Received: 22 May 2024 | Revised: 11 September 2024 | Accepted: 31 October 2024

IET Quantum Communication

DOI: 10.1049/qtc2.12117

ORIGINAL RESEARCH

Quantum anonymous one vote veto protocol based on entanglement swapping

Yanmeng Wang[1] | Min Jiang[1,2] | Yuzhen Wei[3] | Wenhao Zhao[1]

[1]School of Electronics & Information Engineering, Soochow University, Suzhou, Jiangsu, China

[2]Key Laboratory of System Control and Information Processing, Ministry of Education, Shanghai, China

[3]School of Information Engineering, Huzhou University, Huzhou, Zhejiang, China

Correspondence

Min Jiang.
Email: jiangmin08@suda.edu.cn

Funding information

National Natural Science Foundation of China, Grant/Award Number: 61873162; Key Laboratory of System Control and Information Processing, Ministry of Education, China, Grant/Award Number: Scip20240106

Abstract

As a special voting method, one-vote veto voting also has a wide range of applications. A veto means that when the voting council puts forward a proposal, it cannot pass unless all the voters agree to it. If there is a no vote, the proposal will be rejected, but no one will know how anyone else votes. In most existing quantum anonymous one-vote veto voting protocols, an absolutely honest third party is generally required to assist the voting. However, it is difficult to find a fully trusted third party in reality. In addition, the existing quantum anonymous one-vote veto protocol does not consider the attack from the insider voters. Therefore, based on the characteristics of entanglement swapping between the Cat state and Bell state, the authors propose a new quantum anonymous one-vote veto protocol, which can not only calculate the voting result quickly and effectively but also demonstrate higher security.

KEYWORDS

quantum communication, quantum computing, quantum cryptography, quantum information

1 | INTRODUCTION

Voting is one kind of daily social activity in modern society which is used widely in our lives. Important decisions and democratic elections often depend on the voting system. Initially, voting systems require voters to cast their ballots at the designated locations, followed by supervised manual counting. A common example is the ballot box voting. Each voter is assigned a blank ballot on which the voter writes his ballot. The voter then places the filled ballot into a pre-assigned ballot box. The authorisation server discloses the voting results after collecting all the votes. This approach implements the functionality of elections but some limitations affect its security. For instance, a voter may attempt to manipulate the election results by tampering with a marked ballot, all while evading detection. The challenges arising from geographical and temporal barriers make it challenging for voters to participate in real-time, face-to-face voting. These factors contribute to a demanding voting environment and hinder overall operability.

With the rapid development of information technology and the popularity of the Internet, the electronic voting technology came into being and gradually replaced the previous voting technology. Since Chaum proposed the first private electronic voting scheme in 1981, a variety of different electronic voting protocols have been proposed [1–3]. A common feature of the protocols is that the security is supported by the computational complexity of some hard problems, such as the discrete logarithm problem and many factorisation problems. Since then, people have carried out a lot of research on electronic voting and found that the security of classical electronic voting protocols was not enough under the background of the continuous enhancement of computer computing power.

In 2005, literature [4] proposed the concept of quantum voting, which applied the knowledge of quantum cryptography to the voting process for the first time and provided a new idea for traditional voting. In order to make up for the lack of security in the traditional voting scheme, Hillery [5] proposed two voting models based on the existing quantum communication methods in 2006. One was the distributive voting model, and the other was the mobile voting model. In 2007, Vaccaro et al. [6] proposed an accurate concept of the criteria for quantum voting protocols. In 2008, Li et al. [7] proposed

one protocol for voter anonymity, which made full use of the entanglement characteristics of quantum states. In 2009, Dmitri et al. [8] designed one anonymous quantum voting protocol based on Bell states. In 2010, Xu et al. [9] improved the efficiency and other performance of the voting protocol based on Vaccaro's protocol. In 2012, Li et al. [10] proposed one anonymous quantum voting protocol in order to change the shortcomings of previous voting protocols that participants could not verify each other. In 2012, Jiang et al. discussed the binary voting and multi-value voting scheme [11]. They used the entangled states of continuous variables as the information carriers to ensure the privacy and anonymity of each voter. In 2016, Tian et al. [12] selected the GHZ state for communication in order to ensure the security of the voting scheme. Thapliyal et al. [13] designed a quantum voting protocol based on quantum secure direct communication. Wang et al. proposed the first quantum anonymous voting protocol for any number of candidates that simultaneously satisfied privacy, non-reusability, verifiability, fairness and self-counting in literature [14].

In 2020, Mahender et al. in literature [15], proposed an end-to-end verifiable Internet voting system (E2E-IVS), which provided a good mobility for voters and enabled voters to vote secretly without revealing any information about the vote. In 2021, Emil et al. [15] described a scheme that exploited the exponential separation between quantum and classical communication complexity to authenticate voters and prevent forgery. Wu et al. detailed the construction of a one-vote veto using qubits in their work, referencing literature [16]. They also introduced the inaugural quantum anonymous voting protocol, leveraging qubits and Pauli operations Z and X. Mishra et al. proposed several quantum anonymous veto protocols in literature [17], based on some quantum resources, and classified the protocols according to probabilistic, iterative and deterministic methods to finish the task and achieve the expected result. Wang et al. proposed one quantum anonymous veto voting protocol based on GHZ state entanglement in literature [18].

The use of the one-vote veto system can effectively protect the minority's specific power from being violated and prevent 'majority tyranny' [19]. For example, in an investment company, certain investors hold veto power over specific voting matters related to their interests to safeguard their critical profits. Internationally, the permanent members of the UN Security Council possess veto power which helps prevent conflicts between countries. To date, quantum anonymous one-vote veto protocols have rarely been considered. Most existing quantum anonymous one-vote veto voting protocols generally require an absolutely honest third party to assist in the voting process [20–29]. However, finding a fully trusted third party in reality is difficult. Moreover, the existing quantum anonymous one-vote veto protocols do not account for attacks from insider voters [30–36]. Therefore, based on the entanglement exchange of Cat states and Bell states, we propose a new quantum anonymous one-vote veto protocol that not only calculates the voting results quickly and efficiently but also offers enhanced security.

