Self-tallying quantum anonymous voting

Qingle Wang,[1,2] Chaohua Yu,[1] Fei Gao,[1,*] Haoyu Qi,[2] and Qiaoyan Wen[1]

[1]*State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing 100876, China*

[2]*Hearne Institute for Theoretical Physics and Department of Physics and Astronomy, Louisiana State University, Baton Rouge, Louisiana 70820, USA*

(Received 8 June 2016; published 24 August 2016)

Anonymous voting is a voting method of hiding the link between a vote and a voter, the context of which ranges from governmental elections to decision making in small groups like councils and companies. In this paper, we propose a quantum anonymous voting protocol assisted by two kinds of entangled quantum states. Particularly, we provide a mechanism of opening and permuting the ordered votes of all the voters in an anonymous manner; any party who is interested in the voting results can acquire a permutation copy and then obtains the voting result through a simple calculation. Unlike all previous quantum works on anonymous voting, our quantum anonymous protocol possesses the properties of privacy, self-tallying, nonreusability, verifiability, and fairness at the same time. In addition, we demonstrate that the entanglement of the quantum states used in our protocol makes an attack from an outside eavesdropper and inside dishonest voters impossible. We also generalize our protocol to execute the task of anonymous multiparty computation, such as anonymous broadcast and anonymous ranking.

DOI: 10.1103/PhysRevA.94.022333

I. INTRODUCTION

The science of cryptography studies how to prevent valuable information from being leaked to unauthorized parties. In practice, most cryptographic protocols are designed to protect a message from being eavesdropped on by an adversary when it is sent from one party to another. However, in some situations, keeping the identity of the message's senders private is just as important as keeping the message secret. One example is anonymous voting, in which each voter votes for one of the candidates anonymously. Therefore, no one but the voter can know for which candidate he or she voted. The context of voting ranges from governmental elections to decision making in rather small groups like councils and companies. To be reliable and useful in practice, voting protocols should have some desirable properties (see [1] for more details) like privacy, nonreusability, verifiability, fairness, and eligibility as follows.

(1) *Privacy*. Only the individual voter knows how he or she votes.

(2) *Nonreusability*. Each voter can vote only once and cannot change the vote of someone else.

(3) *Verifiability*. Each voter can verify whether his or her vote has been counted properly but cannot prove to anyone else how he or she has voted.

(4) *Fairness*. Nobody can obtain a partial vote tally before the end of the protocol.

(5) *Eligibility*. Only eligible voters can vote.

In recent decades, a number of voting protocols pursuing the above properties have been proposed. The first voting protocol to guarantee voting privacy was proposed by Chaum in 1981 [2]. Since then various voting protocols based on some cryptographic primitives, such as homomorphic encryption and blind signature, were proposed. Most of these voting protocols adopt public-key cryptographic primitives like large-integer factorization and a discrete logarithm. However, with the advent of quantum algorithms, those voting protocols based on public-key cryptographic primitives are no longer secure [3,4]. To battle with the power of a quantum computer, quantum cryptography was born to encrypt information based upon the principle of quantum mechanics. Surprisingly, some of these fundamental principles like the no-cloning theorem and the observer effect could guarantee unconditional security. Since the first quantum key distribution protocol was proposed in 1984 by Bennett and Brassard [5], a variety of quantum cryptographic protocols have been proposed, including those for key distribution [6], secret sharing [7,8], coin flipping [9,10], private query [11–14], and so on.

In recent years, researchers have investigated how to use quantum mechanics to preserve the anonymity of senders and receivers in communication tasks. The first quantum protocol to anonymously broadcast classical bits and qubits was proposed by Christandl and Wehner [15]. Subsequently, much attention has been paid to carrying out anonymous voting by using the quantum principle. In 2007, Vaccaro *et al.* presented a quantum anonymous voting protocol [16]. Subsequently, several quantum anonymous voting protocols [17–19] based on entangled states were put forward. Afterwards, Horoshko and Kilin [20] devised a quantum anonymous voting protocol which simply utilized single-particle qubit states to vote and Bell states to check the anonymity. More recently, a series of quantum anonymous voting protocols based on continuous variables have been proposed [21]. However, these protocols are function limited in two aspects: (1) most of them consider only two candidates, and (2) most of them are designed to achieve only the property of privacy, and other properties are rarely pursued. In particular, the property of self-tallying proposed in the classical voting protocol by Kiayias and Yung [22] means anyone who is interested in the voting result can tally votes by himself or herself. The functionality of self-tallying avoids introducing a third party, thus reducing the potential risk of security. As far as we know, no previous quantum anonymous voting protocols have this property, which requires at least one third party to tally votes, and most of them neglect the cheating of a third party, e.g., if the third party tampers with the voting results.

*gaof@bupt.edu.cn

Is there a quantum voting protocol which not only overcomes the above limitations but also satisfies all these favorable properties? We address this question in this paper. We propose a quantum anonymous voting protocol for any number of candidates meeting privacy, nonreusability, verifiability, fairness, and self-tallying at the same time. With a slight generalization, we show that our protocol can be used for any anonymous multiparty computation (AMC) task. This paper is structured as follows. In Sec. II, we introduce two kinds of entangled quantum states which will be the key resources in our protocol. We present our self-tallying quantum anonymous voting (SQAV) protocol in Sec. III. Then we analyze the security of our protocol in Sec. IV. In Sec. V, we generalize our protocol to AMC and briefly discuss two possible applications. Finally, we discuss the properties of self-tallying, nonreusability, verifiability, and fairness that our protocol satisfies in Sec. VI and draw a conclusion in the last section.

II. QUANTUM RESOURCES OF THE PROTOCOL

The security of our SQAV protocol relies on the fact that we use two classes of quantum multiparticle entangled states to distribute the ballot boxes and index numbers to each voter. In this section we introduce these states and some of their properties which are quite useful in our protocol.

Consider a system in m levels with the computational basis $\{|j\rangle_C, j=0,1,\ldots,m-1\}$. The Fourier basis $\{|j'\rangle_F, j=0,1,\ldots,m-1\}$, which can be obtained by applying a Fourier operation on a computational basis, is defined as

$$|j'\rangle_F=\mathcal{F}|j\rangle_C=\frac{1}{\sqrt{m}}\sum_{k=0}^{m-1}\exp\left(\frac{2\pi ijk}{m}\right)|k\rangle_C. \quad (1)$$

Now we give the first quantum entangled state in our protocol, which has been dexterously applied to implement the tasks of anonymous voting [18] and anonymous ranking [23].

The m-level, n-particle state $|\mathcal{X}_n\rangle$ is defined as

$$|\mathcal{X}_n\rangle\equiv\frac{1}{m^{\frac{n-1}{2}}}\sum_{\sum_{k=0}^{n-1}j_k \bmod m=0}|j_0\rangle_C|j_1\rangle_C\cdots|j_{n-1}\rangle_C, \quad (2)$$

where $|j_k\rangle$ is the state of the jth particle in the computational state and $j_k\in\mathbb{Z}_m:=\{0,1,\ldots,m-1\}$.

$|\mathcal{X}_n\rangle$ has the interesting property that it has the form of a Greenberger-Horne-Zeilinger state in the Fourier basis,

$$|\mathcal{X}_n\rangle=\frac{1}{\sqrt{m}}\sum_{j=0}^{m-1}|j'\rangle_F|j'\rangle_F\cdots|j'\rangle_F. \quad (3)$$

Therefore $|\mathcal{X}_n\rangle$ has two nice properties. (1) When the state is measured in the computational basis, the summation of the outcomes of all particles modulo m is equal to zero. (2) When the state is measured in the Fourier basis, the outcomes of all particles are always the same. To take advantage of the above two properties to protect the voting process from being eavesdropped on or attacked, we need to use the following result [23].

Theorem 1. An n-particle, m-level quantum state is in the form of $|\mathcal{X}_n\rangle$ if and only if both of the following conditions are true: (1) when each particle is measured in the computational basis, the sum over all n measurement outcomes modulo m is equal to zero; (2) when each particle is measured in the Fourier basis, the measurement outcomes are all the same.

The other quantum entangled states we will use in the voting protocol are defined as follows.

An n-level, n-particle singlet state $|\mathcal{S}_n\rangle$ is defined as

$$|\mathcal{S}_n\rangle\equiv\frac{1}{\sqrt{n!}}\sum_{S\in\mathcal{P}_n^n}(-1)^{\tau(S)}|s_0\rangle|s_1\rangle\cdots|s_{n-1}\rangle. \quad (4)$$

Here $\mathcal{P}_n^n$ is the set of all permutations of $\mathbb{Z}_n:=\{0,1,\ldots,n-1\}$, and S is a permutation (or sequence) in the form $S=s_0s_1\cdots s_{n-1}$. $\tau(S)$, called the inverse number, is defined as the number of transpositions of pairs of elements of S that must be composed to place the elements in canonical order, $012\cdots n-1$.

