrow,\downarrow} = \varepsilon \mp \lambda(k), \lambda(k)\sqrt{M^2 + \alpha^2 k^2},$$

where M corresponds to a uniform magnetization along the z-axis, which is uncorrelated with the macroscopic magnetic field, whose value is half of the spin splitting. The second of the two contribution terms contributes to the states below the Fermi energy.

$$\sigma_{xy}^{II} = -4e^2 M\alpha^2\int\frac{d^2k}{(2\pi)^2}\frac{f(E_{k\uparrow}) - f(E_{k\downarrow})}{(E_{k\uparrow} - E_{k\downarrow})}. \tag{8}$$

Then, we have

$$\sigma_{xy}^{II} = \frac{e^2 M}{4\pi}\left(\frac{1}{\lambda(k_{F\downarrow})} - \frac{1}{\lambda(k_{F\uparrow})}\right). \tag{9}$$

The symmetric breaking of topological material structure affects the Berry phase and causes the QAHE, while the Hamiltonian

$$H = \varepsilon_k + \lambda(k)\sigma\cdot\mathbf{n}(k), \tag{10}$$

where the unit normal vector to the sphere gives

$$\mathbf{n}(\mathbf{k}) = \left(\frac{\alpha\mathbf{k_y}}{\lambda(\mathbf{k})}, -\frac{\alpha\mathbf{k_x}}{\lambda(\mathbf{k})}, \frac{\mathbf{M}}{\lambda(\mathbf{k})}\right),$$

so the conductivity can be expressed in terms of $\mathbf{n}(\mathbf{k})$.

$$\sigma_{xy}^{II} = -\frac{e^2}{2}\int\frac{d^2\mathbf{k}}{(2\pi)^2}f(E_{\mathbf{k}\uparrow})\varepsilon_{\alpha\beta\gamma}n_\alpha\frac{\partial n_\beta}{\partial k_x}\frac{\partial n_\gamma}{\partial k_y}. \tag{11}$$

Spin current density in the wire can be defined as follows:

$$J_\alpha^i(\mathbf{r}, t) = \frac{\delta L}{\delta A_\alpha^i(\mathbf{r}, t)}. \tag{12}$$

The aforementioned formula defines a non-conserved equilibrium spin current, and it is related to real motion. The redefinition of spin current in Lagrangian allows for the equilibrium spin current.

$$\begin{aligned}L &= \int\mathrm{d}^3 r\left\{\Psi^\dagger(r, t)\left(\mathrm{i}\frac{\partial}{\partial t} - H\right)\Psi(r, t)\right.\\ L &= \int\mathrm{d}^3\mathbf{r}\Psi^+(\mathbf{r}, t)\left(\mathrm{i}\frac{\partial}{\partial t} + \frac{\nabla^2}{2m} - V(r)\right)\Psi(\mathbf{r}, t)\end{aligned}.$$

In rotation space, the local transformation is

$$\Psi(\mathbf{r}, t) \rightarrow \exp[-ig\mathbf{n}(\mathbf{r}, t)\cdot\sigma]\psi(\mathbf{r}, t).$$

Adopting the Lagrangian transformation, we obtain

$$\begin{aligned}L = \int\mathrm{d}^3\mathbf{r}\psi^\dagger(\mathrm{r}, t)\Bigg[\mathrm{i}\left(\frac{\partial}{\partial t} - \mathrm{i}A_0^i(\mathbf{r}, t)\sigma^i\right) +\\ \frac{1}{2m}\left(\frac{\partial}{\partial r_\alpha} - \mathrm{i}A_\alpha^i(\mathrm{r}, t)\sigma^i\right)^2 - V(\mathbf{r})\Bigg]\psi(\mathbf{r}, t)\end{aligned}. \tag{13}$$

The gauge vectors in the fields are

$$A_0^i(\mathbf{r}, t) = g\frac{\partial n^{\mathrm{i}}(\mathbf{r}, t)}{\partial t}, A_\alpha^i(\mathbf{r}, t) = g\frac{\partial n^{\mathrm{i}}(\mathbf{r}, t)}{\partial r_\alpha}.$$

Thus, the spin density and spin current density can be expressed as follows:

$$S^i(r, t) = \frac{\delta L}{\delta A_0^i(r, t)}, J_\alpha^i(r, t) = \frac{\delta L}{\delta A_\alpha^i(r, t)}. \tag{14}$$

For equilibrium spin currents, we consider the simplest model with two interactive spins in local fields, where Hamiltonian is given by

$$H = -\mathbf{J}\mathbf{S}_1\cdot\mathbf{S}_2 - \mathbf{B}_1\cdot\mathbf{B}_2 - \mathbf{B}_2\cdot\mathbf{B}_2.$$

The equation of motion for spin S_1 is expressed as follows:

$$\dot{\mathbf{S}}_1 = (i/\hbar)[H, S_1];$$
$$\dot{S}_1 = (J/\hbar)\mathbf{S}_1\times\mathbf{S}_2 + (1/\hbar)\mathbf{S}_1\times\mathbf{B}_1.$$

The spin current density is expressed as follows:

$$J_{2\rightarrow 1} \equiv \frac{J}{\hbar}\mathbf{S}_1\times\mathbf{S}_2 = -J_{1\rightarrow 2}.$$

The two-point Hubbard model can be used to represent the interaction between present electrons s.t.

$$H = -t\left(c^{\dagger}_{1\alpha}c_{2\alpha} + c^{\dagger}_{2\alpha}c_{1\alpha}\right) + \sum_{i=1,2}\left(Un^{\uparrow}_{i}n^{\downarrow}_{i} - \mathbf{B_i}\cdot\mathbf{S_i}\right).$$

The motion equation is expressed as follows:

$$\begin{aligned}\dot{\mathbf{S}}_1 &= (i/\hbar)[H, S_1]\\ \dot{\mathbf{S}}_1 &= \frac{it}{2\hbar}\left(c^{\dagger}_{1\alpha}c_{2\beta} + c^{\dagger}_{2\alpha}c_{1\beta}\right)\sigma_{\alpha\beta} + \frac{1}{\hbar}\mathbf{S}_1\times\mathbf{B}_1\end{aligned}\cdot \tag{15}$$

The spin current density is expressed as follows:

$$j^{i}_{2\to1} \equiv\ = \frac{it}{2\hbar}\left(c^{\dagger}_{1\alpha}c_{2\beta} + c^{\dagger}_{2\alpha}c_{1\beta}\right)\sigma_{\alpha\beta} = -j_{1\to2}. \tag{16}$$

Therefore, the equilibrium spin current is related to the jump across different positions. Where $-J \equiv 4t^2/U$. Thus, spin current density is given by: Therefore, the equilibrium spin current is related to the jump across different positions.

Applying the six functions based on ground states, we have the strong e–e interaction such that $t/U \ll 1$, and effective Hamiltonian is expressed as follows:

$$\tilde{H} = -J\left(S_1\cdot S_2 - 1/4\right) - \mathbf{B}_1\cdot\mathbf{S}_2 - \mathbf{B}_2\cdot\mathbf{S}_2, \tag{17}$$

where $-J \equiv 4t^2/U$. Thus, the spin current density is given by

$$\tilde{j}_{2\to1} \equiv \frac{J}{\hbar}\mathbf{S}_1\times\mathbf{S}_2. \tag{18}$$

The anomalous Hall effect (AHE) can lead to the rotating Hall effect; that is, by studying the anomalous Hall voltage, the spin Hall voltage and the spin current are generated by rotating electrons. The relationship between them is derived.

$$\begin{aligned}V_H &= 4R_sLj_xn_{\uparrow}\mu_B\\ V_{SH} &= 2\pi R_sLj_xn\mu_B\ ,\end{aligned} \tag{19}$$

$$\begin{aligned}j_\sigma &= V_{SH}\rho L\\ V_{sc} &= 8\pi^2R_s^2l\frac{(n\mu_B)^2}{\rho}j_x\ .\end{aligned} \tag{20}$$

The intrinsic contribution to the spin Hall effect is given as follows:

$$\sigma^{SH}_{xy} = \frac{e}{8\pi}.$$

Considering impurities and as $N_{imp}\to 0$,

$$\sigma^{SH}_{xy} = 0.$$

This cancellation is special for the Rashba model. Next, AHE and SHE are quantized with the 2D Dirac model on graphene.

$$H = v\left(k_x\sigma_x + k_y\sigma_y\right) + \Delta\sigma_z. \tag{21}$$

The energy spectrum is expressed as follows:

$$\varepsilon = \pm E_k,\quad E_k = \sqrt{\Delta^2 + v^2k^2}.$$

Also, the intrinsic Hall conductivity is expressed as follows:

$$\sigma_{xy} = -\frac{e^2}{4\pi}\frac{\Delta}{E_F},\quad E_F > \Delta.$$

With E_F as the gap, the abovementioned expression becomes

$$\sigma_{xy} = -\frac{e^2}{4\pi},\ \sigma^{SH}_{xy} = \frac{2}{e}\sigma_{xy}.$$

In the 2D case, the effective conductivity is expressed as follows:

$$\sigma^{II}_{xy} = \frac{e^2}{2}\sum_n\sum_{\mathbf{k}}f\left(E_{\mathbf{k}n}\right)\varepsilon_{ij}F_{ij}, \tag{22}$$

where “gauge field tensor” is

$$F_{ij} = \frac{\partial A_j}{\partial k_i} - \frac{\partial A_i}{\partial k_j}.$$

Also, the eigenvector gives

$$|\mathbf{k}\uparrow\rangle = \sqrt{\frac{M+\lambda(k)}{2\lambda(k)}}\begin{pmatrix}1\\ \dfrac{i\alpha\left(k_x+ik_y\right)}{M+\lambda(k)}\end{pmatrix}, \tag{23}$$

$$\mathbf{A}(\mathbf{k}) = \left(-\frac{\alpha^2k_y}{2\lambda(k)[M+\lambda(k)]}, \frac{\alpha^2k_x}{2\lambda(k)[M+\lambda(k)]}\right). \tag{24}$$

The sub-number Hall anomaly effect is to be implemented on the lattice model. The key to the fractional topological state is to realize the near-flat-band structure with a non-mean topology. Given that the strict flat band (the zero bandwidth) is non-physical in practical materials, the limit can be relaxed by only requiring the bandwidth to be much narrower than the band gap width. The topological flat-band lattice model is expected to overcome the abovementioned difficulties and implement the FQHE. In these lattice models, by adjusting the short-range transition parameters, the SOC strength, or the staggered magnetic flux, the bandwidth can be made narrower than or even close to the flat band. Based on the similarity between the energy band close to the flat band and the Landau level [6], it can be reckoned that in these flat-band models, the FQHE (or the fractional topological insulator) can exist stably considering the repulsive interaction.

In this paper, we will study in detail the 2D triangular lattice model ignoring the interaction and determine the inhomogeneous flat-band structure by adjusting the sub-nearest neighbor transition strength and the staggered magnetic flux to implement the integer quantum Hall effect (IQHE). In this model, the IQHE can exist stably due to a non-uniform magnetic field being applied with a zero net magnetic field, with the Hall conductivity equal to a topological constant. In addition, in the continuous model under the effect of the normal magnetic field, the number of the Landau levels is typically 1, while in this system, a high number, that is, a $C \geq 2$ topological flat band can be implemented.

3 Non-Abelian gauge theory for the fractional quantum Hall effect

These fractional phenomena of non-Landau energy levels define a new class of fractional topological phases or fractional Chern insulators (FCI). This work studied two situations with Chern number = 1 and 2, respectively.

At the semiconductor heterojunction interface and under the measurement condition below the temperature and above the magnetic field strength, it has been found that $\nu = \sigma_H / (e^2/h) = 1/2, 1/3 \ldots$ appears on the platform and that simultaneous longitudinal resistance is close to zero, that is, the FQHE. When $C = 1$, $\nu = 1/2$, 1/4, and 1/3, corresponding to the boson case. When $C = 2$, $\nu = 1/3$ and 1/5. In the latter case, Laughlin's fermion fractional quantum Hall state abides by the generalized Pauli exclusion principle.

L. Susskind has given a non-communicative geometric explanation about the FHE [7, 8]. Through the study into the Abelian non-exchangeability of the system values of the fermion and boson lattice systems with strong correlative interactions on topological flat bands, the Franklin theory based on Chern's theory and the filling fraction $1/n$ are exactly the same at every level. Similar to the D_0-branes described in the string theory, this theory can also be considered as the quantum theory of mapping between two non-commutative spaces Q_x and Q_y. In the toroidal structure, the FQH state has an odd or even number of quasi-degenerate ground states. There is a wide energy gap between these ground states and the high-energy excited states. The FQHE of the lattice type of the boson system is found to be different from that of the fermion system of conventional electrons, and the corresponding FQH state can be regarded as the chiral spin state in the equivalent spin model. The non-commutative theory exactly reproduces the quantitative connection between the filling fraction (level in the Chern–Simons description) and statistics required by Laughlin's theory.

The phase transition between quantum Hall fluid behavior and the Wigner crystal that occurs at a low filling fraction is a phase transition in the non-commutative Chern–Simons theory. The transition would be associated with the spontaneous breaking of the symmetry under area-preserving diffeomorphisms of real space Q_x. The variation of the gauge field vector is expressed as follows:

$$\begin{aligned}\delta A_i &= 2\pi\rho_0 \frac{\partial \Lambda}{\partial Q y_i} + \frac{\partial A_i}{\partial Q y_j} \frac{\Lambda}{\partial Q y_k} \\ &= 2\pi\rho_0 \left(\frac{\partial \Lambda}{\partial Q y_i} + \theta \{A_i, \Lambda\} \right)\end{aligned}, \tag{25}$$

where the carriers have a density of rho_0; each particle occupies the non-communicative area $\theta = 1/2\pi\rho_0$; Λ is a parameter related to gauge transformation. For quantum phase space Q_x, its conjugate momentum is proportional to its coordination; hence, it is also non-communicative.

