Novel traveling quantum anonymous voting scheme via GHZ states

Wenhao Zhao(赵文浩)[1] and Min Jiang(姜敏)[1,2,†]

[1] *School of Electronics & Information Engineering, Soochow University, Suzhou* 215006, *China*
[2] *Key Laboratory of System Control and Information Processing, Ministry of Education, Shanghai* 200240, *China*

(Received 18 June 2022; revised manuscript received 8 October 2022; accepted manuscript online 19 October 2022)

Based on traveling ballot mode, we propose a secure quantum anonymous voting via Greenberger–Horne–Zeilinger (GHZ) states. In this scheme, each legal voter performs unitary operation on corresponding position of particle sequence to encode his/her voting content. The voters have multiple ballot items to choose rather than just binary options "yes" or "no". After counting votes phase, any participant who is interested in voting results can obtain the voting results. To improve the efficiency of the traveling quantum anonymous voting scheme, an optimization method based on grouping strategy is also presented. Compared with the most existing traveling quantum voting schemes, the proposed scheme is more practical because of its privacy, verifiability and non-repeatability. Furthermore, the security analysis shows that the proposed traveling quantum anonymous voting scheme can prevent various attacks and ensure high security.

Keywords: quantum anonymous voting, quantum secure communication, GHZ states, verifiability, privacy

PACS: 03.67.–a, 03.67.Dd, 03.67.Hk **DOI:** 10.1088/1674-1056/ac9b2e

1. Introduction

Voting is a significant way of decision-making in politics, economics and people's daily life. With the development of communication science and technology, various voting technologies have been developed rapidly in terms of voting form, security, and efficiency. Nowadays electronic voting is very popular, whose security depends on the computational complexity of solving mathematical problems. However, in recent years, with the development of quantum chips and quantum computers,[1] classical cryptography has to consider the security risks brought by "quantum threats".

Based on the laws of quantum mechanics, during the past years, many efforts have been devoted to the research of quantum anonymous voting (QAV) in order to design a high secure voting scheme. Furthermore, the fundamental researches of quantum computation and information, such as quantum teleportation,[2,3] quantum states preparation,[4,5] and quantum memory for free,[6,7] have laid a foundation for the implementation of quantum voting schemes. In 2005, Christandl and Wehner[8] proposed a quantum communication protocol that could anonymously transmit classical bits using shared quantum states and classical broadcast channels, which was the first time that quantum anonymous voting was proposed. Later, Hillery *et al.*[9] proposed two kinds of quantum voting modes: the traveling ballot mode[10–14] and the distributed ballot mode.[15–21] In 2011, Bonanome *et al.*[22] presented a modified QAV protocol on the basis of Hillery's voting protocol, which improved privacy protection in voting and examined the security of protocol under certain types of attacks. In the following years, various QAV schemes have been proposed based on the traveling voting mode. Most existing traveling QAV schemes have some security deficiencies that cannot avoid repetitive voting and voters cannot verify the voting results.

In 2020, Shi *et al.*[23] proposed a traveling QAV protocol based on the Chinese remainder theorem. In their scheme, the voters could verify the correctness of their votes. However, in the initial and verification phase of his scheme, the voter's identity information and the corresponding voting content were broadcast by classical encryption and classical channels. If the eavesdropper used quantum computing to eavesdrop on the voting information, the voters' identity information and voting content would be leaked, and the privacy would not be guaranteed. As a matter of fact, in most traveling quantum anonymous voting schemes, the voters have only two options "yes" or "no" to choose. It is important to improve its scalability in various voting scenes. Recently, Li *et al.*[24] adopted grouping strategy to improve the efficiency of distributed quantum voting protocol. Hence, it is worth considering how to adopt grouping strategy to improve the practicality of our traveling quantum anonymous voting scheme.

In this paper, we present a secure traveling quantum anonymous voting scheme via Greenberger–Horne–Zeilinger (GHZ) states. Our traveling QAV scheme satisfies the following features: (i) Privacy: The identity information of each voter and its corresponding voting information are known only to himself/herself, and other participants cannot obtain it. (ii) Verifiability: After the voting closes, according to

†Corresponding author. E-mail: jiangmin08@suda.edu.cn

© 2023 Chinese Physical Society and IOP Publishing Ltd

the final announcement information, each voter can verify whether his/her voting content is correctly counted. (iii) Non-repeatability: Each voter is only allowed to cast one vote and cannot vote more than once, and so on. These are also the three most important principles in voting scheme. Furthermore, the security analysis shows that our voting scheme can resist various attacks.

