IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received October 14, 2021, accepted October 23, 2021, date of publication October 27, 2021, date of current version November 4, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3123681

A Secure Quantum Protocol for Anonymous One-Vote Veto Voting

SONGYANG WU[1], WENQI SUN[1], QINGLE WANG[2,3], RONGHUA CHE[4], MENG HU[2], ZHIGUO DING[1], AND XUE XUE[2]

[1]The Third Research Institute of Ministry of Public Security, Shanghai 200031, China
[2]School of Control and Computer Engineering, North China Electric Power University, Beijing 102206, China
[3]State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing 100876, China
[4]Liaocheng Infant Normal School, Liaocheng 252000, China

Corresponding author: Qingle Wang (wqle519@gmail.com)

This work was supported in part by the NSFC under Grant 61801126; in part by the Open Foundation of State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, under Grant SKLNST-2021-1-05; in part by the Fundamental Research Funds for the Central Universities under Grant 2020MS014; and in part by The Third Research Institute of The Ministry of Public Security 2021 Special Funding for Fundamental Research under Grant C21353.

ABSTRACT Voting is one of the most prominent components of democracy. The one-vote veto, which requires the voting result to be only ''yes'' or ''no'', is a particularly noteworthy type of voting with widespread application. When obtaining a ''no'' result, no useful information about the number of ''no'' votes and who votes ''no'' is disclosed. In this paper, we introduce a protocol for anonymous one-vote veto utilizing qubits and local Pauli operations $\mathbb{Z}$ and $\mathbb{X}$, building simple processes for easy implementation under the current technology. For better elaboration, we give two examples: all voters cast ''yes'' votes and only one voter casts a ''no.'' Then, the corresponding experiment tests are conducted on the simulated IBM quantum computer to verify their feasibility. We also show that the proposed protocol has the desirable properties of privacy, fairness, verifiability and robustness. Furthermore, we analyze the proposed protocol's security against cheating from eavesdroppers, a semi-honest server and malicious voters. This work is the first attempt to illustrate how qubits can be useful for building a secure anonymous one-vote veto strategy.

INDEX TERMS Quantum anonymous voting, one-vote veto, privacy, security.

I. INTRODUCTION

Voting is a daily social activity in modern society. Often, the adoption of significant decisions and the conduct of democratic elections depend on voting systems. Initially, voting systems require voters to cast votes at designated places, followed by manual tallying of votes under supervision. One common example is ballot box voting. Each voter is assigned one blank ballot paper, and he (she) writes his (her) vote on it. Then, the voters place their filled ballot papers into pre-designated ballot boxes. Some authorized servers collect all votes and publicize the voting results. This method achieves specific functions, but some limitations affect security. For example, voters can cheat by tracing marked ballot papers without being detected. Because of time and geographical barriers, voters' difficulty engaging in real-time and face-to-face voting has led to relatively harsh conditions for voting and poor operability.

With the rapid development of information technology and the popularity of the Internet, electronic voting technology arose to meet the demands of the times and has gradually replaced primary voting. Since Chaum presented the first private electronic election in 1981 [1], various distinctive electronic voting protocols have been proposed [2]–[4]. One common characteristic of most of them is that the security is supported by the computing complexity of some difficult problems, such as discrete logarithmic problems and many factorization problems.

Based on quantum physics and computers, quantum computers with unparalleled advantages in infinite computing power and global attention have been invented. The power of quantum computers can solve difficult problems in a short time, leading most classical cryptographic protocols to face serious security threats. To meet these challenges, various quantum cryptographic protocols, such as quantum key distribution (QKD) [5]–[10], quantum secure direct communication (QSDC) [11]–[15], quantum secret sharing (QSS) [16]–[19], quantum anonymous communication (QAC) [20],

The associate editor coordinating the review of this manuscript and approving it for publication was Dominik Strzalka.

[36], quantum private query (QPQ) [21]–[23], quantum secure multiparty computation (QSMC) [24], [25] and others [26]–[28], have been proposed.

In 2007, Vaccaro *et al.* presented quantum anonymous voting based on a multiparticle entangled state [29], which inspired many researchers to explore the advantages of quantum mechanics in solving anonymous voting problems. Subsequently, based on different quantum mechanics principles, many significant quantum anonymous voting protocols have been proposed [30]–[33]. The one-vote veto is a particular and meaningful type of voting. In the voting activity of the one-vote veto, the voted content will be denied as long as there is a negative vote. The use of the one-vote veto system can effectively protect the minority's specific power from being violated and prevent ''majority tyranny''. For example, in an investment company, some investors have veto power on certain voting matters related to their interests to protect their vital profits. Internationally, the UN Security Council's permanent members own veto power, preventing conflict among countries. To date, quantum anonymous one-vote veto protocols have rarely been considered. In 2015, Rahaman and Kar propose the first quantum anonymous one-vote veto protocol (QAV) [34] with *prior* entanglement of Greenberger-Horne-Zeilinger (GHZ) state $|GHZ_n\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle^{\otimes n} + |1\rangle^{\otimes n}\right)$. At the cost of reduced privacy, such as even votes of ''yes'' or odd votes of ''no,'' the proposed protocol can perfectly achieve the voting result. However, an essential challenge in their protocol is how to distribute GHZ states among distrustful voters. As is well-known, entanglement is a valuable resource. When the number of particles n is very large, $|GHZ_n\rangle$ is quite difficult to prepare in experiments. Furthermore, entangled particles are prone to lose their coherence due to external interference. Hence, in practice, the QAV based on GHZ states can be implemented neither efficiently nor economically. This motivates us to research QAV based on qubits, which has better stability and operability.

In this paper, we explore the first QAV protocol based on qubits and Pauli operations $\mathbb{Z}$ and $\mathbb{X}$ (QAVSP in short). Our QAVSP protocol satisfies the following properties.

1. Privacy: For each of the voters, no one else can obtain any useful information about his (her) vote. The information about the partial tally of the votes in any voters' set is only computable by all remaining voters' cooperation.

2. Fairness: Each voter cannot obtain any other voters' voting information before his (her) voting to ensure that the voters' willingness is protected from other objective factors.

3. Verifiability: According to the nature of a one-vote veto, every voter who votes ''no'' can predict that the voting result is rejected or his (her) option is uncounted.

4. Robustness: If any voter refuses to follow the QAVSP protocol, then the voting result is rejected.

The remainder of the paper is organized as follows. In section 2, we present the detailed process of our QAVSP protocol. In section 3, we show two examples of three voters and perform experimental tests on the online quantum computers of IBM. In section 4, we analyze the correctness and properties of privacy, fairness, verifiability and robustness in detail. The paper concludes in section 5 with a summary and some open questions.