The paper is organised as follows. In Section 2, we introduce the quantum resources used by the protocol. In Section 3, we propose the flow of the protocol. In Section 4, we analyse the performance of the protocol. The paper concludes in Section 5 with a summary.

2 | QUANTUM RESOURCE

The d-level Bell state is a generalisation of the two-level Bell state to the multi-level Bell state, and its general form first appeared in [20], which is described in detail as follows:

$$|\phi(u,v)\rangle = \frac{1}{\sqrt{d}} \sum_{k=0}^{d-1} e^{\frac{2\pi iku}{d}} |k\rangle |k \oplus v\rangle, \tag{1}$$

where $\oplus$ represents the addition module d operation and $u, v \in \{0, 1, 2, \cdots, d-1\}$.

Let's introduce the unitary transformation $U^{(u,v)}$, whose expression is written as follows:

$$U^{(u,v)} = \frac{1}{\sqrt{d}} \sum_{k=0}^{d-1} e^{\frac{2\pi iku}{d}} |k \oplus v\rangle\langle k|. \tag{2}$$

The unitary transformation $U^{(u,v)}$ applied to $|\phi(0,0)\rangle$ can give the arbitrary d-level Bell state, which can be described as follows:

$$\left(I \otimes U^{(u,v)}\right)|\phi(0,0)\rangle = |\phi(u,v)\rangle. \tag{3}$$

The d-level Cat state with n particles can be regarded as the extension of the d-level Bell state to many particles, which was first proposed in the literature [21], and its general form is described as follows:

$$\begin{aligned} &|\xi(w_0, w_1, w_2 \ldots, w_n)\rangle \\ &= \frac{1}{\sqrt{d}} \sum_{k=0}^{d-1} e^{\frac{2\pi ikw_0}{d}} |k, k+w_1, k+w_2, \cdots, k+w_n\rangle, \end{aligned} \tag{4}$$

where $w_0, w_1, w_2 \ldots, w_n \in \{0, 1, 2, \cdots, d-1\}$.

Entanglement swapping is one important operation in quantum information processing, which can cause the entanglement of quantum systems without any direct interaction, and has been widely used in various quantum cryptography protocols [22–24]. In 2001, Karimipour et al. [21] first proposed the law of entanglement swapping between d-level Cat and d-level Bell states, which can be specifically described as follows:

$$\begin{aligned} &|\xi(w_0, w_1, w_2, \ldots, w_t \ldots, w_n)\rangle_{p_0,p_1,p_2,\ldots,p_t,\ldots p_n} \otimes |\phi(u,v)\rangle_{g,h} \\ &= \frac{1}{d} \sum_{r,s=0}^{d-1} e^{\frac{2\pi irs}{d}} |\xi(w_0 \oplus r, w_1, w_2 \ldots, s \oplus v, \ldots w_n)\rangle_{p_0,p_1,p_2,p_3,\ldots,h,\ldots,p_n} \\ &\otimes |\phi(u \ominus r, w_t \ominus s)\rangle_{g,p_t}, \end{aligned} \tag{5}$$

where $\ominus$ represents the module d subtraction. After the d-level Bell state measurement is performed on particles g and p_t $(1 \le t \le n)$, the measurement result is assumed to be one of the following forms:

$$|\phi(u \ominus r, w_t \ominus s)\rangle_{g,p_t}. \tag{6}$$

Next we get a new Cat state

$$|\xi(w_0 \oplus r, w_1, w_2 \ldots, s \oplus v, \ldots w_n)\rangle_{p_0,p_1,p_2,p_3,\ldots,h,\ldots,p_n}. \tag{7}$$

It shows an intuitive representation of the entanglement swapping between the Cat state and Bell state in Figure 1. In the upper part of Figure 1, the particles $p_0, p_1, p_2, \ldots, p_t, \ldots p_n$ form the Cat state, and the particles g and h form the Bell state. In the lower part of Figure 1, entanglement swapping occurs between the Cat state and the Bell state.

3 | PRODUCE OF THE PROTOCOL

In quantum anonymous one-vote veto protocol based on entanglement switching, the voting network is managed by a voting council, CA, which is also responsible for the preparation and the counting of Cat states. In practice, voting activities often take place between parties who only partially trust each other, or even between direct competitors. In this context, the server is considered semi-honest, meaning it may attempt any quantum mechanics-constrained attacks, except for being bribed by or conspiring with malicious voters. Under the framework of quantum mechanics, a malicious voter may independently carry out any possible aggressive actions or collaborate with other malicious voters. Theoretically, we assume that both the classical and quantum channels are authenticated, and the environment is ideal—meaning no noise, no loss of particles, and perfect equipment performance. Suppose that when a CA makes a proposal, each voter will cast a "yes" or "no" vote on the proposal. The proposal can be passed only if all the voters approve it. This means that if the voters vote against the proposal, it will not pass. Figure 2 illustrates a schematic diagram of the quantum anonymous one-vote veto voting protocol.

3.1 | The initialisation phase

Step 1: Voter $V_i(i = 1, 2 \ldots, n)$ sends the voting application to the Voting Council CA with its real identity information. The CA verifies the voting request information. If the identity of the requested user is legitimate and it is the first time to apply for voting, the CA calculates the identity information of the voter to the local database. Assuming the number of legitimate voters is n, CA will publish the addresses of these legitimate voters. Then, based on the multi-party quantum key negotiation technique, as shown in reference [4], all voters V_i will share the key K.

$$K = [k_1, k_2, \ldots, k_i], \tag{8}$$

where $K \in \{0, 1\}$.