The remainder of this paper is structured below: In Section 2, we briefly introduce the primary preliminaries. In Section 3, we elaborate the proposed traveling quantum anonymous voting scheme. In Section 4, we analyze the security of the proposed protocol from several aspects. Then the Section 5 shows the comparisons between existing schemes and ours from several aspects. Finally, we give a short conclusion in Section 6.

2. Preliminaries

In d-dimensional Hilbert space, a single particle has two kinds of common orthonormal bases: the computational basis $B_{\rm C}=\{|0\rangle_{\rm C},|1\rangle_{\rm C},|2\rangle_{\rm C},\ldots,|d-1\rangle_{\rm C}\}$ and the fourier basis $B_{\rm F}=\{|0\rangle_{\rm F},|1\rangle_{\rm F},|2\rangle_{\rm F},\ldots,|d-1\rangle_{\rm F}\}$. The fourier basis can be obtained by the quantum fourier transform $\mathcal{F}$ on the computational basis, which can be defined as

$$|k\rangle_{\rm F}=\mathcal{F}|k\rangle_{\rm C}=\frac{1}{\sqrt{d}}\sum_{j=0}^{d-1}\exp\left(\frac{2\pi {\rm i}kj}{d}\right)|j\rangle_{\rm C}, \tag{1}$$

where $|k\rangle_{\rm C}\in\{|0\rangle_{\rm C},|1\rangle_{\rm C},|2\rangle_{\rm C},\ldots,|d-1\rangle_{\rm C}\}$.

The three-particle d-level Greenberger–Horne–Zeilinger (GHZ) state in Fourier basis can be defined as

$$|\psi\rangle_{0,1,2}=\frac{1}{\sqrt{d}}\sum_{k=0}^{d-1}|k\rangle_{\rm F}|k\rangle_{\rm F}|k\rangle_{\rm F}. \tag{2}$$

$|\psi\rangle_{0,1,2}$ has an interesting property[25] that it can be written as the following form in computational basis:

$$|\psi\rangle_{0,1,2}=\frac{1}{d}\sum_{(k_0+k_1+k_2)\bmod d=0}|k_0\rangle_{\rm C}|k_1\rangle_{\rm C}|k_2\rangle_{\rm C}. \tag{3}$$

Therefore, when each particle of $|\psi\rangle_{0,1,2}$ is measured in Fourier basis, the measurement outcomes are the same for each particle. When each particle of $|\psi\rangle_{0,1,2}$ is measured in computational basis, the summation of the measurement outcome modulo d is always equal to zero.

We introduce a $d\times d$ unitary operation U^r,[26] which can be described as

$$U^r=\sum_{k=0}^{d-1}\exp\left(\frac{2\pi {\rm i}rk}{d}\right)|k\oplus r\rangle\langle k|, \tag{4}$$

where $r\in\{0,1,2,\ldots,d-1\}$ and $\oplus$ denotes addition module d. For example, when the unitary operation U^r is performed onto the d-level single qubit $|k\rangle_{\rm C}$ and $|k\rangle_{\rm F}$, these states can be transformed to

$$\begin{aligned}U^r|k\rangle_{\rm C}&=\exp\left(\frac{2\pi {\rm i}rk}{d}\right)|k\oplus r\rangle_{\rm C},\\ U^r|k\rangle_{\rm F}&=\exp\left(\frac{-2\pi {\rm i}r(k\oplus r)}{d}\right)|k\oplus r\rangle_{\rm F},\end{aligned} \tag{5}$$

where $k\in\{0,1,2,\ldots,d-1\}$. The unitary operations will be used as the encoding operators in the proposed voting protocol.

When the unitary operation U^v $(0\le v\le d-1)$ and U^t $(0\le t\le d-1)$ are performed onto the first particle and the second particle of the GHZ state $|\psi\rangle_{0,1,2}$ in the computational basis, the state becomes

$$\begin{aligned}|\psi'\rangle_{0,1,2}&=U_0^vU_1^t|\psi\rangle_{0,1,2}\\ &=\frac{1}{d}\sum_{(k_0+k_2+k_2)\bmod d=0}\exp\left(\frac{2\pi {\rm i}\,(vk_0+tk_1)}{d}\right)\\ &\quad\times|k_0\oplus v\rangle_{\rm C}|k_1\oplus t\rangle_{\rm C}|k_2\rangle_{\rm C}.\end{aligned} \tag{6}$$