$|\mathcal{S}_n\rangle$ is n-lateral rotationally invariant, which means the measurements of all particles are all different in any basis [24]. In Appendix A, we give a proof of this property. Specifically,

$$|\mathcal{S}_n\rangle_C=e^{i\phi}|\mathcal{S}_n\rangle_F, \quad (5)$$

where ϕ is a phase factor. This property will be exploited to ensure the security of our voting protocol based on Theorem 2.

Theorem 2. An n-particle, n-level quantum state is in the form of $|S_n\rangle$ if and only if the following condition is satisfied: whenever the state is measured in the computational basis or the Fourier basis, the permutation of the outcomes of n particles $\{s_0,s_1,\ldots,s_{n-1}\}$ is a random element of the set $\mathcal{P}_n^n$.

We give a proof of Theorem 2 in Appendix B.

III. QUANTUM ANONYMOUS VOTING PROTOCOL

We first briefly outline our quantum anonymous voting protocol before delving into details. Assume there are n voters labeled $V_0,V_1,\ldots,V_{n-1}$. Each voter can vote for m candidates labeled by integer $0,1,\ldots,m-1$. Our protocol consists of three steps. First, a number of n-particle entangled states $|\mathcal{X}_n\rangle$ are distributed to n voters, with each voter holding one particle for each state. After a security test to check for eavesdropping, each voter obtains n random numbers, called *ballot numbers*, from n secret "ballot boxes" by measuring the remaining n states $|\mathcal{X}_n\rangle$. Second, a number of n-particle entangled states $|\mathcal{S}_n\rangle$ are distributed to n voters, and each voter also holds one particle for each state. After a security test, each voter gets a random number, called the *index number*, through measuring the remaining one state $|\mathcal{S}_n\rangle$, which determines which ballot box each voter will use for voting. Finally, each voter casts a vote to his or her indicated ballot box anonymously, and all voters open all ballot boxes at the same time. By this method, a random permutation of all votes appears, and any party who is interested in the voting result can obtain a copy of the permutation, thus learning the voting result. The details of our protocol are presented as follows, and the communications in our protocol are shown in Fig. 1. It is noted that all classical communication in the protocol takes place using pairwise authenticated channels.

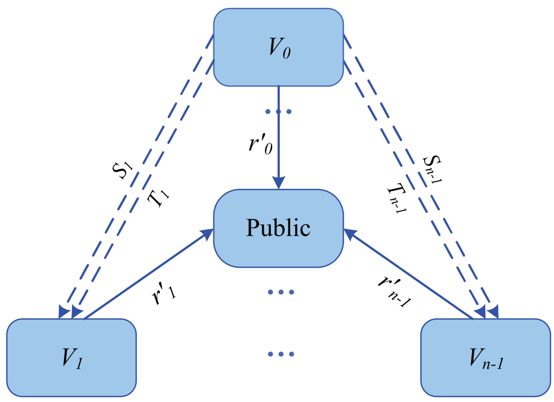

FIG. 1. Communications in our protocol. For simplicity, communications in the eavesdropping checks are not considered. The dashed lines represent quantum channels, and the solid lines represent classical simultaneous broadcast channels.

A. Procedure of the protocol

Step 1. Distributing secret ballot boxes

(1.1) *Prepare quantum states*. One of n voters is chosen randomly to prepare $n + n\delta_0$ copies of quantum state $|\mathcal{X}_n\rangle$, where δ_0 is the security strength. Without loss of the generality, we assume V_0 is appointed as the distributor. The jth copy of state $|\mathcal{X}_n\rangle$ lives in the Hilbert space of n particles, $p_{j,0}, p_{j,1}, \ldots, p_{j,n-1}$. Therefore we have a *particle matrix* $p_{j,k}$ with $0 \leqslant j \leqslant n + n\delta_0 - 1, 0 \leqslant k \leqslant n - 1$.

(1.2) *Distribute to each voter.* The distributor V_0 sends each column of the particle matrix, $S_k = \{p_{0,k}, p_{1,k}, \ldots, p_{n+n\delta_0-1,k}\}$, to each voter V_k (V_0 keeps S_0).

(1.3) *Perform security test.* After each voter has received his or her particle sequence, each voter as the checker performs the security check processes to ensure the state distributed is intact. Starting from voter V_0 (the order does not matter), he or she randomly picks out δ_0 particles as the test particles,

$$\vec{p}^{\,0}_{\text{test}} = p_{i_0,0} p_{i_1,0} \ldots p_{i_{\delta_0-1},0}. \tag{6}$$

V_0 also needs to choose randomly from the computational basis or Fourier basis with uniform distribution for each test state, in which he or she will measure his or her test particles with the chosen basis. Then he or she publishes the row index of his or her test particles and the measurement basis he or she chose to do the measurement. After receiving this information, all other voters are required to measure their particles with the same row index,

$$\vec{p}^{\,k}_{\text{test}} = p_{i_0,k} p_{i_1,k} \ldots p_{i_{\delta_0-1},k}, \quad k = 1,2, \ldots ,n - 1, \tag{7}$$

in the basis picked by the checker V_0. In other words, the i_0th, i_1th, $\ldots, i_{\delta_0-1}$th copies of $|\mathcal{X}_n\rangle$ are samples and measured in either the computational basis or Fourier basis. Then all voters send their measurement outcomes to the checker V_0 in the order designed by V_0. Let's label the result of measuring each test particle as $r_{i_j,k}$. If V_0 chooses the computational basis, he or she then needs to check if $\sum_{j=0}^{n-1} r_{i_j,k} \bmod m = 0$. If V_0 chooses the Fourier basis, he or she needs to verify whether $r_{i_j,0}, r_{i_j,1}, \ldots, r_{i_j,n-1}$ are all same. If the test is failed, V_0 informs the other voters to abort the protocol. If the test is passed, the same test procedure is performed by the next checker. The same procedure is repeated until the test performed by each voter is passed or the protocol is aborted in some intermediate step.

(1.4) *Generate ballot numbers.* If the security test is successful, each voter now has n particles left after discarding all test particles. Each voter then measures his or her remaining n particles in the computational basis. This will generate n ballot numbers for each voter. Ballot numbers of all voters form a *ballot matrix*, $r_{j,k} \in \{0,1, \ldots ,m - 1\}$. The kth column contains n private ballot numbers for V_k. Since the security is passed, each remaining copy of $|\mathcal{X}_n\rangle$ is intact, and according to Theorem 1, ballot numbers must satisfy the condition

$$\sum_{k=0}^{n-1} r_{j,k} \bmod m = 0 \tag{8}$$

for $j = 0,1, \ldots ,n - 1$.

Step 2. Distributing secret indexes

(2.1) *Prepare quantum states*. Similar to step (1.1), one of the n voters is chosen randomly to prepare $1 + n\delta_1$ copies of quantum state $|\mathcal{S}_n\rangle$, where δ_1 is the security strength. The jth copy of state $|\mathcal{S}_n\rangle$ lives in the Hilbert space of n particles, $t_{j,0}, t_{j,1}, \ldots, t_{j,n-1}$. Therefore we have a *particle matrix* $t_{j,k}$ with $0 \leqslant j \leqslant n\delta_1, 0 \leqslant k \leqslant n - 1$.

(2.2) *Distribute to each voter*. The distributor sends each column of the particle matrix, $T_k = \{t_{0,k}, t_{1,k}, \ldots, t_{n\delta_1,k}\}$, to the voter V_k.

(2.3) *Perform security test*. After each voter has received his or her particle sequence, each voter performs the security check processes to ensure the state distributed is intact. Starting from voter V_0 (the order does not matter), he or she randomly picks out δ_1 particles as the test particles,

$$\vec{t}^{\,0}_{\text{test}} = t_{i_0,0}, t_{i_1,0}, \ldots, t_{i_{\delta_1-1},0}. \tag{9}$$

V_0 also needs to choose randomly from the computational basis or Fourier basis with uniform distribution for each test particle, in which he or she will measure his or her test particle with the chosen basis. Then he or she publishes the row index of his or her test particles and the corresponding measurement basis he or she chose to do the measurement. After receiving this information, all other voters are required to measure their particles with the same row index,

$$\vec{t}^{\,k}_{\text{test}} = t_{i_0,k}, t_{i_1,k}, \ldots, t_{i_{\delta_1-1},k} \tag{10}$$

for $k = 0,1,2, \ldots ,n - 1$ in the basis picked by the checker V_0 and send their measurement outcomes to the checker V_0 in the order appointed by V_0. That is, the i_0th, i_1th, $\ldots, i_{\delta_1-1}$th copies of $|\mathcal{S}_n\rangle$ are measured in either the computational basis or the Fourier basis. Label the result of measuring each test particle as $d_{i_j,k}$. Regardless of whether V_0 chooses the computational basis or the Fourier basis, he or she then needs to check if $\{d_{i_j,0}, d_{i_j,1}, \ldots, d_{i_j,n-1}\} \in \mathcal{P}^n_n$ according to Theorem 2. If the test is successful, the same test procedure is performed by the next checker. If the test fails, V_0 informs the other voters to abort the protocol. The same procedure is repeated until the test performed by each voter is passed or the protocol is aborted in some certain intermediate step.