Step 2: Each voter V_i prepares one d-level Bell state $|\phi(0,0)\rangle_{g,h_i}$ for voting, where $d > n$. CA produces the d-level Cat state of an $n+1$ particle $|\xi(w_0, w_1, w_2, w_3 \ldots, w_n)\rangle_{p_0,p_1,p_2,p_3,\ldots,p_n}$. Then, CA prepares n single particle

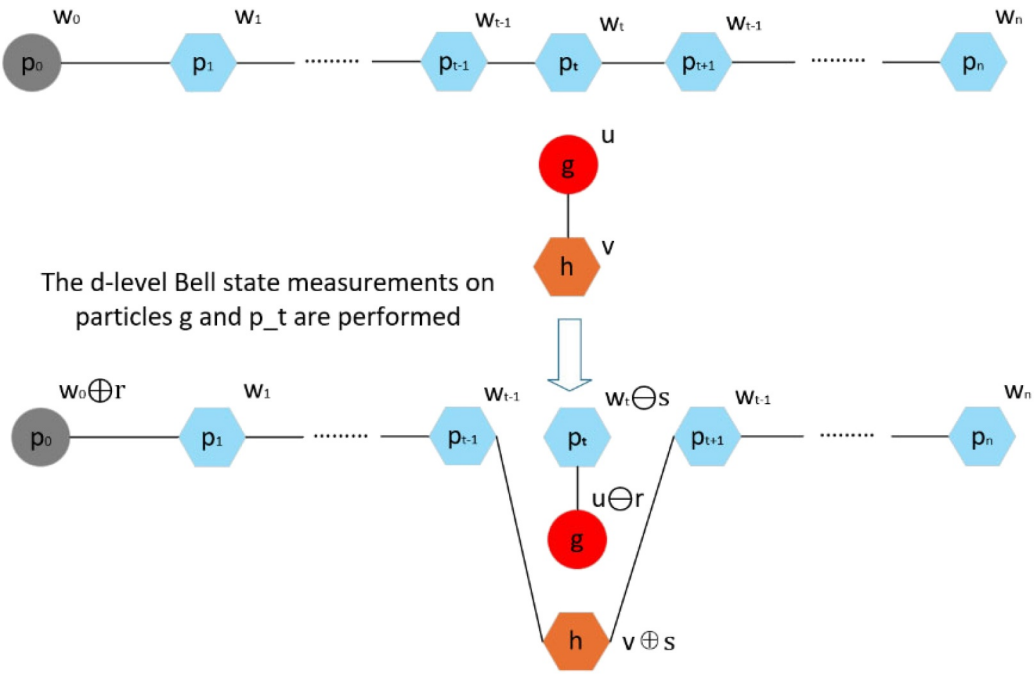

FIGURE 1 Entanglement swapping between one d-level Cat state and one d-level Bell state.

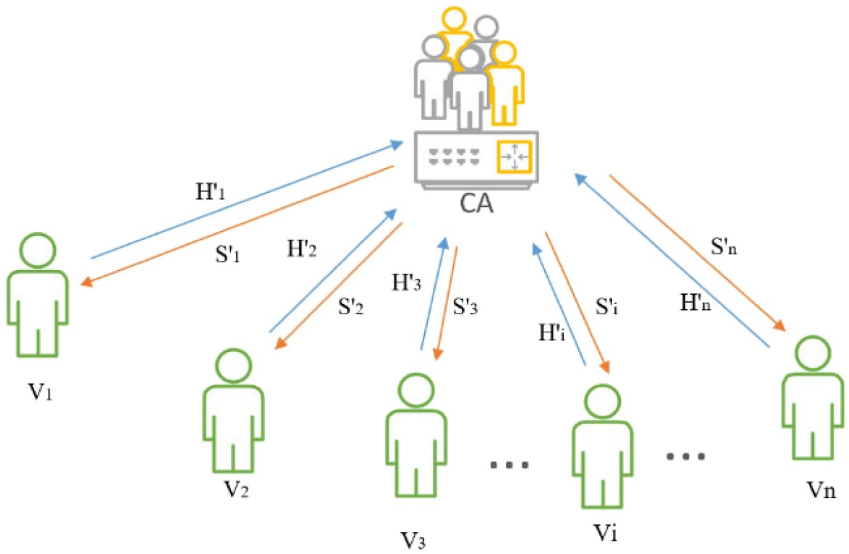

FIGURE 2 Schematic of quantum anonymous one-vote veto protocol based on entanglement swapping.

sequences $S_i(i = 1, 2, 3, \ldots, n)$. Each sequence S_i has δ decoy photons, and each of these decoy photons from $\{|k\rangle_C, |k\rangle_F\}(k = 0, 1, 2, \ldots d-1)$ is selected and arranged randomly. Then, CA inserts the particle $p_i(i = 1, 2, 3, \ldots, n)$ of the Cat state $|\xi(w_0, w_1, w_2, w_3 \ldots, w_n)\rangle_{p_0,p_1,p_2,p_3,\ldots p_n}$ into the particle sequence $S_i(i = 1, 2, 3, \ldots, n)$ at a random position. In this way we can get a new particle sequence $S_i'(i = 1, 2, 3, \ldots, n)$. CA retains the particle p_0 and the parameter information $\{w_0, w_1, w_2 \ldots, w_n\}$ locally, and simultaneously sends $S_i'(i = 1, 2, 3, \ldots, n)$ to the voter $V_i(i = 1, 2, 3, \ldots, n)$ via quantum channels.

