Quantum Voting Scheme Based on Conjugate Coding

Tatsuaki Okamoto†*, Koutarou Suzuki, and Yuuki Tokunaga*

Abstract

We describe a quantum voting scheme in which a ballot is an unknown quantum state for a voter. Such a ballot is hard to forge because it is difficult in principle to make a copy of an unknown quantum state. Moreover, our quantum voting scheme guarantees anonymity because the ballot can be randomized by voters. We also describe a distributed variant of our scheme that is robust against a dishonest administrator. This scheme should remain usable in the coming era of quantum computers, which are expected to break most existing cryptographic schemes.

1. Introduction

There are several types of voting systems. Open ballot voting is a system in which voters write their own names on their ballots for self-identification and to prevent double voting. In such a voting system, the privacy of the voters is not guaranteed. If voter privacy is desired, an anonymous voting system is better than open ballot voting. To achieve fair anonymous voting, the voting scheme should satisfy the following requirements.

1. Correctness: A valid vote by an authorized voter should be counted correctly and an invalid vote should not be counted. This is known as the *one-voter one-vote* principle.

2. Anonymity: Voters should be able to vote anonymously.

3. Receipt-freeness: Voters should not be able to prove how they voted to prevent a buyer or coercer from corrupting voters.

Unlike in open ballot voting, in anonymous voting we need to achieve correctness while keeping anonymity. Since this is a challenging issue for cryptography, there has been a lot of research on cryptographic anonymous voting schemes. However, almost all existing practical electronic voting schemes that satisfy these requirements are based on the computational complexity assumption of discrete logarithm or integer factoring, which will be broken by quantum algorithms. Therefore, when a quantum computer is made in the future, we will lose almost all our practical electronic voting schemes.

On the other hand, quantum information technology (QIT), which includes quantum communications and quantum computation, should be suitable for constructing a voting scheme because it is difficult to make a copy of an unknown quantum state in quantum physics. That is, if an unknown quantum state is used for a ballot, it is hard to forge, which is very suitable for a voting scheme.

In this paper, we describe the new concept of *quantum voting*. The anonymity of the protocol is guaranteed unconditionally because the ballots can be randomized by voters. Correctness, i.e., the one-voter one-vote principle, is guaranteed by a quantum complexity assumption called *one-more unforgeability*, which means that it is impossible to forge an additional valid ballot.

We also present a cut-and-choose protocol and a distributed protocol for preventing the administrator from dishonestly executing procedures. In a distributed version of our scheme, no central entity (center)

† NTT Information Sharing Platform Laboratories
Musashino-shi, 180-8585 Japan
Email: okamoto.tatsuaki@lab.ntt.co.jp

knows enough of the whole secret to issue blank ballots, which is better in terms of keeping secrecy.

1.1 Related work

Quantum voting: There have been a few proposals of quantum voting schemes [1], [2] for specialized situations. The key technique of these voting schemes is distributing quantum entanglement for obtaining anonymity. Unlike those schemes, ours does not use quantum entanglement, so it should be easier to achieve and be more flexible for various circumstances.

Electronic voting: There have been many proposals of classical electronic voting schemes. They can be classified into three approaches: (1) blind-signature-based schemes [3]–[5], (2) mix-net-based schemes [6]–[10], and (3) homomorphic-encryption-based schemes [11]–[14]. Some of these achieve receipt-freeness [12] under the assumption of a one-way untappable channel [5], [8], [15] or two-way untappable channel [12], [16], [17].

2. Our quantum voting scheme

Let $\mathcal{H}$ be a 2-dimensional Hilbert space, i.e., the space of a 1-qubit state and let $\mathcal{H}^{\otimes k}$ be the k-times tensor product of $\mathcal{H}$, i.e., the space of the k-qubit state. We define 1-qubit state $|\psi_{a,\,b}\rangle \in \mathcal{H}$ as

$$\begin{aligned} |\psi_{0,\,0}\rangle &= |0\rangle, \\ |\psi_{1,\,0}\rangle &= |1\rangle, \\ |\psi_{0,\,1}\rangle &= \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \\ |\psi_{1,\,1}\rangle &= \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle). \end{aligned} \tag{1}$$

The value of b determines the basis: if b is 0, then a is encoded in basis Z; if b is 1, then a is encoded in basis X. This encoding is the same as BB84 quantum cryptography [18] or conjugate coding [19]. Similarly, the qubit measurement is performed in basis Z or X if the measurement basis b is specified to be 0 or 1, respectively.

For basis $K = (b_1, ..., b_{n+1}) \in \{0, 1\}^{n+1}$ and $r = (a_1, ..., a_{n+1}) \in \{0, 1\}^{n+1}$, we denote

$$|\phi_{r,\,K}\rangle = |\psi_{a_1,\,b_1}\rangle \otimes \cdots \otimes |\psi_{a_{n+1},\,b_{n+1}}\rangle \in \mathcal{H}^{\otimes(n+1)}. \tag{2}$$

We call state $|\phi_{r,\,K}\rangle$ a *blank piece* with respect to basis K if $a_{n+1} = a_1 \oplus \cdots \oplus a_n$. A blank piece is a fraction of a blank ballot, as described later.