(2.4) *Generate index numbers*. If the security test is successful and then discards all test particles, each voter now has only one particle left. Each voter then measures his or her particle in the computational basis. This will generate an index number for each voter. Index numbers of all voters form an *index array*, $d_k \in \{0,1,\ldots,m-1\}$. d_k indicates anonymously that the d_kth ballot box is the box V_k should use to cast the vote. Since the security has been tested, the only remaining copy of $|\mathcal{S}_n\rangle$ is intact according to Theorem 2. Here $d_0,d_1,\ldots,d_{n-1} \in \mathcal{P}_n^n$.

Step 3. Vote casting

(3.1) *Vote casting*. After steps 1 and 2, each voter V_k has n ballot numbers $r_{0,k},r_{1,k},\ldots,r_{n-1,k}$ and one index number d_k. Now voter V_k votes for the candidate $v_k \in \{0,1,\ldots,m-1\}$ by adding v_k to $r_{d_k,k}$. He or she then renews ballot numbers $r'_{jk} = (r'_{0,k},r'_{1,k},\ldots,r'_{n-1,k})$, in which

$$r'_{j,k} = \begin{cases} r_{j,k} + v_k \bmod m & \text{if } j = d_k, \\ r_{j,k} & \text{if } j \neq d_k. \end{cases} \tag{11}$$

All voters publish all the updated ballot numbers through simultaneous broadcast channels [25–27]. At last we have a *vote matrix* $r'_{j,k}$ which is available for every party at the same time.

Here we briefly discuss how does simultaneous broadcast work and be implemented in our protocol. A regular broadcast channel is an authentic broadcast channel in which the sender is confident that the receivers receive the same value sent from the sender and the receivers know the identity of the sender. In contrast, a simultaneous broadcast channel allows the participants to simultaneously announce their values independently in the way that no participant can announce his/her value based on the values broadcast by other participants. Our protocol utilizes the simultaneous broadcast channel to announce the updated ballot numbers r'_{jk} in step (3.2) to avoid the possibility that the voter who lastly announces the values can change his/her values to his/her benefit. However, it is required that the number of honest voters to be at least half of the number of all voters in the simultaneous broadcast scheme [26]. Here we give an alternative simultaneous broadcast scheme by using the regular broadcast channel, which is more suitable for our protocol and, more importantly, does not limit the number of honest voters. This scheme is consisted of two steps: (1) each voter V_j announces his/her updated ballot numbers r'_{jk} in an order only known to himself/herself; (2) after announcement each voter announces the right order of updated ballot numbers. If the voter who is the last one to announce the order of his/her updated ballot number does not announce a right order for cheating, the other voters can not pass the security check in step (3.3) and the protocol will be aborted.

(3.2) *Self-tallying*. With the vote matrix, each party who is interested in the voting result can count the votes for each candidate. They take the summation of each row,

$$R_j = \sum_{k=0}^{n-1} r'_{j,k} \bmod m \tag{12}$$

$$= \sum_{k=0}^{n-1} r_{j,k} + v_{k_0} \bmod m. \tag{13}$$

Here $d_{k_0} = j$. Therefore $\{R_0,R_1,\ldots,R_{n-1}\}$ is a permutation of the votes $\{v_0,v_1,\ldots,v_{n-1}\}$. The number of votes candidate V_i got is given by

$$N_i = \sum_{R_j=i} 1 \tag{14}$$

for $i = 0,1,\ldots,m-1$.

(3.3) *Security check*. Each voter V_k needs to verify that $R_{d_k} = v_k$. If the answer is yes, his or her vote has been counted correctly; otherwise, the protocol is aborted since the voting step has been compromised.

TABLE I. A simple example of SQAV with $n = 4$ and $m = 3$. Each voter adds his or her votes to the ballot assigned by his or her index number. The tallying results are calculated according to Eq. (12).

	V_0	V_1	V_2	V_3	R_j
$r'_{0,k}$	0	1+2	2	0	2
$r'_{1,k}$	2+1	2	1	1	1
$r'_{2,k}$	1	0	2	0+0	0
$r'_{3,k}$	0	1	1+1	1	1

B. Example

To illustrate the protocol, we give a simple example (see Table I) with $n = 4$ voters and $m = 3$ candidates. For simplicity, we assume no eavesdropping or attack happened. Thus we ignore the security tests [steps (1.3), (2.3), and (3.3)]. After executing step 1, suppose the ballot matrix held by four voters is

$$r_{j,k} = \begin{pmatrix} 0 & 1 & 2 & 0 \\ 2 & 2 & 1 & 1 \\ 1 & 0 & 2 & 0 \\ 0 & 1 & 1 & 1 \end{pmatrix}. \tag{15}$$

After step 2, assume the index numbers are

$$(d_0,d_1,d_2,d_3) = (1,0,3,2). \tag{16}$$

Then in step 3, assume the four voters V_0,V_1,V_2, and V_3 cast votes

$$(v_0,v_1,v_2,v_3) = (1,2,1,0). \tag{17}$$

The voting and self-tallying processes are described in Table I. The final published results are

$$(R_0,R_1,R_2,R_3) = (2,1,0,1), \tag{18}$$

which is indeed a permutation of the votes v_k as we expected.

IV. PRIVACY ANALYSIS

Privacy is the primary property of a SQAV protocol. In this section, we focus on discussing the privacy of our SQAV, and other properties will be given in Sec. VI. Generally, the top priority is to protect the privacy of each voter. That is, no outsider or voter should know which vote is cast by whom except the one he or she cast. In our SQAV, the attacker could be an outside eavesdropper, one dishonest voter [28,29], or an adversary which includes some dishonest voters. If an attacker successfully eavesdrops on the ballot random numbers or the index number of voter V_k without being detected, he or she can easily know which candidate V_k votes for. Therefore preserving privacy in our SQAV requires preventing ballot numbers and index numbers from being eavesdropped on. The security tests in steps (1.3) and (2.3) are designed to protect the ballot matrix, the index array, and the voting process from being compromised.

A. Outside eavesdropper

As an outside eavesdropper, Eve could intercept S_k or T_k during step (1.2) or (2.2). Let's consider the case that Eve intercepts arbitrary x particles in S_k. If $x < n$, then there is a chance that all x particles happen to be among the n particles which are not included in the tests. Actually, the probability of this happening is

$$P_e = \binom{n}{x}\Big/\binom{n+n\delta_0}{x} = \frac{n!}{(n-x)!}\frac{(n+n\delta_0-x)!}{(n+n\delta_0)!} = \prod_{k=n}^{n-x+1}\frac{k}{k+n\delta_0} \quad (19)$$

$$\sim O\left(\left(\frac{1}{\delta_0}\right)^x\right), \quad (20)$$

which approaches zero if we make the security strength δ_0 large enough. Actually, the more particles Eve intercepts, the faster the probability that she could pass the security check goes to zero. Similarly, we could argue that the probability of Eve intercepting and modifying T_k in step 2 without being found is negligible. Therefore, for large enough δ_0,δ_1, the disturbed particles cannot escape from the security tests in steps (1.3) and (2.3).

Let's consider another scenario. Assume Eve intercepts and modifies $p_{j_0,k}$ in S_k, thus changing the j_0th copy of $|\mathcal{X}_n\rangle$. Suppose that the new state due to Eve's disturbance is $|\phi_e\rangle$. The probability that all security tests in step (2.3) are passed is

$$P_e = \left(\tfrac{1}{2}P_C + \tfrac{1}{2}P_F\right)^{n\delta_0}, \quad (21)$$

where

$$P_C = \sum_{\sum_k j_k \bmod m=0} |\langle\phi_e|j_0,j_1,\ldots,j_{n-1}\rangle_C|^2, \quad (22)$$

$$P_F = \sum_{j=0}^{m-1} |\langle\phi_e|j,j,\ldots,j\rangle_F|^2. \quad (23)$$

Since $\langle\phi_e|\mathcal{X}_n\rangle \neq 1$ according to Theorem 1, $P_C + P_F < 1$. Therefore, for large enough δ_0,

$$P_e \to 0. \quad (24)$$

The argument for Eve modifying the index number is similar. Eve cannot pass the security tests if δ_1 is large enough based on Theorem 2. In summary, as long as the security strengths δ_0,δ_1 are large enough, the attack from an outside eavesdropper can be prevented. It should be noted that the security analysis applies to the case where δ_0 and δ_1 are infinite, and a more careful analysis, for the practical finite case, that can bound the probabilities of passing security tests for different types of cheating when δ_0 and δ_1 increase, deserves to be performed in our future work.