The non-exchangeable parameter $1/eB$ ($\mathcal{B}_A$ is a substitute for $\mathcal{B}$ in anomalous situation) indicates a single flux subspace. The NC-CS theory describes the mapping between these two non-commutative spaces. It should be noted that the space Q_y is incompressible and that the function $f(Q_y)$ defined on the space Q_y is non-gauge invariant observables. In the space Q_x, we define

$$\rho(Qx) = \rho_0 - \frac{1}{2\pi} \nabla \times A. \tag{26}$$

As the layers are adiabatically brought together so that the electrons are easily shared between them, the state must approach the fractional quantum Hall state with $\nu = p/n$. Experience with D-branes suggests that the resulting theory should be a non-Abelian version of the gauge theory. A natural guess is that it may be the non-commutative Chern–Simons $U(p)$ theory at level n. The non-communicative geometrical theory means both the phase and energy band are (quasi) flat, with certain interaction between different layers. This causes the symmetry breaking; hence, Chern number $C_1 > 1$, that is, the FQHE.

The non-dissipative quantum spin current, by the Kubo formula, in the case of the SOC of the Luttinger Hamiltonian for p-type semiconductors, it is possible to define a precisely conserved spin current, that is, the non-dissipative quantum spin current [9]. For the 1/3 filled boson fractional quantum anomalous Hall state, when the boundary phase angle is adjusted, the ground state group maintains its quasi-degeneracy and a wide energy gap in the low-energy excited state, indicating that the topological phase is stable. Under the effect of $SU(2)$, the non-Abelian gauge field, its curvature tensor results in the non-dissipative spin Hall effect.

The quasi-hole excitation spectrum shows a characteristic energy gap between the excited and high-energy excited states, and there are multiple low-energy quasi-hole excited states touching at the Γ-point in each momentum partition below the characteristic energy gap. In a hole-doped semiconductor with four valence bands of spin–orbit interaction, each hole contains three quasi-cavities, and the generalized Pauli exclusion principle is incompatible with the Laughlin 1/3 fermion fractional quantum Hall state. The spin current of the two-dimensional subspace of the band can be expressed in terms of the operator P.

$$J_i = \frac{\partial H}{k_j}, \quad J_i^{ab} = \frac{1}{2} \left\{ P^l \Gamma^{ab} P^l + P^h \Gamma^{ab} P^h \right\}. \tag{27}$$

Luttinger Hamiltonian can be presented with valence bands by giving $SO(5)$ Clifford algebra. Under a certain amount of momentum, the SOC is in a fixed direction of the five-dimensional space, and the symmetry breaking can be decomposed into $SO(4) = SU(2) \times SU(2)$. This symmetry can be expressed as a conservative spin current in the light and heavy cavity bands, and its quantum response can be accurately calculated by the Kubo formula.

The Berry curvature and the multi-body number can explain the non-Abelian unipolar field, equivalent to a vector—or technically defined as momentum and true Yang-monopole—in the five-dimensional vector space. The correctness of quantum mechanical results is determined due to the entanglement of spin and velocity, a phenomenon that can be traced back to the non-commutative entanglement between the current spin operators. In physical systems, the entangled state driven by the decoherence mechanism may achieve semi-classical results. Notwithstanding the traditional definition of spin current, the semi-classical results, using the non-zero correlation between spin and velocity, combined with the terms “spin dipole” and “torque moment” in the wave packet form, can be obtained. The Kubo formula has achieved the same results.

Using a theoretical model of non-dissipative spin current, the finite longitudinal charge conductance and dissipation values associated with charge transport can be calculated [9]. The SOC system with a gap in the electron excitation spectrum results in the quantized spin Hall effect. The facts show that the integral of σ_{xy} is expressed as the gauge curvature in the occupied state and that the Fermi surface of the particle cavity excitation may not occur. The transition of spin-polarized electrons, usually described by an unbalanced Green function, can be derived from the first-principle calculation. The density function is used to calculate the steady-state electronic structure. The effect of the semi-infinite electrode is described by the self-energy function.

The spin $SU(2)$ symmetry type of the SOC model includes two types of models: Rashba and Dresselhauss. Based on this symmetry, there may exist a persistent spin helix [10], though other relaxation mechanisms may lead to its eventual decline. From the coupling of Rashba and Dresselhauss, the transition equations for arbitrary strength are provided to explain the chiral helix states. Will the chiral symmetry be preserved under anomalous circumstances?

From the analysis in the previous section, the cause of the anomalous Hall effect falls into three parts: the internal, external, and chiral effects. Since a non-Abelian gauge field is present around the Hall device with non-local features, there exits the chiral symmetry breaking in bilayer graphene, as described in the γ^5 breaking in the non-Abelian field theory, which will cause FQAH.

The gauge theory implements the basic laws of physics through local symmetry constraints. Literature [48] reported a quantum simulation of the extended U(1) lattice gauge theory and experimentally quantified the gauge invariance in a multi-body system containing matters and gauge fields. These fields are realized in an array of boron atoms in a 71-site optical superlattice. The model parameters are fully tunable, and the object–gauge interaction is calibrated by sweeping the quantum phase transition. The degree of violation of Gauss’s law is measured by extracting the probability of the local gauge invariant state from related atomic experiments. As such, a method has been provided for exploring the gauge symmetry breaking in basic FQAHE particle interaction.

The research in [11] shows that the Coulomb interaction is strong enough for the sublattice symmetry breaking to take place in undoped graphene and for the formation of a strong coupling extension in the Coulomb Hamiltonian ground state by jumping kinetic perturbation.

In a two-dimensional graphene with a hexagonal array of carbon atoms, the Coulomb interaction has the intrinsic property of interacting the relativistic Fermi subsystem with $U(4)$ symmetry. The dynamics of the continuous field theory can be described by its low-energy $(<1ev)$ action.

$$\begin{aligned} S = &\int d^3x \sum_{k=1}^{4} \bar{\psi}_k \left[\partial^t \left(i\partial_t - A_t\right) + v_F \vec{\gamma} \cdot \left(i\vec{\nabla} - \vec{A}\right)\right] \psi_k \\ &- \frac{\epsilon}{4e^2} \int d^3x F_{ab} \frac{1}{2\sqrt{-\partial^2}} F^{ab} \end{aligned}, \tag{28}$$

where the integral is taken over the Q_x plane; v_F is the velocity of the massless electron in graphene; γ is a Dirac matrix in quantum field theory (for the band matrix using Γ and γ_B to present); the superscript t means a hopping term; F_{ab} is the gauge field term. Herein, non-dimensional parameters can be used to perform extensions that can be renormalized with a parameter $\frac{1}{N}$.

Further generalizing the previous expression to a strong coupling field, we have two terms of Hamilton: a hopping term and a Coulomb interaction term. The generation and annihilation operators of an electron are denoted by $\psi^{\dagger}_{\sigma,n}$ and $\psi_{\sigma,n}$, respectively. The state has two rotation states, identified by ↑ or ↓ for a rotating spin label as σ, on either A or B sublattice. The parameter u_0 is the on-site self-energy of the electron and the hole [11].

$$\begin{aligned} H &= H_t + H_e \\ H_t &= t \sum_{A,i,\sigma} \left(\psi^{\dagger}_{\sigma,A+s_i} \psi_{\sigma,A} + \psi^{\dagger}_{\sigma,A} \psi_{\sigma,A+s_i}\right) \\ H_e &= \frac{e^2}{8\pi\epsilon a} \sum_n u_0 \rho_n^2 + \frac{e^2}{8\pi\epsilon a} \sum_{n \neq n'} \rho_n \frac{1}{|n - n'|} \end{aligned}. \tag{29}$$

The lattice translation symmetry breaking is spontaneously related to some sort of gap generation. The symmetry breaking parameter can be expressed as the following operator’s mathematical expectation:

$$H_m = \left(\sum_{n \in A} - \sum_{n \in B}\right) \left[\mu_0 \psi^{\dagger}_{\sigma,n} + \vec{\mu} \cdot \psi^{\dagger}_{\sigma,n} \vec{\sigma}_{\sigma\sigma'} \psi_{\sigma',n}\right]. \tag{30}$$

This mass term is constant at time reversal and flat valence, but the $U(4)$ pattern of symmetry breaking is formed by the fermion surface state and the chiral Landau level of the magnetic field Weyl semimetal film. If the parameters of μ are non-zero,

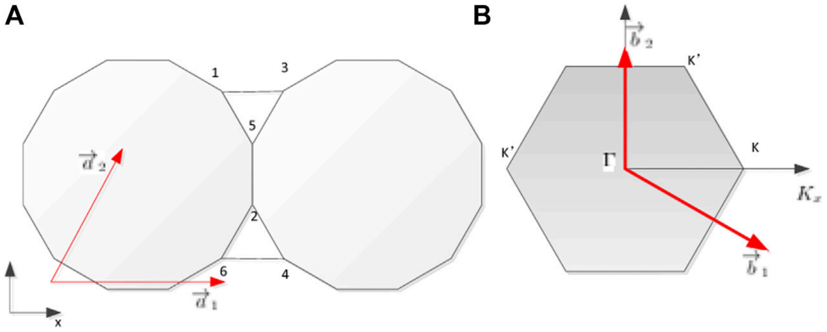


FIGURE 1
(A) Star-like lattice with primitive vectors of the Bravais lattice and **(B)** reciprocal vectors.

the symmetry breaking forms $U(4) \to U(1)$ pattern, only one of which is zero, hence, the $U(4) \to U(2) \times U(2)$ pattern.

Within a fairly wide range of resonant potentials, changing the strength of the binding potential makes no difference to the edge excitation sequence, which also shows the topological stability of the quantum Hall state. The ground state approximation to the complete Hamiltonian has been found, with the Coulomb energy usually greater than the kinetic energy of the electron. By integrating over the Brillouin region, the charge density of the diagonal energy is obtained.

$$H_e = \frac{e^2}{4\pi\epsilon a}\int d^2k|\hat{\rho}(k)|^2\left(\frac{u_0}{2}+ \sum_{n\neq 0,n\in A} e^{ik\cdot n}\left[\frac{1}{|n|}+\frac{\cos k}{|n+s_1|}\right]\right). \tag{31}$$

The perturbation theory is applied to calculate Hamilton's effect, with the finding that the lower energy state is an antiferromagnetic state. While Hamiltonian for the degenerate ground states proves effective as

$$\begin{aligned} H_{eff} &= -H_t\frac{1}{H_e}H_t \\ &= \frac{-t^2}{\frac{e^2}{4\pi\epsilon a}(u_0-1)}\sum_{A,s_i,\sigma}\left(\psi^\dagger_{\sigma,A+s_i}\psi_{\sigma,A}\psi^\dagger_{\sigma,A}\psi_{\sigma,A+s_i}\right. \\ &\left.+\psi^\dagger_{\sigma,A}\psi_{\sigma,A+s_i}\psi^\dagger_{\sigma,A+s_i}\psi_{\sigma,A}\right) \end{aligned} \tag{32}$$

The abovementioned equation can be simplified through the Pauli matrix. The Haldane–Bose–Hubbard model is used to describe the ground state and its low-energy dynamics. The topological flat-band model is an extended version of the Haldane model. At least one band has a non-mean topology, that is, a non-zero Chern number $C = 1$; each band has a narrow bandwidth; and there is a wide gap between the bands. For the cellular lattice Haldane model, if only the nearest neighbor and the next nearest neighbor are allowed to jump, the flatness ratio is only 7; if the next nearest neighbor jump is allowed, a large class of parameter space can be found by numerical search in the non-zero number of topological flat bands.

Each location corresponds to the basic excited state of an electronic lattice, whose energy is expressed as U and is approximately 10 ev.

The Hubbard model interaction discloses many properties of graphene, especially its sublattice symmetry breaking ground state is an antiferromagnetic Mott insulator. Illustrations are provided on both the quantum phase diagram of the top half of the top-filled fill and also on the quantum phase transition from the FQAH state to other symmetrically fractured phases. Derived from the strong correlative effect of hard bosons (unlike the Coulomb interaction between conventional electron or fermion systems), the lattice type of the FQHE of the boson system can be regarded as a chiral symmetry in an equivalent spin model.Meanwhile, most theories and experience predict the fractional quantum anomalous Hall effect (FQAHE) on lattice structures, such as the honeycomb or quantum flux state, which is also known as the topological nematic state. In the topological flat-band model, considering the short-range interaction between the hard boson systems, a large number of numerical calculations and systematic theoretical analysis have provided strong evidence for lattice FQHE [12]. In the toroidal structure, the fractional quantum anomalous Hall state has an even number of quasi-degenerate ground states that share a quantized number, with wide energy gaps between the excited states.

The quantum Hall effect is a dissipation-free quantum transport property caused by the quantization of the Landau level under an externally enhanced magnetic field. At present, the quantum anomalous Hall effect that has been proposed or realized is concentrated in the small Chern number system with a Chern number of 1 (based on magnetic topological insulator films) or 2 (based on single-layer graphene), and the size of the Chern number directly corresponds to the quantum. The number of channels and the status of the low Chen number also significantly affect the working efficiency of quantum anomalous Hall devices.

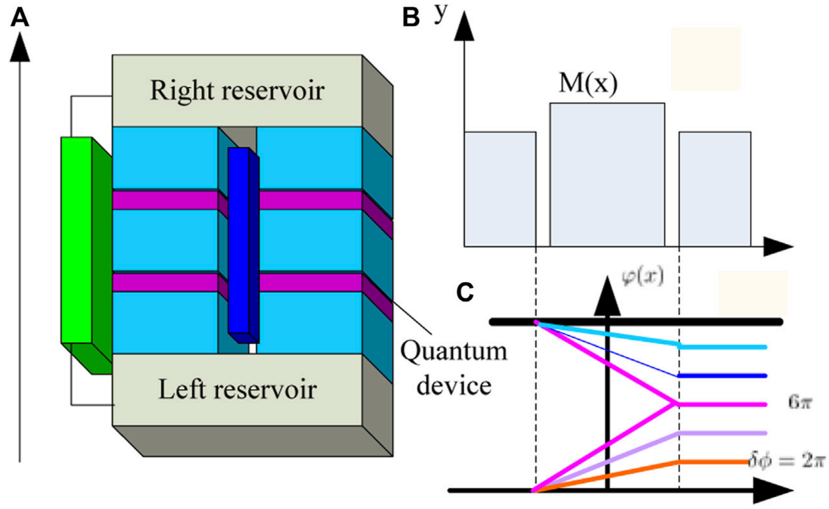


FIGURE 2
(A) Schematic of the three-dimensional quantum device interface with two-layer localized system evolution with a coupling scale factor. **(B)** Pairing spatial profile for amplitude and tunneling strength M(x) induced by the superconductors and insulator. **(C)** Energy band and band gap diagram along the high-symmetry line.