II. PRODUCE OF THE QAVSP PROTOCOL

In this paper, the quantum voting network is controlled and managed by a server that has sufficient capacity to prepare quantum states and tally votes. Suppose that a voting activity involves n voters $V_0, V_1, \cdots, V_{n-1}$, and each of them privately votes ''yes'' or ''no'' on one proposal. Once at least one ''no'' is received, the proposal is rejected. In practice, voting activities usually occur between partially distrusted voters or even between competitors. Here, the server is semi-honest and would like to perform any attacks constrained by quantum mechanics, except bribing by malicious voters and conspiring with any of them. There are no attack limits on voters. Under quantum mechanics, an active malicious voter can take any possible aggressive actions by himself (herself) or conspire with other evil voters. In theory, we assume that the classical and quantum channels are authenticated and the implemented environment is ideal, such as noiseless, no lost particles, and perfect equipment performance. The diagram of the entire voting process of the QAVSP protocol is given in Figure 1.

A. SHARING BINARY BIT KEY SEQUENCES

The server shares two private binary strings:

$$\begin{aligned} k_{i,1} &= \left\{k_{i,1}^1, \cdots, k_{i,1}^j, \cdots, k_{i,1}^m\right\}; \\ k_{i,2} &= \left\{k_{i,2}^1, \cdots, k_{i,2}^j, \cdots, k_{i,2}^m\right\}, \end{aligned} \tag{1}$$

where $k_{i,1}^j$, $k_{i,2}^j \in \{0, 1\}$ for $1 \le i \le n$ and $1 \le j \le m$, with each voter V_i based on some secure manners, such as QKD [5]–[8] and private face-to-face sharing technologies.

Furthermore, the server randomly generates two key strings $l_{t,1}$, $l_{t,2}$ of length m with binary bit elements $l_{t,1}^j$, $l_{t,2}^j$ for $j = 1, 2, \cdots, m$, and privately retains them.

B. PREPARING QUANTUM VOTING STATES

The server prepares one sequence $S_{t,1}$ of m qubits, $p_t^1, \cdots, p_t^j, \cdots, p_t^m$, according to the following rule.

For $l_{t,1}^j = 0$, the voting carrier is prepared on a rectilinear basis as follows:

$$p_t^j = \begin{cases} |0\rangle, & \text{if } l_{t,2}^j = 0; \\ |1\rangle, & \text{if } l_{t,2}^j = 1. \end{cases} \tag{2}$$

For $l_{t,1}^j = 1$, the voting carrier is prepared on a diagonal basis as follows:

$$p_t^j = \begin{cases} |+\rangle, & \text{if } l_{t,2}^j = 0; \\ |-\rangle, & \text{if } l_{t,2}^j = 1. \end{cases} \tag{3}$$

The server prepares δ detection particles $d_t^1, \cdots, d_t^\delta$, where δ is a security strength depending on the actual application environment. Each d_t^j $(1 \le j \le \delta)$ is randomly chosen

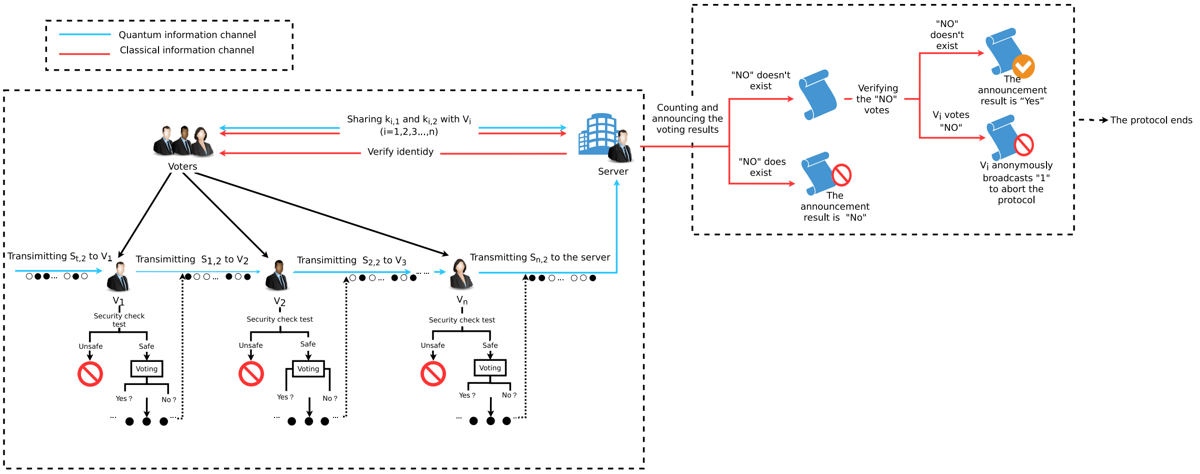

Quantum information channel
Classical information channel
Sharing $k_{i,1}$ and $k_{i,2}$ with V_i (i=1,2,3...,n)
Verify identidy
Voters
Server
Transimitting $S_{t,2}$ to V_1
Transimitting $S_{1,2}$ to V_2
Transimitting $S_{2,2}$ to V_3
Transimitting $S_{n,2}$ to the server
V_1
V_2
V_n
Security check test
Unsafe
Safe
Voting
Yes ?
No ?
Counting and announcing the voting results
"NO" doesn't exist
"NO" does exist
The announcement result is "No"
Verifying the "NO" votes
"NO" doesn't exist
The announcement result is "Yes"
V_i votes "NO"
V_i anonymously broadcasts "1" to abort the protocol
The protocol ends

FIGURE 1. The entire voting process of the QAVSP protocol.

in four states $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ with a uniform probability of $\frac{1}{4}$. Then, the server inserts each detection particle d_t^j in the sequence $S_{t,1}$ in a random position, and the new sequence is $S_{t,2}$ with a length of $m+\delta$.

C. TRANSMITTING QUANTUM VOTING STATES

The server sends the sequence $S_{t,2}$ to voter V_1 through a regular quantum authentication channel. After V_1 receives the complete sequence $S_{t,2}$, they cooperate to perform a security check test to ensure that the quantum authentication channel between the server and V_1 is secure. To do so, the server first publishes the positions and corresponding bases, rectilinear basis or diagonal basis ($\{|0\rangle\langle 0|, |1\rangle\langle 1|\}$ or $\{|+\rangle\langle +|, |-\rangle\langle -|\}$, respectively), of all detection particles. Then, V_1 measures each detection particle in the correct basis and records its classical measurement result. Next, V_1 announces all classical measurement results of δ detection particles, and the server announces their initial states. According to the open information, V_1 and the server set check whether the initial states and the measurement results are consistent. For example, if the initial state is $|+\rangle$, the corresponding classical measurement result should be 1 when measuring in basis $\{|+\rangle, |-\rangle\}$. When all δ detection particles are consistent, the test passes, and the protocol continues; otherwise, the test fails, and they (V_1 and the server) abort the protocol.

