frontiers | Frontiers in Physics

TYPE Original Research
PUBLISHED 09 August 2022
DOI 10.3389/fphy.2022.979838

Check for updates

OPEN ACCESS

EDITED BY
Tian-Yin Wang,
Luoyang Normal University, China

REVIEWED BY
Tingting Song,
Jinan University, China
Jinjing Shi,
Central South University, China
Lvzhou Li,
Sun Yat-sen University, China

*CORRESPONDENCE
Ping Wang,
wangping@szu.edu.cn
Zhiwei Sun,
smeker@szpt.edu.cn

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

RECEIVED 28 June 2022
ACCEPTED 13 July 2022
PUBLISHED 09 August 2022

CITATION
Wang P, Su Y and Sun Z (2022), All-or-nothing oblivious transfer based on the quantum one-way function. *Front. Phys.* 10:979838. doi: 10.3389/fphy.2022.979838

COPYRIGHT
© 2022 Wang, Su and Sun. This is an open-access article distributed under the terms of the Creative Commons Attribution License (CC BY). The use, distribution or reproduction in other forums is permitted, provided the original author(s) and the copyright owner(s) are credited and that the original publication in this journal is cited, in accordance with accepted academic practice. No use, distribution or reproduction is permitted which does not comply with these terms.

All-or-nothing oblivious transfer based on the quantum one-way function

Ping Wang[1,2]*, Yiting Su[1] and Zhiwei Sun[3,4]*

[1]College of Electronics and Information Engineering, Shenzhen University, Shenzhen, China, [2]Guangdong Key Laboratory of Intelligent Information Processing, Shenzhen, China, [3]School of Artificial Intelligence, Shenzhen Polytechnic, Shenzhen, China, [4]Institute of Applied Artificial Intelligence of the Guangdong-Hong Kong-Macao Greater Bay Area, Shenzhen Polytechnic, Shenzhen, China

Oblivious transfer (OT) is one of the keystones of secure multi-party computation. It is generally believed that unconditionally secure OT is impossible. In this article, we propose a practical and secure quantum all-or-nothing oblivious transfer protocol based on the quantum one-way function. The protocol is built upon a quantum public-key encryption construction, and its security relies on the no-cloning theorem and no-communication theorem. Practical security is reflected in limitations on non-demolition measurements.

KEYWORDS

oblivious transfer, quantum one-way function, no-communication theorem, practical secure, multi-party computation

1 Introduction

Rabin pioneered the concept of oblivious transfer in 1981 [1]. In Rabin's OT (also called all-or-nothing OT) protocol, Alice sends a message m to Bob, and Bob receives the message m with a probability of 1/2. Toward the end of the protocol interaction, Alice does not know whether Bob received the message m while Bob does. Later in 1985, Even et al. [2] proposed a more practical OT called 1-out-of-2 oblivious transfer, which can be used to implement a wide variety of protocols [2, 3]. In this version of OT, Alice has a message pair (m_0, m_1), Bob makes a choice, and one of the messages is chosen. At the end of the protocol, Bob is allowed to retrieve one message from Alice's message pair corresponding to his choice without knowing anything about the other message, while Alice is unaware of Bob's choice. However, Crépeau demonstrated that the two kinds of oblivious transfer protocols are similar when the messages are single bits, meaning that one may be created from the other and vice versa [4]. Furthermore, one can build a 1-out-of-2 oblivious transfer protocol that transmits bit-string messages from a 1-out-of-2 oblivious transfer protocol for single bits [5–7].

The versatility of these protocol settings motivates a wider study on the power of secure two-party computation. Classical OT relies on computational hardness assumptions. Typically, these assumptions fall into two categories: general hardness assumptions such as the existence of one-way functions (OWFs) and specific hardness

assumptions such as factoring integers, discrete logarithms, and lattice-based problems, also known as trapdoor one-way functions. However, Shor's algorithm [8] can be used to solve difficult mathematical problems such as integer factorization, discrete logarithms, and elliptic curve discrete logarithms, posing a risk that the security of trapdoor one-way functions generated by certain existing number-theoretic-based cryptography is threatened. Moreover, OT protocols that rely only on the assumption of the existence of one-way functions are resistant to quantum attacks.

The principles of quantum mechanics can be used to design more secure cryptographic protocols. In 1983, Wiesner proposed that the uncertainty principle [9] could be used in cryptography [10]. In 1984, Bennett and Brassard used the quantum no-cloning theorem to implement basic cryptographic protocols, proposing the first unconditionally secure quantum key distribution protocol, BB84 [11, 12]. However, Mayers [13], Lo, and Chau [14, 15] proved that all previously proposed quantum bit commitment (QBC) protocols and quantum oblivious transfer (QOT) protocols are not unconditionally secure. Because the sender Alice can almost always cheat successfully by using an Einstein–Podolsky–Rosen (EPR)-type attack and delaying the measurement until disclosing her commitment. Moreover, OT generally requires a secure BC, so unconditionally secure OT is also impossible. The no-go theorem (based on the Hughston–Jozsa–Wootters (HJW) theorem [16, 17]) was proposed, resulting in the non-existence of unconditionally secure BC and unconditionally secure OT being widely accepted.

Following the classical equivalence [4] between the two flavors of oblivious transfer, one might conclude that the impossibility of having an unconditionally secure 1-out-of-2 oblivious transfer would imply the same for oblivious transfer. However, the laws of quantum physics allow for a greater range of scenarios, potentially jeopardizing classical reduction theories. One must run numerous oblivious transfer protocols as black boxes to create the 1-out-of-2 oblivious transfer, and this raises the risk of so-called coherent attacks (joint quantum measurements on several black boxes). Thus, having a secure quantum all-or-nothing oblivious transfer protocol does not necessarily mean that it is possible to construct a secure 1-out-of-2 oblivious transfer. We can implement all-or-nothing OT multi-party computation without using the BC protocol. As a consequence, no matter how high the security level our all-or-nothing OT has, this fact alone is not in contradiction with the Lo–Chau–Mayers no-go theorem. The alternative, ensuring practical security of such protocols, is to consider noisy or bounded memories [18–20]. Recently, a (quantum) computationally secure version of the oblivious transfer protocol was presented in [21].

In 2017, João et al. proposed a practical all-or-nothing QOT [22] based on single-qubit rotations in which the authors improve the public-key encryption scheme. However, there are two issues in the scheme that need to be addressed, which are also the main concerns of this article: 1) if all the secret keys s_i are indeed chosen uniformly at random, then some of them will be close to 0 or $\pi/2$, and this part of the measurement will always be correct. Therefore, the authors added the step of checking whether $\boldsymbol{s}$ is likely to be a possible output of a random process to avoid Alice cheating. Nevertheless, when Bob chooses the wrong direction of rotation, the state of each qubit becomes $|\tilde{m}_i\rangle = \cos(\frac{2s_i\theta_n + m_i\pi}{2})|0\rangle + \sin(\frac{2s_i\theta_n + m_i\pi}{2})|1\rangle$. It is obvious that when Bob follows the protocol honestly, the two measurements do not collapse with the same probability, and the measurement he gets is not a complete meaningless random number. This departs from the original purpose of the all-or-nothing OT, which was to give Bob a message with a probability of 1/2 or nothing at all. 2) The protocol only discusses the fact that Bob has no strategy to get the whole message and does not consider the fact that a dishonest Bob can get more than half of the message. More specifically, the protocol encodes the message directly on the quantum public key and divides the message into units, each of which corresponds to a parity bit (hash value). Dishonest Bob's cheating strategy is to measure a limited number of message units and compare them with the corresponding parity bits, thereby determining whether the rotation direction chosen is correct, and if it is not, he can always change the rotation direction to get the rest of the message. It is considered that t units are sufficient to determine that, as the number of units increases, corruption of the t-unit message is negligible for the whole message. This is fatal to the probabilistic transfer properties of the OT protocol. Considering the aforementioned two problems, we design a higher optimal all-or-nothing OT protocol based on one-way functions.

The one-way function is one of the most fundamental cryptographic primitives, as it can be used as a component of other, more complex cryptographic protocols. Recently, two independent works [23, 24] proved that secure one-way functions imply secure computation in a quantum world. They showed that quantum oblivious transfer can be obtained from the black-box use of any statistically binding, quantum computationally hidden commitment. Additionally, they pointed out that such commitments can be constructed by quantum-secure one-way functions (classic one-way functions that can be resistant to quantum attacks). Although exhaustive search is the only way to attack classical ideal secure one-way functions, cryptographic protocols based on classical secure one-way functions require the assumption that the attacker's computing power is limited. If we can design one-way functions based on physical laws, i.e., quantum mechanics principles, then we can potentially obtain secure quantum one-way functions. Thus, it is possible for us to construct secure OTs. In view of this, we will focus on the design of specific quantum one-way functions (QOWFs). Following that, we build more complex quantum oblivious transfer protocols based on the one-way function.