For the measurement of an $(n+1)$-qubit state $\rho \in \mathcal{H}^{\otimes(n+1)}$ in basis $K = (b_1, ..., b_{n+1}) \in \{0, 1\}^{n+1}$, we say that the measurement result is *valid* if the result $\tilde{a}_1, ..., \tilde{a}_{n+1}$ satisfies $\tilde{a}_{n+1} = \tilde{a}_1 \oplus \cdots \oplus \tilde{a}_n$. Note that if we measure blank piece $|\phi_{r,\,K}\rangle$ in basis K, the measurement result is always valid.

2.1 One-more unforgeability

Now, we define the one-more-unforgeability assumption, on which our quantum voting scheme is constructed. We consider the following game involving adversary F that models an adversarial voter who tries to forge blank pieces, i.e., tries to create a total of $(w + 1)$ blank pieces when given w blank pieces.

Let adversary F be a polynomial-time quantum Turing machine and n be a security parameter. At the beginning of the game, basis $K = (b_1, ..., b_{n+1}) \in \{0, 1\}^{n+1}$ is selected uniformly. Adversary F is given w (which is polynomial in n) blank pieces $|\phi_{r_j,\,K}\rangle \in \mathcal{H}^{\otimes(n+1)}$ $(j = 1, ..., w)$ with respect to basis K. Here, $r_j = (a_{j,\,1}, ..., a_{j,\,n+1}) \in \{0, 1\}^{n+1}$, $a_{j,\,1}, ..., a_{j,\,n}$ are selected uniformly, and $a_{j,\,n+1} = a_{j,\,1} \oplus \cdots \oplus a_{j,\,n}$ $(j = 1, ..., w)$. Note that F is not given K and r_j. Finally, adversary F outputs a $(w+1)(n+1)$-qubit state $\rho \in \mathcal{H}^{\otimes(w+1)(n+1)}$.

We define the advantage $\mathrm{Adv}(F)$ of adversary F as

$$\begin{aligned} \mathrm{Adv}(F) = \Big|\Pr[\rho \leftarrow F(|\phi_{r_1,\,K}\rangle, ..., |\phi_{r_w,\,K}\rangle) : (\tilde{a}_{j,\,1}, \\ ..., \tilde{a}_{j,\,n+1}) \text{ is valid for all } j = 1, ..., w{+}1] - \frac{1}{2}\Big|, \end{aligned} \tag{3}$$

where $(\tilde{a}_{j,\,1}, ..., \tilde{a}_{j,\,n+1})$ are the measurement results of the j-th $(n+1)$ qubits of ρ in basis K and the probability is taken over the choice of K, the choice of r_j $(j = 1, ..., w)$, and the postulate of quantum measurement.

Assumption. (One-more unforgeability) We say that the one-more unforgeability assumption holds if, for every polynomial-time quantum adversary F, the advantage $\mathrm{Adv}(F)$ is negligible with respect to security parameter n.

2.2 Quantum voting protocol

In this subsection, we describe our quantum voting protocol. The anonymity of this protocol is guaranteed unconditionally, and correctness is guaranteed if the one-more-unforgeability assumption holds.

Let n be a security parameter and $m = O(n)$ be the bit length of the voting message. There are an administrator A, counter C, and v voters V_i $(i = 1, ..., v)$. We assume (1) an authenticated channel, where sender and receiver are authenticated, from administrator A to voter V_i and (2) a sender-anonymous channel, where the sender is anonymous and the receiver is authenticated, from voter V_i to counter C. For simplicity, we assume that these channels are secure, i.e.,

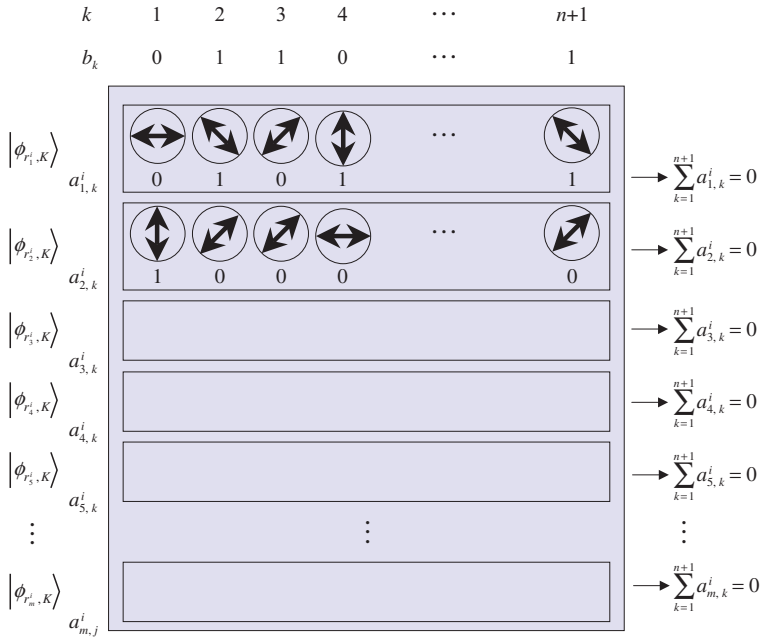

Fig. 1. Quantum blank ballot $|\eta^i\rangle$.

error-free. Counter C is assumed to carry out protocols correctly; otherwise, the result of voting could be manipulated as C desired. C just acts as a fair procedure and other aspects of security do not especially depend on his existence, i.e., C does not have any secrets of his own and all results of measurement are published.