D. CASTING VOTES

If V_1 votes "yes", he (she) applies the operation $U_1^j = \mathbb{X}^{k_{1,1}^j}\mathbb{Z}^{k_{1,2}^j}$ on the jth voting carrier according to the keys $k_{1,1}^j$ and $k_{1,2}^j$ for $1 \leq j \leq m$. Here,

$$\mathbb{X} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad \mathbb{Z} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}. \tag{4}$$

$\mathbb{X}$ can turn $|0\rangle$ to $|1\rangle$ and $|1\rangle$ to $|0\rangle$, $\mathbb{Z}$ can protect $|0\rangle$ from being changed, and $|1\rangle$ turns to $-|1\rangle$. Otherwise, he (she) applies a random operation $U_1^j = \mathbb{X}^{x_{1,1}^j}\mathbb{Z}^{x_{1,2}^j}$ on the jth voting carrier p_t^j, where $x_{1,1}^j, x_{1,2}^j$ are randomly chosen in the set $\{0, 1\}$.

V_1 arbitrarily disturbs the order of voting carriers. To achieve this, V_1 randomly selects a permutation $C_1 = c_1^1 c_1^2 \cdots c_1^m$ from the set $\mathcal{P}_m$ with a uniform probability, where $\mathcal{P}_m$ is constructed by all permutations of $\mathbb{Z}_m := \{1, \cdots, m\}$ [35]. Taking C_1 as the private address index, voting carrier p_t^j temporarily moves from the jth position to the c_1^jth position. The renumbered voting carrier sequence is $S_{1,1}$. Hereafter, as the server does, V_1 prepares δ detection particles $d_1^1, \cdots, d_1^\delta$ and inserts each detection particle d_1^j into $S_{1,1}$ randomly. The newly combined sequence is $S_{1,2}$; furthermore, all the qubits are labeled as $s_{1,2}^1, s_{1,2}^2, \cdots, s_{1,2}^{m+\delta}$.

V_1 sends sequence $S_{1,2}$ to the next voter V_2 through a regular quantum authentication channel. Using all δ detection particles, V_1 and V_2 first cooperate to perform a security check test. If the test passes, V_1 announces the original order of all voting carriers, and V_2 resets the voting carriers into the original order arrangement. The following voting process for V_2 is the same as that for V_1.

Other voters, individually, take the same actions as V_1 and V_2, including performing security check tests, casting votes and transmitting particle sequences. Finally, all traveling voting carriers $p_t^1, \cdots, p_t^j, \cdots, p_t^m$ return to the server securely.

A special note that should be mentioned is that if any voter does not strictly follow the established procedure of the protocol, the voting result is "no", which means the proposal is rejected.

E. DETERMINING THE VOTING RESULT

For each voting carrier p_t^j $(1 \leq j \leq m)$, the server measures it in its original basis, rectilinear basis or diagonal basis, encoded by $l_{t,1}^j$, obtaining the classical measurement result r_j. Then, the server compares whether r_j is consistent with $U_n^j \cdots U_1^j p_t^j$. For all voting carriers $p_t^1, p_t^2, \cdots, p_t^m$, if there is any inconsistency, the server rejects the proposal. Otherwise, the proposal is accepted.

F. VERIFYING THE "NO" VOTES

Whenever the proposal passes, any voter V_i who votes "no" can use anonymous quantum communication technology [20], [36] to broadcast the abort signal "1". Once "1" appears, the protocol aborts.

III. EXAMPLE AND EXPERIMENT

Thus far, we have shown the details of the QAVSP protocol. For a better understanding, we set the number of voters n to be 3 and give two simple examples for two cases, where all voters cast "yes" votes and only one voter casts a "no" vote. Then, we perform two experimental tests of the examples on the online quantum computer, (i.e., ibmq_qasm_simulator), of the IBM Corporation placed on the cloud [37]. For simplicity, we present only the core of the encoding and decoding votes process and ignore some parts of the state distribution and security check tests.

A. EXAMPLE 1: ALL VOTERS CAST "YES" VOTES

Following the QAVSP protocol, the server shares two private binary strings $k_{1,1}$ and $k_{1,2}$ with V_1, $k_{2,1}$ and $k_{2,2}$ with V_2, and $k_{3,1}$ and $k_{3,2}$ with V_3. Assume that

$$\begin{aligned} k_{1,1} &= \{0,0,0,0,0\}\,; \quad & k_{1,2} &= \{1,0,0,0,1\}\,; \\ k_{2,1} &= \{0,0,0,1,1\}\,; \quad & k_{2,2} &= \{0,1,0,0,0\}\,; \\ k_{3,1} &= \{1,1,1,0,1\}\,; \quad & k_{3,2} &= \{1,0,1,0,0\}\,. \end{aligned} \tag{5}$$

Suppose the 5 voting carriers are

$$p_t^1, p_t^2, p_t^3, p_t^4, p_t^5 = |0\rangle, |1\rangle, |+\rangle, |-\rangle, |0\rangle. \tag{6}$$

Since all voters cast "yes" votes, according to $k_{i,1}$ and $k_{i,2}$ for $i = 1,2,3$, V_i applies $\mathbb{X}^{k_{i,1}}\mathbb{Z}^{k_{i,2}}$ on p_t. That is, V_1 applies the unitary operations $\mathbb{Z}, \mathbb{I}, \mathbb{I}, \mathbb{I}, \mathbb{Z}$ on voting carriers $p_t^1, p_t^2, p_t^3, p_t^4, p_t^5$, respectively. Successively, V_2 applies $\mathbb{I}$, $\mathbb{Z}$, $\mathbb{I}$, $\mathbb{X}$, $\mathbb{X}$ and V_3 applies $\mathbb{X}\mathbb{Z}$, $\mathbb{X}$, $\mathbb{X}\mathbb{Z}$, $\mathbb{I}$, $\mathbb{X}$ on the five voting carriers. Thus, the casting votes process can be described as follows:

$$\begin{aligned} |1\rangle &= \mathbb{X}\mathbb{Z}\cdot\mathbb{I}\cdot\mathbb{Z}|0\rangle; \\ |0\rangle &= \mathbb{X}\cdot\mathbb{Z}\cdot\mathbb{I}|1\rangle; \\ |-\rangle &= \mathbb{X}\mathbb{Z}\cdot\mathbb{I}\cdot\mathbb{I}|+\rangle; \\ |-\rangle &= \mathbb{I}\cdot\mathbb{X}\cdot\mathbb{I}|-\rangle; \\ |0\rangle &= \mathbb{X}\cdot\mathbb{X}\cdot\mathbb{Z}|0\rangle. \end{aligned} \tag{7}$$

In step 2.5, the server measures each voting carrier p_t^j $(1 \le j \le 5)$ in its original basis decided by $l_{t,1}^j$. In other words, the server measures p_t^1, p_t^2, p_t^5 on a rectilinear basis and p_t^3, p_t^4 on a diagonal basis. From the foregoing equation (7), the measurement outcomes $|1\rangle, |0\rangle, |-\rangle, |-\rangle, |0\rangle$ entirely follow the rule of all voters casting "yes" votes. Therefore, the server accepts the proposal, which is exactly what all voters expect.