In this article, we study the design of quantum one-way functions as well as introduce and enhance a quantum public-key encryption

(qPKE) construction. Then, we design a practical secure quantum all-or-nothing OT protocol based on a specific QOWF. The soundness of the protocol relies on secure communication by applying qPKE. The security of the protocol can be reduced to one-wayness of the quantum one-way function, the no-cloning theorem, and the no-communication theorem. It is worth mentioning that the application of the hash function (digest algorithm) and the idea of secret sharing ensures that honest Bob can check whether he has obtained the message and dishonest Bob gets nothing about the message. More specifically, the distributor divides a secret into t-shared units, such that any of the t-shared units can be combined to reconstruct the secret, but no information about the secret is available to any of the $t-1$-shared units. The t-shared units are transferred to Bob in cipher, and each shared unit corresponds to exactly one check unit, attempting to necessarily check and destroy the shared units.

The rest of the article is organized as follows: first, in Section 2, we discuss the definition of quantum one-way functions and prove the security of a rotation-based quantum one-way function. Then, in Section 3, we introduce and improve the quantum public-key encryption system based on the classical-to-quantum one-way function. In Section 4, we describe in detail the construction of the all-or-nothing oblivious transfer protocol based on the qPKE. In Section 5, we analyze the proposed OT protocol and show that the security of the new scheme can be reduced to the one-wayness of the quantum one-way function. Finally, we give a summary in Section 6.

2 Quantum one-way functions

A function f: $\{0,1\}^* \to \{0,1\}^*$ is one-way if f can be computed by a polynomial-time algorithm, but any polynomial-time randomized algorithm F that attempts to compute a pseudo-inverse for f succeeds with negligible probability. That is, a one-way function is a function that is easy to compute on every input but hard to invert given the image of random input. By definition, the function must be "hard to invert" in the average-case sense, rather than the worst-case sense [25]. The existence of such one-way functions is still an open conjecture. In fact, their existence would prove that the complexity classes P and NP are not equal. The converse is not known to be true, i.e., the existence of proof that P ≠ NP would not directly imply the existence of one-way functions.

Generally, a one-way function designed based on quantum mechanical principles (such as the no-cloning theorem [9]) is called a quantum one-way function. One-wayness needs to be satisfied, i.e., the function can effectively (polynomial time) get the output according to the input, while the input cannot be obtained according to the output. The concept of classical-to-quantum one-way function (CQ-OWF) was first proposed by Gottesman and Chuang [26], who showed that such a function can be obtained by mapping classical bit strings to quantum states of a collection of qubits, and designed a quantum signature scheme based on it, where the classical-to-quantum one-way function is defined as a function that can be easily solved by quantum algorithms but cannot be inverted by any polynomial-time quantum algorithm [26]. That is, we can obtain a natural generalized version of the classical one-way function for quantum one-way functions by extending the probabilistic polynomial-time Turing machine to quantum algorithms.

Definition 1. (Quantum one-way function). Let

$$f\colon \{0,1\}^n \to \left(\mathcal{H}^2\right)^{\otimes m}$$

be a classical-to-quantum function that maps n bits of input to m qubits of output, where

$$\left(\mathcal{H}^2\right)^{\otimes m} = \mathcal{H}^2 \otimes \cdots \otimes \mathcal{H}^2 = \mathcal{H}^{2^m}$$

is a 2^m-dimensional Hilbert space made up of m copies of a single qubit space $\mathcal{H}^2$.

Denote the function as f: $x \mapsto |f(x)\rangle$. Then, f is a quantum one-way function if it satisfies the following three properties:

Deterministic: the same input always gives the same output.
Easy to compute: for any input x, one can get the output $|f(x)\rangle$ in polynomial time.
Hard to invert: given $|f(x)\rangle$, it is impossible to invert x by virtue of the fundamental quantum information theory.

The input and output of a classical one-way function involve only classical bits, and given a pair (input, output), one can efficiently verify whether the output is generated by f according to the input. However, for quantum one-way functions, because the input and output involve quantum states, it is not always the case that we can verify the pair (input, output) effectively. Furthermore, given two outputs $|f(x)\rangle$ and $|f(x')\rangle$, we are not able to definitively determine whether they are equal or not. This involves the comparison of quantum states, such as the swap-test, and the result of the test is probabilistic. If the states are the same, the swap-test is always passed, but if they are different, the swap-test is sometimes failed.

Nikolopoulos [27] constructed a practical CQ-OWF using single-qubit rotations, explored the one-wayness of functions mapping integers to single quantum bit states, and proposed a quantum public-key cryptographic theoretical framework based on it, which is provably secure even against powerful quantum eavesdropping strategies. The scheme proposed in this article will also make use of this cryptosystem. To have a clearer understanding of the characteristics of this CQ-OWF, we re-elaborate this function in formal language, define its constituent elements as single-qubit OWFs, and give rigorous proof that this function satisfies one-wayness under the constraint of the no-cloning theorem.

2.1 Single-qubit OWF

The single-qubit OWF can be defined as $f_{cq}\colon \{0,1\}^n \to \mathcal{H}^2$, whose input is an integer $s \in \mathbb{Z}_{2^n}$ and whose output is the state of

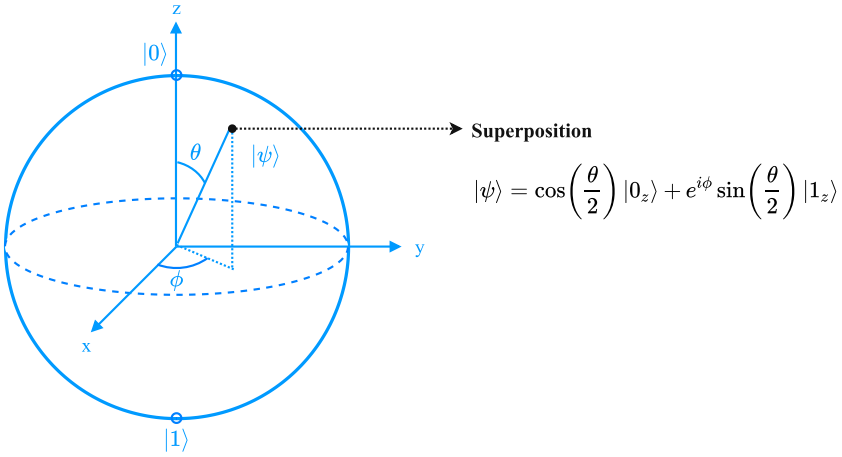

FIGURE 1
Superposition quantum state.

a quantum system, say $|\psi_s(\theta_n)\rangle$. For the sake of simplicity, we present a specific single-qubit OWF in the context of single-qubit states lying on the $x-z$ plane of the Bloch-sphere. A general qubit state lying on the $x-z$ plane can be written as

$$|\psi(\theta)\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle + \sin\left(\frac{\theta}{2}\right)|1\rangle,$$

where $0 \le \theta < 2\pi$, $\phi = 0$, is shown in Figure 1. Hence, unlike the classical bit, which can store a discrete variable taking only two real values (that is "0" and "1"), a qubit may represent a continuum of states on the $x-z$ plane. Introducing the rotation operator about the y axis, $\hat{\mathcal{R}}(\theta) = e^{-i\theta\hat{\mathcal{Y}}/2}$ with $\hat{\mathcal{Y}} = i(|1\rangle\langle 0| - |0\rangle\langle 1|)$, we may alternatively write $\hat{\mathcal{O}}(\theta)$: $|\psi(\theta)\rangle = \hat{\mathcal{R}}(\theta)|0\rangle$.