Issuing. Administrator A uniformly selects a secret $K = (b_1, ..., b_{n+1}) \in \{0, 1\}^{n+1}$. Then, for $i = 1, ..., v$, administrator A selects $r^i = (r^i_1, ..., r^i_m) = (a^i_{1,1}, ..., a^i_{1,n+1}, ..., a^i_{m,1}, ..., a^i_{m,n+1}) \in \{0, 1\}^{m(n+1)}$, where $a^i_{j,1} ... a^i_{j,n}$ $(j = 1, ..., m)$ are selected uniformly and $a^i_{j,n+1} = a^i_{j,1} \oplus \cdots \oplus a^i_{j,n}$ $(j = 1, ..., m)$, and constructs a *blank piece* $|\phi_{r^i_j, K}\rangle$ and a *blank ballot*

$$|\eta^i\rangle = |\phi_{r^i_1, K}\rangle \otimes \cdots \otimes |\phi_{r^i_m, K}\rangle. \quad (4)$$

A blank ballot is depicted in **Fig. 1**.

Administrator A sends the blank ballot $|\eta^i\rangle$ to voter V_i through the authenticated channel.

Randomization. Voter V_i receives the blank ballot $|\eta^i\rangle$ from administrator A through the authenticated channel. He selects $t^i = (t^i_1, ..., t^i_m) = (d^i_{1,1}, ..., d^i_{1,n+1}, ..., d^i_{m,1}, ..., d^i_{m,n+1}) \in \{0, 1\}^{m(n+1)}$, where $d^i_{j,1} ... d^i_{j,n}$ $(j = 1, ..., m)$ are selected uniformly and $d^i_{j,n+1} = d^i_{j,1} \oplus \cdots \oplus d^i_{j,n}$ $(j = 1, ..., m)$, and obtains a *randomized blank ballot*

$$|\eta'^i\rangle = U^{(t^i)}|\eta^i\rangle, \quad (5)$$

where $U^{(t^i)} = U^{(t^i_1)}_1 \otimes \cdots \otimes U^{(t^i_m)}_m$ and $U^{(t^i_j)}_j = Y^{d^i_{j,1}} \otimes \cdots \otimes Y^{d^i_{j,n+1}}$, where $Y = XZ = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ and $Y^0 = I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

A randomized blank ballot is depicted in **Fig. 2**.

Remark: The unitary transformation Y flips a for both bases Z and X. Sometimes, it also changes the global phase, but no one can distinguish the difference in global phase. Consequently, the global phase change caused by Y does not affect the user's anonymity.

Remark: Since each blank ballot has a randomly chosen pattern of information r^i, if a voter utilizes a blank ballot without any modification, the administrator may be able to trace the ballot by recording r^i, so the voter's privacy cannot be guaranteed.

Voting. Let $M \subset \{0, 1\}^m$ be the set of all the valid voting messages, where the number of valid voting messages $|M|$ is constant for security parameter n and $m = O(n)$, so the probability that a random bit string becomes a valid voting message is negligible for n. On the randomized blank ballot $|\eta'^i\rangle$, voter V_i writes his/her voting message $c^i = (c^i_1, ..., c^i_m) \in M \subset \{0, 1\}^m$, where c^i is the name of the candidate for whom voter V_i wants to vote. Voter V_i makes his/her *voting ballot*

$$|\eta^{(c^i)}\rangle = U^{(c^i)}|\eta'^i\rangle, \quad (6)$$

where $U^{(c^i)} = U^{(c^i_1)}_1 \otimes \cdots \otimes U^{(c^i_m)}_m$, $U^{(c^i_j)}_j = I \otimes \cdots \otimes I \otimes Y^{c^i_j}$. A voting ballot is depicted in **Fig. 3**. Voter V_i sends the ballot $|\eta^{(c^i)}\rangle$ to counter C through the sender-anony-

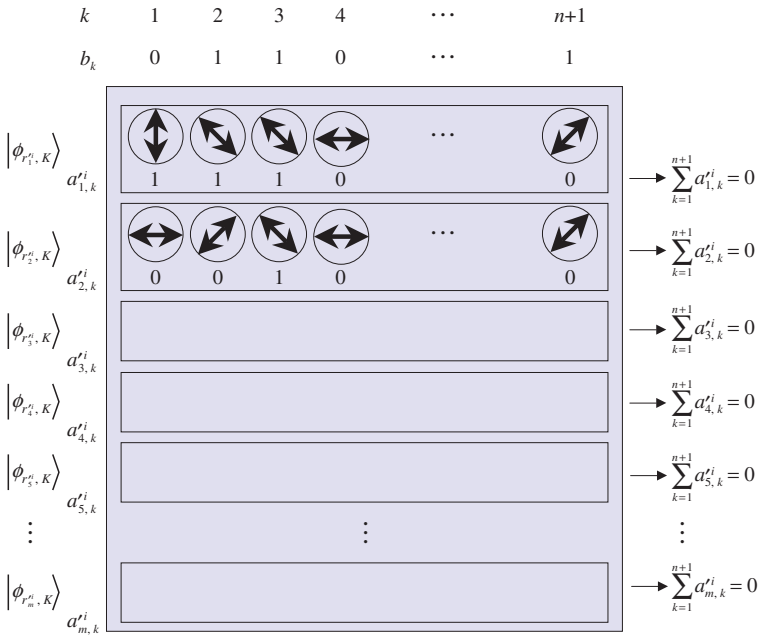

Fig. 2. Randomized quantum blank ballot $|\eta'^{i}\rangle$.