If the single-particle measurement with the computational basis is performed onto each particle of state $|\psi'\rangle_{0,1,2}$, we will obtain the measurement outcomes σ^0, σ^1, and σ^2, respectively. The relationship between the measurement outcomes and the parameters of unitary operation can be described as follows:

$$\sum_{j=0}^{2}\sigma^j\equiv v+t\,(\bmod d)\,. \tag{7}$$

If we obtain the measurement results of each particle of the state $|\psi'\rangle_{0,1,2}$ and the parameter t of the unitary operation U^t, the parameter v of unitary operation U^v can be deduced. This feature can be used to count and verify the voting results in the proposed voting scheme.

3. Description of the proposed QAV scheme

3.1. Procedures of the scheme

In this voting scheme, the quantum voting network is managed by the voting service center (VSC), which wants the real voting results. The teller T has the responsibilities for collecting the voting particle sequence and participating in the counting of votes. Suppose that there are totally m ballot items in the voting activity, which are encoded as the integers $0,1,2,\ldots,m-1$. Each legitimate voter V_i $(i=0,1,2,\ldots,n-1)$ can select a vote object from the set $\{0,1,2,\ldots,m-1\}$. The diagram of the voting process of the traveling anonymous voting scheme is shown in Fig. 1.

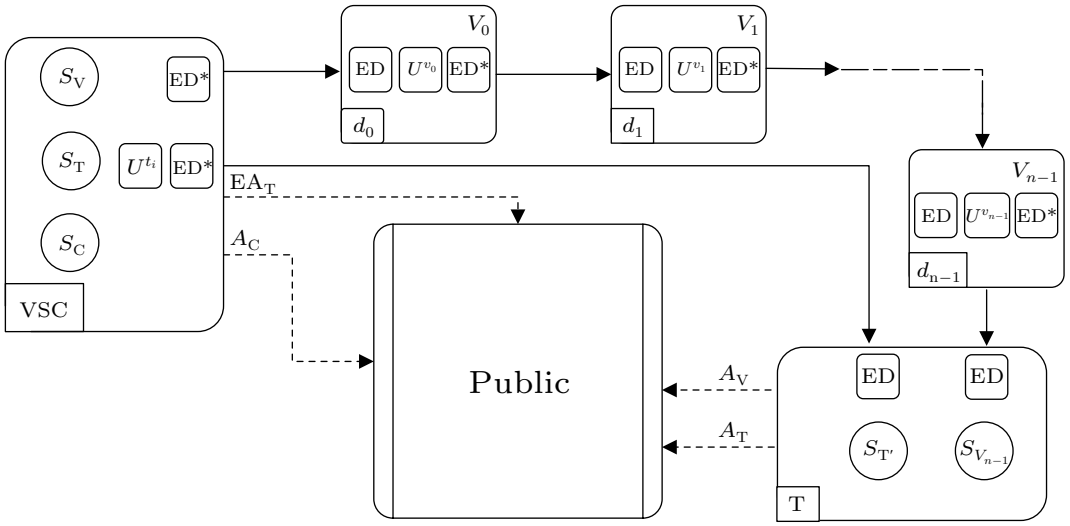


Fig. 1. The flow diagram of the proposed traveling anonymous voting scheme voting. ED and ED* indicate the eavesdropping detection. U^x indicates the unitary operation. The solid lines and dashed lines indicate the quantum channel and the classical channel, respectively.

3.1.1. Initial phase

Step 1 The citizens send the identity information and the voting application to the VSC. The VSC checks whether the citizen is legal and whether the citizen is applying to vote for the first time. Assume that the number of legal voters who pass the checking is n.

Step 2 Each legal voter V_i obtains a unique private index d_i based on quantum random draw protocol.[27] According to the index d_i, the voter will perform the unitary operation to encode in corresponding position in follow-up steps.