The input of the proposed single-qubit OWF is a random integer $s \in \mathbb{Z}_{2^n} \coloneqq \{0, 1, \ldots, 2^n - 1 | n \in \mathbb{N}\}$ uniformly distributed over $\mathbb{Z}_{2^n}$ with $n \gg 1$, and a qubit initially prepared in $|0\rangle$. Thus, n-bit strings suffice as labels to identify the input s for fixed n. For given values of $n \in \mathbb{N}$ and $s \in \mathbb{Z}_{2^n}$, the qubit state is rotated by $s\theta_n$ around the y axis with $\theta_n = \pi/2^{n-1}$. For some fixed $n \in \mathbb{N}$, the output of the OWF pertains to the class of states $\mathbb{Q}_n = \{|\psi_s(\theta_n)\rangle \,|\, s \in \mathbb{Z}_{2^n}, \theta_n = \pi/2^{n-1}\}$, with $\hat{\mathcal{O}}(n,s)$: $|\psi_s(\theta_n)\rangle \equiv \hat{\mathcal{R}}(s\theta_n)|0\rangle = \cos(s\theta_n/2)|0\rangle + \sin(s\theta_n/2)|1\rangle$. Therefore, the single-qubit OWF f_{cq} described previously maps from an arbitrary n-bit classical string to the two-dimensional Hilbert space, which can also be expressed as f_{cq}: $\{n, s\} \to |\psi_s(\theta_n)\rangle$.

However, in quantum public-key encryption, we use a one-way function with multiple integers input and multiple qubits output, so we define the CQ-OWF based on the single-qubit OWF as follows: consider two sets, $\mathbb{S}$ and $\mathbb{Q}$, which involve numbers and quantum states of a physical system, respectively. The input $\mathbb{S}$ includes an arbitrary integer string $\boldsymbol{s}$ of length k, i.e., $\boldsymbol{s} = (s_1, s_2, \ldots, s_k)$, with $\forall s_j \in \mathbb{Z}_{2^n}$ independently. The output $\mathbb{Q}$ contains k-qubit states, which are mapped independently depending on each item s_j of the input set $\mathbb{S}$ to obtain $|\Psi_{\boldsymbol{s}}(\theta_n)\rangle \equiv \otimes_{j=1}^{k}|\psi_{s_j}(\theta_n)\rangle_j$. The mapping of the CQ-OWF is F_{cq}: $\{n, \boldsymbol{s}\} \to |\Psi_{\boldsymbol{s}}(\theta_n)\rangle$, which operates the mapping procedure of the single-qubit OWF f_{cq}: $\{n, s\} \to |\psi_s(\theta_n)\rangle$ k times.

Theorem 1. The function denoted as F_{cq}: $\{n, \boldsymbol{s}\} \to |\Psi_{\boldsymbol{s}}(\theta_n)\rangle$ consisting of k single-qubit OWF blocks, is a secure CQ-OWF with the following properties:

Deterministic: the same input always results in the same output.
Easy to compute: for any input $\boldsymbol{x} = \{n, \boldsymbol{s}\}$, one can get the output $F_{cq}(\boldsymbol{x})$ in polynomial time.
Hard to invert: given $|\Psi_{\boldsymbol{s}}(\theta_n)\rangle$, it is impossible to invert $\boldsymbol{x} = \{n, \boldsymbol{s}\}$ by virtue of the fundamental quantum information theory.

Proof. As follows, we first prove the one-wayness of the single-qubit OWF and then the one-wayness of the CQ-OWF.

2.2 One-wayness of the single-qubit OWF

To further illustrate the two expressions "easy to compute" and "hard to invert," a quantum system initially prepared in a state of $|0\rangle$ is considered, and let $\mathcal{H}^2$ be its corresponding Hilbert space. We apply an operation $\hat{\mathcal{O}}(n,s)$: $\mathcal{H}^2 \mapsto \mathcal{H}^2$ on the system with a randomly selected $s \in \mathbb{Z}_{2^n}$. This operation converts the initial state such that $|0\rangle \to |\psi_s(\theta_n)\rangle = \hat{\mathcal{O}}(n,s)$. The ensemble of all probable output states of the single-qubit OWF is $\mathbb{Q}_n \equiv \{|\psi_s(\theta_n)\rangle | s \in \mathbb{Z}_{2^n}\}$, and corresponds to $\mathcal{H}^2$. In case, the

mapping $\mathfrak{M}$: $\mathbb{Z}_{2^n} \mapsto \mathbb{Q}_n$ is a bijection, there is a unique $s \in \mathbb{Z}_{2^n}$, i.e., $\mathfrak{M}$ is one-to-one and $|\mathbb{Z}_{2^n}| = |\mathbb{Q}_n|$. Consequently, we conclude that the single-qubit OWF meets the properties "deterministic."

It is common knowledge that the mapping $\{n, s\} \rightarrow |\psi_s(\theta_n)\rangle$ must be "easy to compute." For a given $s \in \mathbb{Z}_{2^n}$, the transformation on the system $|0\rangle \rightarrow |\psi_s(\theta_n)\rangle$, can be efficiently executed on a single-qubit OWF. For a given pair of integers $\{n, s\}$, the function $|0\rangle \rightarrow |\psi_s(\theta_n)\rangle$ is easy to compute since it involves single-qubit rotations only. In particular, it is known that any single-qubit operation can be simulated to an arbitrary accuracy of $\epsilon > 0$ by a quantum algorithm involving a universal set of gates (i.e., Hadamard, phase, controlled-NOT, and $\pi/8$ gates) [28]. Additionally, this simulation is efficient since its implementation requires an overhead of resources that scales polynomially with $\log(\epsilon^{-1})$. In a nutshell, there is always a family of quantum circuits $\mathrm{C} = \{\mathcal{C}_i\}_{i>0}$ involving a universal set of gates for f_{cq} such that $\forall s \in \{0,1\}^n$, $\|\mathcal{C}_i\| \leq O(\log(\epsilon^{-1}))$.

Inversion of the map $\{n, s\} \rightarrow |\psi_s(\theta_n)\rangle$ must be a "hard" problem by virtue of some fundamental principles of quantum mechanics. The number of non-orthogonal states increases as we increase n, whereas for $n \gg 1$ we have the nearest-neighbor overlap $|\psi_s(\theta_n)\rangle\langle\psi_{s+1}(\theta_n)| = \cos(\theta_n/2) \rightarrow 1$. Distinguishing between the two can be infeasible by virtue of the quantum uncertainty principle. To get the detailed information of the quantum state $|\psi_s(\theta_n)\rangle$, we must resort to measurements, which inevitably interfere with the quantum state. According to the theorem of Holevo [28], the classical information extracted from a single quantum bit by measurement is at most 1 bit. When n is fixed, a random selection of $s \in \mathbb{Z}_{2^n}$ requires n bits for recognition. Thus, we can conclude that the mapping is hard to invert when n is larger than 1 and sufficiently large. In fact, we do not publish n, which makes it more difficult to invert the mapping. Given a state $|\psi_s(\theta_n)\rangle$ chosen at random from an unknown set $\mathbb{Q}_n \equiv \{|\psi_s(\theta_n)\rangle | s \in \mathbb{Z}_{2^n}\}$, there is no efficient quantum algorithm $\mathrm{C}^{-1} = \{\mathcal{C}_i^{-1}\}_{i>0}$ to recover the integer s from the given state $|\psi_s(\theta_n)\rangle$ with a non-negligible probability. In other words, for all the family of quantum circuits C^{-1} and for all n sufficiently large, it is always the case that their probability of getting back the correct input x is $\Pr(\mathcal{C}_i^{-1}(f_{cq}(x)) = x) \leq \frac{1}{2^n}$.

Hence, we see that for a given $n \gg 1$, the map $\{n, s\} \rightarrow |\psi_s(\theta_n)\rangle$ acts as a secure QOWF that is "easy to compute" but "hard to invert," and the quantum one-way function under consideration is provably secure [27]. Furthermore, we will discuss the CQ-OWF proposed by Nikolopoulos, which consists of a number of single-qubit OWF blocks stitched together and whose validity can be statistically compared to a single-qubit OWF.

2.3 One-wayness of the CQ-OWF

In general, there will always exist a family of quantum circuits $\mathrm{C} = \{\mathcal{C}_i\}_{i>0}$ involving a universal set of gates for F_{cq} such that $\forall \boldsymbol{s} \in \{0,1\}^{nk}$, $\|\mathcal{C}_i\| \leq O(k\log(\epsilon^{-1}))$. For all families of quantum circuits C^{-1} and for all n sufficiently large, it is always the case that their probability of getting back the correct input $\boldsymbol{x}$ is $\Pr(\mathcal{C}_i^{-1}(F_{cq}(\boldsymbol{x})) = \boldsymbol{x}) \leq (\frac{1}{2^n})^{kt}$. Eventually, we can conclude that the function F_{cq}: $\{n, \boldsymbol{s}\} \rightarrow |\Psi_{\boldsymbol{s}}(\theta_n)\rangle$ is one-way function, which is "easy to compute" but "hard to invert."