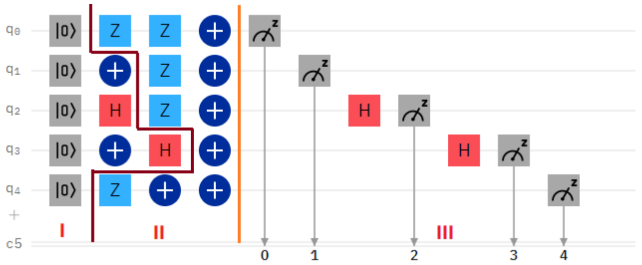


FIGURE 2. IBM quantum circuit for performing example 1.

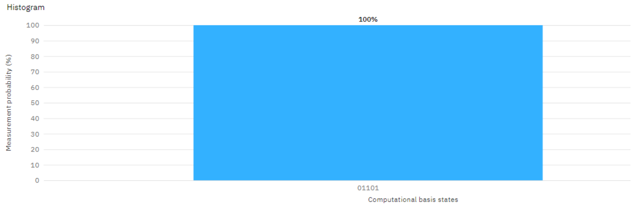


FIGURE 3. The experimental results of example 1 by ibmq_qasm_simulator.

To verify the realization of the protocol, we perform an experimental test of the above example on the online IBM quantum computer (ibmq_qasm_simulator).

In Figure 2, the five voting carriers $p_t^1, p_t^2, p_t^3, p_t^4, p_t^5$ are denoted by q_0, q_1, q_2, q_3, q_4, respectively. Part I is the stage of preparing quantum voting states. Since the initial states are all $|0\rangle$ in the IBM quantum computer, the process of preparing five voting carriers can be described as follows:

$$\begin{aligned} p_0 &: |0\rangle; \\ p_1 &: |1\rangle = \mathbb{X}|0\rangle; \\ p_2 &: |+\rangle = \mathbb{H}|0\rangle; \\ p_3 &: |-\rangle = \mathbb{H}\cdot\mathbb{X}|0\rangle, \\ p_4 &: |0\rangle; \end{aligned} \tag{8}$$

where $\mathbb{H}$ gate is in the form of

$$\mathbb{H} \equiv \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}. \tag{9}$$

$\mathbb{H}$ can turn $|0\rangle$ into $|+\rangle \equiv \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $|1\rangle$ into $|-\rangle \equiv \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$.

Part II is the vote casting stage, and the measuring states and collecting votes stages are in part III.

In Figure 3, after running 2048 shots on ibmq_qasm_simulator and measuring p_t^1, p_t^2, p_t^5 in basis $\{|0\rangle, |1\rangle\}$, p_t^3, p_t^4 in basis $\{|+\rangle, |-\rangle\}$, the classical measurement results of $p_t^1, p_t^2, p_t^3, p_t^4, p_t^5$ are 1, 0, 1, 1, 0 with a probability of 100%. Obviously, the experimental results are consistent with the theoretical results deduced in equation (7). Therefore, the proposal is accepted as all voters expect.

B. EXAMPLE 2: ONLY ONE VOTER CASTS A "NO" VOTE

We suppose $k_{i,j}$ $(1 \le i \le 3, 1 \le i \le 2)$ is the same as equation (5) and p_t^j $(1 \le j \le 5)$ is the same as equation (7).

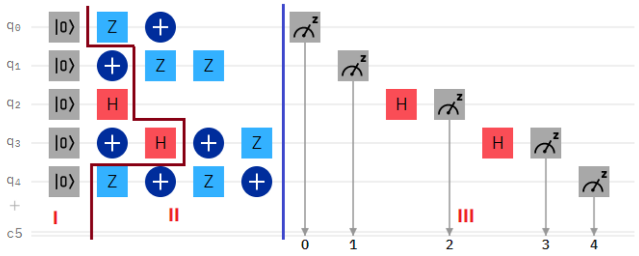


FIGURE 4. IBM quantum circuit for performing example 2.

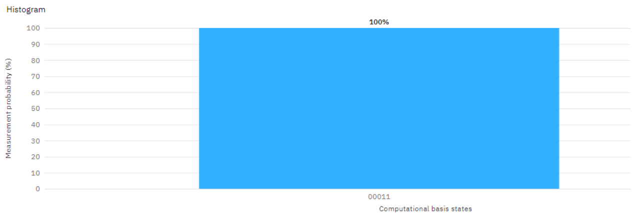


FIGURE 5. The experimental results of example 2 by ibmq_qasm_simulator.

Without any loss of generality, suppose that V_3 is the voter who casts "no". Thus, for each voting carrier p_t^j $(1 \leq j \leq 5)$, V_3 randomly applies one unitary operation in $\{\mathbb{I}, \mathbb{X}, \mathbb{Z}, \mathbb{XZ}\}$ on each p_t^j. Suppose that V_3 chooses $\mathbb{X}, \mathbb{Z}, \mathbb{I}, \mathbb{Z}, \mathbb{XZ}$ for $p_t^1, p_t^2, p_t^3, p_t^4, p_t^5$, respectively. As usual, controlled by $k_{1,1}$, $k_{1,2}$ and $k_{2,1}$, $k_{2,2}$, V_1 applies $\mathbb{Z}, \mathbb{I}, \mathbb{I}, \mathbb{I}, \mathbb{Z}$ and V_2 applies $\mathbb{I}, \mathbb{Z}, \mathbb{I}, \mathbb{X}, \mathbb{X}$ on the five voting carriers in turn. The voting process can be given as follows:

$$\begin{aligned}
|1\rangle &= \mathbb{X} \cdot \mathbb{I} \cdot \mathbb{Z}|0\rangle; \\
|1\rangle &= \mathbb{Z} \cdot \mathbb{Z} \cdot \mathbb{I}|1\rangle; \\
|+\rangle &= \mathbb{I} \cdot \mathbb{I} \cdot \mathbb{I}|+\rangle; \\
|+\rangle &= \mathbb{Z} \cdot \mathbb{X} \cdot \mathbb{I}|-\rangle; \\
|0\rangle &= \mathbb{XZ} \cdot \mathbb{X} \cdot \mathbb{Z}|0\rangle. \qquad (10)
\end{aligned}$$

As above, in Figure 4, part I is the stage of preparing quantum voting states. Part II describes how each voter is voting. The voting results are opened in part III.