Step 3 The VSC prepares n copies of m-level GHZ states $|\psi\rangle_{0,1,2}$ and picks up all the qubit labels with 0s, 1s, and 2s to compose the ordered particle sequences[28] S_V, S_T, and S_C, respectively. After that, the VSC performs the unitary U^{t_i} on each particle of sequence S_T, in which each t_i is a random number chosen from the set $\{0,1,\ldots,m-1\}$. At the same time, the VSC records the parameters of the unitary operation U^{t_i} and their corresponding positions as the array $EA_T = \{t_0,t_1,\ldots,t_{n-1}\}$. Before transmitting the particle sequences S_V and $S_{T'}$, the VSC randomly generates enough decoy single qubits from the basis B_C or B_F, and inserts them into the sequences S_V and $S_{T'}$, respectively. The VSC will obtain the new particle sequences S_V^* and $S_{T'}^*$. Then the VSC keeps the sequence S_C and sends the sequence $S_{T'}^*$, S_V^* to the teller T and the first voter V_0, respectively.

3.1.2. Voting phase

Step 1 After confirming that the voter V_0 has received the sequence S_V^*, the VSC declares the initial states and the corresponding insertion positions of decoy particles to V_0 by classical channel. The voter V_0 measures the decoy particles with the corresponding measurement basis and calculates the error ratio by comparing with the initial states. If the error ratio is greater than the secure threshold, the process will be stopped and restarted. Otherwise, the process will continue.

Step 2 The voter V_0 discards the decoy particles and obtains the sequence S_V. According to his private index d_0, V_0 performs the unitary operation U^{v_0} onto the d_0-th single particle of the ordered sequence S_V, where v_0 is V_0's expected item number. After that, V_0 obtains the new sequence S_{V_0}. To avoid the risk of eavesdropping, V_0 inserts enough decoy particles to S_{V_0} as the same way of step 1 in initial phase, and gets sequence $S_{V_0}^*$. Then he sends the sequence $S_{V_0}^*$ to the next voter V_1 by quantum channel.

Step 3 The voter V_1 performs eavesdropping detection on the sequence $S_{V_0}^*$. Assume that this sequence passes the eavesdropping detection, the voter will discard the decoy particles and get the sequence S_{V_0}. Similar to the Step 2 in this phase, V_1 performs the unitary operation U^{v_1} onto the d_1-th single particle of the sequence S_{V_0}, where d_1 is V_1's private index and v_1 is V_1's expected item number. After that, V_1 obtains the sequence S_{V_1} and inserts decoy particles to get $S_{V_1}^*$. Then V_1 sends $S_{V_1}^*$ the next voter V_2.

Step 4 As the same operation as the voter V_0 and V_1, the other voters V_i $(i = 2,3,\ldots,n-1)$ orderly perform the similar voting process. After the last voter V_{n-1} finishes his voting process and gets the sequence $S_{V_{n-1}}^*$ that are inserted decoy particles, he will send the sequence $S_{V_{n-1}}^*$ to the teller T.

3.1.3. Counting votes phase

Step 1 After confirming that the teller T has received the sequence $S_{V_{n-1}}^*$, T sends a flag signal to the VSC. The VSC orderly measures each particle of the reserved sequence S_C in computational basis, and gets the outcome array $A_C = \{\sigma_0^C,\sigma_1^C,\ldots,\sigma_i^C,\ldots,\sigma_{n-1}^C\}$.

Step 2 The teller performs eavesdropping detection on the sequence $S_{V_{n-1}}$. If the sequence $S_{V_{n-1}}^*$ passes the eavesdropping detection, the teller T discards its decoy particles and

gets the sequence $S_{V_{n-1}}$. Then he orderly measures each single particle of the sequence $S_{V_{n-1}}$ in the computational basis $B_{\rm C}$, and the measurement outcome can be described as $A_V = \{\sigma_0^{\rm V}, \sigma_1^{\rm V}, \ldots, \sigma_i^{\rm V}, \ldots, \sigma_{n-1}^{\rm V}\}$, where $\sigma_i^{\rm V} \in \{0,1,2,\ldots,m-1\}$. In addition, after the teller T performs the eavesdropping checking on the sequence $S_{\rm T'}^*$ and recovers the sequence $S_{\rm T'}$, he orderly performs single-particle measurement on the sequence $S_{\rm T'}$ in the computational basis $B_{\rm C}$. This measurement outcome can be described as $A_{\rm T} = \{\sigma_0^{\rm T}, \sigma_1^{\rm T}, \ldots, \sigma_i^{\rm T}, \ldots, \sigma_{n-1}^{\rm T}\}$, where $\sigma_i^{\rm T} \in \{0,1,2,\ldots,m-1\}$. Then the teller broadcasts the classical information $A_{\rm V}$ and $A_{\rm T}$ by classical channel.

Step 3 After the VSC receives the teller T's information, the VSC broadcasts the classical information $\mathrm{EA_T}$ and $A_{\rm C}$ by classical channel.