3 Quantum public-key encryption

In this section, we will discuss and improve the quantum public-key encryption construction proposed by Nikolopoulo [27], which has been proven to be secure. Based on the CQ-OWF mentioned in Section 3, when it comes to two consecutive rotations, the map $s \mapsto |\psi_s(\theta_n)\rangle$ can act as a trapdoor OWF. Let us assume that after $\hat{\mathcal{R}}(s\theta_n)$, a second rotation $\hat{\mathcal{R}}(m\theta_n)$ is applied to the same qubit, with a randomly chosen integer $m \in \mathbb{Z}_{2^n}$, such that $s + m = c \bmod 2^n$. After the second rotation is applied, the qubit's state becomes $|\psi_c(\theta_n)\rangle = \hat{\mathcal{R}}(c\theta_n)|0\rangle = \hat{\mathcal{R}}(m\theta_n)\hat{\mathcal{R}}(s\theta_n)|0\rangle$. In general, we are interested in extrapolating m because it usually represents clear textual information. However, this assignment (for eavesdroppers) requires more explicit information about the figures s and c, which is impossible for $n \gg 1$. More strictly speaking, the information about the randomly chosen s extracted from the state $|\psi_s(\theta_n)\rangle$ is negligible, so it remains practically unknown. Similarly, for a legitimate user with only information s, it is impossible to extract m from $|\psi_m(\theta_n)\rangle = \hat{\mathcal{R}}(m\theta_n)|0\rangle$, and the number m remains practically hidden. In the following, through the analysis of the quantum public-key encryption scheme, we will have a clearer understanding of the one-way and trapdoor properties of the map $s \mapsto |\psi_s(\theta_n)\rangle$. The specific quantum public-key encryption scheme consists of the following three stages.

3.1 Stage 1—Key generation

Choose a random integer string $\boldsymbol{s}$ of length k, i.e., $\boldsymbol{s} = (s_1, s_2, \ldots, s_k)$, with s_j chosen independently of $\mathbb{Z}_{2^n}$ and then apply $\hat{\mathcal{R}}^{(j)}(s_j\theta_n)$ rotations to the j-th qubit. Until here, we defined the secret key as $S_k = \{n, \boldsymbol{s}\}$ and the public key as $e = \left\{k, |\Psi_{\boldsymbol{s}}^{(\mathrm{pk})}(\theta_n)\rangle\right\}$, with the k-qubit state $|\Psi_{\boldsymbol{s}}^{(\mathrm{pk})}(\theta_n)\rangle \equiv \otimes_{j=1}^{k}|\psi_{s_j}(\theta_n)\rangle_j$. Clearly, in the proposed protocol, the secret key is classical, whereas the public key is quantum as it involves the state of k qubits, and $|\psi_{s_j}(\theta_n)\rangle$ are presented in Section 3. Moreover, note that its copying does not violate the no-cloning theorem.

3.2 Stage 2—Encryption

Assume a sender wants to transfer a k-bit string $m \triangleq m_1, m_2, \ldots, m_k$, with $m_j \in \{0, 1\}$ to a receiver. To encrypt the message, the sender will take the following steps without altering the order of the public-key qubits:

(1) Obtain authentic public key e.
(2) When encrypting the jth bit of message, say m_j, by applying the rotation $\hat{\mathcal{R}}^{(j)}(m_j\pi + \frac{b\pi}{2})$ where $b \in \{0, 1\}$ (i.e., $\hat{\mathcal{R}}^{(j)}(m_j\pi)$ or $\hat{\mathcal{R}}^{(j)}(m_j\pi + \frac{\pi}{2})$) on the corresponding qubit of the public key, whose state becomes $|\psi_{s_j,m_j}(\theta_n)\rangle_j = \hat{\mathcal{R}}^{(j)}(m_j\pi + \frac{b\pi}{2})|\psi_{s_j}(\theta_n)\rangle_j$. In general, b is defined as the coding basis.
(3) Now that, we generate the quantum ciphertext (or else cipher state) that is the new state of the k qubits, i.e., $|\Psi^{(c)}_{s,m}(\theta_n)\rangle = \otimes_{j=1}^{k}|\psi_{s_j,m_j}(\theta_n)\rangle_j$.

3.3 Stage 3—Decryption

To recover the plaintext m from the cipher state $|\Psi^{(c)}_{s,m}(\theta_n)\rangle$, the receiver needs to perform the following steps:

(1) Undo initial rotations, i.e., to apply $\hat{\mathcal{R}}^{(j)}(s_j\theta_n)^{-1}$ to the j-th qubit of the cipher state.
(2) Measure each qubit of the cipher state on the basis of $\{|0\rangle, |1\rangle\}$ or $\{|+\rangle, |-\rangle\}$ corresponding to the coding basis b. This completes the process of secure communication.

In the introduction to quantum public-key cryptography [27], only one encryption method is included, which is $\hat{\mathcal{R}}^{(j)}(m_j\pi)$. Under this situation, it is always easy for the receiver (with the secret key) to get the encoded message m (here, b defaults to 0) when he receives the cipher state. In other words, the information encoded on the public key is plaintext information to the receiver. Given that we are designing an all-or-nothing OT protocol, the protocol requires that the receiver Bob cannot learn the message in more than 50% of the cases. Therefore, we will make relevant improvements to qPKE construction to satisfy the probabilistic transfer condition. In our improved version, we extend the encryption method into two, namely, $\hat{\mathcal{R}}^{(j)}(m_j\pi)$ and $\hat{\mathcal{R}}^{(j)}(m_j\pi + \frac{\pi}{2})$, corresponding to the coding basis $b = 0$ and $b =$, respectively. Note that if the coding basis is known, Bob can get the encoded message m with probability 1. However, if Bob does not possess the coding basis, after undoing initial rotations, Bob will not be able to determine the measurement basis to get the exact encoded m. In this article, we set the coding basis at $\hat{\mathcal{R}}^{(j)}(m_j\pi + \frac{b\pi}{2})$ where $b \in \{0, 1\}$. Here, we define basis $\{|0\rangle, |1\rangle\}$ as computational and basis $\{|+\rangle, |-\rangle\}$ as Hadamard. In the following section, we will discuss why Bob can receive bit $m'_j = m_j$ with a probability of 1 when choosing the correct basis.

In Section 3.2, we would like to analyze the encryption encoding method $|\psi_{s_j,m_j}(\theta_n)\rangle_j = \hat{\mathcal{R}}^{(j)}(m_j\pi + \frac{b\pi}{2})|\psi_{s_j}(\theta_n)\rangle_j$ in further detail. It means that when $m_j = 0$ and $b = 0$, there is

$$\begin{aligned}\left|\psi_{s_j,0}(\theta_n)\right\rangle_j &= \hat{\mathcal{R}}^{(j)}(0)\left|\psi_{s_j}(\theta_n)\right\rangle_j \\ &= \cos\left(\frac{s_j\theta_n}{2}\right)|0\rangle_j + \sin\left(\frac{s_j\theta_n}{2}\right)|1\rangle_j.\end{aligned}$$

When $b = 1$, there is

$$\begin{aligned}\left|\psi'_{s_j,0}(\theta_n)\right\rangle_j &= \hat{\mathcal{R}}^{(j)}\left(\frac{\pi}{2}\right)\left|\psi_{s_j}(\theta_n)\right\rangle_j \\ &= \cos\left(\frac{s_j\theta_n}{2}\right)|+\rangle_j + \sin\left(\frac{s_j\theta_n}{2}\right)|-\rangle_j,\end{aligned}$$

where $|+\rangle = \hat{\mathcal{R}}(\pi/2)|0\rangle, |-\rangle = \hat{\mathcal{R}}(\pi/2)|1\rangle$. We would like to point out that for a single qubit, the cipher states $|\psi_{s_j,0}(\theta_n)\rangle_j$ and $|\psi'_{s_j,0}(\theta_n)\rangle_j$ are non-orthogonal when encoding the same binary bit with different encoding methods, and no quantum circuit can distinguish them, i.e., the indistinguishability of non-orthogonal states of quantum physics. Similarly, it means that when $m_j = 1$, $b = 0$, there is

$$\begin{aligned}\left|\psi_{s_j,1}(\theta_n)\right\rangle_j &= \hat{\mathcal{R}}^{(j)}(\pi)\left|\psi_{s_j}(\theta_n)\right\rangle_j \\ &= \cos\left(\frac{s_j\theta_n}{2}\right)|1\rangle_j + \sin\left(\frac{s_j\theta_n}{2}\right)|0\rangle_j.\end{aligned}$$

When $b = 1$, there is

$$\begin{aligned}\left|\psi'_{s_j,1}(\theta_n)\right\rangle_j &= \hat{\mathcal{R}}^{(j)}\left(\pi + \frac{\pi}{2}\right)\left|\psi_{s_j}(\theta_n)\right\rangle_j \\ &= \cos\left(\frac{s_j\theta_n}{2}\right)|-\rangle_j + \sin\left(\frac{s_j\theta_n}{2}\right)|+\rangle_j.\end{aligned}$$

In contrast, encoding different binary bits with the same encoding method, the cipher states $|\psi'_{s_j,0}(\theta_n)\rangle_j$ and $|\psi'_{s_j,1}(\theta_n)\rangle_j$ are orthogonal and can be distinguished by performing a measurement with a probability of 1.