The first Chern number is defined as $C_1 = \int d^2\mathbf{k} f_{xy}(\mathbf{k})$ with $f_{xy}(\mathbf{k}) = \partial_\mathbf{x}\mathbf{A}_\mathbf{y} - \partial\mathbf{A}_\mathbf{x}$ and $A_i(\mathbf{k}) = -\mathbf{i} \sum_{\mathbf{En<Ef}} \langle n,\mathbf{k}|\partial_\mathbf{i}|\mathbf{n},\mathbf{k}\rangle$, and the QAHE is described in terms of the nontrivial Chern number.

By calculating the Berry curvature distribution, the quantized five Chern numbers are found to be $C_1 = -1$, 2, 1, 1, and 2, respectively, with the Fermi level lying in these five gaps. In a general quantum anomalous Hall system, a honeycombed Kagome lattice structure can be obtained, where there exists a near-flat band with $C_1 = 1$. The FQAHE may be implemented. The zigzag star-like lattice has chiral edge states, which endow the system with topological properties.

With respect to the hopping of

$$H = t\sum_{A,i}\left(\psi^\dagger_{A+s_i}\psi_A + \psi^\dagger_A\psi_{A+s_i}\right) + \frac{U}{2}\sum_{n\in A,B}\left(\sum_{\sigma=\uparrow\uparrow\downarrow}\psi^\dagger_{\sigma n}\psi_{\sigma n} - 1\right)^2, \tag{33}$$

there are two terms in Figure 1. Assuming that the magnitude of the jump between adjacent points takes the same value within each of the triangles t_1 and t_2 as between them, with $t_2 < \frac{3}{2}t_1$, the probability that the electrons jump out of each of the triangles is less than the probability of jumping between the triangles. This assumption means that the three points can be strongly combined into one single point. The result in this case is similar to that in the case of graphene in the low-energy band, which is similar to the Kagome lattice in the opposite case with $t_2 < \frac{3}{2}t_1$. At this point, $t_2 = t_1$ will cause the gap to shrink. In the absence of Rashba SOC and exchange fields, the six-site cells form six bands with double degradation.

For the Berry curvature and multi-body calculations, the boundary phases θ_1 and θ_2 are introduced in two directions of periodic boundary conditions, and the number of quantum multi-body states (the corresponding Berry phase $2\pi C$) is obtained by integrating throughout the boundary phase space. $C = \frac{1}{2\pi}\iint d\theta_1 d\theta_2 F(\theta_1,\theta_2)$, Berry curvature. $F(\theta_1,\theta_2) = \mathrm{Im}(\langle\frac{\partial\Psi}{\partial\theta_2} \mid \frac{\partial\Psi}{\partial\theta_1}\rangle - \langle\frac{\partial\Psi}{\partial\theta_1} \mid \frac{\partial\Psi}{\partial\theta_2}\rangle)$.

For $N_s = 24$, 36, and 40 lattices, the two ground states in the quasi-degenerate ground state group are in separate momentum partitions. As the boundary phase is adjusted, the two ground states evolve and cross the energy levels, but there remains a wide characteristic energy gap between these ground states with the low-energy excited states. For $N_s = 32$ lattices, the two ground states in the quasi-degenerate ground state group are at momentum partitions; as the boundary phase is adjusted, each ground state evolves to itself and avoids crossing energy levels. In the case where the two ground states are in separate momentum partitions, numerical calculations show that each ground state contributes almost equally to the Berry phase of π, that is, provided the total number of turns $C = 1$, each ground state corresponds to a fractional number of 1/2. In the case where the two ground states are in the same momentum partition, numerical calculations show that one of the ground states contributes a Berry phase of 2π, while the other contributes a Berry phase of zero; still, provided the total number of turns $C = 1$, each ground state is the average of Chern number, 1/2.

Generally, the filling factor and the Chern number can be related by $\nu = k/(C_1 + 1)$ [20], where k is the wave number. From recent research reports [13–22], it can be known that the FQAHE exists with fill numbers 1/2, 1/3, 2/5, 4/5, 5/2, and 7/2.

4 Wannier's function of the fractional quantum Hall effect

For the extended Haldane model with topological flat bands, the three-body hardcore bosons filled with strong correlative interactions were studied, with the discovery of the non-Abelian type (non-Abelian) quantum Hall effect. The non-Abelian quantum Hall effect of this lattice type has characteristic triplet ground state topological degeneracy, a quantized Chern number, a wider characteristic energy gap, a characteristic quasi-hole excitation spectrum, and a number of particles with topological degeneracy parity effect. The non-Abelian quantum Hall effect of bosons discovered by the author has similar topological properties to the Moore-Read state filled with Landau level 5/2. In contrast, the image of the Fermi-type and Moore-Read states in the two-dimensional electron gas has not been fully created so far. There remain some differences and disputes between numerical calculation and theoretical analysis.

For quasi-hole fraction statistics, since the Laughlin wave single-particle and the many-body function for FQH states are not directly connected with FQAH states, the quasi-hole states in non-Abelian quantum anomalous Hall phases can be counted by the generalized Pauli exclusion principle. Using the Wannier representation of the topological flat band, a $N_{orb} = N_s/2$ periodic single-particle orbit is formed. Now, take $N_{orb} = 12$ as an example. The number of bosons occupied in two consecutive orbits does not exceed two, and the generalized Pauli exclusion principle gives the following three configurations of ground state distribution $|n_{\lambda_1}, n_{\lambda_2}, \ldots, n_{\lambda_{N_{orb}}}\rangle$: $(02) \equiv |02020202\rangle, (20) \equiv |202020202020\rangle$ and $(11) \equiv |11111111\rangle$. Now, count the number of bosons from the three ground state configurations (02), (20), and (11). The occupancy configuration of the double quasi-hole state of the boson should be a mixture of two ground-state configurations that forms two domain walls, each of which represents a fractional charge of 1/2. A simple analysis gives six configurations with an odd number of 1 s: $|\ldots 20|1|020 \ldots\rangle, |\ldots 20|111|020 \ldots\rangle, |\ldots 020|11111\ |020 \ldots\rangle, \ldots$, and $|0|11111111111\rangle$. Two of the domain walls (quasi-holes) are represented by two vertical lines (‖). Considering the 12 translations of the abovementioned six configurations, there are finally 72 (generally $N_{orb} = N_s/2$) double quasi-cavity states in total. This count is completely consistent with the numerical calculation results. In the band calculated by DFT, the construction of a tightly bound Hamiltonian is implemented with the help of the largest localized Wannier function (ML-WF).

Through the Brillouin zone, the wavefunction cannot be regarded as single valued; then, unidimensional Wannier functions are maximally localized in the y direction by taking the eigenstates of k_y on y. Let the occupied band of a QAH system be $|k_x, k_y\rangle$, with the Berry phase gauge field vector A_i, $A_y = 0$, the Wannier function with local maximization has explicit form [23].

$$\left|W\left(k_y, x\right)\right\rangle = \frac{1}{\sqrt{L_x}} \sum_{k_x} e^{-i\int_0^{k_x} A_x\left(p_x, k_y\right) dp_x} \cdot e^{-ik_x\left(x - \frac{\theta\left(k_y\right)}{2\pi}\right)} \left|k_x, k_y\right\rangle, \tag{34}$$

where p_x , p_y are the branches of the projection operator on each coordinate. For lattice sites' labels,

$$\theta\left(k_y\right) = \int_0^{2\pi} A_x\left(p_z, y_k\right) dp_x, x \in \mathbf{Z},$$

the phase factor $e^{i\theta(k_y)k_x/2\pi}$ of the Bloch function is periodically guaranteed with $k_x \to k_x + 2\pi$. Hence, the Wannier function satisfies the following warp boundary condition:

$$\left|W\left(k_y + 2\pi, x\right)\right\rangle = \left|W\left(k_y, x + C_1\right)\right\rangle. \tag{35}$$

This method can be easily extended to more general FQAH states such as the Moore-Read state of non-Abelian quasiparticles, thus determining the various topological properties of the fractional quantum anomalous Hall (FCI/FQAH) state. Considering that the fractional quantum anomalous Hall (FCI/FQAH) state is first realized in the optical lattice cold atomic system, a feasible experimental detection method can also be devised for edge excitation. The edge space excitation spectrum in dish geometry is found in the real space strict diagonalization (ED) calculation, and similar results are obtained based on the study of the quantum entanglement spectrum [23]. In the hard boson-filled Haldane dish model and the Kagome lattice dish model, a series of characteristic edge excitation spectra have been found consistent with the chiral Luttinger liquid theory. By inserting and adjusting the magnetic flux in the center of the dish structure, it is further verified that the compressibility of the excited state is indeed the chiral edge state of the carrying current. Within the particular lattice structure of this system, the intrinsic and additional Rashba SOCs compete with each other, allowing one to adjust the number and position of Dirac cones. When the time inversion invariance is no longer preserved, the energy band structure of the system will exhibit various QAHEs with distinct Chern numbers ($C_1 > 1$).

It is also predicted that a large number of turns can be achieved in a magnetic three-dimensional topological insulator film, in which case the film system needs to jump out of two-dimensional limitations. Under two-dimensional constraints, the number of QAHEs derived from the direct coupling of the upper and lower surface states of the sample is the minimum. When the film is thicker, the conduction band energy band and the valence band energy band, which are constrained in two directions, will cause multiple band inversions under the influence of the coupling between the Zeeman field and the spin–orbit, with the state $|FTI\rangle = |1/m, \uparrow\rangle \otimes |-1/m, \downarrow\rangle$. Therefore, the number of QAHEs strongly depends on the relative size between the Zeeman field and the sample thickness, which determines the spacing between the sub-bands. For samples of different thicknesses, increasing the Zeeman field strength can increase the number of turns to a larger integer, which is contrary to the fact that the Hall conductivity of the general quantum Hall effect decreases as the magnetic field strength increases.

Another way to build a local Wannier function is to use the largest localization method proposed by Marzari and Vanderbilt. In this method, they introduce a local function to strictly define the locality of the Wannier function and transform the matrix $U(N)$ by optimizing the specification so that the local function reaches a minimum. Then, generalize the expression of the maximally localized Wannier function with N occupied bands [23]:

$$\begin{aligned}\left|W^i\left(k_y, x\right)\right\rangle = \frac{1}{\sqrt{L_x}} \sum_{k_x,m,n} e^{-ik_x\left(x-\frac{\theta_i\left(k_y\right)}{2\pi}\right)} u_m^i \\ \cdot\left[Pe^{-i\int_0^{k_x} A_x\left(p_x,k_y\right)dp_x}\right]_{mn} \left|n, k_x, k_y\right\rangle\end{aligned} . \tag{36}$$

With $e^{i\theta_n(k_y)}$, $\quad i = 1, 2, \ldots, N$, they are the eigenvalues of Wilson's loop operator (inside []) and u_m^i the corresponding eigenstates. Here, $A_x(p_x, k_x)^{mn}$ is the gauge field vector of the Berry curvature.

For the multilayer FQAH system with $C_1 = 2$, $|W(k_y + 2\pi, n)\rangle = |W(k_y, n + 2)\rangle$. We will see that all components of the stretch function can be represented by overlapping matrices. In practical calculations, each overlap matrix needs to be given from the first-principle calculation.

$$\begin{aligned}\left|W^1_{K=k_y+2\pi n}\right\rangle = \left|W\left(K_y, 2n-1\right)\right\rangle \\ \left|W^2_{K=k_y+2\pi n}\right\rangle = \left|W\left(k_y, 2n\right)\right\rangle\end{aligned} \tag{37}$$

such that both the parameters K and $|W_K^{1,2}\rangle$ are continuous and that the contributions of all components of the broadening function in the x direction are interrelated.

Multilayer FQH states can exhibit a great diversity of topological states. The wavefunction of Laughlin states at states (mnl) can be expressed as follows [24]:

$$\begin{aligned}\Psi(\{z_i\}, \{w_i\}) = \prod_{i<j}\left(z_i - z_j\right)^m\left(w_i - w_j\right)^n \\ \prod_{i,j}\left(z_i - z_j\right)^l \cdot \left[-\sum_i\left(|z_i|^2 + |w_i|^2\right)\Big/4l_B^2\right],\end{aligned} \tag{38}$$

where l_B is the magnetic length in each layer; z_i and w_i are the ith particle's complex coordinates, which are intrinsically in the non-Abelian states for multilayer.

In the actual calculation process of two-layer FQAH, the Bloch wavefunction is usually projected onto some appropriate local orbits and used as the initial value of the maximum localization process. T_x and T_y, in the Wannier states, are given by [25]

$$\begin{aligned}T_x\left|W_K^1\right\rangle = \left|W_K^2\right\rangle, \quad T_x\left|W_K^2\right\rangle = \left|W_{K+2\pi}^1\right\rangle \\ T_y\left|W_K^a\right\rangle = e^{iK}\left|W_K^a\right\rangle\end{aligned} . \tag{39}$$

We calculated the electronic structure of the interfacial region and its evolution with the interface coupling scale factor. For the two subsystems that are not coupled, we found that the QSH insulator had a one-dimensional Dirac edge state, while the edge of the QAH insulator, with a number $C = 2$, had two edge states with chiral edge states. The valence band of the energy valley position (K and K') and the energy gap state of the conduction band construct the two QAH edge states. They have the same spin polarization but are localized in the K or K′ energy valley. The torus with the misaligned layer can be connected by the "wormhole" of the branch cutting, and it has a nontrivial topological degeneracy [26].