Step 4 With the arrays $A_{\rm V}$, $A_{\rm T}$, $A_{\rm C}$, and $\mathrm{EA_T}$, any participant who is interested in the voting results can work out the votes for each ballot item. He/she calculates the array $\zeta = \{r_0, r_1, \ldots, r_i, \ldots, r_{n-1}\}$, in which

$$r_i = \left(\left(\sum_{l={\rm V,T,C}} \sigma_i^l \right) \bmod m + m - t_i \right) \bmod m. \tag{8}$$

Then the number of votes for each ballot item j ($j = 0,1,\ldots,m-1$) can be calculated as

$$N_j = \sum_{r_i=j} 1 \tag{9}$$

for $i = 0,1,2,\ldots,n-1$.

3.1.4. Verifying phase

When obtaining the array ζ, each voter V_i can verify whether $r_{d_i} = v_i$. If the answer is yes, the vote content v_i of voter V_i is correctly counted. Otherwise, V_i anonymously broadcasts an aborted signal. Once there is an aborted singal, the voting protocol will be aborted and the voting results will be abandoned.

3.2. Grouping strategy

For the proposed traveling quantum anonymous voting scheme, with the number of voters increasing, it will take more time to complete the voting process. We can adopt voter grouping strategy and candidate grouping strategy to improve the practicality and flexibility of voting.

When adopting voter grouping strategy, we divide n voters into l groups, which can be named as $G_1, G_2, \ldots, G_l$. The number of voters in group G_a is Z_a, which meets $\sum_{a=1}^{l} Z_a = n$. For each group G_a, the VSC prepares Z_a copies of m-level GHZ states. At the same time, the proposed traveling quantum voting protocol takes place in each group. Each group G_a will get the voting outcomes $N_j^{G_a}$ of the intra-group vote on the ballot items, where $j = 0,1,\ldots,m-1$ refers to the number of ballot item. Finally, the number of votes N_j for each ballot item can be calculated as $N_j = \sum_{a=1}^{l} N_j^{G_a}$. Although the voter grouping strategy cannot reduce the demand of quantum resources, it can improve the efficiency of traveling quantum anonymous voting protocol by means of parallel voting.

When adopting candidate grouping strategy, we first divide m ballot items into l groups, which can be named as $R_1, R_2, \ldots, R_h$. The number of ballot items in group R_b is Y_b, which meets $\sum_{b=1}^{h} Y_b = m$. For each group R_b, all voters perform traveling quantum voting to vote the ballot item with the highest number. Suppose that the ballot items with the highest votes in each group are $h_{R_1}, h_{R_2}, \ldots, h_{R_h}$, respectively. The VSC puts them into a new group G_e. Then the VSC renumbers the ballot items of group R_e as $0,1,2,\ldots,h$ and performs a traveling quantum voting to vote the final winner. The number of ballot items in candidate group R_b ($b = 1,2,\ldots,h$) and R_e directly determine the dimension of quantum states. Hence, the dimension of quantum states required in each traveling QAV process will be greatly decreased. With the dimension of quantum states decreasing, the difficulty of preparing quantum states will be reduced.

4. Security analysis

4.1. Intercept–resending attack

When one voter V_j sends the ballot sequence $S_{V_j}^*$ to the next voter V_j, suppose that one eavesdropper intercepts the transmitted sequence $S_{V_j}^*$ and sends a fake sequence[29] to V_{j+1}. In our QAV protocol, the sequence is inserted with enough decoy particles before being sent. The decoy particles are chosen from $\{|0\rangle_{\rm C}, |1\rangle_{\rm C}, \ldots, |m-1\rangle_{\rm C}\}$, $\{|0\rangle_{\rm F}, |1\rangle_{\rm F}, \ldots, |m-1\rangle_{\rm F}\}$ and randomly inserted into the transmitted sequence. The eavesdropper does not know the positions where these decoy particles are inserted and the corresponding measurement basis. The probability that the intercept–resending attack is deteced by eavesdropping detection can be described as

$$P_{\rm ira}(D) = 1 - \prod_{i=0}^{u-1} \left(P_i(R|B_{\rm C}) P_i(B_{\rm C}) + P_i(R|B_{\rm F}) P_i(B_{\rm F}) \right). \tag{10}$$