B. Dishonest voters and ballot numbers

In step 1, to gain the information of ballot numbers of honest voters, the dishonest voters could cooperate to attack the particles during their transmission in step (1.2) and could announce the wrong results to avoid being detected by the honest voters in step (1.3). Since V_0 is the only voter who prepares and distributes the quantum states, it seems that V_0 plays a different role from the other voters. To analyze the possible attacks from dishonest voters in more detail, two cases are considered: (1) V_0 is honest, and (2) V_0 is dishonest.

For case 1, without loss of generality, we suppose there are l dishonest voters, $V_{i_0},V_{i_1},\ldots,V_{i_{l-1}}$. The most general attack by the dishonest voters is that they intercept some particles during the transmission from V_0 to honest voters, and then they perform a unitary operation (attack operation) on the intercepted particles and an auxiliary system to yield a new state, denoted by $|\Phi\rangle$, of the composite system. To avoid being detected by the honest voters in step (1.3) when they measure their particles with the Fourier basis and the measurement outcomes are required to be the same, $|\Phi\rangle$ should be in the form

$$|\Phi\rangle = \frac{\sum_{j=0}^{m-1}|j'\rangle_0|j'\rangle_{j_0}\cdots|j'\rangle_{j_{n-l-2}}|\phi_j\rangle}{\sqrt{m}}, \quad (25)$$

where $|\phi_j\rangle$ are the unnormalized states of the composite system (denoted by E_0) of l particles sent from V_0 to the dishonest voters and the auxiliary system and the subscripts $0,j_0,j_1,\ldots,j_{n-l-2}$ represent the particles held by honest voters $V_0,V_{j_0},V_{j_1},\ldots,V_{j_{n-l-2}}$. It can be rewritten in the computational basis as

$$|\Phi\rangle = \sum_{k_0,k_{j_0},\ldots,k_{j_{n-l-2}}=0}^{m-1}\frac{|k_0\rangle|k_{j_0}\rangle\cdots|k_{j_{n-l-2}}\rangle}{m^{\frac{n-l+1}{2}}} \otimes |\varphi_{k_0k_{j_0}\cdots k_{j_{n-l-2}}}\rangle, \quad (26)$$

where $|\varphi_{k_0k_{j_0}\cdots k_{j_{n-l-2}}}\rangle = \sum_{j=0}^{m-1}\exp\left(\frac{2\pi i j(k_0+k_{j_0}+\cdots+k_{j_{n-l-2}})}{m}\right)|\phi_j\rangle$ is the unnormalized state vector of system E_0. The dishonest voters could measure the system E_0 and obtain some $|\varphi_{k_0k_{j_0}\cdots k_{j_{n-l-2}}}\rangle$ to infer the measurement outcomes $k_0k_{j_0}\cdots k_{j_{n-l-2}}$ of honest voters in step (1.4). From the form of $|\varphi_{k_0k_{j_0}\cdots k_{j_{n-l-2}}}\rangle$, it is easy to see that, for any two different outcomes $k_0k_{j_0}\cdots k_{j_{n-l-2}}$ and $k'_0k'_{j_0}\cdots k'_{j_{n-l-2}}$ such that $k_0+k_{j_0}+\cdots+k_{j_{n-l-2}} = k'_0+k'_{j_0}+\cdots+k'_{j_{n-l-2}} \bmod m$, $|\varphi_{k_0k_{j_0}\cdots k_{j_{n-l-2}}}\rangle = |\varphi_{k'_0k'_{j_0}\cdots k'_{j_{n-l-2}}}\rangle$. This means that the dishonest voters can only, at most, know the information about the sum $k_0k_{j_0}\cdots k_{j_{n-l-2}}$ mod m by measuring the system E_0. However, this attack is trivial in the sense that without any eavesdropping attack a dishonest voter can cooperate to directly infer the sum of measurement outcomes (ballot numbers) of honest voters after executing step (1.4).

For case 2, in which V_0 is dishonest, we assume there are l other dishonest voters $V_{i_0},V_{i_1},\ldots,V_{i_{l-1}}$. The most general attack for them is similar to case 1. The only difference could be that the dishonest voters can directly prepare and distribute fake states to the honest voters instead of intercepting the particles. To avoid being detected by honest voters, these states should be in a form similar to Eq. (25) or (26). From the above analysis for case 1, it is not hard to draw the same conclusion as in case 1 that, in order to avoid being detected, the dishonest voters can only perform a trivial attack to obtain the sum of ballot numbers of the honest voters.

C. Dishonest voters and index numbers

In step 2, to eavesdrop on the information of index numbers of honest voters, the dishonest voters could also attack the particles during their transmission in step (2.2) and announce the wrong results to avoid being detected by the honest voters in step (2.3). Just as we analyzed eavesdropping on the ballot numbers in the last section, we also consider two cases: (1) V_0 is honest, and (2) V_0 is dishonest.

For case 1, we also assume there are l dishonest voters, $V_{i_0}, V_{i_1}, \ldots, V_{i_{l-1}}$. The most general attack for them is that they first intercept some transmitted particles in step (2.2), entangle them with an auxiliary system prepared in advance, and then return the corrupted particles to honest voters. The state of the whole composite system is denoted by $|\Psi\rangle$. To elude detection in step (2.3), it is required that all the measurement outcomes should be distinct when measuring each particle held by honest voters in the Fourier basis, and thus $|\Psi\rangle$ should be of the form

$$|\Psi\rangle = \sum_{S\in\mathcal{P}_n^{n-l}} \frac{(-1)^{\tau(S)}\mathcal{F}^{\otimes(n-l)}|S\rangle}{\sqrt{|\mathcal{P}_n^{n-l}|}} \otimes |u_S\rangle, \tag{27}$$

where $S = s_0 s_{j_0}\cdots s_{j_{n-l-2}}$. $|u_S\rangle$ are the unnormalized states of composite system (denoted by E_1) of l particles sent to the dishonest voters and auxiliary system. $\mathcal{P}_n^{n-l} = \{x_0x_1\cdots x_{n-l-1}|x_0,x_1,\ldots,x_{n-l-1}\in\mathbb{Z}_n, \forall\, j\neq k, x_j\neq x_k\}$ is the set of all the $(n-l)$ permutations of $\mathbb{Z}_n$, and $|\mathcal{P}_n^{n-l}| = \frac{n!}{l!}$ is its size. $\mathcal{P}_n^{n-l}$ can be divided into $\binom{n}{n-l} = \frac{n!}{(n-l)!l!}$ subsets, each of which corresponds to the set of all $(n-l)!$ permutations of a $(n-l)$ combination of $\mathbb{Z}_n$. In addition, any two states $|u_{S_0}\rangle$ and $|u_{S_1}\rangle$ such that $S_0\in\mathcal{P}_n^{n-l,w_0}, S_1\in\mathcal{P}_n^{n-l,w_1}$, and $w_0\neq w_1$ should be orthogonal to each other, i.e., $\langle u_{S_0}|u_{S_1}\rangle = 0$. If not, the dishonest voters cannot deterministically know subset $\mathcal{P}_n^{n-l,w}$, which contains the honest voters' measurement outcomes, and thus they cannot announce the correct measurement outcomes to avoid being detected. Rewriting $|\Psi\rangle$ in the computational basis, we have

$$|\Psi\rangle = \frac{n^{-\frac{n-l}{2}}}{\sqrt{|\mathcal{P}_n^{n-l}|}} \sum_{T\in\mathcal{R}_n^{n-l}} |T\rangle\otimes|v_T\rangle, \tag{28}$$

where $T = t_0 t_{j_0}\cdots t_{j_{n-l-2}}$. $\mathcal{R}_n^{n-l} = \{x_0x_1\cdots x_{n-l-1}| x_0,x_1,\ldots,x_{n-l-1}\in\mathbb{Z}_n\}$, and

$$\begin{aligned}|v_T\rangle &= \sum_{S\in\mathcal{P}_n^{n-l}} (-1)^{\tau(S)} \exp\left(\frac{2\pi i\left(s_0t_0+\sum_{k=0}^{n-l-2} s_{j_k}t_{j_k}\right)}{n}\right)|u_S\rangle\\ &= \sum_w \sum_{S\in\mathcal{P}_n^{n-l,w}} (-1)^{\tau(S)}\\ &\quad\times\exp\left(\frac{2\pi i\left(s_0t_0+\sum_{k=0}^{n-l-2} s_{j_k}t_{j_k}\right)}{n}\right)|u_S\rangle.\end{aligned}$$