In Section 3.3, we would like to point out that the aforementioned two steps are basically equivalent to a von Neumann measurement, which projects the jth qubit onto the basis $\left\{|\psi_{s_j}(\theta_n)\rangle, \hat{\mathcal{R}}(\pi)|\psi_{s_j}(\theta_n)\rangle\right\}$. Here, we notice that $\hat{\mathcal{R}}^{(j)}(\alpha)^{-1} = \hat{\mathcal{R}}^{(j)}(\alpha)^{\dagger} = \hat{\mathcal{R}}^{(j)}(-\alpha)$, while different rotations around the same axis commute, i.e., $[\hat{\mathcal{R}}^{(j)}(\alpha), \hat{\mathcal{R}}^{(j)}(\beta)] = 0$. Next, we first describe the state after undoing the initial rotations in further detail, which means that when $m_j = 0$, $b = 0$, there is

$$\begin{aligned}\hat{\mathcal{R}}^{(j)}\left(s_j\theta_n\right)^{-1}\left|\psi_{s_j,0}(\theta_n)\right\rangle_j &= \cos(0)|0\rangle_j + \sin(0)|1\rangle_j = |0\rangle_j \to m_j \\ &= 0,\end{aligned}$$

where $|0\rangle = \frac{1}{\sqrt{2}}(|+\rangle + |-\rangle)$ and when $b = 1$, there is

$$\begin{aligned}\hat{\mathcal{R}}^{(j)}\left(s_j\theta_n\right)^{-1}\left|\psi'_{s_j,0}(\theta_n)\right\rangle_j &= \cos(0)|+\rangle_j + \sin(0)|-\rangle_j \\ &= |+\rangle_j \to m_j = 0,\end{aligned}$$

where $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$. It means that when $m_j = 1$, $b = 0$, there is

$$\begin{aligned}\hat{\mathcal{R}}^{(j)}\left(s_j\theta_n\right)^{-1}\left|\psi_{s_j,1}(\theta_n)\right\rangle_j &= \cos(0)|1\rangle_j + \sin(0)|0\rangle_j = |1\rangle_j \to m_j \\ &= 1.\end{aligned}$$

When $b = 1$, there is

$$\hat{\mathcal{R}}^{(j)}\left(s_j\theta_n\right)^{-1}\left|\psi'_{s_j,1}(\theta_n)\right\rangle_j = \cos(0)|-\rangle_j + \sin(0)|+\rangle_j$$
$$= |-\rangle_j \rightarrow m_j = 1.$$

We can see that the quantum state after undoing the original rotation will only be in one of the four most common states $\{|0\rangle, |+\rangle, |1\rangle, |-\rangle\}$, which is the reason why we additionally picked $\hat{\mathcal{R}}^{(j)}(m_j\pi + \frac{b\pi}{2})$. So far, we can record the measurements with the two common measurement bases, namely, computational and Hadamard. If Bob has chosen the correct basis, the correct m_j is obtained with a probability of 1. Otherwise, the correct m_j is obtained with a probability of just 1/2.

In summary, the improvement version, which does not change the original features of qPKE construction, still guarantees secure communication. To be compatible with the proposed oblivious transfer scheme, new encryption has been added to ensure that Bob cannot distinguish between the two encryption methods. In addition, the inherent property of qPKE is not broken, i.e., the message can always be correctly decrypted by following the correct steps. Lastly, we have agreed on only two bases, computational and Hadamard, to ensure that the protocol is oblivious.

Notice that, unlike the classical public keys that can be reused unlimited times, in the qPKE construction, the same public key e can also be reused, but it cannot be reused unlimited times. The public and secret keys need to be replaced after the security factor is exceeded, i.e., the upper bound needs to be bounded as follows: $I(x, d) \leq kN$. When N copies of the public key circulate simultaneously, the mutual information between Eve and the key $I(x, d)$ increases, and the confidentiality of the secret key is always guaranteed if $\log_2(|\tilde{\mathbb{N}}|) + k\bar{n} \gg kN$. In the proposed OT scheme, the public key is not required to be used many times, so the communication process of qPKE is still secure within this boundary. As a result, while the qPKE is not strictly speaking public-key encryption, it can still be used to design an all-or-nothing OT scheme.

4 New quantum all-or-nothing oblivious transfer

In this section, we will design a secure all-or-nothing oblivious transfer protocol based on the aforementioned CQ-OWF as well as qPKE. Moreover, the hash function is applied in this scheme, along with the idea of secret sharing.

A hash function creates a digest (a string that is shorter) of a message in such a way that 1) the probability of generating at random strings with the same hash value is negligible; and 2) the hash values are distributed almost uniformly over the set of all possible digests. A digest algorithm (hash function) is a method used to prevent a message from being altered privately, and Bob's choice of the wrong decryption method is considered a private alteration of the message. Therefore, Bob can verify whether the message was obtained or not after the opening phase. In the proposed scheme, the proposed hash function to be used to generate the digest is: Consider dividing a random key r into t successive blocks of bits $\bar{r}_i$, $(1 \leq i \leq t)$, each of length k, where $\bar{r}_i = r_{k(i-1)+1}r_{k(i-1)+2}\ldots r_{k(i-1)+k}$. The hash value $d = h(\bar{r}_1\bar{r}_2\ldots\bar{r}_t) \triangleq d_1d_2\ldots d_t$ has a value of $r_{k(i-1)+1} \oplus r_{k(i-1)+2} \oplus\ldots\oplus r_{k(i-1)+k}$ for each bit d_i. Essentially, d_i is the parity bit of the ith unit of the random key. As a result, each bit in hash value is independent of the others. Assume that the hash value enables the recovery of the random key with a non-negligible probability p. With the same probability p, the bit $d_i = r_{k(i-1)+1} \oplus r_{k(i-1)+2} \oplus\ldots\oplus r_{k(i-1)+k}$ then specifically aids in recovering the potential unit $\bar{r}_i$. If the cryptographic system [27], used to create the proposed protocol, is secure, then we assert that this is impossible. Here, t is a threshold sufficient to determine whether the message was obtained or not, and the probability that Bob will mistake an altered message as a correct message is negligible, i.e., $\frac{1}{2}t$.

Shamir's secret sharing, formulated by Adi Shamir, is one of the first secret-sharing schemes in cryptography. It is based on polynomial interpolation over finite fields [29]. The basic idea is that the distributor divides a secret into n-shared units by a polynomial, such that any of the t-shared units can be combined to reconstruct the secret, but no information about the secret is available to any of the $t-1$-shared units. As mentioned previously, consider dividing the random key r into t successive units of bits $\bar{r}_i$, $(1 \leq i \leq t)$; the random key of each unit represents the shared unit. Thus, for $k = n$, the message be recovered only by assembling the shared units of each unit, and inaction on any unit will result in getting nothing. In summary, with the idea of secret sharing, it is possible to achieve that only honest Bob (measure all qubits on the same measurement basis) can recover the message, with a probability of 1/2. Shamir's secret sharing based on the Lagrange interpolation theorem is an inefficient implementation. Fortunately, for $t = n$, there is also a simple and efficient implementation of Shamir's secret sharing, to which the proposed scheme applies. The message that will be transmitted is the shared secret. That is, take any $t-1$ random numbers $(\bar{r}_1, \bar{r}_2, \ldots, \bar{r}_{t-1})$ and for message m computing $\bar{r}_t = m \oplus \bar{r}_1 \oplus \bar{r}_2 \oplus\ldots\oplus \bar{r}_{t-1}$. This enables the message $m = \oplus_{i=1}^{t}\bar{r}_i$ to be obtained, while any $t-1$-shared units will get nothing about the message.