The topological degeneracy from the edge state can also be explained by chiral symmetry breaking, since hardcore bosons have been filled into the Haldane dish model and the Kagome lattice dish model, and a series of characteristic edge excitation spectra have been found, which is consistent with the chiral Luttinger liquid theory. By inserting and adjusting the magnetic flux in the center of the dish structure, it is further verified that the compressibility of these excited states is indeed the chiral edge state of the carrying current. Let N_0 be the number of all possible states, (mnl) are the Laughlin states in Eq. 39. Then, the topological degeneracy of pairs of dislocations is as follows [27]:

$$N = \frac{N_0}{(m+1)^{2n-1}} = \left|\left(m^2 - l^2\right)(m - l)^{n-1}\right|. \tag{40}$$

The two oppositely polarized interfacial states are localized in two energy valleys that are far apart in the momentum space. That is to say, the formation of the QSH/HQAH interface makes the spin polarization of the interfacial state dependent on the energy valley, with $d = \sqrt{m}$ as the quantum dimension. The coupling of spin and energy physics for the interface makes it possible to distinguish the energy of the valley by controlling the degree of spin freedom [28].

The effective Hamiltonian of the interface system is constructed directly from the Wannier Hamiltonian of two individual materials using the effect term $U(2)$. Finally, we use the Green function method for interfaces to calculate the local state density of the interfacial region. It is noteworthy that when the Wannier function is generated to handle interface problems, Wannier-based functions in two systems should be selected as consistently as possible. Only in this way can the coupling matrix of the material passing through the interface be well defined as $U(1) \times U(1)$ by Chern–Simons theory [29]. Therefore, we used the projected atomic orbital Wannier function and rejected the maximum localization process. Using the vacuum level as a reference, we aligned the valence bands of two bulk materials in the interface system to a uniform Fermi energy [30].

As a new topological quantum state, quantum anomalous Hall insulators (Chern insulators) have attracted wide attention due to their unique edge state characteristics. Combining the first-principle calculation method and the tight-binding model based on the Wannier function, we prove that SOC can transform a typical semi-Dirac system, namely, TiO2/VO2 composite structure, into a quantum anomalous Hall insulator, with the further discovery that there is only one special type[31].

This transformation can only be implemented in the semi-Dirac system. Unlike the usual semi-Dirac spectrum, temporarily called the second type of semi-Dirac spectrum, that system can actually be regarded as a combination of three common Dirac cones. Our results reveal the non-mean topological properties of this type of semi-Dirac system and provide new ideas and approaches for implementing QAHEs in real systems [32]. In addition, we have proposed other composite systems that can implement Chern insulation. These solutions are expected to not only to create new possibilities for developing more accessible, higher temperature Chern insulators but also to lay a necessary material basis for designing topological quantum devices [33].

Due to the unique Dirac cone surface state that not only has topological insulators become a research hotspot in condensed matter physics and material science, but they also promise potential application prospects in low-energy electronic devices. Therefore, once the topological insulator phase can be realized in the traditional III–V semiconductor, it will be of great significance to spintronic applications and quantum computing methods. We propose a universal strategy for implementing topological insulators in III–V semiconductors by means of helium atom doping and applied stress. Using the first-principle method based on the maximum localized Wannier function to directly calculate the $\mathbf{Z}_2$ topological invariants and surface states of the system, we find that under applied stress, AlBi (GaBi and InBi) can serve as topological insulators (semimetals). We further demonstrate that erbium doping can induce topological phase transitions in traditional III–V semiconductors such as GaAs semiconductors. In view of the maturity of modern technology in the semiconductor industry and the wide application of III–V semiconductors in electronic devices, our proposed method provides new design ideas for the preparation of large-scale topological insulator electronic devices that are easy to integrate and control [34].

By studying the interface between quantum spins and quantum anomalous Hall insulators and analyzing the effective model, we find that there are stable and specific chiral topological interfacial states at the interface between the two. Using the tight-binding model and the first-principle calculation based on the maximum localized Wannier function, we move on to systematically analyze the unique properties of the interfacial state between quantum spin Hall insulators and different quantum anomalous Hall insulators, including single-energy valley QAH [14], the multi-energy valley high number QAH, and valley-polarized QAH insulators. Despite the existence of topological interfaces on these interfaces, they have different specific behaviors. Since the interface exists between two materials, its state is naturally protected from the effects of edge defects, chemical modifications, and the like. Therefore, the interfacial state should be more stable and less sensitive to external disturbances than the surface state. Our results have not only gained an important understanding of the topological properties of materials but also provided a possible way to enhance the performance and stability of topological electronic devices in real-world environments [35–40].

5 Multilayer fractional quantum Hall effect model

We propose an approach to implement the multilayer FQAH model. The top and bottom sides are connected to two external charge reservoirs. The quantum devices have two TI layers with different chiral properties and FQAHE at their edge. The wave vector is fixed somewhere in the y direction, with periodic phases in the x direction, which can be expanded by the Wannier function to create a band gap due to the intrinsic topological invariant, hence, the FQAH nematic state. Now, the device can be divided into two parts, as shown in Figure 2, the one on the left side $g < 0$ and the other on the right side $g > 0$ (g is the Landau factor). The two sides are connected by a quantum wire matrix (the blue block) to change Majorana fermions.In the case of bilayer graphene, expand the Hamiltonian, considering the effects of Rashba SOC α, intrinsic exchange field M, and imbalance $U(\tau)$ means the Pauli matrix of the layer degrees of freedom [28].

$$\begin{aligned} H = &\left[v\sigma\cdot\mathbf{k}\psi_{\mathbf{s}} + \mathbf{M}\psi_{\sigma+\mathrm{sz}} + \left(\frac{\alpha_1+\alpha_{\mathbf{h}}}{2}\right)(\sigma\times\mathbf{s})_{\mathbf{z}}\right]\psi_\tau \\ &+\left[(\alpha_l-\alpha_h)(\sigma\times\mathbf{s})_{\mathbf{z}} + \mathbf{U}\psi_{\sigma+\mathbf{s}}\right]\tau_z \\ &+\frac{1}{2}t_\perp\psi_s\left({}_x\tau_x+\sigma_y\tau_y\right) \end{aligned} . \tag{41}$$

Subject to the boundary condition $\psi(y=0,L)=0$ and according to the calculation from [28–34], l is the energy dispersion in terms of λ.

$$\begin{aligned} \epsilon = \mu\{&M^2 + v^2\left(k_x^2-\lambda\right) + 2\alpha^2 \\ &+2s\sqrt{\alpha^4 + v^2\left(k_x^2-\lambda^2\right)\left(M^2+\alpha^2\right)}\,\Big\}^{1/2}. \end{aligned} \tag{42}$$

The magnetic heterostructures in which two sub-monolayers of transition metals embedded in the semiconductor TI host form the ferromagnetic delta (δ)-layers within which there may appear two distinct types of in-gap bound states: the symmetric and antisymmetric states. The symmetric state is a one-to-one correspondence to the origin of the convenient confinement states of carriers at interface insertions in traditional semiconductor-layered structures, while the antisymmetric state is a close analogy to the topological surface states attributed to the Z_2 invariant for TI [41–45]. The latter emerges near the δ layer, where the topological invariance is locally destroyed, and the antisymmetric state represents the anomalous topological properties of the host material [46–50].

Therefore, it is feasible to design a control gate for quantum spin transport on the clean surface holding the helical electrons.

The essential advantage of this mechanism is that the time reversal symmetry breaking and the helical state gapping are achieved on the surface [51, 52].

6 Conclusion and discussion

In this paper, we have discussed the cause of FQAH with a non-Abelian quantum field theory. We have also investigated the physical reliability of a FQAH device. The spontaneously topological chiral symmetry breaking of fermions hopping on a honeycomb lattice in the presence of a synthetic non-Abelian gauge potential has been identified as the cause of FQAH. The topological quantum Berry phase transition indicates the hopping of sublattice and the Coulomb energy through interaction between many-body particles causes a pre-formed band inversion in the band structure. With the integration on continuous breaking, the non-locality symmetry breaking of the Higgs field will affect the band topological phase property and the gap amplitude in a way that will engender different energy level platforms with distinct phase shifting.

A novel type of the FQHE is found on the topological flat belt. The VASP simulation and experiment have shown the following items: the topologically quasi-degenerate ground state group, topologically stable characteristic energy gap, the characteristic momentum correlation of the ground state group, the topological evolution of the ground state group, the smooth Berry curvature, fractional Hall conductivity (or fractional aging number), quasi-hole excited fractional charge statistics, and chiral edge excitation. This effect is distinct from the continuous FQHE on the traditional Landau level. Without requiring any external magnetic field, it has a large characteristic energy gap and can exist at higher temperatures. It does not require a single-particle Landau level and cannot be used in conventional ways. The Laughlin wave function describes these fractional phenomena with no external magnetic field and no Landau energy levels and defines a new class of fractional topological phases, also known as fractional insulators. The fractional quantum Hall effect is also called the fractional quantum anomalous Hall effect.

Some possible theoretical research directions are outlined as follows: proposal of other topological flat belt models, including a better topological flat-belt model with high Chern numbers and a lattice model with multiple topological flat belts at the same time; exploration into the abnormal edges of fractional topological phases on topological flat belts excitation; exploration into Abelian and non-Abelian fractional statistics on topological flat belts; exploration into singular fraction statistics and edge excitations on topological flat belts with high Chern numbers; exploration into possible fractional superconducting phases and superfluid phases; a qualitative and quantitative comparative study on the numerical wavefunction and analytical wavefunction of the FQHE on the topological flat belt; exploration into the topological order and the superfluid phase, the solid phase, and the topological quantum phase change characteristics. Experimental research in this field is in more urgent need of working out how to realize topological flat bands in condensed matter materials and in cold atom optical lattices, how to realize fractional quantum anomalous Hall states in both types of systems, how to detect the exact topological order, and how to detect the fractionalization.

A recent systematic experiment found that the quantum anomalous Hall effect with different Chern numbers can be achieved by regulating the magnetization direction of a single-layer transition metal oxide material by applying a weak magnetic field. At the Fermi level, both materials have six spin-polarized Dirac points. After introducing spin–orbit coupling, each Dirac point contributes half a quantized Hall conductance, but in different directions. When the magnetization direction is in-plane and the vertical mirror symmetry is broken, four Dirac points have the same Berry curvature, and the remaining two Dirac points have opposite Berry curvatures; at this time, the system has a Chern number of 1. This constitutes an integer order quantum anomalous Hall effect. When the magnetization direction deviates from the system plane, the six Dirac points contribute to the same direction of the Berry curvature. At this time, the system has a quantum anomalous Hall effect with a Chen number of 3. This experiment not only provides a new material platform to study the quantum anomalous Hall effect but more importantly reveals the existence of the quantum anomalous Hall effect with tunable Chen number (i.e., fractional order) and its physical causes.

Data availability statement

The original contributions presented in the study are included in the article/Supplementary Material; further inquiries can be directed to the corresponding author.

Author contributions

All authors listed have made a substantial, direct, and intellectual contribution to the work and approved it for publication.

Conflict of interest

JS, WD, XS, JW, YW, and HL were employed by State Grid Wind and Solar Energy Storage and Transportation New Energy Co., Ltd.

Publisher's note

All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors, and the reviewers. Any product that may be evaluated in this article, or claim that may be made by its manufacturer, is not guaranteed or endorsed by the publisher.

References

1. Bernevig BA, Hughes TL, Zhang S-C. Quantum spin Hall ef-fect and topological phase transition in HgTe quantum wells. *Science* (2006) 314(5806): 1757–61. [2010-03-25]. doi:10.1126/science.1133734

2. Quantized Anomalous Hall Effect in; Mag-netic Topological Insulators Rui YuZhang HJ, Zhang SC, Dai X, Fang Z. Quantized anomalous Hall effect in magnetic topological insulators. *Science* (2010) 329:61–4. doi:10.1126/science.1187485

3. Zhang J, Chang CZ, Tang P, Zhang Z, Feng X, Li K, et al. Topology-driven magnetic quantum phase transition in topological insulators. *Science* (2013) 339: 1582–6. doi:10.1126/science.1230905

4. Stagraczynski S, Chotorlishvili L, Dugaev VK, Jia CL, Ernst A, Komnik A, et al. Topological insulator in a helicoidal magnetization field. *Phys Rev B* (2016) 94(1-17):174436. doi:10.1103/physrevb.94.174436

5. Sinitsyn NA. *Anomalous Hall effect in 2D Dirac band: Link between kubo-streda formula and semiclassical Boltzmann equa-tion approach* (2011). arXiv: cond-mat/0608682v3.

6. Dugaev VK. *Nonlinear anomalous Hall effect and negative magnetoresistance in a system with random Rashba field* (2011). arXiv:1211.5304v1.

7. Hou BY. *Differential geometry for physics*. Beijing: Science press (2004). p. 689–703.

8. Susskind L. *The quantum Hall fluid and non-commutative chern simons theory* (2001). arXiv:hep-th/0101029v3.

9. Murakami S, Nagaosa N, Zhang SC. *SU(2) non-abelian holonomy and dissipationless spin current in semiconductors* (2011). arXiv:cond-mat/0310005.

10. Bernevig BA, Zhang SC. An exact SU(2) symmetry and persistent spin helix in a spin-orbit coupled system" phys. *Rev Lett* (2006) 97:236601.

11. Semenoff GW. *Chiral symmetry breaking in graphene* (2011). arXiv: 1108.2945v2.

12. Chen M, Wan S. *Quantum anomalous Hall effect on star lattice with spin-orbit coupling and exchange field* (2012). arXiv:1203.2855v2 [cond-mat.str-el].

13. Goerbig MO. *From fractional chern insu-lators to a fractional quantum spin Hall effect* (2011). arXiv: 1107. 1986 v3.

14. Clarke DJ, Alicea J, Shtengel K. *Exotic non-Abelian anyons from conventional fractional quantum Hall states zero* (2011). arXiv:1204.5479v1.

15. Liu X, Wang Z, Xie XC, Yu Y. *Abelian and non-abelian anyons in integer quantum anomalous Hall effect and topological phase transitions via superconducting proximity effect* (2011). arXiv:1011.3885v4.

16. Ryu S, Moore JE, Ludwig AWW. *Elec-tromagnetic and gravitational responses and anomalies in topological insulators and su-perconductors* (2011). arXiv:1010.0936v2.

17. Carrega M, Ferraro D, Braggio A, Magnoli N, Sassetti M. *Anomalous charge tunneling in the fractional quantum Hall edge states at filling factor = 5/2* (2011). arXiv:1102.5666v2.

18. Liu Y, Kamburov D, Shayegan M, Pfeier LN, West KW, Baldwin KW. *Anomalous robustness of the = 5/2 frac-tional quantum Hall state near a sharp phase boundary* (2011). arXiv:1106.0089v3.