$\{|v_T\rangle\}$ are the unnormalized state vectors of system E_1. To avoid being detected by the honest voters who measure their particles in the computational basis in step (2.3) in which the measurement outcomes are required to be distinct, two conditions should be satisfied: (a) in Eq. (28) there are no terms $|v_T\rangle$ for $T\notin\mathcal{P}_n^{n-l}$, or, equivalently, $T\in\mathcal{Q}_n^{n-l} = \{x_0x_1\cdots x_{n-l-1}|x_0,x_1,\ldots,x_{n-l-1}\in\mathbb{Z}_n, \exists\, j\neq k, x_j = x_k\}$; (b) any two states $|v_{T_0}\rangle$ and $|v_{T_1}\rangle$ for $T_0\in\mathcal{P}_n^{n-l,w_0}, T_1\in\mathcal{P}_n^{n-l,w_1}$, and $w_0\neq w_1$ should be orthogonal to each other, i.e., $\langle v_{T_0}|v_{T_1}\rangle = 0$. Here we focus on analyzing what $|\Psi\rangle$ [in Eq. (28)] should be to satisfy condition (a). Since $\langle u_{S_0}|u_{S_1}\rangle = 0$ for $S_0\in\mathcal{P}_n^{n-l,w_0}, S_1\in\mathcal{P}_n^{n-l,w_1}$, and $w_0\neq w_1$, condition (a) is equivalent to the one where $\sum_{S\in\mathcal{P}_n^{n-l,w}}(-1)^{\tau(S)}\exp(\frac{2\pi i(s_0t_0+\sum_{k=0}^{n-l-2}s_{j_k}t_{j_k})}{n})|u_S\rangle = 0$ for arbitrary w and arbitrary $T\in\mathcal{Q}_n^{n-l}$. To satisfy this condition, for arbitrary w, all $|u_S\rangle$ such that $S\in\mathcal{P}_n^{n-l,w}$ should be equal (denoted by $|u_w\rangle$), which is implied by the Corollary 1 in Appendix B. Thus $|v_T\rangle$ can be rewritten as

$$\begin{aligned}|v_T\rangle &= \sum_w \sum_{S\in\mathcal{P}_n^{n-l,w}} (-1)^{\tau(S)}\\ &\quad\times\exp\left(\frac{2\pi i\left(s_0t_0+\sum_{k=0}^{n-l-2} s_{j_k}t_{j_k}\right)}{n}\right)|u_w\rangle.\end{aligned} \tag{29}$$

Once the dishonest voters successfully elude the eavesdropping-check process in step (2.3), they could measure the system E_1 and get some $|v_T\rangle$ to infer the index numbers $T = t_0t_{j_0},\ldots,t_{j_{n-l-2}}$ of honest voters in step (2.4). However, from the form of $|v_T\rangle$ in Eq. (29), it is easy to verify that for any two sequences T_0, T_1 which are in the same subset $\mathcal{P}_n^{n-l,w}$, $|v_{T_0}\rangle = |v_{T_1}\rangle$. Therefore the dishonest voters can, at most, know the information about which subset (i.e., w) the honest voters' index numbers are in. However, this general entangle-measure attack is trivial in the sense that the dishonest voters can cooperate to obtain this information without any attack.

For case 2, in which V_0 is dishonest, the general attack performed by the dishonest voters would be the same as in case 1 except that the dishonest voters would prepare and distribute the fake states in a form similar to Eq. (27) to the honest voters instead of intercepting the particles in step (2.2). According to the analysis in case 1, we can conclude that the dishonest voters cannot obtain the index numbers of honest voters without being detected.

V. GENERALIZATION TO ANONYMOUS MULTIPARTY COMPUTATION

One important feature of SQAV is to make each vote open without any relation to any voter. Actually, it provides a mechanism to implement a class of multiparty tasks. That is, as used for voting, our protocol can be used for multiparty tasks which require broadcasting the data of each party anonymously. Therefore we define a more general class of problem, anonymous multiparty computation (AMC), as follows.

Definition 1. Anonymous multiparty computation is a task to compute a function of the form $f(y_0^0,\ldots,y_0^{i_0-1}, y_1^0,\ldots,y_1^{i_1-1},y_{n-1}^0,\ldots,y_{n-1}^{i_{n-1}-1})$ by n parties. The function f

is invariant under the permutation of integer inputs $\{y_k^i\}$. Each party P_k feeds $y_k^0,\ldots,y_k^{i_k-1}$ in the function anonymously and obtains the result without assistance from any other person. All the inputs are bounded by $0 \leqslant y_k < m$.

The protocol for AMC is very similar to that for SQAV.

(1) P_0 prepares $\bar{n} + n\delta_2$ copies of m-level, n-particle state $|\mathcal{X}_n\rangle$, where $\bar{n} = \sum_{k=0}^{n-1} i_k$. Then P_0 keeps the column S_0 to himself or herself and then distributes S_k to P_k. Here the particle columns S_k are defined as in step (1.2) of our previous quantum anonymous voting protocol. After distribution, each party P_k executes the security test procedure in step (1.3). If all n tests are passed, each party P_k measures his or her $\bar{n}$ particles, so again there is a ballot column

$$r_{j,k} = \begin{pmatrix} r_{0,k} \\ r_{1,k} \\ \vdots \\ r_{\bar{n}-1,k} \end{pmatrix}. \tag{30}$$

(2) P_0 prepares $1 + n\delta_3$ copies of $|\mathcal{S}_{\bar{n}}\rangle$ and distributes particle columns $T_{\sum_{t=0}^{k-1} i_t},\ldots,T_{\sum_{t=0}^{k} i_t - 1}$ to P_k ($k \geqslant 1$), while keeping the particle columns $T_0,\ldots,T_{i_0-1}$. Here the particle columns T_k are defined as in step (2.2) of our previous quantum anonymous voting protocol. In order to protect the process from attack, each party is required to choose δ_3 copies of $|\mathcal{S}_{\bar{n}}\rangle$ to examine if $|\mathcal{S}_{\bar{n}}\rangle$ is intact. If all tests are passed, each party P_k measures the remaining particles with the computation basis, and then there are index arrays $d_{\sum_{t=0}^{k-1} i_t,k},\ldots,d_{\sum_{t=0}^{k} i_t-1,k}$, where $d_{i,k} \in \{0,1,\ldots,\bar{n}-1\}$.

(3) Finally, each party adds his or her data to the ballot number decided by the corresponding index number, and we have a *data matrix* $r'_{j,k}$. Finally, every party can calculate

$$R_j = \sum_{k=0}^{n} r'_{j,k} \mod m, \tag{31}$$

where $\{R_j\}$ is a permutation of all the data $\bigcup y_j^i$. Therefore all the data are broadcasted anonymously.

(4) With holding all data, each party can obtain the result of

$$f\left(y_0^0,\ldots,y_0^{i_0-1},y_1^0,\ldots,y_1^{i_1-1},y_{n-1}^0,\ldots,y_{n-1}^{i_{n-1}-1}\right)$$

through simple calculation by himself or herself.

Actually, AMC is a subclass of a secure multiparty computation (SMC) problem, in which a number of parties also jointly compute a function over their inputs while the inputs are kept private. SMC focuses on the function result without publication of all inputs. To illustrate it, we give a simple example in which three parties want to jointly compute the function $f(y_0,y_1,y_2) = y_0 + y_1 + y_2$ over their inputs y_0,y_1, and y_2. Suppose $y_0 = 2, y_1 = 3, y_2 = 6$; by SMC, the parties have the result $f(y_0,y_1,y_2) = 11$. However, each party can only know the sum of the inputs of the other two parties. By AMC, in addition, to obtain the result $f(y_0,y_1,y_2) = 11$, every party also gets a permutation of the original inputs of the others. For example, each party knows (3,6,2), but the index of each party's input is known only to himself or herself. As a result, P_0 knows $(y_1,y_2) = (3,6)$ or $(6,3)$, P_1 knows $(y_0,y_2) = (2,6)$ or $(6,3)$, and P_2 knows $(y_0,y_1) = (2,3)$ or $(3,2)$. In fact, for some particular tasks, the function result leads to opening all inputs. In this sense, there is no difference between AMC and SMC. In the following, we give two examples to explain this.

A. Anonymous broadcast

The simplest application of AMC is to implement anonymous broadcast (AB). AB channels are primitives of many anonymous communication protocols.

An anonymous n-party broadcast task [15] is to publish the datum $y_k \in \{0,1,\ldots,m-2\}$ held by sender P_k anonymously, and all parties obtain y_k at the same time. In this scenario, the protocol is basically the same as SQAV with m candidates and n voters. If a sender would like to broadcast message y, he or she just needs to "vote" for "candidate" y following the protocol in Sec. III. However, if a party does not want to send any message, he or she just needs to vote for candidate $m-1$. Finally, each $R_k \in \{0,1,\ldots,m-2\}$ will be the message sent by one of the senders. Therefore each sender broadcasts the intended message anonymously.

B. Anonymous ranking

Anonymous ranking (AR) [23] is an important problem in AMC and has significant practical applications [23]. An AR task generally involves two steps. (1) Each party needs to broadcast his or her data $y_k = \{y_k^0,y_k^1,\ldots,y_k^{i_k-1}\}$ to the community anonymously. (2) Each party can rank the published data by himself or herself and obtain the rank of his or her data anonymously. Obviously, the first step could be done safely using our AMC protocol. Finally, similar to self-tallying in SQAV, self-ranking is obtained.