In Figure 5, after running 2048 shots on ibmq_qasm_simulator and measuring p_t^1, p_t^2, p_t^5 in basis $\{|0\rangle, |1\rangle\}$, p_t^3, p_t^4 in basis $\{|+\rangle, |-\rangle\}$, the classical measurement results of $p_t^1, p_t^2, p_t^3, p_t^4, p_t^5$ are 1, 1, 0, 0, 0 with a probability of 100%. Obviously, the experimental results are different from the theoretical results 1, 0, 1, 1, 0. These results indicate that there is at least one voter who is voting "no". The server rejects the proposal while protecting the privacy of each voter. V_3 can anonymously verify that the voting result is the same as his (her) wish, which means his (her) vote "no" is correctly counted.

IV. ANALYSIS

First, we analyze the correctness of our protocol. The voting result is successfully obtained, with a small probability of failure approaching 0 as m increases. Then, we analyze the desirable properties of reliability, privacy, fairness and verifiability.

A. CORRECTNESS

Theorem 1: If the voters all agree to the proposal, then the protocol achieves the perfect result with a probability of 1. If there exists at least one voter who disagrees with the proposal, then the probability of success of the protocol is at least $1 - \frac{1}{2^m}$.

Proof: If all the voters vote "yes", they honestly implement the protocol as planned, and the final state obtained by the server is in $U_n^j \cdots U_2^j U_1^j p_t^j$ for $j = 1, 2, \cdots, m$ without any deviation. Obviously, the proposal passes with a probability of 1.

If at least one voter rejects the proposal, then the voting result should be "no". Without any loss of generality, we assume that V_j is one of the voters voting "no". For each voting carrier, V_j applies an operation that is random in $\{\mathbb{I}, \mathbb{X}, \mathbb{Z}, \mathbb{XZ}\}$ with a uniform probability of $\frac{1}{4}$, leading to the final voting carrier obtained by the server being a state in the set of $\{|0\rangle, |1\rangle\}$ or $\{|+\rangle, |-\rangle\}$ with probability $\frac{1}{2}$. When the server measures the voting state in its original basis, the disturbance of each voting carrier escapes detection successfully with a probability of $\frac{1}{2}$. For m voting carriers, the error rate of passing the proposal is $\frac{1}{2^m}$. Hence, the probability of rejecting the proposal is $1 - \frac{1}{2^m}$, which approaches 1 as m increases to a sufficiently large number.

What needs to be pointed out is that the above correctness is considered under the ideal situation. Apparently, when some attackers exist in the transmission process, they might disturb voting carriers, leading to an incorrect voting result without being detected.

In our protocol, the voting carriers and detection particles are thoroughly mixed and transmitted in the form of quantum blocks. For any outside attacker, each transmitted particle is randomly encoded in two mutually unbiased orthogonal bases. Through theoretical guessing, each $s_{i,2}^j$ for $i = t$, $1 \leq i \leq n$, $1 \leq j \leq m + \delta$ is in the rectilinear basis $\{|0\rangle, |1\rangle\}$ or diagonal basis $\{|+\rangle, |-\rangle\}$ with a uniform probability of $\frac{1}{2}$; thus, the density matrix of each transmitted particle $s_{i,2}^j$ for any outside attackers is always

$$\begin{aligned}
\rho_{s_{i,2}^j} &= \frac{1}{4}\left(|0\rangle\langle 0| + |1\rangle\langle 1| + |+\rangle\langle +| + |-\rangle\langle -|\right) \\
&= \frac{1}{2}\mathbb{I}. \qquad (11)
\end{aligned}$$

Since all transmitted particles are in the maximally mixed states, the attackers cannot distinguish the detection particles from the voting carriers. Actually, the security of every quantum authenticated channel between two participants is ensured by a security check test, which is similar to that of the BB84 protocol [5]. Directly referring to the security proof of the BB84 protocol, we know that regardless of the type of attack an attacker utilizes, his (her) active action will inevitably disturb some of the detection states and be detected by honest participants, thus failing the protocol. Hence, it is impossible for attackers to affect the voting results.

B. RELIABILITY

Theorem 2: In the ideal model, if all quantum authentication channels are secure, no legal voter can abort the voting process.

Proof: Under the ideal environment hypothesis, the process of security check tests can ensure that all quantum states traveling among all participants are secure. If any voter V_i $(1 \leq i \leq n)$ refuses to implement the protocol as it is planned, such as terminating the transmission of the quantum states, the voting result is rejected.

C. PRIVACY

Theorem 3: For each voter, the value of his (her) vote is kept secret from all others. After the voting protocol, the output is only agreement or rejection. No useful information regarding how many voters vote "no" is leaked whenever the voting result is rejection.

Proof: In our protocol, the adversaries might be outside eavesdroppers and malicious participants, i.e., malicious voters and semi-honest servers. The next part will focus on how to achieve privacy and defend against potential adversaries.

As we mentioned above, each transmitted particle is in the maximally mixed state for an outside eavesdropper, and she is unable to acquire any useful information for breaking privacy without being detected by the server or honest voters. Hereafter, we mainly discuss participant attacks. Generally, participant attacks are a much more powerful threat in multiparty quantum protocols [38], [39]. In participant attacks, the participants have an unparalleled advantage in reasonably obtaining valuable resources, such as intermediate data $k_{i,1}$, $k_{i,2}$, voting carriers p_t^j and detection particles d_i^j. Here, we analyze two possible cases of participant attacks in detail as follows.

Case 1 (Attacks by a Semi-Honest Server):

During transmission, the voting carriers and detection particles are intensively mixed. Even with two private binary strings $k_{i,1}$ and $k_{i,2}$, the server still cannot separate voting carriers from detection particles. Actually, if he (she) makes some active attacks on the transmitted particles, he (she) will be detected by honest voters as an outside eavesdropper in testing detection particles. In addition, the number of traveling voting carriers is disrupted, and it is impossible for the server to obtain the original order when the security check test fails. Hence, compared with outside eavesdroppers, the server has no advantages in breaking privacy.

Case 2 (Attacks by Malicious Voters):

Taking V_i as an example, suppose that V_{i+1} wants to attack V_i by eavesdropping on the transmitted voting carriers $p_t^1, \cdots, p_t^j, \cdots, p_t^m$. Following the protocol process, V_{i+1} does not know the exact state of $p_t^1, \cdots, p_t^j, \cdots, p_t^m$ received by V_i. To ensure how V_i is voting, V_{i+1} should determine the Pauli operations applied by V_i. Without any loss of generality, assume that the compound systems of all transmitted voting carriers $p_t^1, \cdots, p_t^j, \cdots, p_t^m$ are in state ρ^A when V_i just receives them from V_{i-1}.

This occurs because the set of 2^{2m} unitary matrices $\mathbb{X}^{a_1}\mathbb{Z}^{b_2}$ $\{a_1, b_2 \in \{0,1\}^m\}$ forms an orthogonal basis. Expanding any message state, ρ^A in $\mathbb{X}^{a_1}\mathbb{Z}^{b_2}$ base is given [40]:

$$\rho^A = \sum_{a_1,b_1} l_{a_1,b_1}\mathbb{X}^{a_1}\mathbb{Z}^{b_1}, \tag{12}$$

where $l_{a_1,b_1} = \frac{tr(\rho^A\mathbb{Z}^{b_1}\mathbb{X}^{a_1})}{2^m}$.