19. Luo W-W, Chen W-C, Wang Y-F. *Chang-de gong "edge excitations in fractional chern insulators* (2011). arXiv:1304.4338v1.

20. Sterdyniak A, Repellin1 C, Andrei Bernevig B, Regnault N. *Series of abelian and non-abelian states in C > 1 fractional chern insulators* (2011). arXiv:1207.6385v1.

21. Zhao L, Emil J. *Bergholtz "From fractional Chern insulators to Abelian and non-Abelian fractional quantum Hall states: Adiabatic continuity and orbital entanglement spec-trum* (2011). arXiv:1209.5310v2.

22. Gabriel D, Lima LS, Dias SA. *Edge modes in the fractional quantum Hall effect without extra edge fermions* (2011). arXiv:0910.3661v7.

23. Qi XL. Generic wavefunction description of fractional quantum anomalous Hall states and fractional topological insulators. *Phys Rev Let* (2011). arXiv:1105.4298v1.

24. Barkeshli M, Qi XL. *Topological nematic states and non-Abelian lattice dislocations* (2011). arXiv:1112.3311v2.

25. Hinarejos M, Perez1 A, Banuls MC. *Wig-ner function for a particle in an infinite lat-tice* (2011). doi:10.1088/1367-2630/14/10/103009

26. Vetsigian K. *Chern-simons theory of fractional quantum Hall effect* (2011).

27. Steuernagel O, Kakofengitis D, Ritter G. *Wigner flow reveals topological order in quantum phase space dynamics* (2011). arXiv:1208.2970v2.

28. Tse GWK, Qiao ZH, Yao YG, MacDonaldNiu AHQ. *Quantum anom-alous Hall effect in single-layer and bilayer* (2011). arXiv:1101.2042v2.

29. Qi X-L, Hughes TL, Zhang S-C. *Chiral topological superconductor from the quantum Hall state* (2011). arXiv:1003.5448v1.

30. Sacramento PD, Arajo MAN, Vieira1 VR, Dugaev VK, Barnas J. *Anoma-lous Hall effect in superconductors with spin-orbit interaction* (2011). arXiv:1111.6748v1.

31. Liu S, Yu-Zhen Y, Hu L-B. Characteristics of anomalous Hall effect in spin-polarized two-dimensional electron gases in the presence of both intrinsic, extrinsic, and external electric-field induced spin orbit couplings" Chin. *Phys B* (2012) 21:027201.

32. Li T. *Spontaneous quantum Hall effect in quarter doped Hubbard model on honey-comb lattice and its possible realization in quarter doped graphene system* (2011). arXiv:1103.2420v1.

33. Qi X-L, Zhang S-C. *Topological insulators and superconductors* (2011). arXiv: 1008.2026v1.

34. Yang Y-f. *Anomalous Hall effect in heavy electron materials* (2011). arXiv: 1207.0646v1.

35. men"shov VN, Tugushev VV, Chulkov EV. Bound states induced by a ferromagnetic delta-layer inserted into a three-dimensional topological insulator. *Jetp Lett* (2012) 96(7):445–51. doi:10.1134/s0021364012190113

36. Zhang C, Zhang Y, Xiang Y, Lu S, Zhang J, Narayan A, et al. Quantum Hall effect based on Weyl or-bits in Cd3As2. *Nature* (2018) 565:331–6. doi:10.1038/s41586-018-0798-3

37. Qi XL. Generic wave-function description of fractional quantum anomalous Hall states and fractional topological insulators. *Phys Rev Lett* (2011) 107(12): 126803. doi:10.1103/physrevlett.107.126803

38. Vshivtsev AS, Magnitskii BV, Klimenko KG. A gluon condensate and the three-dimensional (bar "") 2 field theory[J]. *Phys At Nuclei* (1994) 57(12):2171–5.

39. Bangrong Z. Proof of chiral symmetry breaking and persistent mass condition in vector-like gauge theory. *Commun Theor Phys* (1991) 15(3):319–30. doi:10.1088/0253-6102/15/3/319

40. Clark TE, Nitta M, Ter Veldhuis T. Non-BPS brane dynamics and dual tensor gauge theory. *Phys Rev D* (2004) 70(12):125011. doi:10.1103/physrevd.70.125011

41. Zhang YH, Mao D, Cao Y, Jarillo-Herrero P, Senthil T. Nearly flat Chern bands in moiré superlattices superlattices[J]. *Phys Rev B* (2019) 99(7):075127. doi:10.1103/physrevb.99.075127

42. Deng Y, Yu Y, Shi MZ, Wang J, Chen XH, Zhang Y. *Quantum Anomalous Hall Effect in Intrinsic Magnetic Topological Insulator MnBi2Te4[C]// APS March Meeting 2020* (2020). Denver, United States: American Physical Society.

43. Zhao L, Bergholtz EJ. *Heng Fan,Fractional chern insulators in topolog-ical flat bands with higher chern number* (2012). arXiv:1206.3759v3 [cond-mat.str-el].

44. Jacak J, Jacak L. Unconventional fractional quantum Hall effect in monolayer and bilayer graphene. *Sci Technol Adv Mater* (2016) 17(1):149–65. doi:10.1080/14686996.2016.1145531

45. Milz S, Sakuldee F, Pollock FA. *Kolmogorov extension theorem for (quan-tum) causal modelling and general probabil-istic theories[J]* (2017). arXiv.

46. Sheng DN, Gu ZC, Sun K, Sheng L. Fractional quantum Hall effect in the absence of Landau levels. *Nat Commun* (2011) 2(1):389. doi:10.1038/ncomms1380

47. Simon M, Pollock FA, Kavan M. Reconstructing non-Markovian quantum dynamics with limited control. *Phys Rev A (Coll Park)* (2018) 98(1):012108. doi:10.1103/physreva.98.012108

48. Yang B, Sun H, Ott R. *Observation of gauge invariance in a 71-site Bose-Hubbard quantum simulator[J]* (2020).

49. Zhang XL, Liu LF, Liu WM. Quantum anomalous Hall effect and tunable topological states in 3d transition metals doped silicene. *Sci Rep* (2013) 3:2908. doi:10.1038/srep02908

50. Song ZG, Zhang YY, Song JT, Li SS. Route towards localization for quantum anoma-lous Hall systems with chern number 2. *Sci Rep* (2016) 6:19018. doi:10.1038/srep19018

51. Wang Y, Gong C. Fractional quantum anomalous Hall effect on topolog-ical flat bands (1)[J]. *J Zhejiang Normal University:Natural Sci Edition* (2013)(04) 361–71.

52. Wang Y, Gong C. Fractional quantum anomalous Hall effect on topolog-ical flat bands (2)[J]. *J Zhejiang Normal Univ* (2014)(01) 42–9. Natural Science Edition.

TYPE Original Research
PUBLISHED 12 December 2022
DOI 10.3389/fphy.2022.1048325

Check for updates

OPEN ACCESS

EDITED BY
Tianyu Ye,
Zhejiang Gongshang University, China

REVIEWED BY
Lihua Gong,
Nanchang University, China
Jinjing Shi,
Central South University, China

*CORRESPONDENCE
WanQing Wu,
wuwanqing8888@126.com

SPECIALTY SECTION
This article was submitted to Quantum Engineering and Technology, a section of the journal Frontiers in Physics

RECEIVED 19 September 2022
ACCEPTED 21 October 2022
PUBLISHED 12 December 2022

CITATION
Wu W, Guo L and Xie M (2022), Multi-party semi-quantum private comparison based on the maximally entangled GHZ-type states.
Front. Phys. 10:1048325.
doi: 10.3389/fphy.2022.1048325

Multi-party semi-quantum private comparison based on the maximally entangled GHZ-type states

WanQing Wu[1,2]*, LingNa Guo[1,2] and MingZhe Xie[1,2]

[1]School of Cyber Security and Computer, Hebei University, Baoding, China, [2]Key Laboratory on High Trusted Information System in Hebei Province, Hebei University, Baoding, China

The goal of semi-quantum privacy comparison (SQPC) is to use a small amount of quantum capabilities to compare private information for equality. In recent years, research on semi-quantum privacy comparison protocol has made some achievements. However, most of SQPC protocols can merely compare the private information of two parties, and the research of multi-party SQPC protocols are still scarce. If the number of participants is more than two, the protocol needs to be executed multiple times. Therefore, we proposed a multi-party semi-quantum private comparison protocol based on the maximally entangled GHZ-type state, which has the capability to compare the equality of *n* parties by executing the protocol once. What is more, the transmission of participant's encrypted information is not through the classical channel, which improves the security of the protocol. Finally, the security analysis shows that outsider attacks, dishonest participants attacks and semi-honest TP attacks are all invalid for this protocol.

KEYWORDS

semi-quantum private comparison, multi-party, GHZ states, quantum cryptography, information security

1 Introduction

Secure multi-party computing (SMC) is an momentous topic in classical cryptography. It originates from the millionaire problem proposed by Yao [1] in 1982, that is, comparing two millionaires who are richer without disclosing their real assets. With the proposal of quantum parallel algorithm, the security of SMC based on computational complexity is seriously challenged. In order to overcome the shortcomings of classical SMC in security, classical SMC has been extended to the field of quantum mechanics.

In 1984, Bennett and Brassard [2] applied quantum mechanics to classical cryptography and proposed the first quantum key distribution protocol. Since then, various quantum cryptography protocols have been proposed, such as quantum key distribution (QKD) [2–6], quantum dialogue (QD) [7, 8], quantum summation [9, 10], quantum encryption (QPQ) [11, 12], quantum signature [13–16].

The quantum privacy comparison protocol (QPC) is an essential branch of the SQPC protocol, which has attracted extensive attention of many scholars. In 2009, Yang and Wen

[17] presented the first quantum privacy comparison protocol using Bell states as carrier particles. Since then, QPC protocols with different quantum states as quantum resources have been proposed one after another. For example, many QPC protocols are based on single photon [18], Bell state [19–21], GHZ state [22, 23], multi-particle entangled state [24–26], and so on.

The most of quantum privacy comparison protocols require participants to have full quantum capabilities. In other words, all participants are allowed to use various quantum devices, such as quantum memory [27], entangled state generator [28] and quantum unitary operators [29]. However, quantum resources are currently very scarce, and it is impractical for all participants to have full quantum capabilities.

In order to solve the problem of scarcity of quantum resources, in 2007, Boyer et al. [30, 31] proposed the concept of semi-quantum and designed the first semi-quantum key distribution (SQKD) protocol, where he defined two kinds of participants. One is a "full quantum user" with complete quantum capabilities, and the other is a "classical user" who is limited to the following four operations: (1) reflecting the received qubits directly.; (2) measuring the received qubits with Z basis $\{|0\rangle, |1\rangle\}$; (3) preparing a new qubit with Z basis $\{|0\rangle, |1\rangle\}$; (4) reordering the qubits *via* different delay lines. Since the semi-quantum protocol can reduce the use of quantum resources, the concept of semi-quantum is applied to the QPC protocol. In 2016, Chou et al. [32] introduced the semi-quantum concept into the QPC protocol and proposed the first semi-quantum privacy comparison protocol based on Bell entanglement exchange. Similar protocols have been proposed from then on. In 2018, Ye et al. [33] constructed a SQPC protocol using two-particles entangled state with measure-resend characteristics. The next year, Lin et al. [34] put forward an efficient SQPC protocol with an semi-honest third party based on single photons. Recently, Tian et al. [35] proposed a robust SQPC protocol with W-state, which can resist the loss of a single qubit. In 2021, Zhou et al. [36] proposed a semi-quantum secret comparison protocol based on Bell state, which can compare the secret relationship between two classical participants in one execution without revealing their secrets. In 2022, Tang et al. [37] presented two SQPC protocol with DF states with good robustness properties against noise in the channel.

However, most of the current SQPC protocols can only compare the equality of two parties, and it is difficult to extend to multiple parties. If one want to use these two-party SQPC protocols to complete the comparison among n participants, the protocol need to be executed $n-1$ times. To solve this problem, we propose a SQPC protocol using the maximally entangled GHZ-type state, which can compare multi-party information *via* execute the protocol at once. What is more, the quantum states and quantum operations required in our protocol can be realized under the existing technology.

The structure of this paper is organized as follows: Section 2 describes the proposed protocol explicitly and analyze its correctness; in Section 3, the security analysis is demonstrated in terms of outsider attack and insider attack. In Section 4, we compare our protocol with some existing; finally, we give a summary about this paper in Section 5.

2 The proposed scheme

2.1 Prerequisites

Before the description of our protocol, some prerequisites of the proposed protocol should be put forward in advance as following.

1. Suppose the protocol has n participants $P_i (i = 1, 2, \ldots, n)$. Every participant owns the private information $X_i = x_i^1 x_i^2 \cdots x_i^m$, where $x_i^j \in \{0, 1\}$, $j = 1, 2, \ldots, m$. And the aim is to compare their private information for equality with the help of the semi-honest third-party (TP). Semi-honest refers to that TP may misbehave, but cannot conspire with others.
2. All participants use SQKD to generate the same secret key $K_P = (k_P^1, k_P^2, \ldots, k_P^m)$. Here, $k_p^j \in \{0, 1\}, (j = 1, 2, \ldots, m)$. Then, P_i encodes his secrets x_i^j with the shared keys k_p^j:

$$R_i^j = x_i^j \oplus k_P^j,$$

where $R_i = \{R_i^1, R_i^2, \ldots, R_i^m\}$, $R_i^j \in \{0, 1\}$ is the jth bit of R_i. And "$\oplus$" indicates the modulo 2 addition operation.