VI. DISCUSSION

We discuss in detail how our SQAV ensures privacy in Sec. IV. However, in addition to being able to maintain privacy for each voter, our protocol has several other nice properties which are not fulfilled by other existing protocols [16–21] at the same time.

(1) *Self-tallying*. In our protocol, any voter or other third party who is interested in voting results can tally the votes by himself or herself by counting the votes in $\{R_j\}$ in step (3.2). Through simple calculation, they can obtain the voting result.

(2) *Nonreusability*. In our voting protocol, no voter cannot cast more than one vote. More specifically, a voter cannot vote for one candidate more than once or vote for more than one candidate. Suppose voter V_k wants to vote twice, v_k and v_e, in step (3.1). To do so, he or she first casts v_k to the ballot box determined by his or her index number, d_k, as usual. Then he or she casts v_e to another ballot box labeled by d_e. However, since the index array $\{d_k\}$ is a permutation of $\mathbb{Z}_n$,d_e must be the index number of another voter V_j. Therefore V_j will find that $R_{d_j} = v_j + v_e \neq v_j \mod m$ and knows that someone cheated, thus aborting the voting protocol. Our protocol ensures that each voter only has one vote, and he or she can only use it once.

(3) *Verifiability*. In step (3.3) of our protocol, each voter can verify if his or her vote has been modified by attackers. As

long as V_k finds $R_{d_k} \neq v_k$, he or she knows that his or her vote has not been counted correctly.

(4) *Fairness*. If a voter could know some useful information about other votes beforehand, he or she might change his or her mind, thus voting for another candidate to his or her benefit. In our protocol, the voters vote only in step 3, and the vote tally is obtained by doing statistics on R_k, which is the sum over the numbers $r'_{j,k}$. However, the numbers $r'_{j,k}$ are announced via simultaneous broad channels in step (3.1), which means that a voter cannot acquire the other voters' information on $r'_{j,k}$ and thus cannot obtain a partial vote tally beforehand. Therefore, fairness can be maintained.

VII. CONCLUSION

We have presented a quantum protocol for implementing the task of anonymous voting with the help of two entangled quantum states, $|\mathcal{X}_n\rangle$ and $|\mathcal{S}_n\rangle$. Through our protocol, any individual party can acquire a permutation of all the votes, which means anyone can tally the votes without resorting to a third party. The protocol has been demonstrated to possess the properties of privacy, self-tallying, nonreusability, verifiability, and fairness. We also generalize our SQAV to the more general AMC task. Our generalized protocol can let each party broadcast his or her data anonymously and safely to be further fed into the AMC function.

An interesting open question is whether our protocol can be used to implement more tasks on AMC or SMC. This deserves further investigations in the future.

ACKNOWLEDGMENTS

The authors would like to thank the anonymous referee for their important suggestions. This work is supported by the NFSC (Grants No. 61272057 and No. 61572081) and funded by the China Scholarship Council (Grant No. 201506470043). H.Q. is supported by the Air Force Office of Scientific Research, the Army Research Office, and the National Science Foundation.

APPENDIX A: PROOF $|\mathcal{S}_n\rangle$ IS n-LATERAL ROTATIONALLY INVARIANT

Property 1. An n-dimensional quantum state on Hilbert space $\mathcal{H}_n$ is the superposition of computational basis $\{|i\rangle_C | i = 0,1,\ldots,n-1\}$. Consider state $|\mathcal{S}_n\rangle$ of n such particles on $\mathcal{H}_n^{\otimes n}$ in the following form:

$$|\mathcal{S}_n\rangle = \sum_{S\in\mathcal{P}_n^n}(-)^{\tau(S)}|S\rangle \tag{A1}$$

$$\equiv \sum_{S\in\mathcal{P}_n^n}(-)^{\tau(S)}|s_0s_1,\ldots,s_{n-1}\rangle. \tag{A2}$$

Consider another basis $\{|i'\rangle\}$ connected with the computational basis by a unitary transformation U, where

$$|i\rangle = \sum_j U_{ji}|j'\rangle. \tag{A3}$$

Then in this new basis the state $|\mathcal{S}_n\rangle$ takes the same form up to a global phase factor ϕ. That is,

$$|\mathcal{S}_n\rangle = e^{i\phi}\sum_{M\in\mathcal{P}_n^n}(-)^{\tau(M)}|M'\rangle \tag{A4}$$

$$\equiv e^{i\phi}\sum_{M\in\mathcal{P}_n^n}(-)^{\tau(M)}|m'_0m'_1\cdots m'_{n-1}\rangle. \tag{A5}$$

Here $\mathcal{P}_n^n = \{x_0x_1\cdots x_{n-1}|x_0,x_1,\ldots,x_{n-1}\in\mathbb{Z}_n,\forall\, j\neq k, x_j\neq x_k\}$, and the phase factor is given by

$$e^{i\phi} = \det(U). \tag{A6}$$

Proof. Expanding Eq. (A2) in the new basis by using the unitary transformation Eq. (A3), we have

$$|\mathcal{S}_n\rangle = \sum_{S\in\mathcal{P}_n^n}(-)^{\tau(S)}\sum_{m_0=0}^{n-1}U_{m_0,s_0}|m'_0\rangle\otimes\cdots\otimes \times\sum_{m_{n-1}=0}^{n-1}U_{m_{n-1},s_{n-1}}|m'_{n-1}\rangle \tag{A7}$$

$$= \left(\sum_{M\in\mathcal{P}_n^n}+\sum_{M\notin\mathcal{P}_n^n}\right) \times\left[\sum_{S\in\mathcal{P}_n^n}(-)^{\tau(S)}U_{m_0,s_0}U_{m_1,s_1}\cdots U_{m_{n-1},s_{n-1}}\right]|M\rangle \tag{A8}$$

$$= \left(\sum_{M\in\mathcal{P}_n^n}+\sum_{M\notin\mathcal{P}_n^n}\right)\det\left(U_{m_j,s_i}\right)|M\rangle \tag{A9}$$

if $M\notin\mathcal{P}_n^n, \exists\, s\neq t$, such that $m_s = m_t$; then there are two identical columns for matrix U_{m_j,s_i}. This means $U_{m_s,s_i} = U_{m_t,s_i}$. Therefore $\det U_{m_j,s_i} = 0$, and we have

$$|\mathcal{S}_n\rangle = \sum_{M\in\mathcal{P}_n^n}\det\left(U_{m_j,s_i}\right)|M\rangle$$

$$= \sum_{M\in\mathcal{P}_n^n}(-)^{\tau(M)}\det\left(U_{j,s_i}\right)|M\rangle$$

$$= \sum_{M\in\mathcal{P}_n^n}(-)^{\tau(M)}\det(U)|M\rangle$$

$$= e^{i\phi}\sum_{M\in\mathcal{P}_n^n}(-)^{\tau(M)}|M\rangle \tag{A10}$$

■

APPENDIX B: PROOF OF THEOREM 2

To prove Theorem 2, we first give two lemmas and one corollary.

Lemma 1. Let q be an arbitrary element of $\{1,2,\ldots,n-1\}$, and let $s_0,s_1,\ldots,s_{q-1}\in\mathbb{Z}_n$ be distinct. If $\sum_{j=0}^{q-1}\exp(\frac{2\pi i s_j t}{n})\alpha_j = 0$ always holds for any $t\in\mathbb{Z}_n$, we have $\alpha_0 = \alpha_1 = \cdots = \alpha_{q-1} = 0$.

Proof. If $\sum_{j=0}^{q}\exp(\frac{2\pi i s_j t}{n})\alpha_j = 0$ always holds for any $t \in \mathbb{Z}_n$, we have linear equations

$$A\begin{pmatrix}\alpha_0\\ \alpha_1\\ \vdots\\ \alpha_{q-1}\end{pmatrix} = \begin{pmatrix}0\\0\\ \vdots\\ 0\end{pmatrix}, \tag{B1}$$

where A is an $n\times q$ matrix with elements $A_{jk} = \exp(\frac{2\pi i(j-1)s_k}{n}) = [\exp(\frac{2\pi i s_k}{n})]^{j-1}$. Taking the first q rows of A as a new square matrix $\overline{A}$ with size $q\times q$, it is easy to see that $\overline{A}$ is a Vandermonde matrix [30]. Since $s_0,s_1,\dots,s_{q-1}$ are distinct, the determinant of $\overline{A}$ is nonzero, and thus the rank of A is q. Consequently, Eq. (B1) has only the solution $\alpha_0=\alpha_1=\cdots=\alpha_{q-1}=0$.

