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, ρ_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 $n = 4$.

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

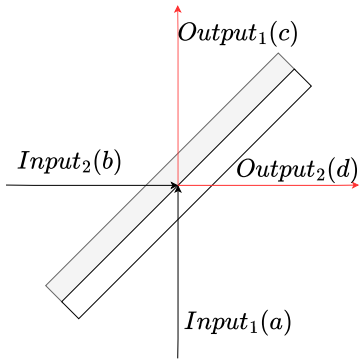

FIGURE 2
Beam splitter is an optical device that can split one beam of light into two beams. It is a key part of most interferometers. When two beams of light get into the beam splitter from $Input_1$ and $Input_2$, respectively, each of them will be split into two beams. $Output_1$ and $Output_2$ will output the interfering results of the split beams.

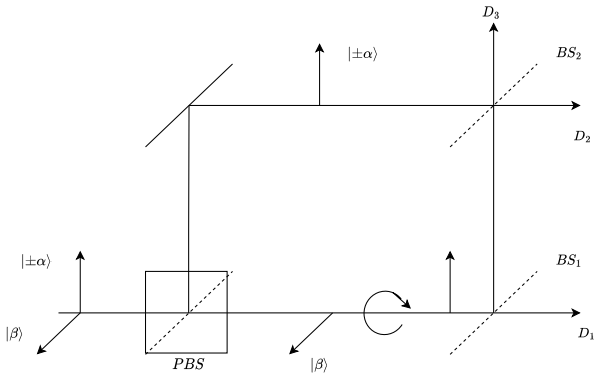

FIGURE 3
USD measurement device.

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 $\boldsymbol{s} = (1, 2, \ldots, 2\,nL)$ as V_1's voting code, denoted by $\boldsymbol{s_1} = (s_1^{(1)}, s_1^{(2)}, \ldots, s_1^{(L)})$. 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, …, n and j = 1, 2, …, 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 $2 \le i \le n-1$, 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 $X_1 \ge s_a p_{USD} nL$. So, the probability of "the protocol aborts" is

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

According to Hoeffding's inequalities, we obtain

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

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

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

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' 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

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

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

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

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 $2s_aL$.

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