Step 3: After receiving the sequence S_i', the voter V_i returns the confirmation signal to the CA. After receiving the confirmation signal, the CA sends the position information of the decoy photons in the sequence S_i' and the corresponding measurement base to the voter. According to the position information of the decoy photon, the voter uses the corresponding measurement base for each decoy photon to perform the measurement. The V_i then sends the measurement results to the CA, which calculates the error rate by comparing the measurement results of the decoy photon with its initial state, and compares it with the error rate threshold to determine whether there is an eavesdropper. If the error rate exceeds the threshold, the voting process will be stopped and the protocol will be voted again. Otherwise, the voting agreement goes ahead.

3.2 | Voting phase

Step 1: After voter V_i abandons all decoy photons, only the particles p_i of the Cat state are retained. We suppose that the voting intention of voter V_i is v_i, where $v_i = 0$ indicates that he agrees with the proposal, and $v_i = 1$ indicates that he opposes the proposal. V_i performs the operation $I \otimes U^{(u_i,v_i)}$ onto the particles g_i and h_i to generate the d-level Bell state $|\phi(u_i, v_i)\rangle_{g_i h_i}$, namely the following equation:

$$|\phi(u_i, v_i)\rangle_{g_i h_i} = I \otimes U^{(u_i,v_i)} |\phi(0, 0)\rangle_{g_i h_i}, \tag{9}$$

where u_i is randomly generated by voter V_i, *and* $u_i \in \{0, 1, 2, \cdots, d-1\}$. V_i then performs the d-level Bell state measurement onto particles g_i and p_i, assuming that the measurement results are as follows:

$$|\phi(l_i, l_i')\rangle_{g_i p_i}, \tag{10}$$

where $l_i' = u_i \ominus r_i, l_i = w_i \ominus s_i$, $L_i = w_i \ominus s_i \ominus r_i$.

Step 2: All voters cooperate to calculate the following equation:

$$T = \sum_{i=1}^{n} L_i \; mod \; d, \tag{11}$$

and send T to CA. To prevent the classical information L_i from being eavesdropped when the voters cooperate to calculate T, voters can use the shared key K to encrypt L_i and transmit information and sum the T. The particular encryption technique employed is as follows: V_i prepares a detection sequence D_i, containing i ordered detection particles $\{d_0, d_1, \ldots, d_i\}$. d_i is in a specific state that depends on the K. If $k_i = 0, d_i = |+\rangle; k_i = 1, d_i = |-\rangle$. Then, mixing L_i and D_i together, V_i inserts each D_i randomly into L_i. The new combined sequence is P_i. Then, via a quantum channel, each voter V_i sends the particle h_i to the CA. To prevent eavesdropping, we introduce the decoy photons and obtain the particle sequence H_i' before sending it to the CA.

3.3 | Counting phase

Step 1: After CA performs the safety detection on particle sequence $H_i'(i = 1, 2, \cdots, n)$ and passes the detection, CA will recover particle h_i, and then make the d-level Cat state

measurement on particles $p_0, h_1, h_2, \cdots, h_n$. The measurement results are written as follows:

$$|\xi(\tilde{w}, \tilde{v_1}, \tilde{v_2}, \ldots, \tilde{v_i} \ldots, \tilde{v_n})\rangle_{p_0,h_1,h_2,\ldots,h_i,\ldots h_n}, \quad (12)$$

where

$$\tilde{w} = \left(w_0 + \sum_{i=1}^{n} r_i\right) mod\ d,$$

$$\tilde{v_i} = (s_i + v_i) mod\ d. \quad (13)$$

Step 2: CA further calculates the following equation:

$$R = T \oplus \tilde{w} \oplus \sum_{i=1}^{n} \tilde{v_i} \ominus \sum_{i=0}^{n} w_i. \quad (14)$$

If $R = 0$, it means that all voters unanimously approve CA's proposal. Otherwise, it indicates that some voters have voted against the proposal, and the proposal will be rejected.

3.4 | Verification phase

If the motion still passes when a voter votes against the motion, the voter will anonymously broadcast the termination signal. CA will then publish $\tilde{v_i}$ and w_i for ticket verification. V_i will calculate whether $l_i \oplus \tilde{v_i} \ominus w_i = v_i$. If $l_i \oplus \tilde{v_i} \ominus w_i \neq v_i$, the voting information in the protocol is likely to be tampered with, and the voting protocol will be executed again.

4 | ANALYSIS

4.1 | Correctness

In this voting protocol, CA prepares the d-level Cat state of $n + 1$ particles

$$|\xi(w_0, w_1, w_2, \cdots, w_i, \ldots, w_n)\rangle_{p_0,p_1,p_2,p_3,\ldots,p_i,\ldots,p_n}. \quad (15)$$

The voting content of each voter $V_i(i = 1, 2, 3, \cdots n)$ is $v_i(i = 1, 2, 3, \cdots n)$ respectively, where $v_i \in \{0, 1\}$. In step 1 of the voting phase, after encoding the voting content by the corresponding unitary operation, each voter will obtain one Bell state:

$$|\phi(u_i, v_i)\rangle_{g_i,h_i}. \quad (16)$$

After V_i performs one d-level Bell measurement on the particle g_i from the Bell state and the particle p_i from the Cat state, the measurement result will be obtained:

$$|\phi(u_i \ominus r_i, w_i \ominus s_i)\rangle_{g_i,p_i}. \quad (17)$$

After the all voters perform the d-level Bell measurement, the entanglement swapping can be achieved by the Cat state and the Bell state. Figure 3 shows in detail the entire process of entanglement swapping between one $(n + 1)$-particle d-level Cat state and n d-level Bell states.