Lemma 2. Let m be an arbitrary element of $\{2,3,\dots,n\}$, $\mathcal{R}_n^m = \{x_0x_1\cdots x_{m-1}|x_0,x_1,\dots,x_{m-1}\in\mathbb{Z}_n\}$, $\mathcal{P}_n^m = \{x_0x_1\cdots x_{m-1}|x_0,x_1,\dots,x_{m-1}\in\mathbb{Z}_n,\forall j\neq k,x_j\neq x_k\}$, and $\mathcal{Q}_n^m = \{x_0x_1\cdots x_{m-1}|x_0,x_1,\dots,x_{m-1}\in\mathbb{Z}_n,\exists j\neq k,x_j=x_k\}$. Apparently, $\mathcal{P}_n^m\cap\mathcal{Q}_n^m=\emptyset$ and $\mathcal{R}_n^m=\mathcal{P}_n^m\cup\mathcal{Q}_n^m$. Divide $\mathcal{P}_n^m$ into $\binom{n}{m}=\frac{n!}{(n-m)!m!}$ subsets, each of which corresponds to the set of all $m!$ permutations of an m combination of $\mathbb{Z}_n$, denoted by $\mathcal{P}_n^{n,w}[w=0,1,\dots,\binom{n}{m}-1]$. For an arbitrary subset $\mathcal{P}_n^{m,w}$, if the equation

$$\sum_{S\in\mathcal{P}_n^{m,w}}(-1)^{\tau(S)}\prod_{j=0}^{m-1}\exp\left(\frac{2\pi i s_j t_j}{n}\right)\ \beta_S = 0 \tag{B2}$$

holds for any $t_0t_1\cdots t_{m-1}\in\mathcal{Q}_n^m$, we have that all β_S for $S\in\mathcal{P}_n^{m,w}$ are equal.

Proof. We use the method of induction to prove this lemma. For $m=2$, suppose $\mathcal{P}_n^{2,w}=\{\hat{s}_0\hat{s}_1,\hat{s}_1\hat{s}_0\}$ with $\hat{s}_0<\hat{s}_1, \mathcal{Q}_n^2=\{t_0t_1|t_0=t_1=t\in\mathbb{Z}_n\}$, and the equation $\sum_{s_0s_1\in\mathcal{P}_n^{2,w}}(-1)^{\tau(s_0s_1)}\exp(\frac{2\pi i(s_0t_0+s_1t_1)}{n})\beta_{s_0s_1}=0$ holds for any $t_0t_1\in\mathcal{Q}_n^2$. Since $t_0=t_1=t$, the equation can also be written as $\exp(\frac{2\pi i(\hat{s}_0+\hat{s}_1)t}{n})\beta_{\hat{s}_0\hat{s}_1}-\exp(\frac{2\pi i(\hat{s}_0+\hat{s}_1)t}{n})\beta_{\hat{s}_1\hat{s}_0}=0$. Obviously, $\beta_{\hat{s}_0\hat{s}_1}=\beta_{\hat{s}_1\hat{s}_0}$ is obtained.

We assume that, for $m=k$ and an arbitrary subset $\mathcal{P}_n^{k,w}$, if Eq. (B2) always holds for any $t_0t_1\cdots t_{k-1}\in\mathcal{Q}_n^k$, all $\beta_{s_0s_1\cdots s_{k-1}}$ for $s_0s_1\cdots s_{k-1}\in\mathcal{P}_n^{k,w}$ are equal. Now we analyze the case for $m=k+1$. We suppose the $(k+1)$ combination is $\mathcal{P}_n^{k+1,w}$, corresponding to the set $\hat{S}=\{\hat{s}_0,\hat{s}_1,\dots,\hat{s}_k\}$, with $\hat{s}_0<\hat{s}_1<\cdots<\hat{s}_k$. Namely, $\mathcal{P}_n^{k+1,w}$ is the set of all $(k+1)!$ permutations of $\hat{S}$. In this case, observing that s_p $(p\in\{0,1,\dots,k\})$ can take each value from $\hat{S}$ in Eq. (B2), the equation can be written as

$$\sum_{l=0}^{k}\left[\sum_{S\in\mathcal{P}_n^{k+1,w},s_p=\hat{s}_l}(-1)^{\tau(S)}\exp\left(\frac{2\pi i\hat{s}_l t_p}{n}\right)\prod_{j=0,j\neq p}^{k}\exp\left(\frac{2\pi i s_j t_j}{n}\right)\beta_S\right]=0. \tag{B3}$$

Noting that $(-1)^{\tau(S)}=(-1)^{l-p}(-1)^{\tau(s_0\cdots s_{p-1}s_{p+1}\cdots s_k)}$, Eq. (B3) can also be written as

$$\sum_{l=0}^{k}(-1)^{l-p}\exp\left(\frac{2\pi i\hat{s}_l t_p}{n}\right)\left[\sum_{S\in\mathcal{P}_n^{k+1,w},s_p=\hat{s}_l}(-1)^{\tau(s_0\cdots s_{p-1}s_{p+1}\cdots s_k)}\prod_{j=0,j\neq p}^{k}\exp\left(\frac{2\pi i s_j t_j}{n}\right)\beta_S\right]=0. \tag{B4}$$

We now prove that, if Eq. (B4) holds for any $t_0t_1\cdots t_k\in\mathcal{Q}_n^{k+1}$, all β_S for $S\in\mathcal{P}_n^{k+1,w}$ are equal. Especially, when $t_0\cdots t_{p-1}t_{p+1}\cdots t_k\in\mathcal{Q}_n^k$ is fixed and t_p takes every value from $\mathbb{Z}_n$, Eq. (B4) always holds. Hence, according to Lemma 1, we can derive that for arbitrary $l\in\{0,1,2,\dots,k\}$,

$$\sum_{S\in\mathcal{P}_n^{k+1,w},s_p=\hat{s}_l}(-1)^{\tau(s_0\cdots s_{p-1}s_{p+1}\cdots s_k)}\prod_{j=0,j\neq p}^{k}\exp\left(\frac{2\pi i s_j t_j}{n}\right)\beta_{s_0s_1\cdots s_k}=0. \tag{B5}$$

Here Eq. (B5) holds for arbitrary $t_0\cdots t_{p-1}t_{p+1}\cdots t_k\in\mathcal{P}_n^{k,w}$. Based on the previous assumption for the case $m=k$, all β_S for $S\in\mathcal{P}_n^{k+1,w}$ and $s_p=\hat{s}_l$ are equal. If Eq. (B2) holds for any $t_0t_1\cdots t_k\in\mathcal{Q}_n^{k+1}$ when $m=k+1,l$ and p can take arbitrary values from $\{0,1,2,\dots,k\}$, we can draw the conclusion that all β_S for $S\in\mathcal{P}_n^{k+1,w}$ are equal.

By mathematical induction above, we can derive that for an arbitrary $m\in\{2,\dots,n\}$, if Eq. (B2) holds for any $t_0t_1\cdots t_{m-1}\in\mathcal{Q}_n^m$, all $\beta_{s_0s_1\cdots s_{m-1}}$ for $s_0s_1\cdots s_{m-1}\in\mathcal{P}_n^{m,w}$ are equal.

Now we give a corollary of Lemma 2 below.

Corollary 1. Let $m,\mathcal{R}_n^m,\mathcal{P}_n^m$, and $\mathcal{Q}_n^m$ be defined in Lemma 2. For an arbitrary subset $\mathcal{P}_n^{m,w}$, if the equation

$$\sum_{s_0s_1\cdots s_{m-1}\in\mathcal{P}_n^{m,w}}(-1)^{\tau(s_0s_1\cdots s_{m-1})}\prod_{j=0}^{m-1}\exp\left(\frac{2\pi i s_j t_j}{n}\right)\ \vec{\beta}_{s_0s_1\cdots s_{m-1}}=\vec{0} \tag{B6}$$

holds for any $t_0t_1\cdots t_{m-1}\in\mathcal{Q}_n^m$, where $\vec{\beta}_{s_0s_1\cdots s_{m-1}}$ are vectors and $\vec{0}$ is a zero vector, all $\vec{\beta}_{s_0s_1\cdots s_{m-1}}$ for $s_0s_1\cdots s_{m-1}\in\mathcal{P}_n^{m,w}$ are equal.

The only difference between this corollary and Lemma 2 is that $\beta_{s_0s_1\cdots s_{m-1}}$ is generalized to the vector $\vec{\beta}_{s_0s_1\cdots s_{m-1}}$. Hence the corollary can be directly proved.

Now we use Lemma 2 to prove Theorem 2.

Proof. Restricting the measurement basis to the computation basis or Fourier basis, the necessity of our theorem can be directly obtained from Property 1.