The framework of the proposed all-or-nothing OT protocol is shown in Figure 2. The detailed steps are described as follows:

Notations:

Security parameters: $n, k, t \in \mathbb{N}$, with $k \gg t$, $\theta_n = \pi/2^{n-1}$;

Secret key: $\boldsymbol{s} = (s_1, s_2, \ldots, s_{kt})$, where each $s_i \in \{0,1\}^n$;

Random key: $r = \bar{r}_1\bar{r}_2\ldots\bar{r}_t = r_1\ldots r_k r_{k+1}\ldots r_{2k}r_{2k+1}\ldots r_{kt}$;

Hash function: h: $\{0,1\}^{kt} \rightarrow \{0,1\}^t$;

Message to transfer: $m = m_1m_2\ldots m_k$.

Transferring phase:

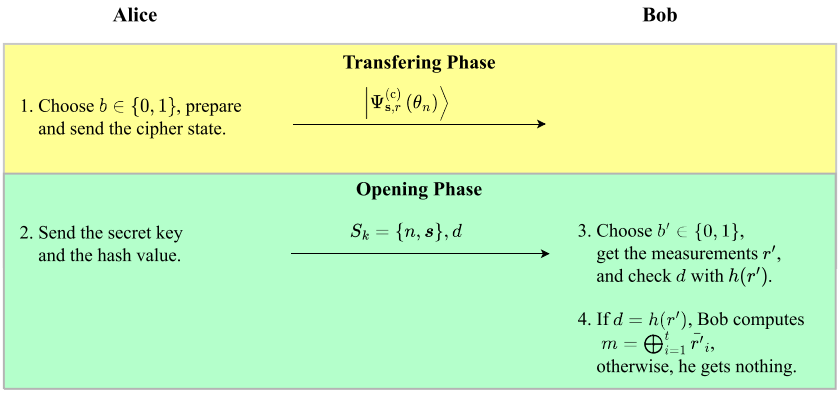

FIGURE 2
All-or-nothing oblivious transfer based on CQ-OWF.

(1) Alice uniformly at random takes any $t-1$ random numbers $(\bar{r}_1, \bar{r}_2, \ldots, \bar{r}_{t-1})$ and for message $m = \oplus_{i=1}^{t} \bar{r}_i$ computes $\bar{r}_t$, where the random key $r = \bar{r}_1 \bar{r}_2 \ldots \bar{r}_t = r_1 r_2 \ldots r_{kt}, r_j \in \{0,1\}$. To encrypt the bit string r, Alice prepares the secret key as $S_k = \{n, s\}$ and chooses one of the two encryption encoding methods as $b \in \{0,1\}$. Then, she encodes her bit string r as a sequence of qubits on the same basis, using the same encryption scheme as before without altering the order of the public key qubits:

$$\left|\Psi_{s,r}^{(c)}(\theta_n)\right\rangle = \bigotimes_{j=1}^{kt} \hat{\mathcal{R}}\left(s_j\theta_n + \frac{b\pi}{2} + r_j\pi\right)|0\rangle.$$

(2) After coding, she sends the result, $|\Psi_{s,r}^{(c)}(\theta_n)\rangle$, to Bob.

Opening phase:

(3) Alice sends to Bob the secret key as $S_k = \{n, s\}$ and the hash as $d = h(r)$.
(4) Bob applies $\hat{\mathcal{R}}(s_i\theta_n)^{-1}$ to each qubit of $|\Psi_{s,r}^{(c)}(\theta_n)\rangle$.
(5) Bob chooses uniformly at random $b' \in \{0, 1\}$ and measures each qubit of the cipher state on the basis of $\{|0\rangle, |1\rangle\}$ or $\{|+\rangle, |-\rangle\}$ corresponding to b'.
(6) Let r' be the random key that Bob recovers. He checks if $d = h(r')$. If that is the case, then Bob is almost sure that $r' = r$; otherwise, he knows that r' is not the correct random key. Finally, if $r' = r$, dividing the random key r' into t successive units of bits $\bar{r}_i$, he will get $m = \oplus_{i=1}^{t} \bar{r}_i$.

This ends the proposed protocol.

5 Security analysis and discussion

In the proposed protocol, Bob's main goal is to recover plaintext information from the cipher state, a goal that seems too ambitious to achieve under the quantum no-cloning theorem, and he may use different methods to try to compromise the security of the protocol. Alice's main goal is to know whether Bob received the correct message or not. As long as one of these two goals is accomplished, the OT protocol is considered invalid. The security of the proposed OT protocol is then examined. All-or-nothing OT must fulfill the following four requirements (the first expresses correctness, while the next three ensure the security of the protocol):

(1) Soundness: if Bob and Alice are both honest, there is a 1/2 probability that Bob will get the correct message m. Bob is aware of whether he received the correct message or not, but Alice is not.
(2) Concealing: Bob cannot learn the message Alice intended to transfer before the opening phase if Alice is honest.
(3) Probabilistic transfer: after the opening phase, Bob is unable to learn the message in more than 50% of instances.
(4) Oblivious: if Bob is honest, Alice can only guess with a probability of 1/2 as to whether Bob received the message.

Definition 2. when a function $f(x)$, for each polynomial function $P(x)$, has the following equation held, $\exists k \in \mathbb{N}$ such that $\forall n > k$, $f(n) < 1/P(n)$ can be said to be negligible.

5.1 Soundness

In the following paragraphs, we prove the soundness of the proposed protocol: if both Alice and Bob are honest, then with a probability of $1/2 + \epsilon(k)$, Bob will get the correct message, where $\epsilon(k)$ is a negligible function of the size of the message $m = m_1 m_2 \ldots m_k$. Bob is aware of whether he received the correct message or not, but Alice is not. As mentioned previously, the message can be recovered using the random key, and the information Bob receives about the random key consists of two parts: one belonging to the cipher state sent by Alice, and the other belonging to its hash value. It has shown that, by the nature of the digest algorithm, the hash function does not help Bob recover the random key r. This is because the hash is obtained in a lossy and irreversible way.

Without loss of generality, assume that Alice chooses $b = 0$, i.e., the computational method $\hat{\mathcal{R}}^{(j)}(m_j\pi)$ is chosen to encode each qubit of the cipher state. The qubits Alice sent to Bob are the following:

$$|\psi\rangle = \overset{kt}{\underset{j=1}{\otimes}} \hat{\mathcal{R}}\left(s_j\theta_n + r_j\pi\right)|0\rangle$$
$$= \overset{kt}{\underset{j=1}{\otimes}} \cos\left(\frac{s_j\theta_n + r_j\pi}{2}\right)|0\rangle + \sin\left(\frac{s_j\theta_n + r_j\pi}{2}\right)|1\rangle.$$

In the opening phase, Bob receives the secret key S_k from Alice, where $\boldsymbol{s} = s_1 s_2 \ldots s_k$. Later, he undoes their initial rotations, i.e., to apply $\hat{\mathcal{R}}^{(j)}(-s_j\theta_n)$ to the jth qubit of the cipher state. The states he gets are either $|0\rangle$ or $|1\rangle$. In fact:

$$|\psi'\rangle = \overset{kt}{\underset{j=1}{\otimes}} \hat{\mathcal{R}}\left(-s_j\theta_n\right)\hat{\mathcal{R}}\left(s_j\theta_n + r_j\pi\right)|0\rangle = \overset{kt}{\underset{j=1}{\otimes}} \hat{\mathcal{R}}\left(r_j\pi\right)|0\rangle$$
$$= \overset{kt}{\underset{j=1}{\otimes}} \cos\left(\frac{r_j\pi}{2}\right)|0\rangle + \sin\left(\frac{r_j\pi}{2}\right)|1\rangle = |r_j\rangle.$$

By the assumption $b' = 0$, Bob chooses to measure each qubit on the basis of $\{|0\rangle, |1\rangle\}$, and the result is r_j with a probability 1. Clearly, there is $r' = r$ and $h(r') = d$. Moreover, he can get the whole message $m = \oplus_{i=1}^{t} \bar{r}_i$.