Then, each voter sends particle $h_i(i = 1, 2, \cdots n)$ to CA, which performs the d-level Cat state measurement on particles $p_0, h_1, h_2, \cdots$, and h_n to obtain the measurement results

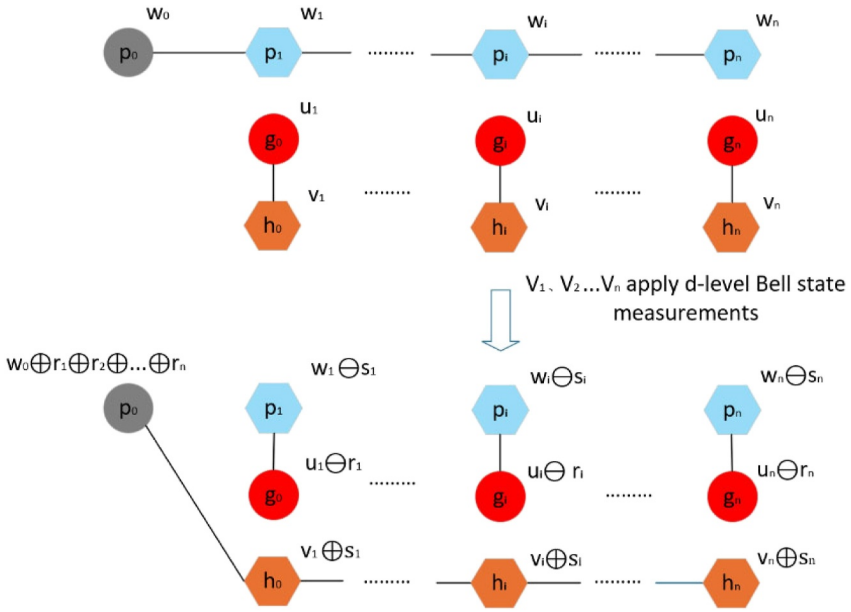

FIGURE 3 Entanglement swapping between one $(n + 1)$-particle d-level Cat state and n d-level Bell states.

$$\left|\xi\left(\left(w_0+\sum_{i=1}^{n} r_i\right) mod\ d, s_1 \bigoplus v_1, s_2 \bigoplus v_2, \ldots, . \right.\right. \\ \left.\left. s_i \bigoplus v_i \ldots, s_n \bigoplus v_n\right)\right\rangle . \tag{18}$$

Now equation (10) can be rewritten as follows:

$$\begin{aligned} T &= \sum_{i=1}^{n} L_i\ mod\ d \\ &= \left(\sum_{i=1}^{n} w_i \ominus s_i \ominus r_i\right) mod\ d \\ &= \left(\sum_{i=1}^{n} w_i\ mod\ d - \sum_{i=1}^{n} s_i\ mod\ d - \sum_{i=1}^{n} r_i\ mod\ d\right) mod\ d. \end{aligned} \tag{19}$$

Therefore, R is written as follows:

$$\begin{aligned} R &= \left[T + \left(w_0 + \sum_{i=1}^{n} r_i\right) mod\ d + \sum_{i=1}^{n} s_i\ mod\ d \right. \\ &\quad \left. + \sum_{i=1}^{n} v_i\ mod\ d - \sum_{i=0}^{n} w_i\ mod\ d\right] mod\ d \\ &= \sum_{i=1}^{n} v_i\ mod\ d. \end{aligned} \tag{20}$$

If all voters agree to the proposal, $v_1 = v_2 = v_3 = \cdots v_n = 0$, $R = 0$ is obtained. If there are voters who do not support the proposal, that is, $v_i = 1$, then $R \neq 0$. So the voting protocol is correct.

4.2 | Privacy

In this protocol, although the address of each voter is public, the classic information T calculated by the voters does not carry any voting information v_i. Therefore, the voting content of any voter is known only by himself. In addition, although CA can obtain classical information T and $s_i \bigoplus v_i$, since s_i is a random number obtained by voter V_i after Bell measurement and CA cannot obtain the specific value of s_i, CA cannot infer anyone's voting content v_i. Therefore, this voting agreement can well protect the privacy of voters.

Hereafter, we mainly discuss participant attacks. Generally, participant attacks are a much more powerful threat in multi-party quantum protocols. Here, we analyse two possible cases of participant attacks in detail as follows.

4.2.1 | Case 1: external attack

When quantum states are transmitted, an eavesdropper, Eve, might use external attacks such as intercept-retransmission, measurement-retransmission, or entanglement measurement attacks to eavesdrop on quantum information. To counteract these external attacks, this protocol uses decoy particle technology to monitor the quantum channel. Additionally, Eve could potentially compromise the privacy of the voting process by intercepting classical messages in transit. In step 2 of the voting phase, while voters send the classical information R to CA, Eve might intercept the classical information T and obtain information $w_i \ominus s_i \ominus r_i$ from T. However, since T does not contain any information related to the voting content $v_i (i = 1, 2, \cdots n)$, the intercepted classical information T will not reveal any details about the voting results.

4.2.2 | Case 2: insider attack

A vicious attack by voters

Malicious voters V_j pose a threat to voting protocol security. They can intercept or tamper with other voters' content, leading to the potential risks. During the transmission of quantum states in step 2 of the initialisation phase and step 1 of the voting phase, if a malicious voter V_j intends to intercept or eavesdrop on the quantum information of others, he will perform a similar manner to an external attack and thus be detectable. In step 2 of the voting stage, all voters cooperate to calculate the classical information T. But T does not carry any voter's voting content, and V_j cannot get any voting information from T. In addition, we suppose that there are r voters against the proposal in a certain voting scenario, but the voter V_j attempts to pass the proposal. Then V_j will no longer obey the voting rules and directly execute $U^{(u_j, d-r)}$ on the Bell particle h_j, resulting in the final statistical result of $R = 0$. But the probability that V_j guesses r as the number of negative votes is $\left(\frac{1}{2}\right)^{n-1}$. When there are a certain number of voters, the probability of correctly guessing will be extremely low. Even if V_j is lucky enough to tamper with the vote, this protocol can detect the malicious behaviour of tampering with the vote in the counting stage.