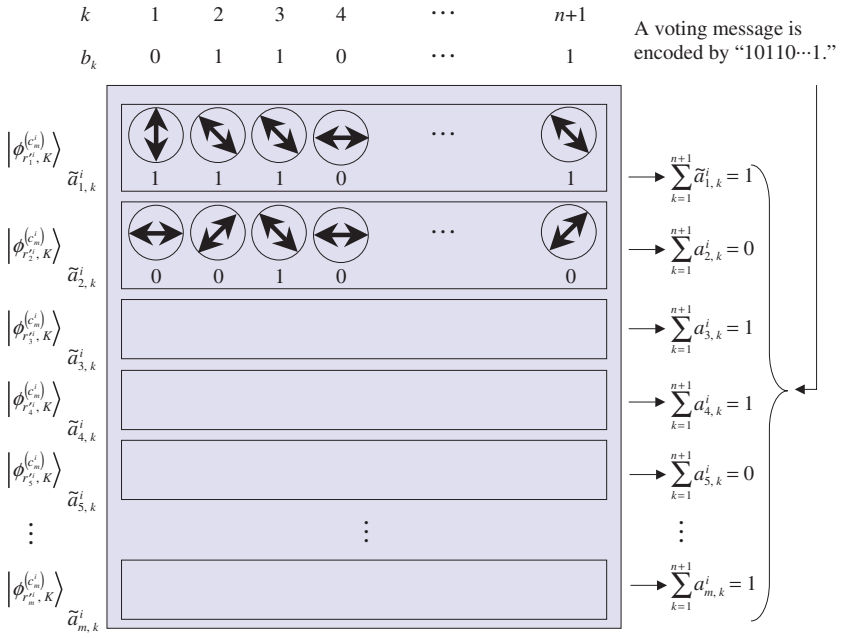

Fig. 3. Quantum voting ballot $|\eta^{(c^i)}\rangle$.

mous channel.

Counting. Counter C receives secret K from administrator A through a classical secure channel after all voters have sent their votes. He receives all ballots $|\eta^{(c^i)}\rangle$ (i = 1, ..., υ) from all voters V_i (i = 1, ..., υ) through the sender-anonymous channel. He measures all ballots $|\eta^{(c^i)}\rangle$ (i = 1, ..., υ) and obtains the measurement results ($\tilde{a}^i_{j,\,1}$, ..., $\tilde{a}^i_{j,\,n+1}$) (i = 1, ..., υ, j = 1, ..., m), where ($\tilde{a}^i_{j,\,1}$, ..., $\tilde{a}^i_{j,\,n+1}$) are the measurement results of j-th (n+1) qubits of $|\eta^{(c^i)}\rangle$ in basis K = (b_1, ..., b_{n+1}). He computes $\tilde{c}^i_j = \tilde{a}^i_{j,\,1} \oplus \cdots \oplus \tilde{a}^i_{j,\,n+1}$ (i = 1, ..., υ, j = 1, ..., m), and checks whether or not $\tilde{c}^i$ = ($\tilde{c}^i_1$, ...,

$\tilde{c}^i_m) \in M \subset \{0, 1\}^m$. If $\tilde{c}^i \in M$, then $\tilde{c}^i$ is counted as the result of the voting; otherwise, $\tilde{c}^i$ is discarded.

2.3 Cut-and-choose protocol for issuing

If a malicious administrator issues invalid blank pieces, correctness and anonymity can be violated because the administrator can nullify and/or trace a ballot by mixing invalid pieces into it. To avoid the risk of this, we can use a cut-and-choose technique to verify the validity of blank pieces issued by the administrator. Our cut-and-choose protocol is explained below.

In the issuing stage, administrator A creates $2mv$ blank pieces $|\phi_{r,K}\rangle$ and puts them in register R. Each voter V_i randomly picks m blank pieces as his/her blank ballot $|\eta^i\rangle$.

Before the counting stage, after all voters have cast their votes, counter C receives secret K from administrator A through a classical secure channel and performs the following check. Counter C measures mv blank pieces left in register R using secret basis K and checks whether or not all the results of these measurements are valid. If some are found to be invalid, we judge that administrator A issued invalid blank pieces and abort the voting process.

Note that a malicious administrator can mingle a small number of invalid blank pieces into a voter's blank ballot without detection even if we use the cut-and-choose protocol.

2.4 The t-out-of-l threshold protocol for issuing

Here, we present a threshold distributed protocol based on threshold quantum cryptography. If an administrator who knows secret K illegally casts a valid voting ballot in the voting stage, or dishonestly gives secret K to adversaries, then the adversaries can freely forge ballots as they like. To avoid the risk of this, a distributed scheme is very effective. In such a scheme, several centers each hold a share of secret K, and these centers collaborate to create blank pieces.