If V_i is voting "yes", V_i applies the operation $U_i = \mathbb{X}^{k_{i,1}}\mathbb{Z}^{k_{i,2}}$ on the state ρ^A and the state turns to $\rho^{A'}$. Using this formalism, we can easily determine $\rho^{A'}$. However, for V_{i+1}, he (she) does not know the exact unitary operation that is applied by V_i. That is, U_i is a random element in the set of $\mathbb{X}^{k_{i,1}}\mathbb{Z}^{k_{i,2}}$ $\left\{k_{i,1}, k_{i,2} \in \{0,1\}^m\right\}$ with the same probability of $\frac{1}{4^m}$ for V_{i+1}. The above evolution can be described as follows:

$$\begin{aligned}
\rho^{A'} &= \sum_j P_{U_i}(U_i \otimes \mathbb{I})\rho^A(U_i \otimes \mathbb{I})^\dagger \\
&= \frac{1}{2^{2m}} \sum_{k_{i,1},k_{i,2}} (\mathbb{X}^{k_{i,1}}\mathbb{Z}^{k_{i,2}} \otimes \mathbb{I})\rho^A(\mathbb{X}^{k_{i,1}}\mathbb{Z}^{k_{i,2}} \otimes \mathbb{I})^\dagger \\
&= \frac{1}{4^m} \sum_{k_{i,1},k_{i,2}} (\mathbb{X}^{k_{i,1}}\mathbb{Z}^{k_{i,2}} \otimes \mathbb{I})(\sum_{a_1,b_1} l_{a_1,b_1}\mathbb{X}^{a_1}\mathbb{Z}^{b_1}) \\
&\quad (\mathbb{X}^{k_{i,1}}\mathbb{Z}^{k_{i,2}} \otimes \mathbb{I})^\dagger \\
&= \frac{1}{4^m} \sum_{k_{i,1},k_{i,2}} l_{a_1,b_1} \sum_{a_1,b_1} (\mathbb{X}^{k_{i,1}}\mathbb{Z}^{k_{i,2}} \otimes \mathbb{I})\mathbb{X}^{a_1}\mathbb{Z}^{b_1} \\
&\quad (\mathbb{X}^{k_{i,1}}\mathbb{Z}^{k_{i,2}} \otimes \mathbb{I})^\dagger \\
&= \frac{1}{4^m} \sum_{k_{i,1},k_{i,2}} l_{a_1,b_1} \sum_{a_1,b_1} \mathbb{X}^{k_{i,1}}\mathbb{Z}^{k_{i,2}}\mathbb{X}^{a_1}\mathbb{Z}^{b_1}\mathbb{X}^{k_{i,1}}\mathbb{Z}^{k_{i,2}} \\
&= \frac{1}{4^m} \sum_{k_{i,1},k_{i,2}} l_{a_1,b_1} \sum_{a_1,b_1} (-1)^{a_1 \cdot k_{i,2} \oplus b_1 \cdot k_{i,1}}\mathbb{X}^{a_1}\mathbb{Z}^{b_1} \\
&= \frac{1}{4^m} \sum_{k_{i,1},k_{i,2}} l_{a_1,b_1} \sum_{a_1,b_1} \delta_{a_1,0}\delta_{b_1,0}\mathbb{X}^{a_1}\mathbb{Z}^{b_1} \\
&= \frac{1}{2^m} \cdot \mathbb{I}.
\end{aligned} \tag{13}$$

If V_i is voting "no", V_i randomly applies an operation in the set of $\mathbb{I}, \mathbb{X}, \mathbb{Z}, \mathbb{XZ}$ on each traveling voting carrier p_t^j $(1 \leq j \leq m)$. Similar to the above analysis, for V_{i+1}, the evolutionary process is as follows:

$$\begin{aligned}
\rho^{A'} &= \sum_j P_{U_i'}(U_i' \otimes \mathbb{I})\rho^A(U_i' \otimes \mathbb{I})^\dagger \\
&= \frac{1}{2^m} \cdot \mathbb{I}.
\end{aligned} \tag{14}$$

Regardless of what V_i votes, each voting carrier is always in the maximum mixed state. Thus, V_{i+1} cannot determine how V_i is voting. Therefore, the privacy is maintained.

As described above, strictly following the protocol, it is impossible for V_{i+1} to break the privacy of the vote of V_i. If V_{i+1} wants to eavesdrop some useful information, he (she) must take some active actions under quantum mechanics. V_{i+1} has the right to possess $\rho^{A'}$, and he (she) needs to attack ρ^A. Since the transmission process of ρ^A is similar to the BB84 protocol's process, any effective attack will inevitably disturb the detection particles and be discovered by V_{i-1} and V_i in the security check test among them. Therefore, the most predictably successful attack is that V_{i-1} and V_{i+1} are malicious and conspire together. By lying to V_i, V_{i-1} and V_{i+1} can easily escape the security check tests of V_{i-1} and V_i and of V_i and V_{i+1}. In such circumstances, V_{i-1} and V_{i+1} can easily determine the operation U_i applied by V_i. For example, V_{i-1} prepares fake voting carriers $f_t^1, \cdots, f_t^j, \cdots, f_t^m$ and sends them to V_i instead of $p_t^1, \cdots, p_t^j, \cdots, p_t^m$. Then, V_i performs the unitary operation U_i on the fake voting carriers to complete his (her) vote casting process. When V_{i+1} receives the fake voting carriers from V_i, V_{i-1} collaborates with V_{i+1} to measure each voting carrier in his (her) initial basis and compare it to the initial state, thus easily obtaining U_i. Since $k_{i,1}$ and $k_{i,2}$ are private binary strings shared between the server and V_i, V_{i-1} and V_{i+1} have no idea about them. Benefiting from one-time pad encryption technology [40], without $k_{i,1}$ and $k_{i,2}$, V_{i-1} and V_{i+1} still cannot determine how V_i is voting just with U_i. Privacy is still maintained even if V_{i-1} conspires with some other malicious voters. Therefore, each voter can maintain the privacy of his (her) vote.

D. FAIRNESS

Theorem 4: In our protocol, no individual can obtain a partial votes tally or any useful information about someone else's vote before he (she) is voting. He (she) decides to vote entirely on his (her) initial wishes.