Voter V_j may also conspire with m other malicious voters $V_{j+1}, V_{j+2}, \cdots V_{j+m}$ to eavesdrop or tamper with votes. In the initialisation stage of step 2 and the voting stage of step 1, the intercepting or eavesdropping of the voters $V_j, V_{j+1}, V_{j+2}, \cdots V_{j+m}$ will be considered as the mode of external attack, which will be detected by this protocol. In the voting phase of step 2, although $V_j, V_{j+1}, V_{j+2}, \cdots V_{j+m}$ can directly determine L_j, $L_{j+1}, L_{j+2}, \cdots L_{j+m}$, they will not affect other L_i voters. In addition, since the voters do not carry any voter's voting content in the classical information T of cooperative calculation, $V_j, V_{j+1}, V_{j+2}, \cdots V_{j+m}$ cannot extract the voting information of any other voter from T even if they cooperate. Therefore, the poll is resistant to malicious attacks from voters.

An attack from the semi-honest CA

Voting activities may also be subject to attacks from the semi-honest CA. After CA receives the classical information T of

the voter and gets the measurement result of the new Cat state, it can calculate the vote result directly. If the vote does not meet CA's expectations, he may try to find the opponents of the proposal. Although CA can obtain classical information T and $s_i \oplus v_i$, since s_i is a random number obtained by voter V_i after the Bell measurement and CA cannot obtain the specific value of s_i, it cannot obtain anyone's voting content v_i. If CA forcibly announces the false voting results, the voters will find that the voting results have been tampered in the verification phase, and then complain and suspend the voting protocol. Therefore, this protocol can effectively prevent attacks from the semi-honest CA.

4.3 | Legitimacy

In this agreement, only legitimate voters may participate in the voting agreement. In the initialisation phase, the voter $V_i(i = 1, 2\ldots, n)$ send the voting application to the Voting Council CA with its real identity information. If the identity of the user is legitimate and it is the first time to apply for voting, the CA will record the identity information of the legitimate voter in the local database. CA will then publish the physical address of the legal voter to ensure that the voter can establish the contact with other legal voters. In addition, when quantum state or classical information of this protocol is transmitted between the sender and the receiver, it can be transmitted only after authentication by both parties. Thus, this agreement guarantees the legitimacy of the voters.

4.4 | Non-repeatability

Since each voter has a veto, no matter how many voters cast a negative vote, CA will announce that the proposal is not passed. Suppose that in a voting scenario, r voters oppose the proposal, but V_j attempts to pass the proposal. If V_j guesses the wrong number of negative votes, the proposal still fails to pass. If V_j correctly guesses that the number of negative votes is r, then V_j will no longer obey the voting rule, and directly perform $U^{(u_j, d-r)}$ on the Bell particle h_j. Therefore, the final statistic result is $R = 0$. However, the probability of V_j correctly guessing the number of negative votes is $\left(\frac{1}{2}\right)^{n-1}$, and when there are a certain number of voters, the probability of correctly guessing will be extremely low. Even if V_j can be guessed correctly, the protocol can present malicious acts of vote tampering during the counting stage. Therefore, the non-repeatability of our protocol can be maintained.

4.5 | Verifiability

During the verification phase of this protocol, if a voter votes against the proposal but the proposal is still adopted, the voter may anonymously broadcast the termination signal. At the same time, CA will publish $\tilde{v}_i(i = 1, 2, \cdots, n)$ and $w_i(i = 1, 2, \cdots, n)$ for ticket verification. V_i will calculate whether $l_i \oplus \tilde{v}_i \ominus w_i = v_i$ is satisfied. If $l_i \oplus \tilde{v}_i \ominus w_i \neq v_i$, there is a possibility that the votes in this agreement have been tampered with, and the vote will be performed again. Although $\tilde{v}_i(i = 1, 2, \cdots, n)$ and $w_i(i = 1, 2, \cdots, n)$ are disclosed, each voter keeps his information l_i confidential, and other voters cannot eavesdrop on others' voting content during the counting phase.

4.6 | Fairness

The analysis of the insider attacks in Section 3.3 shows that whether a malicious voter attacks or multiple voters conspired to attack, it is impossible to eavesdrop or tamper with the voting content of others without being detected. In addition, each voter has a veto, and if only one voter votes against the proposal, it will not pass. In addition, as we all know, if a voter determines some useful information about some other votes beforehand, he (she) might change his (her) vote. In our protocol, the voters encrypt their votes twice. On one hand, each voter V_i encrypts his (her) vote using the classical one time pad technique with secret key K. In addition to the CA and V_i , no individual can decode the vote from ciphertext. However, the CA cannot cooperate with any voter. On the other hand, V_i encodes the ciphertext by performing the unitary operations $I \otimes U^{(u_i, v_i)}$ on the voting carriers $|\phi(0,0)\rangle_{g_i h_i}$. Since the density matrix of each voting carrier is in a maximum mixed state and invariant under the encoding operations in the entire procedure of the protocol, no useful information about the vote of V_i is leaked. Therefore, no voter can determine how the other voters are voting, and each voter casts a vote based on his (her) initial wishes. Therefore, the fairness of our protocol can be maintained.

4.7 | Robustness

Before transmitting the quantum state, the protocol will introduce decoy photons for security detection. When the voters calculate or transmit the classical information T, because each voter's classical information L_i does not carry any voter's voting content, no voter's voting information will be disclosed. At the same time, the protocol can also resist external and internal attacks. Therefore, the robustness of our protocol can be maintained.