Here u is the number of decoy particles for each eavesdropping detection; i is the i-th decoy single particle; $P_i(B_{\rm C})$ indicates the probability of choosing the measurement basis $B_{\rm C}$; $P_i(R|B_{\rm C})$ indicates the conditional probabilities of passing eavesdropping detection; $P(B_{\rm F})$ indicates the probability of choosing the measurement basis $B_{\rm F}$; $P_i(R|B_{\rm F})$ indicates the conditional probabilities of passing eavesdropping detection. The probabilitites that the eavesdropper guesses the measurement basis $B_{\rm C}$ and $B_{\rm F}$ are $1/2$ and $1/2$, respectively. No matter which measurement basis is guessed, the conditional probability of passing the eavesdropping detection is $1/m$. For each decoy particle, the intercept–resending attack cannot be dected

with the probability of $1/m$. Because there are totally u decoy particles, the intercept–resending attack cannot be dected with the probability $(1/m)^u$. Therefore, the intercept–resending attack will be discovered with probability $1-(1/m)^u$, which approaches infinitely 100% with the number of decoy particles increasing.

4.2. Measure–resending attack

During the sequence transmission, an eavesdropper may also launch the measure–resending attack. The main difference between measure–resending attack and intercept–resending attack is that the eavesdropper selects a measurement basis to measure the tranmitted sequence in measure–resending attack. According to the measurement results, the eavesdropper prepares one fake particle sequence. The probability that the measure–resending attack is deteced by eavesdropping detection can be described as

$$P_{\mathrm{mra}}(D)=1-\prod_{i=0}^{u-1}\left(P_i(S)+P_i(R|F)P_i(F)\right). \tag{11}$$

Here u is the number of decoy particles for each eavesdropping detection; i is the i-th decoy single particle; $P_i(S)$ and $P_i(F)$ indicate the probability of guessing the correct measurement basis and guessing incorrect measurement basis, respectively; $P_i(R|F)$ indicates the conditional probability of passing eavesdropping detection. The eavesdropper does not know any information about decoy particles. For each decoy particle, the probabilities of the eavesdropper guessing correct and incorrect measurement basis are $P_i(S)=1/2$ and $P_i(F)=1/2$, respectively. When the correct measurement basis is used, it will pass the eavesdropping detection. When the incorrect measurement basis is used, the conditional probability of passing eavesdropping detection is $P_i(R|F)=1/m$. For this decoy particle, the measure–resending attack cannot be dected with probability $(1/2)+(1/2m)$. Because there are u decoy particles, the probability that measurement–resending attack cannot be dected is $[(1/2)+(1/2m)]^u$. The intercept–resending attack will be discovered with probability $1-[(2m+1)/(2m)]^u$. As the number of decoy particles increases, this probability approaches infinitely 100%.

4.3. Entangle–measure attack

If the eavesdropper wants to perform the entangle–measure attack,[30] he/she needs to perform the unitary operation U_e onto the intercepted qubit to make it entangle with the auxiliary photon $|e\rangle$. The unitary operation U_e that causes the transmitted qubit to interact coherently with an ancillary qubit $|e\rangle$ can be defined as follows:

$$U_e|k\rangle_{\mathrm{C}}|e\rangle_{\mathrm{C}}=\sum_{l=0}^{m-1}\delta_{kl}|l\rangle_{\mathrm{C}}|\varepsilon_{kl}\rangle_{\mathrm{C}}. \tag{12}$$

Here $k=\{0,1,2,\ldots,m-1\}$. The δ_{kl} satisfies the relationship $\sum_{l=0}^{l=m-1}|\delta_{kl}|^2$ and $|\varepsilon_{kl}\rangle_{\mathrm{C}}$ is pure state. With this condition, when the eavesdropper performs the unitary operation U_e onto the decoy qubit in fourier basis, the following formula can be obtained:

$$\begin{aligned}U_e|k\rangle_{\mathrm{F}}|e\rangle &= U_e\left[\frac{1}{\sqrt{m}}\sum_{l=0}^{m-1}\exp\left(\frac{2\pi \mathrm{i}kl}{m}\right)|l\rangle_{\mathrm{C}}\right]|e\rangle_{\mathrm{C}}=\left[\frac{1}{\sqrt{m}}\sum_{l=0}^{m-1}U_e\exp\left(\frac{2\pi \mathrm{i}kl}{d}\right)|l\rangle_{\mathrm{C}}\right]|e\rangle_{\mathrm{C}}\\ &= \frac{1}{\sqrt{m}}\sum_{l=0}^{m-1}\exp\left(\frac{2\pi \mathrm{i}kl}{d}\right)\sum_{t=0}^{m-1}\delta_{lt}\left[\frac{1}{\sqrt{m}}\sum_{u=0}^{m-1}\exp\left(\frac{-2\pi \mathrm{i}tu}{m}\right)|u\rangle_{\mathrm{F}}\right]|\varepsilon_l t\rangle_{\mathrm{C}}\\ &= \frac{1}{m}\sum_{l=0}^{m-1}\sum_{t=0}^{m-1}\sum_{u=0}^{m-1}\exp\left[\frac{-2\pi \mathrm{i}\,(kl-tu)}{m}\right]\delta_{lt}|u\rangle_{\mathrm{F}}|\varepsilon_{lt}\rangle_{\mathrm{C}},\end{aligned} \tag{13}$$

where $u=\{0,1,2,\ldots,m-1\}$ and δ_{kl} satisfies the relationship $\sum_{l=0}^{l=m-1}|\delta_{kl}|^2$. If the eavesdropper wishes to introduce no error on the decoy particles during the eavesdropping, it should satisfy the following conditions: $\delta_{kl}=0$ (if $k\neq l$), $\delta_{kl}=1$ (if $k=l$), and $|\varepsilon_{00}\rangle=|\varepsilon_{11}\rangle=|\varepsilon_{22}\rangle=\cdots=|\varepsilon_{m-1,m-1}\rangle$. Hence, without being detected, the eavesdropper cannot obtain any useful information with entangle-measure attack.

4.4. Collusive attack

Assume several dishonest voters intend to refuse the honest voter to take part in voting. For instance, the dishonest voters V_j and V_{j+2} do not want the honest voter V_j to participant in voting. The voter V_j directly sends the real ballot $S^*_{V_j}$ to V_{j+2} and sends a deceptive ballot $S^{\mathrm{D}}_{V_j}$ to V_{j+1}. After the voter V_{j+1} finishes his voting operation, he sends $S^{\mathrm{D}}_{V_{j+1}}$ to the next voter V_{j+2}. As a legal voter, the voter V_{j+1} can obtain a private unique index d_{j+1} before starting voting. In the verifying phase, if the voter V_{j+1} find that the element $r_{d_{j+1}}$ of the array ζ is not equal his expected item, he will anonymously broadcast an aborted signal.

4.5. Privacy

The privacy is the most primary property for QAV protocol. In our scheme, each voter has a unique and private index

and other voters cannot get this index. According to the private index, each voter performs the unitary operation on corresponding positions in the ballot state sequence. Although all voting data is open, each voter's voting content is only known by himself/herself. Therefore, the anonymity and privacy of voters can be guaranteed.

4.6. Verifiability

Each voter V_i can verify whether r_{d_i} is equal to v_i. If the answer is yes, V_i's expected item is correctly expressed. Otherwise, each voter can check that whether his voting content has been tampered by the attacker. Hence, this ensures that if a dishonest voter tampers with the content of other honest voters, the dishonest behavior will be perceived.

4.7. Non-repeatability

Each voter has a unique and private index and other voters cannot get this index. If one voter wishes to vote twice or more times, he will perform unitary operation on other particles of sequence, which influences the content of votes cast by legal voters. In verifying phase, each voter V_i verifies $r_{d_i} = v_i$ to make sure that his voting content has not benn tampered. If the honest voters are awared of the risk, the voting process will be aborted.

5. Comparison

The comparisons between several traveling QAV schemes[10,11,13,22,23] and our scheme can be seen in Table 1. Our traveling QAV scheme can ensure basic voting principles, including privacy, verifiability and non-repeatability. In addition, our traveling QAV scheme also supports customizing the number of ballot items, and is suitable for the voting scene with a good deal of ballot items.

Table 1. Comparisons of different schemes in several aspects.

Scheme	Privacy	Verifiability	Non-repeatability	Voting options
Vaccaroet's[10]	yes	no	no	only two
Li's[11]	yes	no	no	user-defined
Xu's[13]	yes	no	no	only two
Bonanome's[22]	yes	no	no	only two
Shi's[23]	risk	yes	yes	only two
Ours	yes	yes	yes	user-defined

6. Conclusion

In this paper, we proposed a secure traveling quantum anonymous voting with GHZ states. The proposed traveling quantum anonymous voting scheme can be applied to the voting scene with a large amount of ballot items. In order to improve the efficiency of the traveling quantum anonymous voting scheme, we proposed an optimization method based on grouping strategy. Compared with the most existing traveling quantum voting schemes, the proposed scheme has higher security, which is manifested in its privacy, verifiability, and non-repeatability. Finally, the security analysis shows that the proposed traveling quantum anonymous voting scheme can resist various attacks and have good safety.