Proof: As we all know, if a voter determines some useful information about some other votes beforehand, he (she) might change his (her) vote. In our protocol, the voters encrypt their votes twice. First, each voter V_i $(0 \leq i \leq n-1)$ encrypts his (her) vote using the classical one time pad technique with secret keys $k_{i,1}$ and $k_{i,2}$. In addition to the server and V_i, no individual can decode the vote from ciphertext. However, the server cannot cooperate with any voter. Second, V_i encodes the ciphertext by performing the unitary operations $\{\mathbb{I}, \mathbb{X}, \mathbb{Z}, \mathbb{XZ}\}^m$ on the voting carriers $p_t^1, \cdots, p_t^j, \cdots, p_t^m$. Since the density matrix of each voting carrier is in a maximum mixed state and invariant under the encoding operations in the entire procedure of the protocol, no useful information about the vote of V_i is leaked. Therefore, no voter can determine how the other voters are voting, and each voter casts a vote based on his (her) initial wishes. The fairness of our protocol can be maintained.

E. VERIFIABILITY

Theorem 5: Any voter in our protocol who votes "no" can verify whether his (her) vote has been correctly counted.

Proof: Directly from the analysis of the correctness, our protocol almost achieves correctness if it completes the implementation as it is planned. Whenever there is an error, any voter who rejects the proposal but finds an inconsistency in the voting results can anonymously declare that his (her) vote has not been counted correctly and abort the protocol in step 2.6.

Actually, the verifiability of each voter will be eclipsed when all voters agree to the proposal and the proposal is rejected. To resist this potential threat, another authority center can be introduced to monitor the behavior of the server in step 2.6.

V. CONCLUSION

We investigate how qubits can be useful for anonymous one-vote veto activity with strong privacy at the expense of the protocol's error rate with respect to m. Any malicious voter cannot arbitrarily abort the protocol, thus achieving reliability. During the entire voting process, each voter votes completely according to his (her) wish without affecting other voters' votes; therefore, the protocol has the property of fairness. Verifiability provides an approach in which any voter who votes "no" can check whether the voting result is consistent with his (her) vote. With the explosive progress of quantum technology, classical one-vote veto protocols are facing serious threats. Our QAVSP protocol is a significant attempt under the current technology. There is one interesting and valuable open question that deserves further investigation in the future. Our QAVSP protocol is just preliminary theoretical research. Future research can assess how to handle the effects of device noise, which is very common in NISQ [41]; and realize the process in a real-world situation.

REFERENCES

[1] D. L. Chaum, "Untraceable electronic mail, return addresses, and digital pseudonyms," *Commun. ACM*, vol. 24, no. 2, pp. 84–90, 1981.

[2] B. Adida, "Helios: Web-based open-audit voting," in *Proc. USENIX Secur. Symp.*, vol. 17, Jan. 2008, pp. 335–348.

[3] P. Ryan, D. Bismark, J. Heather, S. Schneider, and Z. Xia, "Prêt à voter: A voter-verifiable voting system," *IEEE Trans. Inf. Forensics Security*, vol. 4, no. 4, pp. 662–673, Dec. 2009.

[4] M. Kumar, S. Chand, and C. P. Katti, "A secure end-to-end verifiable internet-voting system using identity-based blind signature," *IEEE Syst. J.*, vol. 14, no. 2, pp. 2032–2041, Jun. 2020.

[5] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in *Proc. Int. Conf. Comput., Syst. Signal Process.*, Banglore, India, Dec. 1984, pp. 175–179.

[6] H.-K. Lo and H. F. Chau, "Unconditional security of quantum key distribution over arbitrarily long distances," *Science*, vol. 283, no. 5410, pp. 2050–2056, Mar. 1999.

[7] P. W. Shor and J. Preskill, "Simple proof of security of the BB84 quantum key distribution protocol," *Phys. Rev. Lett.*, vol. 85, no. 2, pp. 441–444, 2000.

[8] G. Z. Tang, C. Y. Li, and M. Wang, "Polarization discriminated time-bin phase-encoding measurement-device-independent quantum key distribution," *Quantum Eng.*, vol. 3, p. e79, Aug. 2021.

[9] L.-C. Kwek, L. Cao, W. Luo, Y. Wang, S. Sun, X. Wang, and A. Q. Liu, "Chip-based quantum key distribution," *AAPPS Bull.*, vol. 31, no. 1, p. 15, Jun. 2021.

[10] Z. W. Sun, C. H. Wu, S. G. Zheng, and C. Zhang, "Efficient multiparty quantum key agreement with a single d-level quantum system secure against collusive attack," *IEEE Access*, vol. 7, pp. 102377–102385, 2019.

[11] G. L. Long and X. S. Liu, "Theoretically efficient high-capacity quantum-key-distribution scheme," *Phys. Rev. A, Gen. Phys.*, vol. 65, no. 3, Feb. 2002, Art. no. 032302.

[12] R. Qi, Z. Sun, Z. Lin, P. Niu, W. Hao, L. Song, Q. Huang, J. Gao, L. Yin, and G.-L. Long, "Implementation and security analysis of practical quantum secure direct communication," *Light: Sci. Appl.*, vol. 8, no. 1, p. 22, Dec. 2019.

[13] C. Wang, "Quantum secure direct communication: Intersection of communication and cryptography," *Fundam. Res.*, vol. 1, no. 1, pp. 91–92, Jan. 2021.

[14] G.-L. Long, "Quantum secure direct communication: Principles, current status, perspectives," in *Proc. IEEE 85th Veh. Technol. Conf. (VTC Spring)*, Sydney, NSW, Australia, Jun. 2017, pp. 1–5.

[15] Z. Qi, Y. Li, Y. Huang, J. Feng, Y. Zheng, and X. Chen, "A 15-user quantum secure direct communication network," *Light: Sci. Appl.*, vol. 10, no. 1, p. 183, Dec. 2021.

[16] M. Hillery, V. Bužek, and A. Berthiaume, "Quantum secret sharing," *Phys. Rev. A, Gen. Phys.*, vol. 59, no. 3, pp. 1829–1834, Mar. 1999.

[17] Y.-G. Yang, Q.-Y. Wen, and X. Zhang, "Multiparty simultaneous quantum identity authentication with secret sharing," *Sci. China G: Phys., Mech. Astron.*, vol. 51, no. 3, pp. 321–327, 2008.

[18] H.-Y. Jia, Q.-Y. Wen, F. Gao, S.-J. Qin, and F.-Z. Guo, "Dynamic quantum secret sharing," *Phys. Lett. A*, vol. 376, nos. 10–11, pp. 1035–1041, Feb. 2012.

[19] C. Hao and M. Wenping, "(t, n) threshold quantum state sharing scheme based on linear equations and unitary operation," *IEEE Photon. J.*, vol. 9, no. 1, pp. 1–7, Feb. 2017.

[20] N. C. Menicucci, B. Q. Baragiola, T. F. Demarie, and G. K. Brennen, "Anonymous broadcasting of classical information with a continuous-variable topological quantum code," *Phys. Rev. A, Gen. Phys.*, vol. 97, no. 3, Mar. 2018, Art. no. 030345.

[21] F. Gao, S. Qin, W. Huang, and Q. Wen, "Quantum private query: A new kind of practical quantum cryptographic protocol," *Sci. China Phys., Mech. Astron.*, vol. 62, no. 7, Jan. 2019, Art. no. 070301.