5 | DISCUSSION

In 2015, Ramij and Guruprasad first proposed how quantum mechanics could be used to achieve anonymous veto (RGQAV, for short), which inspired us to explore this intriguing topic further. RGQAV utilises GHZ states as vote carriers and simple local operations, such as Pauli operations, to implement an anonymous veto protocol. Strictly speaking, RGQAV

provides an initial concept rather than a fully developed solution [37–41]. Our protocol offers the following several advantages.

First, while RGQAV focuses solely on privacy, our protocol encompasses additional properties such as reliability, privacy, verifiability, and fairness which better meet the requirements for anonymous voting applications. Second, our protocol ensures stricter privacy compared to RGQAV. Although RGQAV does guarantee that only the individual voter knows their vote, it may still reveal some information about the number of 'against' votes. In contrast, our protocol ensures that no useful information about the number of 'against' votes is leaked, effectively addressing this security gap. In conclusion, our protocol represents a significant improvement over RGQAV.

6 | CONCLUSION

In this paper, we present a novel quantum anonymous one-vote veto protocol based on entanglement swapping. This protocol facilitates the transmission of voting information between the voter and the semi-honest voting Council (CA) by utilising entanglement swapping between multi-particle Cat states and Bell states. During the voting process, no voter can access the voting content of others, and CA can only compute the final result without acquiring any individual voting information. The protocol effectively safeguards against external attacks, voter attacks, and threats from semi-honest third parties. Thus, this quantum anonymous one-vote veto protocol, based on entanglement swapping, offers enhanced privacy protection for voters. Given the rapid advancement of quantum technology, classical one-vote veto protocols are increasingly under threat. Our QAV protocol represents a significant step forward with current technology, and we hope our findings will inspire further research into developing quantum anonymous voting schemes.

AUTHOR CONTRIBUTIONS

Min Jiang: Conceptualisation; data curation; formal analysis; funding acquisition; methodology; resources; software; supervision; writing - original draft; writing - review and editing. **Yuzhen Wei**: Formal analysis. **Wenhao Zhao**: Data curation.

ACKNOWLEDGEMENTS

Project supported by the National Natural Science Foundation of China (Grant No. 61873162) and Fund from the Key Laboratory of System Control and Information Processing, Ministry of Education, China (Grant No. Scip20240106).

CONFLICT OF INTEREST STATEMENT

The authors declare no conflicts of interest.

PERMISSION TO REPRODUCE MATERIALS FROM OTHER SOURCES

None.

DATA AVAILABILITY STATEMENT

The data that support the findings of this study are available from the corresponding author upon reasonable request.

ORCID

Min Jiang https://orcid.org/0000-0002-3669-2390

REFERENCES

1. Adida, B.: Helios: web-based open-audit voting. In: Proceedings of the 17th Conference on Security Symposium 17, 335–348 (2008)
2. Ryan, P.Y.A., et al.: PrÊt À voter: a voter-verifiable voting system. IEEE Trans. Inf. Forensics Secur. 4, 662–673 (2009). https://doi.org/10.1109/tifs.2009.2033233
3. Kumar, M., Chand, S., Katti, C.P.: A secure end-to-end verifiable internet-voting system using identity-based blind signature. IEEE Syst. J. 14(2), 2032–2041 (2020). https://doi.org/10.1109/jsyst.2019.2940474
4. Christandl, M., Wehner, S.: Quantum Anonymous Transmissions, pp. 217–235. Springer Berlin Heidelberg, Berlin (2005)
5. Vaccaro, J.A., Spring, J., Chefles, A.: Quantum protocols for anonymous voting and surveying. Phys. Rev. 75(1), 12333 (2007). https://doi.org/10.1103/physreva.75.012333
6. Li, Y., Zeng, G.H.: Quantum anonymous voting systems based on entangled state. Opt. Rev. 15(5), 219–223 (2008). https://doi.org/10.1007/s10043-008-0034-8
7. Horoshko, D., Kilin, S.: Quantum anonymous voting with anonymity check. Phys. Lett. 375(8), 1172–1175 (2011). https://doi.org/10.1016/j.physleta.2011.01.038
8. Xu, Q.J., Zhang, S.Y.: Improvement of the security of quantum protocols for anonymous voting and surveying. Sci. China Phys. Mech. Astron. 53(11), 2131–2134 (2010). https://doi.org/10.1007/s11433-010-4130-y
9. Li, Y., Zeng, G.H.: Anonymous quantum network voting scheme. Opt. Rev. 19(3), 121–124 (2012). https://doi.org/10.1007/s10043-012-0021-y
10. Jiang, L., et al.: Quantum anonymous voting for continuous variables. Phys. Rev. 85(4), 160 (2012). https://doi.org/10.1103/physreva.85.042309
11. Tian, J.H., Zhang, J.Z., Li, Y.P.: A voting protocol based on the controlled quantum operation teleportation. Int. J. Theor. Phys. 55(5), 2303–2310 (2016). https://doi.org/10.1007/s10773-015-2868-8
12. Thapliyal, K., Sharma, R.D., Pathak, A.: Protocols for quantum binary voting. Int. J. Quant. Inf. 15(01), 1750007 (2017). https://doi.org/10.1142/s0219749917500071
13. Wang, Q.L., et al.: Self-tallying quantum anonymous voting. Phys. Rev. 94(2), 022333 (2016). https://doi.org/10.1103/physreva.94.022333
14. Kumar, M., Chand, S., Katti, C.P.: A secure end-to-end verifiable internet-voting system using identity-based blind signature. IEEE Syst. J. 14(2), 2032–2041 (2020). https://doi.org/10.1109/jsyst.2019.2940474
15. Khabiboulline, E.T., et al.: Efficient quantum voting with information-theoretic security. arXiv (2021)
16. Wu, S.Y., et al.: A secure quantum protocol for anonymous one-vote veto voting. IEEE Access 9, 146841–146849 (2021). https://doi.org/10.1109/access.2021.3123681
17. Mishra, S., et al.: Quantum anonymous veto: a set of new protocols. Epj Quan. Technol. 9(1), 14 (2022). https://doi.org/10.1140/epjqt/s40507-022-00133-2
18. Wang, Q.L., et al.: Quantum-based anonymity and secure veto. Quant. Inf. Process. 20(3), 85 (2021). https://doi.org/10.1007/s11128-021-03022-2
19. Cerf, N.J.: Asymmetric quantum cloning in any dimension. J. Mod. Opt. 47(2–3), 187–209 (2000). https://doi.org/10.1080/095003400148141
20. Karimipour, V., Bahraminasab, A., Bagherinezhad, S.: Entanglement swapping of generalized cat states and secret sharing. Phys. Rev. 65(4), 042320 (2002). https://doi.org/10.1103/physreva.65.042320
21. Kang, M.S., et al.: Universal quantum encryption for quantum signature using the swap test. Quant. Inf. Process. 17(10), 254 (2018). https://doi.org/10.1007/s11128-018-2029-0