Now we prove the sufficiency. On the one hand, to satisfy the condition that all the measurement outcomes are distinct when measuring each particle of $|\Theta\rangle$ in the Fourier basis, $|\Theta\rangle$ must be in the form

$$\begin{aligned} |\Theta\rangle &= \sum_{S\in\mathcal{P}_n^n}(-1)^{\tau(S)}\beta_S(\mathcal{F}|s_0\rangle)\otimes\cdots\otimes(\mathcal{F}|s_{n-1}\rangle) \\ &= \sum_{S\in\mathcal{P}_n^n}(-1)^{\tau(S)}\beta_S\left(\sum_{t_0}\frac{\exp\left(\frac{2\pi i s_0 t_0}{n}\right)}{\sqrt{n}}|t_0\rangle\right)\otimes\cdots\otimes\left(\sum_{t_{n-1}}\frac{\exp\left(\frac{2\pi i s_{n-1}t_{n-1}}{n}\right)}{\sqrt{n}}|t_{n-1}\rangle\right) \\ &= \sum_{t_0,t_1,\ldots,t_{n-1}}\sum_{S\in\mathcal{P}_n^n}\left[\frac{(-1)^{\tau(S)}}{n^{\frac{n}{2}}}\prod_{j=0}^{n-1}\exp\left(\frac{2\pi i s_j t_j}{n}\right)\beta_S\right]|t_0t_1\cdots t_{n-1}\rangle, \end{aligned} \tag{B7}$$

where $S=s_0s_1\cdots s_{n-1}$. On the other hand, to meet the condition that all the measurement outcomes are distinct when measuring each particle of $|\Theta\rangle$ in the computational basis, the terms $\sum_{S\in\mathcal{P}_n^n}[\beta_S\prod_{j=0}^{n-1}\exp(\frac{2\pi i s_j t_j}{n})]$ for $t_0t_1\cdots t_{n-1}\in\mathcal{Q}_n^n$ are required to be equal to zero. From Lemma 2 (when $m=n$), to satisfy this requirement, we can see that all β_S for $S\in\mathcal{P}_n^n$ are equal. Moreover, to keep normalization of $|\Theta\rangle$, we have

$$\beta_S=\frac{1}{\sqrt{n!}}. \tag{B8}$$

For any $t_0t_1\cdots t_{n-1}\in\mathcal{Q}_n^n$, according to the definition of the square matrix determinant, $\sum_{S\in\mathcal{P}_n^n}\frac{(-1)^{\tau(S)}}{n^{\frac{n}{2}}}\prod_{j=0}^{n-1}\exp(\frac{2\pi i s_j t_j}{n})$ is, in fact, the determinant of the $n\times n$ matrix $\overline{V}$ with elements $\overline{V}_{jk}=\frac{\exp(\frac{2\pi i t_j k}{n})}{\sqrt{n}}$. Namely,

$$\sum_{S\in\mathcal{P}_n^n}\frac{(-1)^{\tau(S)}}{n^{\frac{n}{2}}}\prod_{j=0}^{n-1}\exp\left(\frac{2\pi i s_j t_j}{n}\right)=\det(\overline{V}). \tag{B9}$$

Transposing pairs of rows of $\overline{V}$ to generate a new $n\times n$ matrix $\widetilde{V}$ with elements $\widetilde{V}_{jk}=\frac{\exp(\frac{2\pi i jk}{n})}{\sqrt{n}}$, we have

$$\det(\overline{V})=(-1)^{\tau(t_0t_1\cdots t_{n-1})}\det(\widetilde{V}). \tag{B10}$$

Inserting Eqs. (B8), (B9), and (B10) into Eq. (B7) and discarding the terms for $t_0t_1\cdots t_{n-1}\in\mathcal{Q}_n^n$ in Eq. (B7), we have

$$|\Theta\rangle=\sum_{T\in\mathcal{P}_n^n}\frac{(-1)^{\tau(T)}}{\sqrt{n!}}|T\rangle, \tag{B11}$$

up to the global factor $\det(\widetilde{V})$, where $T=t_0t_1\cdots t_{n-1}$. Therefore $|\Theta\rangle$ has the same form as $|\mathcal{S}_n\rangle$, and Theorem 2 is proved.

[1] B. Schneier, *Applied Cryptography* (Wiley, New York, 1996).

[2] D. Chaum, Untraceable electronic mail, return addresses, and digital pseudonyms, Commun. ACM **24**, 84 (1981).

[3] P. W. Shor, Algorithms for quantum computation: Discrete logarithms and factoring, in *Proceedings of 35th Annual Symposium on the Foundations of Computer Science* (IEEE Computer Society Press, Santa Fe, NM, 1994), pp. 124–134.

[4] L. K. Grover, Quantum Mechanics Helps in Searching for a Needle in a Haystack, Phys. Rev. Lett. **79**, 325 (1997).

[5] C. H. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing* (IEEE Press, New York, 1984), pp. 175–179.

[6] H. K. Lo and H. F. Chau, Unconditional security of quantum key distribution over arbitrarily long distances, Science **283**, 2050 (1999).

[7] M. Hillery, V. Buzek, and A. Berthiaume, Quantum secret sharing, Phys. Rev. A **59**, 1829 (1999).

[8] R. Cleve, D. Gottesman, and H. K. Lo, How to Share a Quantum Secret, Phys. Rev. Lett. **83**, 648 (1999).

[9] D. Aharonov, A. Ta-Shma, U. Vazirani, and A. Yao, Quantum bit escrow, in *Proceedings of 32nd Annual ACM Symposium on Theory of Computing* (ACM Press, New York, 2000), pp. 705–714.

[10] R. W. Spekkens and T. Rudolph, Optimization of coherent attacks in generalizations of the BB84 quantum bit commitment protocol, Quantum Inf. Comput. **2**, 66 (2002).

[11] M. Jakobi, C. Simon, N. Gisin, J. D. Bancal, C. Branciard, N. Walenta, and H. Zbinden, Practical private database queries based on a quantum-key-distribution protocol, Phys. Rev. A **83**, 022301 (2011).

[12] F. Gao, B. Liu, W. Huang, and Q. Y. Wen, Postprocessing of the oblivious key in quantum private query, IEEE J. Sel. Top. Quant. **21**, 6600111 (2015).

[13] B. Liu, F. Gao, and W. Huang, QKD-based quantum private query without a failure probability, Sci. China Phys. Mech. Astron. **58**, 100301 (2015).

[14] C. Y. Wei, T. Y. Wang, and F. Gao, Practical quantum private query with better performance in resisting joint-measurement attack, Phys. Rev. A **93**, 042318 (2016).

[15] M. Christandl and S. Wehner, Quantum anonymous transmissions, in *Proceedings of 11th ASIACRYPT*, Lecture Notes in Computer Science Vol. 3788 (Springer, Berlin, 2005), pp. 217–235.

[16] J. A. Vaccaro, J. Spring, and A. Chefles, Quantum protocols for anonymous voting and surveying, Phys. Rev. A **75**, 012333 (2007).

[17] M. Hillery, M. Ziman, V. Bužek, and M. Bielikova, Towards quantum-based privacy and voting, Phys. Lett. A **349**, 75 (2006).

[18] S. Dolev, I. Pitowsky, and B. Tamir, A quantum secret ballot, arXiv:quant-ph/0602087.

[19] M. Bonanome, V. Bužek, M. Hillery, and M. Ziman, Toward protocols for quantum-ensured privacy and secure voting, Phys. Rev. A **84**, 022331 (2011).

[20] D. Horoshko and S. Kilin, Quantum anonymous voting with anonymity check, Phys. Lett. A **375**, 1172 (2011).

[21] L. Jiang, G. Q. He, D. Nie, J. Xiong, and G. H. Zeng, Quantum anonymous voting for continuous variables, Phys. Rev. A **85**, 042309 (2012).

[22] A. Kiayias and M. Yung, Self-tallying elections and perfect ballot secrecy, in *Proceedings of Public Key Cryptography*, Lecture Notes in Computer Science Vol. 2274 (Springer, Berlin, 2002), pp. 141–158.

[23] W. Huang, Q. Y. Wen, B. Liu, Q. Su, S. J. Qin, and F. Gao, Quantum anonymous ranking, Phys. Rev. A **89**, 032325 (2014).

[24] A. Cabello, N-Particle N-Level Singlet States: Some Properties and Applications, Phys. Rev. Lett. **89**, 100402 (2002).

[25] A. Broadbent and A. Tapp, Information-Theoretic Security Without an Honest Majority, in *Proceedings of Asiacrypt 2007* (Springer, Berlin, 2007), pp. 410–426.

[26] S. Faust, E. Fäsper, and S. Lucks, Efficient simultaneous broadcast, in *International Workshop on Public Key Cryptography* (Springer, Berlin, Heidelberg, 2008), pp. 180–196.

[27] A. Hevia and D. Micciancio, Simultaneous broadcast revisited, in *Proceedings of the Twenty-Fourth Annual ACM Symposium on Principles of Distributed Computing* (ACM Press, New York, 2005), pp. 324–333.

[28] F. Gao, S. J. Qin, Q. Y. Wen, and F. C. Zhu, A simple participant attack on the brádler-dušek protocol, Quantum Inf. Comput. **7**, 329 (2007).

[29] S. Lin, F. Gao, F. Z. Guo, Q. Y. Wen, and F. C. Zhu, Comment on "Multiparty quantum secret sharing of classical messages based on entanglement swapping", Phys. Rev. A **76**, 036301 (2007).

[30] B. Ycart, A case of mathematical eponymy: The Vandermonde determinant, Rev. Historire Math. **19**, 43 (2013).