3. In this paper, the GHZ-type state is used to construct an SQPC protocol, which is described as follows:

$$\begin{aligned} |\varphi\rangle &= \frac{1}{2}(|000\rangle + |011\rangle + |101\rangle + |110\rangle) \\ &= \frac{1}{\sqrt{2}}(|0\rangle|\phi^+\rangle + |1\rangle|\psi^+\rangle). \end{aligned} \tag{1}$$

Here, $|\phi^+\rangle$, $|\phi^-\rangle$, $|\psi^+\rangle$ and $|\psi^-\rangle$ are four Bell states, which can be expressed as:

$$\begin{aligned} |\phi^+\rangle &= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle), \\ |\phi^-\rangle &= \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle), \\ |\psi^+\rangle &= \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle), \\ |\psi^-\rangle &= \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle). \end{aligned} \tag{2}$$

From Eq. 2 we can also infer that:

$$\begin{aligned} |00\rangle &= \frac{1}{\sqrt{2}}(|\phi^+\rangle + |\phi^-\rangle), \\ |01\rangle &= \frac{1}{\sqrt{2}}(|\psi^+\rangle + |\psi^-\rangle), \\ |10\rangle &= \frac{1}{\sqrt{2}}(|\psi^+\rangle - |\psi^-\rangle), \\ |11\rangle &= \frac{1}{\sqrt{2}}(|\phi^+\rangle - |\phi^-\rangle). \end{aligned} \tag{3}$$

2.2 Protocol steps

Now, we present our proposed protocol in detail.

Step 1. TP prepares $2nm$ three-qubit entangle states $|\psi\rangle$ described in Eq.1 to form n quantum sequence $S_1, S_2, \ldots, S_n$, and each sequence S_i ($i \in \{1, 2, \ldots, n\}$) includes $2m$ quantum states $|\psi\rangle$, i.e.

$$S_i = \left(Q^1_{TP_i}Q^1_{T_i}Q^1_{P_i}, Q^2_{TP_i}Q^2_{T_i}Q^2_{P_i}, \ldots, Q^{2m}_{TP_i}Q^{2m}_{T_i}Q^{2m}_{P_i}\right).$$

Here, the order of GHZ-type state in S_i are indicated in superscripts 1, 2, ..., $2m$. Afterwards, TP divides these particles into three sequences:

$$\begin{aligned} S_{TP_i} &= \left(Q^1_{TP_i}, Q^2_{TP_i}, \ldots, Q^{2m}_{TP_i}\right), \\ S_{T_i} &= \left(Q^1_{T_i}, Q^2_{T_i}, \ldots, Q^{2m}_{T_i}\right), \\ S_{P_i} &= \left(Q^1_{P_i}, Q^2_{P_i}, \ldots, Q^{2m}_{P_i}\right). \end{aligned}$$

Finally, TP stores S_{TP_i} and S_{T_i}, and transmits S_{P_i} to P_i.

Step 2. For $i = 1, 2, \ldots, n$:

When P_i receives the sequence S_{P_i} from TP, he selects m qubits randomly to perform measurement operation, and the remaining particles are performed reflection operation. After that, the sequence S_{P_i} becomes S'_{P_i}, and P_i sends it back to TP.

(1) Reflection: P_i reflects the received qubits directly.

(2) Measurement: P_i measures the received qubits with Z basis $\{|0\rangle, |1\rangle\}$ and generates a new qubit according to the value of R^j_i. The entangled particle will collapse to $|0\rangle$ or $|1\rangle$. If $R^j_i = 0$, P_i generates a new particle $Q^{'j}_{P_i}$ is the same as the measurement result. If $R^j_i = 1$, P_i generates a new quantum particle $Q^{'j}_{P_i}$ is contrary to the measurement result.

Step 3. For $i = 1, 2, \ldots, n$:

When TP receives the sequence S'_{P_i} from P_i, TP combines the sequences S_{TP_i}, S_{T_i} and S'_{P_i} to form the S'_i

$$S'_i = \left(Q^1_{TP_i}Q^1_{T_i}Q^{1'}_{P_i}, Q^2_{TP_i}Q^2_{T_i}Q^{2'}_{P_i}, \ldots, Q^{2m}_{TP_i}Q^{2m}_{T_i}Q^{2m'}_{P_i}\right).$$

Then, P_i publishes the location of the measurement and reflection operations. If P_i performs reflection operation, then TP measures each pair of $(Q^j_{T_i}Q^{j'}_{P_i})$ with Bell basis. On the basis of the entanglement properties of the GHZ-type state in Eq. 1, the measurement result should be $|\phi^+\rangle$ or $|\psi^+\rangle$. If $|\phi^-\rangle$ or $|\psi^-\rangle$ emerge in the measurement result, it means that there are eavesdroppers in the channel. After determines that there is no eavesdropper, the protocol will continue to the next step. Otherwise, will restart the protocol.

Step 4. TP removes the particles performing reflection operations. For the remaining particles, TP performs Bell measurement on each $(Q^j_{T_i}Q^{j'}_{P_i})$. If measurement result is $|\phi^\pm\rangle$, TP sets $E^j_i = 0$; and if measurement result is $|\psi^\pm\rangle$, TP sets $E^j_i = 1$. Then, TP performs measurement operation with Z basis on $Q^j_{TP_i}$ and forms the measurement results to a sequence C_i. If measured result is $|0\rangle$, then $C^j_i = 0$; if measured result is $|1\rangle$, then $C^j_i = 1$.

For $j = 1, 2, \ldots, m$: TP calculates:

$$T_j = \sum_{i=1}^{n-1} E^j_i \oplus C^j_i \oplus E^j_{i+1} \oplus C^j_{i+1}.$$

If $T_j = 0$ for all j in the end, TP will announce that the private information X_i are equal. Otherwise, he will announce that the private information X_i are not equal.

For clarity, Figure 1 display the flow chart about the process of the above steps.

2.3 Correctness

The correctness of the proposed protocol has been demonstrated in this subsection. P_i's private information X_i are encoded as $R^j_i = x^j_i \oplus k^j_P$. According to the rules for generating quantum states in step 2, we can deduce:

$$Q^{j'}_{P_i} = Q^j_{P_i} \oplus R^j_i = Q^j_{P_i} \oplus x^j_i \oplus k^j_P. \tag{4}$$

In step 4, TP performs Bell measurement on $(Q^j_{T_i}Q^{j'}_{P_i})$, and assigns value to E^j_i according to the measurement result. Apparently, it can be derived that:

$$E^j_i = Q^j_{T_i} \oplus Q^{j'}_{P_i}. \tag{5}$$

According to Eqs. 1, 4, 5, we will obtain:

$$\begin{aligned} T_j &= \sum_{i=1}^{n-1} E^j_i \oplus C^j_i \oplus E^j_{i+1} \oplus C^j_{i+1} \\ &= \sum_{i=1}^{n-1} Q^j_{T_i} \oplus Q^{j'}_{P_i} \oplus Q^j_{TP_i} \oplus Q^j_{T_{i+1}} \oplus Q^{j'}_{P_{i+1}} \oplus Q^j_{TP_{i+1}} \\ &= \sum_{i=1}^{n-1} Q^j_{T_i} \oplus Q^j_{P_i} \oplus R^j_i \oplus Q^j_{TP_i} \oplus Q^j_{T_{i+1}} \oplus Q^j_{P_{i+1}} \oplus R^j_{i+1} \oplus Q^j_{TP_{i+1}} \\ &= \sum_{i=1}^{n-1} R^j_i \oplus R^j_{i+1} \\ &= \sum_{i=1}^{n-1} x^j_i \oplus k^j_P \oplus x^j_{i+1} \oplus k^j_P \\ &= \sum_{i=1}^{n-1} x^j_i \oplus x^j_{i+1}. \end{aligned} \tag{6}$$

If $T_j = 0$ for all j in the end, TP will announce that the private information X_i are equal. Therefore, by measuring the particles in his hand, TP can easily compare the equality of all participants' secrets.

3 Analysis

According to whether the attacker participates in the protocol, there are two kinds of attack: outsider attack and insider attack. First, we demonstrate that four common outsider attack our protocol can resist four common outsider attack. Second, the analysis of the $n-1$ participant collusion

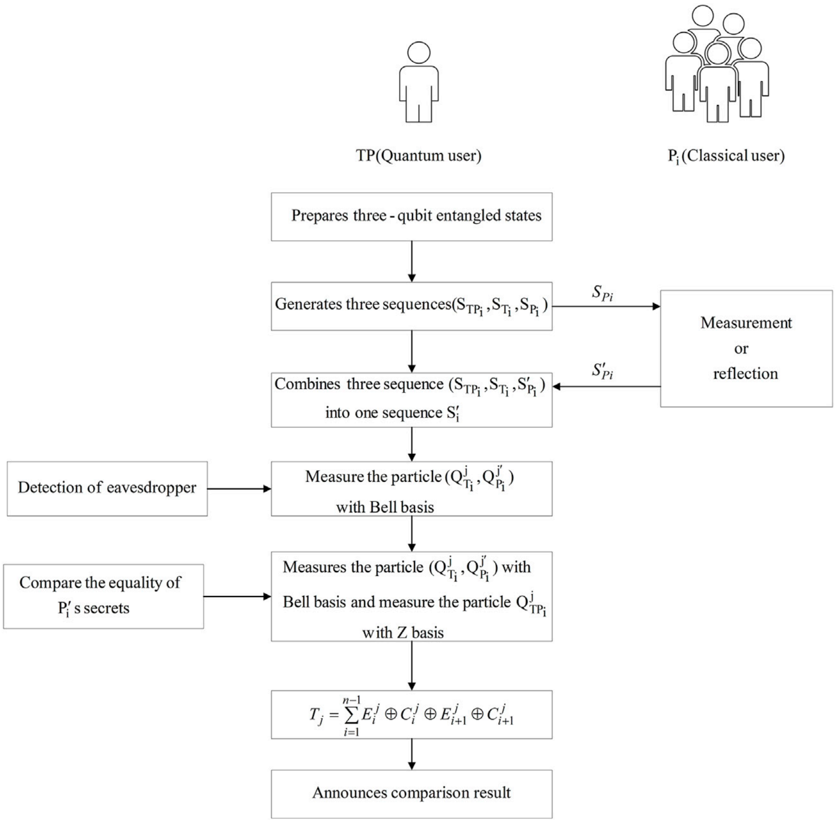

TP(Quantum user)
P_i(Classical user)
Prepares three - qubit entangled states
Generates three sequences(S_{TP_i},S_{T_i},S_{P_i})
S_{Pi}
Measurement or reflection
S'_{Pi}
Combines three sequence (S_{TP_i},S_{T_i},S'_{P_i}) into one sequence S'_i
Detection of eavesdropper
Measure the particle ($Q^j_{T_i}$,$Q^{j'}_{P_i}$) with Bell basis
Compare the equality of P'_is secrets
Measures the particle ($Q^j_{T_i}$,$Q^{j'}_{P_i}$) with Bell basis and measure the particle $Q^j_{TP_i}$ with Z basis
$T_j = \sum_{i=1}^{n-1} E_i^j \oplus C_i^j \oplus E_{i+1}^j \oplus C_{i+1}^j$
Announces comparison result

FIGURE 1
Process of the proposed SQPC protocol.

attack and the TP attack proves that this protocol also has ability resistant to insider attack. Therefore, this protocol can guarantee the privacy of secrets while comparing the equality of secrets among participants.

3.1 Outsider attack

Assuming that Eve is an outsider eavesdropper, he launches some well-known attacks on the transmitted particles to obtains participant's secret x_i^j.

Case 1. Intercept–resend attack

Eve intercepts S_{P_i}. Then, Eve generates a fake sequence S^*_{Pi} and transmites to P_i. As described in step 2, P_i randomly chooses measurement or reflection operation, he sends $S^{*'}_{Pi}$ back to TP. At this time, Eve also intercepts $S^{*'}_{Pi}$ and sends S_{P_i} back to TP. Eve measures the sequence $S^{*'}_{Pi}$ according to the positions of the measurement operation and reflection operation announced by P_i, and obtains the value of $R_i^j = x_i^j \oplus k_P^j$. However, since Eve does not know the shared key k_P^j, he cannot infer the participant's private information x_i^j from R_i^j.

Case 2. Measure-resend attack

Eve intercepts the sequence S_{P_i} sent by TP to P_i. Then, Eve uses Z basis to measures them and the measured sequence is sent to P_i. Nevertheless, in this case, Eve will be detected since he does not know whether P_i will choose the measurement operation or the reflection operation in step 2. If P_i performs the measurement operation, Eve's attack will not be found. If P_i performs the reflection operation, Eve's attack will be found. For example, suppose that $Q^j_{T_i}Q^j_{P_i}$ is $|\phi^+\rangle$, Eve measures the sequence S_{P_i} with the Z basis. Then, $|\phi^+\rangle$ will randomly collapse to $|00\rangle$ or $|11\rangle$. Eve sends the measured sequence to P_i. When TP uses Bell measurement to check the entanglement result of the corresponding reflected qubits in $Q^j_{T_i}Q^{j'}_{P_i}$, the measurement result will be $|\phi^+\rangle$ or $|\phi^-\rangle$. If the measurement is $|\phi^-\rangle$, Eve will be found. In this case, the detection probability for the proposed protocol is $1 - (\frac{1}{2})^m$. The detection probability is approximate to 1 when m is large enough.

Case 3. Entangle-measure attack

We assume that $|e\rangle$ is an ancillary qubit generated by Eve and U_E is the unitary operation. The unitary operation U_E can be described as follows:

$$U_E|0\rangle|e\rangle = a|0\rangle|e_{00}\rangle + b|1\rangle|e_{01}\rangle, \tag{7}$$

$$U_E|1\rangle|e\rangle = c|0\rangle|e_{10}\rangle + d|1\rangle|e_{11}\rangle, \tag{8}$$

where $|e_{00}\rangle$, $|e_{01}\rangle$, $|e_{10}\rangle$, $|e_{11}\rangle$ are pure states uniquely determined by U_E; $|a|^2 + |b|^2 = 1$, and $|c|^2 + |d|^2 = 1$.

According to the entanglement properties of quantum state $|\varphi\rangle$, TP can deduce the state of $(Q^j_{T_i}, Q^j_{P_i})$ through the measurement result of $Q^j_{TP_i}$. If the measurement result of $Q^j_{TP_i}$ is $|0\rangle$, the $(Q^j_{T_i}, Q^j_{P_i})$ should be $|\phi^+\rangle$. If the measurement result of $Q^j_{TP_i}$ is $|1\rangle$, the $(Q^j_{T_i}, Q^j_{P_i})$ should be $|\psi^+\rangle$. Here, we take $(Q^j_{T_i}, Q^j_{P_i})$ is $|\phi^+\rangle$ as an example to analyze the entangle-measure attack in this protocol.