22. Ji, Z.J., Ye, T.Y.: Multi-party quantum private comparison based on the entanglement swapping of d-level cat states and d-level bell states. Quant. Inf. Process. 16(7), 177 (2017). https://doi.org/10.1007/s11128-017-1628-5
23. Wang, Y.L., Hu, P.C., Xu, Q.L.: Quantum secure multi-party summation based on entanglement swapping. Quant. Inf. Process. 20(10), 319 (2021). https://doi.org/10.1007/s11128-021-03262-2
24. Rahaman, R., Kar, G.: Ghz correlation provides secure anonymous veto protocol. arXiv (2015)
25. Wang, Q.L., et al.: Authenticated quantum sortition and application in "picking at random" problems. IEEE Commun. Lett. 25(2), 518–522 (2021). https://doi.org/10.1109/lcomm.2020.3025319
26. Lin, S., et al.: Quantum anonymous ranking based on the Chinese remainder theorem. Phys. Rev. 93(1), 012318 (2016). https://doi.org/10.1103/physreva.93.012318
27. Wang, Q.L., Sun, H.X., Huang, W.: Multi-party quantum private comparison protocol with n-level entangled states. Quant. Inf. Process. 13(11), 2375–2389 (2014). https://doi.org/10.1007/s11128-014-0774-2
28. Hillery, M., Buzek, V., Berthiaume, A.: Quantum secret sharing. Phys. Rev. 59(3), 1829–1834 (1999). https://doi.org/10.1103/physreva.59.1829
29. Yang, Y.G., Wen, Q.Y., Zhang, X.: Multiparty simultaneous quantum identity authentication with secret sharing. Sci. China G 51(3), 321–327 (2008). https://doi.org/10.1007/s11433-008-0034-5
30. Gao, F., et al.: Quantum private query: a new kind of practical quantum cryptographic protocol. Sci. China Phys. Mech. Astron. 62(7), 70301 (2019). https://doi.org/10.1007/s11433-018-9324-6
31. Xue, P., Zhang, X.: A simple quantum voting scheme with multi-qubit entanglement. Sci. Rep. 7(1), 7586 (2017). https://doi.org/10.1038/s41598-017-07976-1
32. Ramij, R., Guruprasad, K.: GHZ correlation provides secure Anonymous Veto Protocol. arXiv: Quan. Phys. (2015)
33. Jiang, X.Q., et al.: Low-complexity adaptive reconciliation protocol for continuous-variable quantum key distribution. Quantum Sci. Technol. 9(2), 025008 (2024). https://doi.org/10.1088/2058-9565/ad1f3c
34. Feng, Y., et al.: Secret key rate of continuous-variable quantum key distribution with finite codeword length. Sci. China Inf. Sci. 66(8), 180511 (2023). https://doi.org/10.1007/s11432-022-3656-4
35. Feng, Y., et al.: Virtual channel of multidimensional reconciliation in a continuous-variable quantum key distribution. Phys. Rev. 103(3), 032603 (2021). https://doi.org/10.1103/physreva.103.032603
36. Jiang, X.Q., et al.: Secret information reconciliation based on punctured low-density parity-check codes for continuous-variable quantum key distribution. Phys. Rev. 95(2), 022318 (2017). https://doi.org/10.1103/physreva.95.022318
37. Li, Q., et al.: An efficient quantum-resistant undeniable signature protocol for the e-voting system. J. Inf. Secur. Appl. 81, 103714 (2024). https://doi.org/10.1016/j.jisa.2024.103714
38. Zhou, S., Xie, Q.-M., Zhou, N.-R.: Measurement-free mediated semi-quantum key distribution protocol based on single-particle states. Laser Phys. Lett. 21(6), 065207 (2024). https://doi.org/10.1088/1612-202x/ad3f96
39. Gong, L.-H., et al.: Novel semi-quantum private comparison protocol with bell states. Laser Phys. Lett. 21(5), 055209 (2024). https://doi.org/10.1088/1612-202x/ad3a54
40. Gong, L.-H., et al.: One-way semi-quantum private comparison protocol without pre-shared keys based on unitary operations. Laser Phys. Lett. 21(3), 035207 (2024). https://doi.org/10.1088/1612-202x/ad21ec
41. Gong, L.H., et al.: Robust multi-party semi-quantum private comparison protocols with decoherence-free states against collective noises. Adv. Quan. Tech. 6(8) (2023). https://doi.org/10.1002/qute.202300097

How to cite this article: Wang, Y., et al.: Quantum anonymous one vote veto protocol based on entanglement swapping. IET Quant. Comm. 5(4), 641–649 (2024). https://doi.org/10.1049/qtc2.12117