In this t-out-of-l threshold distributed protocol, each center chooses its secret by itself and distributes shares of its own secret. Once the secrets have been shared among l centers, an arbitrary t-out-of-l centers can issue valid blank pieces. After the preliminary secret distribution phase, even if $l-t$ centers happen to be down or out of service, at least t centers will still work properly, so the whole scheme works correctly. Moreover, if the number of dishonest centers is smaller than t, they cannot make valid quantum ballots. We apply a threshold technique such as Shamir's secret sharing scheme [21] (i.e., t-out-of-l scheme) for this threshold distributed protocol. We also apply Pederson's idea [22] that several centers share their own secrets.

Distribution. For l centers to distribute shares of their secrets, all centers P_j out of the l centers perform the following procedure.

P_j chooses its own secret $\sigma_j = (b_{j,1}, b_{j,2}, ..., b_{j,n+1})$, where $b_{j,k}$ are uniformly chosen from $\{0, 1\}$.

The center P_j then makes l shares, $S_{j,1}, ..., S_{j,l}$, of σ_j by using Shamir's secret sharing scheme over GF(2^N), where $N = n+1$. Let $f_j(x)$ be a secret $(t-1)$-th-degree polynomial, $S_{j,i} = f_j(x_{j,i})$ for $i = 1, ..., l$, and $\sigma_j = f_j(0)$ over GF(2^N), where $x_{j,i}$ for $i = 1, ..., l$ are l distinct points in GF(2^N) and are published. The center P_j sends $S_{j,i}$ to a center P_i secretly for each $i = 1, ..., l$.

Precomputation. For simplicity, we assume that the t centers $P_1, ..., P_t$ collaborate to issue blank pieces.

For each $i = 1, ..., t$, P_i calculates and secretly stores the following value using the Lagrange interpolation formula

$$K_i = \sum_{j=1}^{l} S_{j,i} \prod_{1 \le w \le t,\, w \ne i} \frac{x_{j,w}}{x_{j,w} - x_{j,i}} \in \mathrm{GF}(2^N). \tag{7}$$

Let

$$K^{[i]} = (b_1^{[i]}, b_2^{[i]}, ..., b_{n+1}^{[i]}) \in \mathrm{GF}(2^N) \tag{8}$$

be the binary representation of K_i in GF(2^N), where $b_k^{[i]}$ are in $\{0, 1\}$. The whole secret is

$$K = \sum_{i=1}^{t} K_i = \sum_{j=1}^{l} \sigma_j \in \mathrm{GF}(2^N). \tag{9}$$

Note that even in the collaboration procedure, K_i and σ_j are kept secret in P_i, and K is not recovered.

Issuing. The t centers $P_1, ..., P_t$ collaborate to construct a blank piece $|\phi\rangle$. Below, we describe the sequential protocol from P_1 to P_t, but the order is not essential: any order is possible.

P_1 generates a quantum state

$$|\phi^{[1]}\rangle = |\psi_{a_1^{[1]} b_1^{[1]}}\rangle \otimes \cdots \otimes |\psi_{a_{n+1}^{[1]} b_{n+1}^{[1]}}\rangle, \tag{10}$$

where $r^{[1]} = (a_1^{[1]}, ..., a_n^{[1]}), \in \{0, 1\}^n$ is a random string uniformly picked by P_1 for each blank piece, and $a_{n+1}^{[1]} = a_1^{[1]} \oplus \cdots \oplus a_n^{[1]}$. Here, $|\psi_{a_i^{[1]} b_i^{[1]}}\rangle$ is defined in the same manner as in Eq. (1).

Next, P_1 sends $|\phi^{[1]}\rangle$ to P_2. When P_i receives $|\phi^{[i-1]}\rangle$ from P_{i-1}, P_i follows the following procedure to generate $|\phi^{[i]}\rangle$ and sends it to P_{i+1}, where $i = 2, ..., l$ and P_{l+1} is a voter.

Then, P_i obtains $|\phi^{[i]}\rangle$ by applying the following unitary transformation $W^{[i]}$ to $|\phi^{[i-1]}\rangle$.

$$|\phi^{[i]}\rangle = W^{[i]} |\phi^{[i-1]}\rangle, \tag{11}$$

where

$$W^{[i]} = Y^{[i]} H^{[i]},\ Y^{[i]} = Y^{a_1^{[i]}} \otimes \cdots \otimes Y^{a_{n+1}^{[i]}},\ H^{[i]} = H^{b_1^{[i]}} \otimes \cdots \otimes H^{b_{n+1}^{[i]}}. \tag{12}$$

Here, $a_{n+1}^{[i]} = a_1^{[i]} \oplus \cdots \oplus a_n^{[i]}$, $r^{[i]} = (a_1^{[i]}, ..., a_n^{[i]}) \in \{0, 1\}^n$ is a random string uniformly picked by P_i for each blank piece, unitary transformation Y follows the previous definition in Subsection 2.2, and

$$H = \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix},\ H^0 = I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}. \tag{13}$$

After repeating this procedure, finally P_l sends $|\phi^{[l]}\rangle$ to a voter as a blank piece.