By the assumption $b' = 1$, Bob chooses to measure each qubit on the basis of $\{|+\rangle, |-\rangle\}$, and the result r_j' is r_j with a probability 1/2. More specifically, if $r_j = 0$, then the aforementioned state becomes $|0\rangle = \cos(\pi/4)|+\rangle + \sin(\pi/4)|-\rangle$ and by measuring the qubit with $\{|+\rangle, |-\rangle\}$ Bob gets the correct result with a probability $\cos^2(\pi/4) = 1/2$. Likewise, if $r_j = 1$, then the aforementioned state becomes $|1\rangle = \cos(\pi/4)|-\rangle - \sin(\pi/4)|+\rangle$ and again Bob gets the correct bit with the probability 1/2. Not knowing b, Bob might make the wrong measurement basis on each qubit, and thus obtains a random key r' differing from r in 1/2 of its bit positions (of course Bob does not know which ones). In this case, for Bob, the end of the protocol is just getting a random number with no meaning.

The two cases, $b' = b$ and $b' \neq b$, occur both with a probability of 1/2. While in the first case Bob always gets r correctly, in the second case, the probability of getting correct r_j is 1/2. Hence, the probability that Bob will get the whole random key r is

$$Pr\left(|\psi'\rangle \to r\right) = Pr\left(b' = b\right) \times Pr\left(r|b' = b\right)$$
$$+ Pr\left(b' \neq b\right) \times Pr\left(r|b' \neq b\right)$$
$$= \frac{1}{2} + \frac{1}{2}\prod_{j=1}^{kt} \cos^2\left(\frac{\pi}{4}\right) = \frac{1}{2} + \frac{1}{2^{kt+1}},$$

where $\epsilon(k) = 1/2^{kt+1}$ is negligible. Therefore, Alice is unaware of whether Bob received the correct message or not.

However, Bob can check whether he has recovered the correct random key r by comparing his hash value $h(r')$ with the second part of the received information d. According to the properties of the hash function, the probability of the first part of the hash value matching the second part is negligible in the case of Alice's coding basis being different from the measurement basis chosen by Bob.

5.2 Concealing

In this section, we show that if Alice is honest, the probability of Bob recovering the message to transfer before the opening phase is negligible.

This part of the statement follows directly from the security of the qPKE construction. The entropy of the entire secret key is given by the joint entropy $H(n, s)$ of the unknown n and s.

$$H(d) = H(n) + H(s|n)$$
$$= \log_2\left(|\tilde{\mathbb{N}}|\right) + \sum_{v\in\tilde{\mathbb{N}}} p(v)H(s|n = v) = \log\left(|\tilde{\mathbb{N}}|\right) + k\left(n_u + n_l\right)\Big/2,$$

where n is distributed uniformly over a finite interval $\tilde{\mathbb{N}} = (n_l, n_u), n_l \gg 1$. It can be seen that the secret key space is related to the range of n and the number of qubits (k). Obviously, the space of secret keys can be huge, and it is meaningless to pick them randomly from an infinite space. It follows that from the quantum public key, the possibility of achieving the inverse operation to obtain the secret key is negligible, which guarantees the unidirectionality of the one-way function.

In addition, the secrecy of the secret key is guaranteed by the fact that the preparation of the public key state is unknown to everyone except Alice before the opening phase. The state of each qubit of the public key is randomly chosen by Alice and is independent of the other qubits. As proven in [27], with a proper choice of n, the qPKE construction is secure against unauthorized users based on the uncertainty principle. Therefore, with the same choice of a proper n, the unidirectionality of the one-way function ensures that Bob cannot learn the message that Alice meant to send before the opening phase, and the protocol is a concealing one.

5.3 Probabilistic transfer

Furthermore, after the opening phase, Bob recovers the message with, up to a negligible value, a probability 1/2 + $\epsilon(k)$. This part of the description can be attributed to the fact that after Bob receives the secret key from Alice in the opening phase, there is still no strategy to get the whole encoded random key.

The proposed scheme divides the random key r into t successive units of bits $\bar{r}_i$, $(1 \le i \le t)$, the random key of each unit represents the shared unit, and the message remains secret for any $t-1$-shared units. To retrieve the message, dishonest Bob needs to know information about every shared unit, i.e., he needs to infer the correct measurement basis without destroying any of the shared units. This cannot be carried out.

Now consider dishonest Bob. First, we analyze the optimal cheating strategy if Bob has infinite ability. Bob chooses a basis to measure the quantum state, and if the projection is successful, i.e., the correct basis is chosen, he will further calculate to get the message. If the projection fails, Bob recovers the quantum state and then chooses another measurement basis and measures the quantum state again to obtain the message. However, both non-demolition measurements of qubits are out of technological reach today and could remain hard for a very long time for high k values [30]. Bob must therefore seek other strategies, such as utilizing the several qubits present in a shared unit to infer the coding basis with a probability greater than 1/2.

After undoing the initial rotation of the quantum state, Bob will get the following state:

$$\begin{aligned}|\psi'\rangle &= \bigotimes_{j=1}^{kt} \hat{\mathcal{R}}\left(-s_j\theta_n\right)\hat{\mathcal{R}}\left(s_j\theta_n + \frac{b\pi}{2} + r_j\pi\right)|0\rangle \\ &= \bigotimes_{j=1}^{kt} \cos\left(\frac{b\pi/2 + r_j\pi}{2}\right)|0\rangle + \sin\left(\frac{b\pi/2 + r_j\pi}{2}\right)|1\rangle.\end{aligned}$$

Let $|0\rangle_x = |+\rangle, |1\rangle_x = |-\rangle$; there is $|\psi'\rangle = \otimes_{j=1}^{kt}|r_j\rangle$ if $b = 0$, and there is $|\psi'\rangle = \otimes_{j=1}^{kt}|r_j\rangle_x$ if $b = 1$. However, to Bob, $|\psi'\rangle_j$ is randomly in one of the states $\{|0\rangle, |1\rangle\}$ or $\{|+\rangle, |-\rangle\}$, i.e., $|\psi'\rangle_j$ is a maximally mixed state whose density matrices are $\rho = \frac{1}{2}(|0\rangle\langle 0| + |1\rangle\langle 1|) = \frac{I}{2}$. No measurement that Bob made could distinguish the maximally mixed state. Furthermore, for more effective cheating, Bob might perform a joint measurement on $|\psi'\rangle$ to replace the one qubit measurement. But his capability of cheating should not increase, as this is equal to measuring a maximally mixed state with multi-dimension. Consequently, dishonest Bob can only guess the basis successfully with a probability of 1/2.

In summary, Bob can only infer whether the measurement basis is correct by parity bits, i.e., he has to try one basis to measure several shared units. According to the idea of secret sharing (any $t-1$-shared units will get nothing about the message), these shared units would also be irreversibly damaged, making it impossible for him to obtain the message.

5.4 Oblivious

To conclude our discussion on security, we demonstrate that the protocol is oblivious. At the end of the protocol, Alice is unaware of whether Bob has received the message or not. The no-communication theorem may be referenced in this section of the statement. It should be noted that Alice's attacks should not have the effect of making it difficult for Bob to know for sure whether he obtained the correct message or not, as this would go against the original objective of OT.

Theorem 2. (No-communication theorem). During the measurement of an entangled quantum state, it is not possible for one observer, by measuring a subsystem of the total state, to communicate information to another observer. The theorem gives conditions under which such transfer of information between two observers is impossible.

As can be seen, Alice communicates with Bob in one-way communication, in which Bob performs local operations and measurements without communicating with Alice. Here, no follow-up communication of entanglement can be used to exchange and obtain information; therefore Alice has no way of knowing through entanglement whether Bob has chosen the correct measurement basis. Otherwise, one could achieve faster-than-light communication, thus explicitly violating causality and the principle of relativity. Indeed, what entanglement effects are the correlations: Bell inequalities are given in terms of various correlation functions, and the violation of local realism can be observed only upon distant observers exchanging the results of their local measurements. Alice honestly chooses the coding basis, sends the quantum state to Bob, and does not receive any feedback from Bob. Therefore, based on the no-communication theorem, Alice is oblivious to whether Bob gets the message or not.

On the one hand, dishonest Alice could not convince Bob that the lack of access to the message was his own business without being detected as cheating. For this reason, Bob can check whether Alice is cheating by following the steps as follows: first, Bob measures the quantum bits at position $[1, kt/2]$. Each bit d_i of the hash value $d = h(r)$ is the parity of the ith unit of the message; hence, all the bits of the digest are mutually independent. If he always observes the parity bit d_i matching the shared unit $\bar{r}_i$ in the opening phase, Bob can be sure that Alice is not cheating. Otherwise, he will choose another basis to measure the remaining quantum bits, and if he fails to observe matching parity bits, this means that Alice cheated and the protocol is terminated. Alice still does not know which basis Bob will use to check the second half. Therefore, she has to be honest, and she does not know whether Bob received the correct message or not.