Acknowledgments

Project supported by the Tang Scholar Project of Soochow University, the National Natural Science Foundation of China (Grant No. 61873162), the Fund from Jiangsu Engineering Research Center of Novel Optical Fiber Technology and Communication Network and Suzhou Key Laboratory of Advanced Optical Communication Network Technology.

References

[1] Xin T, Wang B X, Li K R, Kong X Y, Wei S J, Wang T, Ruan D and Long G L 2018 *Chin. Phys. B* **27** 020308
[2] Yang Lu, Liu Y C and Li Y S 2020 *Chin. Phys. B* **29** 060301
[3] Li H J, Li J and Chen X B 2022 *Chin. Phys. B* **31** 090303
[4] Xu Z H, Wei Y Z, Jiang C and Jiang M 2022 *Chin. Phys. B* **31** 040304
[5] Chen N, Yan B, Chen G, Zhang M J and Pei C X 2018 *Chin. Phys. B* **27** 090304
[6] Sun Z, Song L Y, Huang Q, Yin L G, Long G L, Lu J H and Hanzo L 2020 *IEEE Trans. Commun.* **68** 5778
[7] Zhang H, Sun Z, Qi R, Yin L, Long G L and Lu J 2022 *Light Sci. Appl.* **11** 83
[8] Christandl M and Wehner S 2005 *Advances in Cryptology-ASIACRYPT 2005* (Berlin: Springer-Verlag) p. 217
[9] Hillery M 2006 *Int. Soc. Opt. Eng.* **1598** 2006
[10] Vaccaro J A, Spring J and Chefles A 2007 *Phys. Rev. A* **75** 012333
[11] Li Y and Zeng G H 2008 *Opt. Rev.* **15** 219
[12] Horoshko D and Kilin S 2011 *Phys. Lett. A* **375** 1172
[13] Xu Q J and Zhang S Y 2010 *Sci. China-Phys. Mech. Astron.* **53** 2131
[14] Li Y and Zeng G H 2012 *Opt. Rev.* **19** 121
[15] Zhang X, Zhang J Z and Xie S C 2020 *Int. J. Theor. Phys.* **59** 719
[16] Shi R H, Xiao Y, Shi J J, Guo Y and Lee M H 2016 *Chin. Phys. B* **25** 060301
[17] Tian J H, Zhang J Z and Li Y P 2016 *Int. J. Theor. Phys.* **55** 2303
[18] Thapliyal K, Sharma R D and Pathak A 2017 *Int. J. Quantum Inf.* **15** 1750007
[19] Zhang J L, Xie S C and Zhang J Z 2017 *Int. J. Theor. Phys.* **56** 3019
[20] Wang Q L, Li Y C, Yu C H and Zhang Z C 2021 *Quantum Inf. Process.* **20** 85
[21] Wang Q L, Liu J S, Li Y C, Y C H and P S J 2021 *Quantum Inf. Process.* **20** 142
[22] Bonanome M, Bužek V, Hillery M and Ziman M 2011 *Phys. Rev. A* **84** 022331
[23] Shi R H, Qin J Q, Liu B and Zhang M 2021 *Eur. Phys. J. D* **75** 20
[24] Li Y R, Jiang D H, Zhang Y H and Liang X Q 2021 *Quantum Inf. Process.* **20** 110
[25] Huang W, Wen Q Y, Liu B, Su Q, Qin S J and Gao F 2014 *Phys. Rev. A* **89** 032325
[26] Lin S, Guo G D, Huang F and Liu X F 2016 *Phys. Rev. A* **93** 012318
[27] Wang Q L, Yu C H, Li Y C, Liu J S, Shi R H and Zhou Y Q 2020 *IEEE Commun. Lett.* **25** 518
[28] Long G L and Liu X S 2002 *Phys. Rev. A* **65** 032302
[29] Liu H N, Liang X Q, Jiang D H, Zhang Y H and Xu G B 2019 *Int. J. Theor. Phys.* **58** 1659
[30] Li H H, Gong L H and Zhou N R 2020 *Chin. Phys. B* **29** 110304