Correctness. $|\phi^{[1]}\rangle$ encodes string $a_1^{[1]}$, ..., $a_{n+1}^{[1]}$ using secret bases $K^{[1]}$. By unitary transformation $W^{[2]}$, $|\phi^{[1]}\rangle$ is transformed into $|\phi^{[2]}\rangle$ (here, we ignore the global phase), which encodes $a_1^{[1]} \oplus a_1^{[2]}$, ..., $a_{n+1}^{[1]} \oplus a_{n+1}^{[2]}$ using basis $K^{[1]} \oplus K^{[2]}$. Finally, $|\phi^{[l]}\rangle$ encodes $a_1^{[1]} \oplus \cdots \oplus a_1^{[l]}$, ..., $a_{n+1}^{[1]} \oplus \cdots \oplus a_{n+1}^{[l]}$ using basis $K = K^{[1]} \oplus K^{[2]} \oplus \cdots \oplus K^{[l]}$. Thus, the quantum ballot $|\phi^{[l]}\rangle$ is valid.

Security. If we assume that the communication among l parties during their collaboration is protected from adversaries and that the l parties are honest, then the security of the threshold scheme is at least on the same level as the original voting scheme.

3. Security of our quantum voting scheme

3.1 Security considerations for voting requirements

Correctness. First, we consider an active attack by a voter who tries to forge ballots. In this case, security will depend on the quantum computational complexity problem, i.e., one-more unforgeability (the Assumption in Subsection 2.1), whose hardness is not clearly understood yet, so conclusive security is beyond the scope of this paper. Here, we show that several naïve attacks cannot work well. It is impossible to simply make a copy of an unknown quantum state in principle according to the *no-cloning theorem*. If a forger (including a voter) tries to make a quantum ballot without knowing secret K, i.e., randomly makes a forged quantum ballot, the forged ballot $|\psi\rangle$ is accepted with probability $|M|/2^m$. Since the number of candidates $|M|$ is constant, the probability of successful forging is negligible. If K is derived from valid blank ballots, an adversary can forge valid ballots freely. However, deriving secret key K is intractable, as described in Subsection 3.2. So, it is difficult for a dishonest voter to forge quantum ballots in our scheme.

Next, we consider an active attack by the administrator. If the administrator mixes k invalid blank pieces into $2mv$ blank pieces in the issuing stage, we can detect invalid blank pieces with probability $1–1/2^k$ using our cut-and choose protocol for issuing. If an invalid blank piece is detected, we abort the voting. The invalid blank pieces pass through the checking stage with probability $1/2^k$, so in this case, the administrator can nullify at most k unspecified votes.

Anonymity. A voter cannot break the privacy of another voter because he is isolated from the other voter's procedures and the communication channels are protected to make them secure. Thus, we consider only an active attack by the administrator.

Since all quantum voting ballots are sent through an anonymous channel, if there is no identifiable information in a ballot, then the privacy of voting is kept. The administrator can record randomness r encoded in blank ballot $|\eta\rangle$ in order to try and break the privacy of voters. To prevent this, the voter randomizes $|\eta\rangle$ by applying random unitary transformation U with randomness t and obtains randomized blank ballot $|\eta'\rangle$ with randomness $r' = r \oplus t$. Since t is uniformly selected by the voter, the original randomness r is unconditionally concealed and privacy is protected.

Although the administrator can mix k invalid blank pieces into $2mv$ blank pieces in the issuing stage to trace votes and break privacy, we can detect the invalid blank pieces in the register with probability $1–1/2^k$ using our cut-and choose protocol. If an invalid blank piece is detected, we abort the voting and discard the quantum voting ballots held by counter C. Therefore, in this case, votes are never revealed and privacy is protected. The invalid blank pieces pass through the checking stage with probability $1/2^k$. In this case, the administrator can invalidate at most k unspecified votes and break the privacy of at most k unspecified voters.

Receipt-freeness. A voter might try to embed some information into his/her voting ballot $|\eta^{(c)}\rangle$ in order to prove his/her vote to a buyer/coercer. However, since the voter does not know randomness r encoded in blank ballot $|\eta\rangle$, he/she cannot control randomness r' encoded in blank ballot $|\eta'\rangle$. If the voter mixes errors into the name of candidate c encoded in his/her voting ballot $|\eta^{(c)}\rangle$, then voting ballot $|\eta^{(c)}\rangle$ can be traced, but it will be discarded and not counted.

A voter might try to copy his/her voting ballot $|\eta^{(c)}\rangle$ to make a receipt for the vote buyer/coercer. However, it is difficult to copy quantum voting ballot $|\eta^{(c)}\rangle$, as already described in Correctness.