On the other hand, dishonest Alice cannot ensure that Bob always gets the message. Entanglement attacks do not work, so Alice will look for other strategies, such as the existence of a

quantum state that will collapse to a certain bit r_j with a high probability, regardless of Bob's choice. In the proposed scheme, Bob getting the correct message depends on whether he chooses the basis that is consistent with Alice's basis $\{|0\rangle, |1\rangle\}$ and $\{|+\rangle, |-\rangle\}$. Any single quantum state can be written in the following form:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle = \frac{\alpha+\beta}{\sqrt{2}}|+\rangle + \frac{\alpha-\beta}{\sqrt{2}}|-\rangle,$$

where $|\alpha|^2 + |\beta|^2 = 1$. It is obvious that such a quantum state does not exist. Therefore, it does not convince Bob that he has chosen the correct measurement basis because d and $h(r')$ are not always the same.

Finally, we discuss the relationship between an all-or-nothing oblivious transfer protocol and the no-go theorem in two aspects. On the one hand, it is clear that the all-or-nothing OT protocol is based on a one-way function rather than any quantum bit commitment scheme, so it does not conflict with the result that an unconditionally secure QBC scheme cannot be achieved within non-relativistic physics [13]. On the other hand, the purposes of malicious Alice's attack are different. In bit commitment, Alice may want to change what she has committed, while in oblivious transfer, Alice may want to know whether Bob receives the right state. Therefore, in the all-or-nothing OT, Alice may use coherence to change the coding basis, however, which is not Alice's purpose.

6 Conclusion

In this article, we study the design methods and security analysis of the quantum all-or-nothing OT protocol based on secure quantum one-way functions, mainly in soundness, concealing, probabilistic transfer, and obliviousness. The proposed scheme does not violate the no-go theorem, and its security is based on the laws of quantum physics. In practice, the security of the protocol will remain very reliable for high k values because of limitations on non-demolition measurements. Moreover, the design of secure QOTs is important for building highly trusted cryptographic protocols and algorithms and is the foundation of quantum cryptographic protocols.

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

PW and YS conceived the presented idea. PW and YS developed the theory and the proofs. PW and ZS verified the methods. All authors discussed the results and contributed to the final manuscript.

Funding

This work was supported by the National Natural Science Foundation of China (61872245), Shenzhen Science and Technology Program (JCYJ20210324100813034, JCYJ20190809152003992, and JCYJ20180305123639326), and Shenzhen Polytechnic Research Foundation (6022310031K).

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. Rabin M. How to exchange secrets with oblivious transfer. In: *Technical report tech. Memo TR-81*. Cambridge, MA: Aiken Computation Laboratory (1981).

2. Even S, Goldreich O, Lempel A. A randomized protocol for signing contracts. *Commun ACM* (1985) 28(6):637–47. doi:10.1145/3812.3818

3. Brassard G, Crépeau C, Robert JM. All-or-nothing disclosure of secrets. In: Conference on the Theory and Application of Cryptographic Techniques (1986). p. 234–8.

4. Crépeau C. Equivalence between two flavours of oblivious transfers. In: Conference on the Theory and Application of Cryptographic Techniques. Berlin, Germany: Springer (1987). p. 350–4.

5. Brassard G, Crépeau C, Robert JM. Information theoretic reductions among disclosure problems. In: 27th Annual Symposium on Foundations of Computer Science (sfcs 1986). Toronto, ON, Canada: IEEE (1986). p. 168–73.

6. Crépeau C, Sántha M. Efficient reduction among oblivious transfer protocols based on new self-intersecting codes. In: *Sequences II*. Berlin, Germany: Springer (1993). p. 360–8.

7. Brassard G, Crépeau C, Santha M. Oblivious transfers and intersecting codes. *IEEE Trans Inf Theor* (1996) 42(6):1769–80. doi:10.1109/18.556673

8. Shor PW. Algorithms for quantum computation: Discrete logarithms and factoring. In: Proceedings 35th Annual Symposium on Foundations of Computer Science. Santa Fe, NM, USA: IEEE (1994). p. 124–34.

9. Heisenberg W. Über den anschaulichen inhalt der quantentheoretischen kinematik und mechanik. In: *Original scientific papers wissenschaftliche originalarbeiten* (1985). p. 478–504.

10. Wiesner S. Conjugate coding. *Sigact News* (1983) 15:78–88. doi:10.1145/1008908.1008920

11. Bennett CH, Brassard G, Mermin ND. Quantum cryptography without bell's theorem. *Phys Rev Lett* (1992) 68:557–9. doi:10.1103/physrevlett.68.557

12. Renner R, Gisin N, Kraus B. Information-theoretic security proof for quantum-key-distribution protocols. *Phys Rev A (Coll Park)* (2005) 72(1): 012332. doi:10.1103/physreva.72.012332

13. Mayers D. Unconditionally secure quantum bit commitment is impossible. *Phys Rev Lett* (1997) 78:3414–7. doi:10.1103/physrevlett.78.3414

14. Lo HK, Chau HF. Is quantum bit commitment really possible? *Phys Rev Lett* (1997) 78:3410–3. doi:10.1103/physrevlett.78.3410

15. Lo HK, Chau H. Why quantum bit commitment and ideal quantum coin tossing are impossible. *Physica D: Nonlinear Phenomena* (1998) 120(1-2):177–87. doi:10.1016/s0167-2789(98)00053-0

16. Hughston L, Jozsa R, Wootters W. A complete classification of quantum ensembles having a given density matrix. *Phys Lett A* (1993) 183(1):14–8. doi:10.1016/0375-9601(93)90880-9

17. Halvorson H. Generalization of the hughston-jozsa-wootters theorem to hyperfinite von neumann algebras. *J Math Phys* (2003).

18. Bouman NJ, Fehr S, González-Guillén C, Schaffner C. An all-but-one entropic uncertainty relation, and application to password-based identification. In: Conference on Quantum Computation, Communication, and Cryptography. Berlin, Germany: Springer (2012). p. 29–44.

19. Wehner S, Schaffner C, Terhal BM. Cryptography from noisy storage. *Phys Rev Lett* (2008) 100(22):220502. doi:10.1103/physrevlett.100.220502

20. Konig R, Wehner S, Wullschleger J. Unconditional security from noisy quantum storage. *IEEE Trans Inf Theor* (1984) 58(3):1962–84. doi:10.1109/tit.2011.2177772

21. Souto A, Mateus P, Adao P, Paunković N. Bit-string oblivious transfer based on quantum state computational distinguishability. *Phys Rev A (Coll Park)* (2015) 91(4):042306. doi:10.1103/physreva.91.042306

22. Rodrigues J, Mateus P, Paunković N, Souto A. Oblivious transfer based on single-qubit rotations. *J Phys A: Math Theor* (2017) 50(20):205301. doi:10.1088/1751-8121/aa6a69

23. Grilo AB, Lin H, Song F, Vaikuntanathan V. Oblivious transfer is in miniqcrypt. In: Annual International Conference on the Theory and Applications of Cryptographic Techniques (2021). p. 531–61.

24. Bartusek J, Coladangelo A, Khurana D, Ma F. One-way functions imply secure computation in a quantum world. In: Annual International Cryptology Conference (2021). p. 467–96.

25. Shi J, Lu Y, Feng Y, Huang D, Lou X, Li Q, et al. A quantum hash function with grouped coarse-grained boson sampling. *Quan Inf Process* (2022) 21(2):73–17. doi:10.1007/s11128-022-03416-w

26. Gottesman D, Chuang I. Quantum digital signatures. *arXiv: Quan Phys* (2001).

27. Nikolopoulos GM. Applications of single-qubit rotations in quantum public-key cryptography. *Phys Rev A (Coll Park)* (2008) 77(3):032348. doi:10.1103/physreva.77.032348

28. Nielsen MA, Chuang IL. *Quantum computation and quantum information: 10th anniversary edition*. Cambridge: Cambridge University Press (2010).

29. Shamir A. How to share a secret. *Commun ACM* (1979) 22(11):612–3. doi:10.1145/359168.359176

30. He GP. Coherent attack on oblivious transfer based on single-qubit rotations. *J Phys A: Math Theor* (2018) 51(15):155301. doi:10.1088/1751-8121/aaaea5