Eve intercepts the sequence S_{P_i} and entangles the particles in the sequence S_{P_i} with $|e\rangle$ through the integer transformation U_E. After that, the quantum system becomes

$$\begin{aligned} U_e|\phi^+\rangle|e\rangle &= \frac{1}{\sqrt{2}}[|0\rangle(a|0\rangle|e_{00}\rangle + b|1\rangle|e_{01}\rangle) + |1\rangle(c|0\rangle|e_{10}\rangle + d|1\rangle|e_{11}\rangle)] \\ &= \frac{1}{\sqrt{2}}[a|00\rangle|e_{00}\rangle + b|01\rangle|e_{01}\rangle + c|10\rangle|e_{11}\rangle + d|1\rangle|e_{11}\rangle] \\ &= \frac{1}{2}[a(|\phi^+\rangle + |\phi^-\rangle)|e_{00}\rangle + b(|\psi^+\rangle - |\psi^-\rangle) \\ &\quad + c(|\psi^+\rangle + |\psi^-\rangle)|e_{10}\rangle + d(|\phi^+\rangle - |\phi^-\rangle)|e_{11}\rangle]. \end{aligned} \tag{9}$$

In order to prevent Eve's attack from being detected, the result of measuring the reflected particle $(Q^j_{T_i}, Q^j_{P_i})$ with the Bell basis should be $|\phi^+\rangle$. As a result, we can deduce that:

$$b = c = 0, a = d = 1,$$
$$|e_{00}\rangle = |e_{11}\rangle.$$

Then, the Eq. 9 can be rewritten as:

$$U_e|\phi^+\rangle|e\rangle = \frac{1}{2}[a(|\phi^+\rangle + |\phi^-\rangle)|e_{00}\rangle + d(|\phi^+\rangle - |\phi^-\rangle)|e_{11}\rangle] = |\phi^+\rangle|e_{00}\rangle. \tag{10}$$

It is easy to find that if Eve wants to obtain X_i through ancillary qubits, some error must be introduced and his attack must be detected.

Case 4. Double CNOT attack

Subsequently, we analyze the security of the protocol under the double CNOT attack. For simplicity, we suppose that $|z\rangle (|z\rangle \in \{|0\rangle, |1\rangle\})$ is an ancillary qubit produced by Eve and $|\varphi\rangle$ is GHZ-type state produced by TP. Eve performs the first CNOT operation on the intercepted sequence S_{P_i} and the ancillary qubit $|z\rangle$. After that, Eve sends S_{P_i} directly to P_i without any interference, and the ancillary qubit $|z\rangle$ becomes $|z'\rangle$. At this point, the whole quantum system is:

$$|\varphi\rangle_1 = CNOT(|\varphi\rangle_{123} \otimes |z\rangle_E) = \frac{1}{2}(|000z\rangle + |011\bar{z}\rangle + |101\bar{z}\rangle + |110z\rangle)_{123E} \tag{11}$$

After P_i receives S_{P_i}, he chooses reflection or measurement operation at random and send $S^{\prime}_{P_i}$ to TP. Eve performs the second CNOT operation on the intercepted sequence $S^{\prime}_{P_i}$ and the ancillary qubit $|z'\rangle$. Based on the different operations chosen by P_i, we divide the attack into two situations.

- *Situation 1: P_i chooses the reflection operation*

In this situation, P_i performs reflection operation and do not cause any disturbance to the particles. Therefore, after the second CNOT operation, the whole quantum system becomes:

$$\begin{aligned} |\varphi\rangle_2 &= CNOT\left(\frac{1}{2}(|000z\rangle + |011\bar{z}\rangle + |101\bar{z}\rangle + |110z\rangle)_{123E}\right) \\ &= \frac{1}{2}(|000\rangle + |011\rangle + |101\rangle + |110\rangle)_{123} \otimes |z\rangle_E \end{aligned} \tag{12}$$

Obviously, the ancillary qubit $|z\rangle$ have not changed after two CNOT operations, thus Eve cannot get any information from the ancillary qubit $|z\rangle$.

- *Situation 2: P_i chooses the measurement operation*

In this situation, P_i performs the measurement operation and produces a particle that is inverse or the same as the measurement depending on R^j_i. Since R^j_i can be either 0 or 1, $|\varphi\rangle_1$ collapses to $(|000z\rangle + |011\bar{z}\rangle)_{123E}$ or $(|101\bar{z}\rangle + |110z\rangle)_{123E}$. Then Eve performs the second CNOT operation, the whole quantum system becomes:

$$\begin{aligned} |\varphi\rangle_3 &= CNOT\left(|0\rangle_F \otimes \frac{1}{2}(|000z\rangle + |011\bar{z}\rangle + |101\bar{z}\rangle + |110z\rangle)_{123E}\right) \\ &= \left|0\rangle_F \otimes \frac{1}{2}(|000z\rangle + |011\bar{z}\rangle + |101\bar{z}\rangle + |110z\rangle)_{123E}\right) \end{aligned} \tag{13}$$

or

$$\begin{aligned} |\varphi\rangle_4 &= CNOT\left(|1\rangle_F \otimes \frac{1}{2}(|000z\rangle + |011\bar{z}\rangle + |101\bar{z}\rangle + |110z\rangle)_{123E}\right) \\ &= \left|1\rangle_F \otimes \frac{1}{2}(|000\bar{z}\rangle + |011z\rangle + |101z\rangle + |110\bar{z}\rangle)_{123E}\right). \end{aligned} \tag{14}$$

Eve can judge whether ancillary qubit have changed by measuring. Based on Eqs. 13, 14, the probability of measuring $|\bar{z}\rangle$ is 50%.

According to the above analysis, we summarize the double CNOT attack as follows:

(1) If Eve measures ancillary qubits and the result is $|z\rangle$, then Eve does not get any private information of P_i.

(2) If Eve measures ancillary qubits and the result is $|\bar{z}\rangle$, then Eve adopts Z basis to measure the sequence $S^{\prime}_{P_i}$ to obtain

$Q_{P_i}^{j'} = x_i^j \oplus Q_{P_i}^j \oplus k_i^j$. However, Eve does not know the shared key k_i^j, thus he cannot deduce the private information x_i^j.

According to the analysis, double CNOT attack cannot create a threat to this protocol.

Case 4. Trojan horse attack

As the proposed protocol is a two-way communication protocol, Eve may performs the Trojan horse attack [38] on the sequence S_{P_i} to obtain beneficial information. However, this attack can be easily prevented by using the photon number splitter and the optical wavelength filter devices [39, 40] to detect the Trojan-Horse photons.

Therefore, we proved that the outsider attack can be detected in the proposed SQPC protocol.

3.2 Insider attack

In 2007, Gao et al. [41] proposed that we should pay more attention to attacks from participants because they participated in the implementation of the protocol. In this subsection, we show that the protocol is resistant to participants collusion attack and TP attack.

Case 1. Participants attack

We only consider the worst circumstances that $n-1$ dishonest parties conspired to obtain the remaining participant's private information, because in this situation the threat to the protocol is the greatest. We assume that the dishonest parties P_1, P_2, $\ldots$, P_{i-1}, P_{i+1}, $\ldots$, P_n who collude with each other in an attempt to obtain P_i's secrets. In our protocol, the particles are only transmitted between the TP and the participants, and no particles are transmitted among the participants, so n participants are independent and do not interfere with each other. In order to obtain the secret of P_i, dishonest parties try to launch attacks during particle teleportation. For example, dishonest parties launches measure-resend attack to learn sequence S_{P_i}. Then, they send $S_{P_i}^*$ back to P_i, where $S_{P_i}^*$ is S_{P_i} after dishonest parties' operations. The reflection operation or measurement operation performed by P_i in step 2 is randomly selected, and the dishonest participant can only guess the correct operation with a probability of $\frac{1}{2}$. Therefore, his attack will definitely be detected during the eavesdropping detection. When there are m particles for security detection, the probability of dishonest participants being detected is $1-(\frac{1}{2})^m$. As the value of m increases, the probability of an attack being detected gradually approaches to 1.

Hence, the dishonest have no chance to obtain the secret of P_i.

Case 2. TP attack

In the first prerequisite of our protocol, TP is supposed to be a semi-honest who will do his best to learn participants' secret information, but does not collude with either of them. Without loss of generality, we suppose that TP wants to learn the secret of P_i.

The only way for TP to get X_i is to measure the particles $Q_{P_i}^{j'}$ in sequence S_{P_i}' with Z basis. In step 2, we can deduce that $Q_{P_i}^{j'} = Q_{P_i}^j \oplus x_i^j \oplus k_P^j$. Even though TP can get $Q_{P_i}^{j'}$ and $Q_{P_i}^j$ from the measurement, he still cannot deduce the private information of P_i, since the pre-shared key K_P is used to encrypt X_i, and he has no knowledge about K_P.

Therefore, the attack of TP is invalid for this protocol.

4 Comparison

In this section, we compare some existing protocol with our protocol. Qubit efficiency is an important indicator for evaluating SQPC protocols. Here, the qubit efficiency is defined as

$$\eta_e = \frac{c}{q+b},$$

where c represents the amount of classical information involved in the comparison, and q denotes the number of all particles consumed during the comparison, and b is the total number of classical bits consumed when decoding private information (classic communication for security detection is not included). In this paper, each classical participants have m classical bits respectively, and they compare nm classical bits in total. Then, to compare nm bits of private information, TP is required to generate $2nm$ three-qubit entangle state ($6mn$ bit qubits). During protocol execution, each of P_i choose measurement operation with $\frac{1}{2}$ probability, and they prepare m qubits. Furthermore, our protocol use the SQKD protocol [42] to generate m bits pre-shared key which consumes $24m$ qubits and $16m$ bit to generate one key. Then we can get $q = 6mn + mn + 40m = 7mn + 40m$. As for the number of classical bits consumed in the protocol, P_i does not need to publish information in the classic channel, and TP demands a classical bit to publish the comparison result. Thus, $b = 1$. In summary, the qubit efficiency of this paper is $\frac{nm}{7mn+40m+1}$. Using the same method, we can calculate the qubit efficiency of other related protocols, and the comparison results are shown in Table 1.

Next, the advantages of our protocol compared to existing SQPC protocols are analyzed. It should be note that there are two SQPC protocols in Ref. [43], which we denote by Ref. [43]-A and Ref. [43]-B respectively.

First, in terms of qubit efficiency, the proposed protocol has advantages over the existing SQPC protocols. It is apparent from Table 1, our protocol is more efficient than

TABLE 1 The comparison of our protocol to the other protocols.

	Quantum resource	Quantum measurement of TP	Number of protocol participants	Pre-shared cost	Comparison cost	Qubit efficiency
The protocol of Ref. [43]-A	single-particle states	Single-particle measurement	2	0	$18m + 1$	$\frac{2m}{18m+1}$
The protocol of Ref. [43]-B	single-particle states	Single-particle measurement	n $(n \geq 2)$	$40m \cdot 2^n$	2^n $(2m + mn) + mn + 1$	$\frac{nm}{2^n\,(42m+mn)+mn+1}$
The protocol of Ref. [44]	Bell states	Bell state measurement and single-particle measurement	2	$40m$	$8m + 1$	$\frac{2m}{48m+1}$
The protocol of Ref. [45]	Bell states	Bell state measurement and single-particle measurement	n $(n \geq 2)$	$(n + 1) \cdot 40m$	$3nm + 1$	$\frac{nm}{43mn+40m+1}$
The protocol of Ref. [46]	three-particles entangled states	GHZ measurement	2	0	$16m + 1$	$\frac{2m}{16m+1}$
The protocol of Ref. [47]	three-particles entangled states	Bell state measurement and single-particle measurement	2	0	$34m + 1$	$\frac{2m}{34m+1}$
The protocol of Ref. [35]	three-particles entangled states	Single particle, Bell state and G-like state measurement	2	$40m$	$10m + 1$	$\frac{2m}{50m+1}$
The protocol of Ref. [48]	three-particles entangled states	Bell state measurement and single-particle measurement	2	$40m$	$18m + 1$	$\frac{2m}{58m+1}$
The proposed protocol	three-particles entangled states	Bell state measurement and single-particle measurement	n $(n \geq 2)$	$40m$	$7nm + 1$	$\frac{nm}{7nm+40m+1}$

multi-party SQPC protocols Ref. [43]-B and Ref. [45]. Although the proposed protocol, Ref. [43]-B and Ref. [45] all generate the shared key using the SQKD protocol, we only need one shared key sequence while Ref. [43]-B and Ref. [45] require $n + 1$ shared keys sequences. As we all know, the shared key needs to consume a large number of qubits. Excessive demand for the shared key will increase the total number of qubits transmitted and reduce the efficiency of the protocol. Moreover, comparing with the current two-party protocols Ref. [43]-A, Ref. [35, 44, 46, 47, 48], our proposed protocol still has superiorities in quantum efficiency. When using two-party SQPC protocols to compare the private information of n participants, the protocol need to be executed $n - 1$ times. Repeating the protocol many times will increase the total number of transmitted qubits and reduce the efficiency of the protocol.

Second, our protocol does not use classical channels to transmit information except for security check steps. Most of the SQPC protocols now use quantum technology and classical computing to achieve comparison while ensuring security. As a result, there are usually quantum and classical two kinds of signals to process. The protocols in Refs. [35, 43–48] use the classical channel to transmit information, which increase the risk of classical attacks since the classical channel is the part with weak security. In order to improve the SQPC security, our protocol directly encodes the secret value of the participant to the quantum state through the measure-resend operation. And there is no classical channel to transmit information, which greatly reduces the classical attack and improves the security of the protocol.

Third, our protocol is more flexible, which is possible to compare the equality of any two participants. However, the SQPC protocols [35, 44, 46, 47, 48] can only compare the equality of two parties. When there are n $(n \geq 2)$ participants, the protocol needs to be executed $n - 1$ times, which is not only inefficient but also wastes quantum resources. The protocol proposed in this paper can compare the equality of multiple participants at one time, and can be flexibly applied to various situations.