3.2 Intractability of finding secret key *K*

Let us consider a straightforward individual attack on our voting scheme. An adversary F is given a blank ballot $|\phi\rangle = |\phi_{r_1, K}\rangle \otimes \cdots \otimes |\phi_{r_m, K}\rangle$ and examines the basis K by measuring quantum bits individually as follows. First, F guesses K from $\{0, 1\}^{n+1}$ and measures $|\phi_{r_j, K}\rangle$ with the basis and gets the result $(\tilde{a}_{j, 1}, ..., \tilde{a}_{j, n+1})$. If the guess of K is correct, then all the results are *valid* i.e., $\tilde{a}_{j, n+1} = \tilde{a}_{j, 1} \oplus \cdots \oplus \tilde{a}_{j, n}$ for all j. Then, F is assured that his guess is correct and he has obtained the correct K. The guess of b_k of $K = (b_1, ..., b_{n+1})$ is correct with probability 1/2, so the probability that guesses of all b_k for $k = 1, ..., n+1$ are correct is only $1/2^{n+1}$. Therefore, the secrecy of K against the simple individual attack is proven.

It has been pointed out that a Grover-type attack is applicable to this construction [23] if we allow F to use a general (coherent) attack. However, it still needs exponential time quantum computation. Grover's algorithm [24] has been proven to be optimal within the query-type algorithm to find a unique solution from a database [25]–[27]. Thus, F needs another type of algorithm to get secret bases efficiently, but no efficient attack has been found yet. In our scheme, the parity of random bits $a_{j, 1} \oplus \cdots \oplus a_{j, n} = a_{j, n+1}$ is encoded in $|\psi_{a_{j, n+1}, b_{n+1}}\rangle$ of $|\phi_{r_j, K}\rangle$ and the rest of $|\phi_{r_j, K}\rangle$ is a totally random state for voters who do not know K. The construction of our scheme is very simple and it seems to be difficult to find another type of algorithm that is not a query-type algorithm. Although the difficulty has not been proven, it might be reduced to the difficulty of a well-known computational complexity problem such as [28], which is believed to be difficult even for a quantum computer. We leave this complexity as an open problem.

4. Concluding remarks

In this paper, we described a new cryptographic protocol concept, *quantum voting*. The anonymity of the protocol is unconditionally guaranteed, and correctness is guaranteed if the one-more-unforgeability assumption holds. We also presented a cut-and-choose protocol and a distributed protocol for preventing the administrator from dishonestly executing procedures.

In this paper, we just assumed that the quantum channel is secure (error-free) for simplicity. We could eliminate this assumption by constructing a secure quantum channel using a quantum one-time pad [29], [30] or using some other means.

We leave the analysis of quantum computational complexity as an open problem. Although the security of our protocol is based on quantum computational complexity and does not have unconditional security, it should have many applications in quantum information technology.

To implement a quantum voting scheme, we need a quantum register/memory. Since our scheme does not make use of quantum entanglement, a sufficient register for our scheme is one of the most basic elements of quantum computers, that is, a 1-qubit register that need not keep quantum correlation between two quantum bits. (The situation will be different when we implement quantum error correction.) Even such a quantum register is still beyond our current technologies. However, such technologies are being extensively studied and developed. In addition, the operation needed for our scheme is very simple, only 1-qubit unitary transformation, which is already feasible.

Finally, we emphasize that the use of a quantum state to achieve a voting scheme should be an attractive and fruitful research approach. The work described in this paper is the first step in this direction.

References

[1] J. A. Vaccaro, J. Spring, and A. Chefles, "Quantum protocols for anonymous voting and surveying," Phys. Rev. A, 75, 012333, 2007.

[2] M. Hillery, M. Ziman, V. Bužek, and M. Bieliková, "Towards quantum-based privacy and voting," Phys. Lett. A, Vol. 349, pp. 75–81, 2006.

[3] D. Chaum, "Elections with unconditionally-secret ballots and disruption equivalent to breaking RSA," In EUROCRYPT'88, Vol. 330 of Lecture Notes in Computer Science, pp. 177–182, Springer-Verlag, 1997.

[4] A. Fujioka, T. Okamoto, and K. Ohta, "A practical secret voting scheme for large scale elections," In AUSCRYPT'92, Vol. 718 of Lecture Notes in Computer Science, pp. 244–260, Springer-Verlag, 1993.

[5] T. Okamoto, "Receipt-free electronic voting schemes for large scale elections," In Workshop on Security Protocols'97, Vol. 1361 of Lecture Notes in Computer Science, pp. 25–35, Springer-Verlag, 1997.

[6] C. Park, K. Itoh, and K. Kurosawa, "Efficient anonymous channel and all/nothing election scheme," In EUROCRYPT'93, Vol. 765 of Lecture Notes in Computer Science, pp. 248–259, Springer-Verlag, 1994.

[7] B. Pfitzmann, "Breaking an efficient anonymous channel," In EUROCRYPT'94, Vol. 950 of Lecture Notes in Computer Science, pp. 332–340, Springer-Verlag, 1995.

[8] K. Sako and J. Killian, "Secure voting using partial compatible homomorphisms," In CRYPTO'95, Vol. 839 of Lecture Notes in Computer Science, pp. 411–424, Springer-Verlag, 1995.