[22] C.-Y. Wei, X.-Q. Cai, B. Liu, T.-Y. Wang, and F. Gao, "A generic construction of quantum-oblivious-key-transfer-based private query with ideal database security and zero failure," *IEEE Trans. Comput.*, vol. 67, no. 1, pp. 2–8, Jan. 2018.

[23] B. Liu, Z.-F. Gao, D. Xiao, W. Huang, Z.-Q. Zhang, Y. Li, and B.-J. Xu, "QKD-based quantum private query protocol in the single-photon interference communication system," *IEEE Access*, vol. 7, pp. 104749–104758, 2019.

[24] R.-H. Shi, Y. Mu, H. Zhong, J. Cui, and S. Zhang, "Secure multiparty quantum computation for summation and multiplication," *Sci. Rep.*, vol. 6, no. 1, p. 19655, Jan. 2016.

[25] Q. L. Wang, H. X. Sun, and W. Huang, "Multi-party quantum private comparison protocol with n-level entangled states," *Quantum Inf. Process.*, vol. 13, no. 11, pp. 2375–2389, 2014.

[26] S. Lin, G.-D. Guo, F. Huang, and X.-F. Liu, "Quantum anonymous ranking based on the Chinese remainder theorem," *Phys. Rev. A, Gen. Phys.*, vol. 93, no. 1, Jan. 2016, Art. no. 012318.

[27] F. Xu, M. Curty, B. Qi, and H. K. Lo, "Measurement-device-independent quantum cryptography," *IEEE J. Sel. Topics Quantum Electron.*, vol. 21, no. 3, pp. 148–158, May 2015.

[28] G.-B. Xu and D.-H. Jiang, "Novel methods to construct nonlocal sets of orthogonal product states in an arbitrary bipartite high-dimensional system," *Quantum Inf. Process.*, vol. 20, no. 4, p. 128, Apr. 2021.

[29] J. A. Vaccaro, J. Spring, and A. Chefles, "Quantum protocols for anonymous voting and surveying," *Phys. Rev. A, Gen. Phys.*, vol. 75, no. 1, pp. 10064–10070, Jan. 2007.

[30] M. Hillery, M. Ziman, V. Bužek, and M. Bieliková, "Towards quantum-based privacy and voting," *Phys. Lett. A*, vol. 349, nos. 1–4, pp. 75–81, Jan. 2006.

[31] M. Bonanome, V. Bužek, M. Hillery, and M. Ziman, "Toward protocols for quantum-ensured privacy and secure voting," *Phys. Rev. A, Gen. Phys.*, vol. 84, no. 2, pp. 290–296, Aug. 2011.

[32] L. Jiang, G. He, D. Nie, J. Xiong, and G. Zeng, "Quantum anonymous voting for continuous variables," *Phys. Rev. A, Gen. Phys.*, vol. 85, no. 4, pp. 9335–9340, Apr. 2012.

[33] Q. Wang, C. Yu, F. Gao, H. Qi, and Q. Wen, "Self-tallying quantum anonymous voting," *Phys. Rev. A, Gen. Phys.*, vol. 94, no. 2, Aug. 2016, Art. no. 022333.

[34] R. Rahaman and G. Kar, "GHZ correlation provides secure anonymous veto protocol," 2015, *arXiv:1507.00592*.

[35] Q. L. Wang, C. H. Yu, Y. C. Li, J. S. Liu, R. H. Shi, and Y. Q. Zhou, "Authenticated quantum sortition and application in 'picking at random' problems," *IEEE Commun. Lett.*, vol. 25, no. 2, pp. 518–522, Feb. 2021.

[36] M. Christandl and S. Wehner, "Quantum anonymous transmissions," in *Advances in Cryptology–(ASIACRYPT)*. Chennai, India: Springer, Dec. 2005, pp. 217–235.

[37] *The IBM Quantum Computers*. [Online]. Available: https://quantum-computing.ibm.com

[38] F. Gao, S. J. Qin, Q. Y. Wen, and F. C. Zhu, "A simple participant attack on the brádler-dušek protocol," *Quantum Inf. Comput.*, vol. 7, no. 4, pp. 329–334, May 2007.

[39] 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, Gen. Phys.*, vol. 76, no. 3, Sep. 2007, Art. no. 036301.

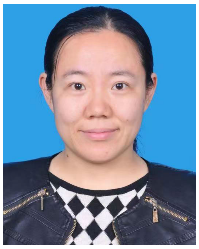
[40] P. O. Boykin and V. Roychowdhury, "Optimal encryption of quantum bits," *Phys. Rev. A, Gen. Phys.*, vol. 67, no. 4, Apr. 2003, Art. no. 042317.

[41] J. Preskill, "Quantum computing in the NISQ era and beyond," *Quantum*, vol. 2, p. 79, Aug. 2018.

SONGYANG WU received the Ph.D. degree in computer science and technology from Tongji University, in 2011. He is currently a Research Fellow with The Third Research Institute of Ministry of Public Security (TRIPMS). He has published about 20 papers in international journals and conferences, and received 18 invention patents in China. His research interests include cyberspace security, cryptography, and digital forensics investigation.

WENQI SUN received the Ph.D. degree in computer science and technology from Tsinghua University, in 2016. She is currently an Associate Research Fellow with The Third Research Institute of Ministry of Public Security (TRIPMS). She has published more than ten papers in international journals and conferences. Her research interests include AI security and digital forensics investigation.

QINGLE WANG received the Ph.D. degree in cryptography from the Beijing University of Posts and Telecommunications, in 2017. From 2015 to 2017, she was a Visiting Scholar with Quantum Sciences and Technologies Group, Department of Physics and Astronomy, Louisiana State University. She is currently a Lecturer with North China Electric Power University. She has published more than 20 articles in international journals. Her research interests include quantum cryptography and quantum information.



RONGHUA CHE received the master's degree in engineering from the School of Control and Computer Engineering, North China Electric Power University, in 2017. She is currently a Lecturer with Liaocheng University. In 2015, she presided over a municipal project, which was successfully concluded in 2017. Her research interests include computer and security.

MENG HU is currently pursuing the B.S. degree with North China Electric Power University. His research interests include quantum cryptography and quantum information.

ZHIGUO DING received the Ph.D. degree in electronic science and technology from the University of Science and Technology of China (USTC), in 2020. He is currently an Associate Research Fellow with The Third Research Institute of Ministry of Public Security (TRIPMS). He has published more than three papers in international journals and conferences, and received two invention patents in China. His research interests include cyberspace security and large-scale data acquisition.

XUE XUE received the B.S. degree in software engineering from Shijiangzhuang University, in 2019. She is currently pursuing the M.S. degree with North China Electric Power University. She has published one articles in Chinese Core Journals. Her research interests include quantum protocol, zero trust networks, and access control.