Finally, semi-quantum protocol settles the problem that quantum communication network is restricted by expensive quantum devices. In the proposed protocol, participants in the protocol only need to have basic quantum abilities such as quantum measurement and quantum preparation, and complete the equality comparison of private information with the help of the third party quantum server. Quantum servers can be configured to the cloud and leased when users need to use them. In addition, The GHZ state we used has been proved in Ref. [49] that it can be prepared by the current quantum technology. Therefore, our protocol can be realized.

5 Conclusion

To sum up, we construct a SQPC protocol using the maximally entangled GHZ-type state. n classical participants can compare their secrets for equality *via* one execution of the protocol without leaking them. Comparing our protocol with some previous SQPC protocols in Section 4, it can be observed that the proposed protocol has obvious advantages in terms of flexibility and efficiency. Security analysis shows that both outsider and insider attacks are ineffective against this protocol. What is more, the participants in the SQPC protocol only need to perform a few limited operations, which reduces the cost of quantum resources to a certain extent. The SQPC protocol can be extended to more applications, because the quantum operations used in this paper can be implemented according to existing quantum technologies.

Data availability statement

The raw data supporting the conclusions of this article will be made available by the authors, without undue reservation.

Author contributions

All authors listed have made a substantial, direct, and intellectual contribution to the work and approved it for publication.

Funding

The authors are supported by the Science and technology research project of Hebei higher education Nos. ZD2021011.

Conflict of interest

The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Publisher's note

All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers. Any product that may be evaluated in this article, or claim that may be made by its manufacturer, is not guaranteed or endorsed by the publisher.

References

1. Yao AC. Protocols for secure computations. In: 23rd annual symposium on foundations of computer science (sfcs 1982); 03-05 November 1982; Chicago, IL, USA. IEEE (1982). 160–4.

2. Bennett CH, Brassard G (2020). Quantum cryptography: Public key distribution and coin tossing. arXiv preprint arXiv:2003.06557.

3. Xu F, Ma X, Zhang Q, Lo HK, Pan JW. Secure quantum key distribution with realistic devices. *Rev Mod Phys* (2020) 92(2):025002. doi:10.1103/revmodphys.92.025002

4. Lucamarini M, Yuan ZL, Dynes JF, Shields AJ. Overcoming the rate–distance limit of quantum key distribution without quantum repeaters. *Nature* (2018) 557(7705):400–3. doi:10.1038/s41586-018-0066-6

5. Ye TY, Li HK, Hu JL. Semi-quantum key distribution with single photons in both polarization and spatial-mode degrees of freedom. *Int J Theor Phys (Dordr)* (2020) 59(9):2807–15. doi:10.1007/s10773-020-04540-y

6. Ye TY, Geng MJ, Xu TJ, Chen Y. Efficient semiquantum key distribution based on single photons in both polarization and spatial-mode degrees of freedom. *Quan Inf Process* (2022) 21(4):123–1. doi:10.1007/s11128-022-03457-1

7. Ye TY, Li HK, Hu JL. Information leakage resistant quantum dialogue with single photons in both polarization and spatial-mode degrees of freedom. *Quan Inf Process* (2021) 20(6):209–13. doi:10.1007/s11128-021-03120-1

8. Qi JM, Xu G, Chen XB, Wang TY, Cai XQ, Yang YX. Two authenticated quantum dialogue protocols based on three-particle entangled states. *Quan Inf Process* (2018) 17(9):247–19. doi:10.1007/s11128-018-2005-8

9. Ye TY, Hu JL. Quantum secure multiparty summation based on the phase shifting operation of d-level quantum system and its application. *Int J Theor Phys (Dordr)* (2021) 60(3):819–27. doi:10.1007/s10773-020-04700-0

10. Ye TY, Xu TJ, Geng MJ, Chen Y. Two-party secure semiquantum summation against the collective-dephasing noise. *Quan Inf Process* (2022) 21(3):118–4. doi:10.1007/s11128-022-03459-z

11. Shi J, Chen S, Lu Y, Feng Y, Shi R, Yang Y, et al. An approach to cryptography based on continuous-variable quantum neural network. *Sci Rep* (2020) 10(1): 2107–13. doi:10.1038/s41598-020-58928-1

12. Qi R, Sun Z, Lin Z, Niu P, Hao W, Song L, et al. Implementation and security analysis of practical quantum secure direct communication, Light. *Sci Appl* (2019) 8(1):1–8.

13. Feng Y, Shi R, Shi J, Zhou J, Guo Y. Arbitrated quantum signature scheme with quantum walk-based teleportation. *Quan Inf Process* (2019) 18(5):154–21. doi:10.1007/s11128-019-2270-1

14. Shi J, Chen S, Liu J, Li F, Feng Y, Shi R. Quantum dual signature with coherent states based on chained phase-controlled operations. *Appl Sci* (2020) 10(4):1353. doi:10.3390/app10041353

15. Feng Y, Shi R, Shi J, Zhao W, Lu Y, Tang Y. Arbitrated quantum signature protocol with boson sampling-based random unitary encryption. *J Phys A: Math Theor* (2020) 53(13):135301. doi:10.1088/1751-8121/ab766d

16. Feng Y, Zhou J, Li J, Zhao W, Shi J, Shi R, et al. Skc-ccco: An encryption algorithm for quantum group signature. *Quan Inf Process* (2022) 21(9):328–9. doi:10.1007/s11128-022-03664-w

17. Yang YG, Wen QY. An efficient two-party quantum private comparison protocol with decoy photons and two-photon entanglement. *J Phys A: Math Theor* (2009) 42(5):055305. doi:10.1088/1751-8113/42/5/055305

18. Wu W, Zhou G, Zhao Y, Zhang H. New quantum private comparison protocol without a third party. *Int J Theor Phys (Dordr)* (2020) 59(6):1866–75. doi:10.1007/s10773-020-04454-9

19. Huang X, Zhang S-B, Chang Y, Hou M, Cheng W. Efficient quantum private comparison based on entanglement swapping of bell states. *Int J Theor Phys (Dordr)* (2021) 60(10):3783–96. doi:10.1007/s10773-021-04915-9

20. Wu W, Zhang H. Cryptanalysis of zhang et al's quantum private comparison and the improvement. *Int J Theor Phys (Dordr)* (2019) 58(6):1892–900. doi:10.1007/s10773-019-04084-w

21. Wu W, Ma X. Quantum private comparison protocol without a third party. *Int J Theor Phys (Dordr)* (2020) 59(6):1854–65. doi:10.1007/s10773-020-04453-w

22. Lang Y-F. Quantum private comparison without classical computation. *Int J Theor Phys (Dordr)* (2020) 59(9):2984–92. doi:10.1007/s10773-020-04559-1

23. Xu Q-D, Chen H-Y, Gong L-H, Zhou N-R. Quantum private comparison protocol based on four-particle ghz states. *Int J Theor Phys (Dordr)* (2020) 59(6): 1798–806. doi:10.1007/s10773-020-04446-9

24. Ji Z, Zhang H, Wang H. Quantum private comparison protocols with a number of multi-particle entangled states. *IEEE Access* (2019) 7:44613–21. doi:10.1109/access.2019.2906687

25. Ji ZX, Ye TY. Quantum private comparison of equal information based on highly entangled six-qubit genuine state. *Commun Theor Phys* (2016) 65(6):711–5. doi:10.1088/0253-6102/65/6/711

26. Ye T-Y, Ji Z-X. Two-party quantum private comparison with five-qubit entangled states. *Int J Theor Phys (Dordr)* (2017) 56(5):1517–29. doi:10.1007/s10773-017-3291-0

27. Julsgaard B, Sherson J, Cirac JI, Fiurášek J, Polzik ES. Experimental demonstration of quantum memory for light. *Nature* (2004) 432(7016):482–6. doi:10.1038/nature03064

28. Yao XC, Wang TX, Xu P, Lu H, Pan GS, Bao XH, et al. Observation of eight-photon entanglement. *Nat Photon* (2012) 6(4):225–8. doi:10.1038/nphoton.2011.354

29. Nielsen MA, Chuang I. *Quantum computation and quantum information*. Cambridge University Press (2002).

30. Boyer M, Kenigsberg D, Mor T. Quantum key distribution with classical bob. In: 2007 First International Conference on Quantum, Nano, and Micro Technologies (ICQNM'07); 02-06 January 2007; Guadeloupe, French Caribbean. IEEE (2007). p. 10.

31. Boyer M, Gelles R, Kenigsberg D, Mor T. Semiquantum key distribution. *Phys Rev A (Coll Park)* (2009) 79(3):032341. doi:10.1103/physreva.79.032341

32. Chou WH, Hwang T, Gu J (2016). Semi-quantum private comparison protocol under an almost-dishonest third party. arXiv preprint arXiv:1607.07961.

33. Ye TY, Ye CQ. Measure-resend semi-quantum private comparison without entanglement. *Int J Theor Phys (Dordr)* (2018) 57(12):3819–34. doi:10.1007/s10773-018-3894-0

34. Lin PH, Hwang T, Tsai CW. Efficient semi-quantum private comparison using single photons. *Quan Inf Process* (2019) 18(7):207–14. doi:10.1007/s11128-019-2251-4

35. Yan L, Zhang S, Chang Y, Wan G, Yang F. Semi-quantum private comparison protocol with three-particle g-like states. *Quan Inf Process* (2021) 20(1):17–6. doi:10.1007/s11128-020-02960-7

36. Zhou NR, Xu QD, Du NS, Gong LH. Semi-quantum private comparison protocol of size relation with d-dimensional bell states. *Quan Inf Process* (2021) 20(3):124–15. doi:10.1007/s11128-021-03056-6

37. Tang YH, Jia HY, Wu X, Chen HM, Zhang YM. Robust semi-quantum private comparison protocols against collective noises with decoherence-free states. *Quan Inf Process* (2022) 21(3):97–24. doi:10.1007/s11128-022-03444-6

38. Cai QY. Eavesdropping on the two-way quantum communication protocols with invisible photons. *Phys Lett A* (2006) 351(1-2):23–5. doi:10.1016/j.physleta.2005.10.050

39. Deng FG, Li XH, Zhou HY, Zhang Zj. Improving the security of multiparty quantum secret sharing against trojan horse attack. *Phys Rev A (Coll Park)* (2005) 72(4):044302. doi:10.1103/physreva.72.044302

40. Deng FG, Zhou P, Li XH, Li CY, Zhou HY (2005). Robustness of two-way quantum communication protocols against trojan horse attack. arXiv preprint quant-ph/0508168.

41. Gao F, Qin S-J, Wen Q-Y, Zhu F-C. A simple participant attack on the brádler-dušek protocol. *Quan Inf Comput* (2007) 7(4):329–34. doi:10.26421/qic7.4-4

42. Krawec WO. Mediated semiquantum key distribution. *Phys Rev A (Coll Park)* (2015) 91:032323. doi:10.1103/physreva.91.032323

43. Chongqiang Y, Jian L, Xiubo C, Yuan T. Efficient semi-quantum private comparison without using entanglement resource and pre-shared key. *Quan Inf Process* (2021) 20(8):262–19. doi:10.1007/s11128-021-03194-x

44. Jiang LZ. Semi-quantum private comparison based on bell states. *Quan Inf Process* (2020) 19(6):180–21. doi:10.1007/s11128-020-02674-w

45. Li Z, Liu T, Zhu H. Private comparison protocol for multiple semi-quantum users based on bell states. *Int J Theor Phys (Dordr)* (2022) 61(6):177–12. doi:10.1007/s10773-022-05167-x

46. Yan L, Chang Y, Zhang S, Wang Q, Sheng Z, Sun Y. Measure-resend semi-quantum private comparison Scheme 熮 sing GHZ class states. *Comput Mater Contin* (2019) 61(2):877–87. doi:10.32604/cmc.2019.06222

47. Tian Y, Li J, Chen XB, Ye CQ, Li CY, Hou YY. An efficient semi-quantum private comparison without pre-shared keys. *Quan Inf Process* (2021) 20(11):360–13. doi:10.1007/s11128-021-03294-8

48. Tian Y, Li J, Ye C, Chen XB, Li C. W-state-based semi-quantum private comparison. *Int J Theor Phys (Dordr)* (2022) 61(2):18–6. doi:10.1007/s10773-022-05005-0

49. Li Q, Chan WH, Long DY. Semiquantum secret sharing using entangled states. *Phys Rev A (Coll Park)* (2010) 82(2):022303. doi:10.1103/physreva.82.022303

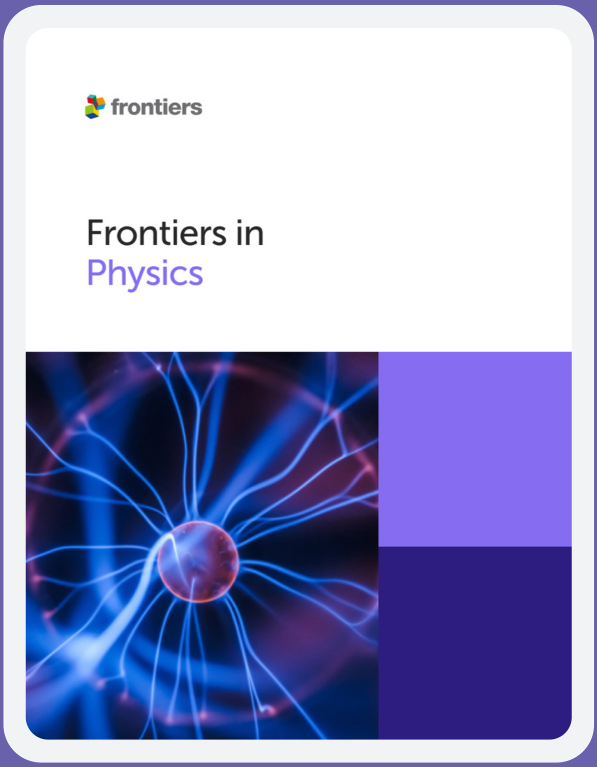
Frontiers in Physics

Investigates complex questions in physics to understand the nature of the physical world

Addresses the biggest questions in physics, from macro to micro, and from theoretical to experimental and applied physics.

Discover the latest Research Topics

See more →



frontiers

Frontiers in
Physics

Frontiers

Avenue du Tribunal-Fédéral 34
1005 Lausanne, Switzerland
frontiersin.org

Contact us

+41 (0)21 510 17 00
frontiersin.org/about/contact