[9] M. Michels and P. Horster, "Some remarks on a receipt-free and uni-

versally verifiable mix-type voting scheme," In ASIACRYPT'96, Vol. 1163 of Lecture Notes in Computer Science, pp. 125–132, Springer-Verlag, 1996.
[10] M. Abe, "Universally verifiable mix-net with verification work independent of the number of mix-servers." In EUROCRYPT'98, Vol. 1403 of Lecture Notes in Computer Science, pp. 437–447, Springer-Verlag, 1998.
[11] J. Benaloh, "Verifiable secret-ballot elections," Ph.D. thesis, Department of Computer Science, Yale University, Sep. 1987.
[12] J. Benaloh and D. Tuinstra, "Receipt-free secret-ballot elections," In *STOC'94*, pp. 544–553, ACM, 1994.
[13] R. Cramer, M. Franklin, B. Schoenmakers, and M. Yung, "Multi-authority secret ballot elections with linear work, "In EUROCRYPT'96, Vol. 1070 of Lecture Notes in Computer Science, pp. 72–83, Springer-Verlag, 1996.
[14] R. Cramer, R. Gennaro, and B. Schoenmakers, "A secure and optimally efficient multi-authority election scheme," In EUROCRYPT'97, Vol. 1233 of Lecture Notes in Computer Science, pp. 103–118, Springer-Verlag, 1997.
[15] M. Hirt and K. Sako, "Efficient receipt-free voting based on homomorphic encryption," In EUROCRYPT'00, Vol. 1807 of Lecture Notes in Computer Science, pp. 539–556, Springer-Verlag, 2000.
[16] B. Lee and K. Kim, "Receipt-free electronic voting through collaboration of voter and honest verifier," In JW-ISC2000, pp. 101–108, 2000.
[17] M. Hirt, "Multi-party Computation: Efficient Protocols, General Adversaries, and Voting," Ph.D. thesis, ETH Zurich, 2001.
[18] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," In Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing, pp. 175–179, 1984.
[19] S. Wiesner, "Conjugate coding," SIGACT News, Vol. 15, No. 1, pp. 78–88, 1983.
[20] Y. Tokunaga, T. Okamoto, and N. Imoto, "Threshold quantum cryptography," Phys. Rev. A, 71, 012341, 2005.
[21] A. Shamir, "How to share a secret," Comm. Assoc. Comput. Mach., Vol. 22, No. 11, pp. 612–613, 1979.
[22] T. Pederson, "A threshold cryptosystem without a trusted party," In Eurocrypt'91, Vol. 547 of Lecture Notes in Computer Science, pp. 522–526, Springer-Verlag, 1991.
[23] H.-K. Lo, personal communication, 2003.
[24] L. K. Grover, "A fast quantum mechanical algorithm for database search," In STOC'96, pp. 212–219, ACM, 1996.
[25] C. H. Bennett, E. Bernstein, G. Brassard, and U. Vazirani, "Strengths and weaknesses of quantum computing," SIAM Journal on Computing, Vol. 26, No. 5, pp. 1510–1523, 1997.
[26] M. Boyer, G. Brassard, P. Høyer, and A. Tapp, "Tight bounds on quantum searching," Fortsch. Phys., Vol. 46, pp. 493–506, 1998.
[27] C. Zalka, "Grover's quantum searching algorithm is optimal," Phys. Rev. A, 60, 2746, 1999.
[28] A. Kawachi, T. Koshiba, H. Nishimura, and T. Yamakami, "Computational indistinguishability between quantum states and its cryptographic application," In EUROCRYPT'05, Vol. 3494 of Lecture Notes in Computer Science, pp. 268–284, Springer-Verlag, 2005.
[29] A. Ambainis, M. Mosca, A. Tapp, and R. de Wolf, "Private quantum channels," In Proceedings of IEEE Symposium on Foundations of Computer Science, pp. 547–553, IEEE, 2000.
[30] D. W. Leung, "Quantum vernam cipher," Quantum Information and Computation, Vol. 2, No. 1, pp. 14–34, 2002.

Tatsuaki Okamoto
Research Fellow, Okamoto Research Laboratory, NTT Information Sharing Platform Laboratories.
He received the B.E., M.E., and Dr.Eng. degrees from the University of Tokyo, Tokyo, in 1976, 1978, and 1988, respectively. He is a member of the Institute of Electronics, Information and Communication Engineers (IEICE) of Japan and the International Association for Cryptologic Research.

Koutarou Suzuki
Research Scientist, Information Security Project, NTT Information Sharing Platform Laboratories.
He received the B.S., M.S., and Ph.D. degrees from the University of Tokyo, Tokyo, in 1994, 1996, and 1999, respectively. He joined NTT Information Sharing Platform Laboratories in 1999. He has been engaged in research on public key cryptography, especially on cryptographic protocols and digital signatures. He is a member of IEICE and the Information Processing Society of Japan. He received the SCIS Paper Award from IEICE in 2002.

Yuuki Tokunaga
Researcher, Okamoto Research Laboratory, NTT Information Sharing Platform Laboratories.
He received the Bachelor's degree for integrated human studies in mathematical information science from Kyoto University in 1999, the M.S. degree in information science from the University of Tokyo in 2001, and the D.S. degree in material physics from Osaka University in 2007. He joined NTT Information Sharing Platform Laboratories in 2001. He has been engaged in research on quantum information science, especially on algorithms, cryptography, and optics. Recently, he has been engaged in research on optical quantum information processing. He is a member of the Physical Society of Japan.