Multi-object quantum traveling ballot scheme

Yuan Li (李 淑)* and Guihua Zeng (曾贵华)
Laboratory of Coding and Communication Security, Department of Electronic Engineering, Shanghai Jiao Tong University, Shanghai 200240
*E-mail: yuanli@sjtu.edu.cn
Received April 3, 2008

Based on quantum mechanics, a traveling ballot scheme with anonymity and secrecy is introduced to realize voting. By searching the objects in large amount of data bases, every voter may cast votes to his desired candidates. Therefore, the proposed scheme may be applied to voting with a great deal of candidates, such as network voting and so on. The security analysis of the present scheme is also performed.

OCIS codes: 060.0060, 260.0260, 270.0270.
doi: 10.3788/COL20090702.0152.

Quantum mechanics provides novel features to information processing, extending the capabilities beyond those classical applications only. As a resource in quantum communication, quantum entanglement is valuable for accomplishing many quantum computation and other applications[1,2]. The most prominent researches are investigated in some fields such as quantum computation [3,4], quantum teleportation [5,6], and quantum cryptography [7], with the latter being the most mature experimentally. Based on the creation of a multipartite entangled state in quantum computation, the quantum gate that lies beyond the capabilities of linear optics, can be implemented practically [8]. Recently, because the Heisenberg spin systems are natural candidates for simulating the interactions between qubits, the entanglement in Heisenberg spin chain has been studied.

Motivated by these development in quantum entanglement, we investigate its application in quantum voting with the relation between entanglement and quantum phase transition. In some situations, ballot protocol is always effective that people want to vote their desired objects among a great deal of candidates such as the electronic balloting or to select more prevalent books in net-

Employing a searching operator $Q$ on the state $|\mathcal{A}\rangle_V$ for times of $r = \text{round}(\frac{N}{2\sqrt{N}})$, $V_1$ may obtain the desired state $|\tau\rangle$ with the possibility near to 1. For ascertaining whether the found element is state $|\tau\rangle$, $V_1$ may resort to an ancilla state $|q\rangle$ in a register $R^{(1)}$ which is held by himself. With a Boolean function $g(x): \{0, \cdots, N-1\} \rightarrow \{0,1\}$, extremely $V_1$ can obtain his desired state. As following, he will cast his vote to the candidate $\tau$. Denote an phase shifting operator acted by $V_k$ as $\mathcal{M}_{\phi}^{(k)} = \exp(i\theta_n)$, where $1 < k < K$, $0 < n < N$, $\theta_n = 2n\pi/N$. The state $|\tau\rangle$ after $V_1$ casting his vote becomes

$|V_1\rangle = \mathcal{M}_{\phi}^{(1)}|\tau\rangle = \exp(i\theta_n)|\tau\rangle$.

After $V_1$ completes his voting, the ballot state $|A\rangle$ may be expressed as

$$|A_1\rangle = \frac{1}{\sqrt{N}}\left(\sum_{n\neq \tau} |n, N-1-n\rangle + |V_1\rangle|N-1-\tau\rangle\right). \quad (4)$$

Then, $V_1$ sends $|A\rangle_1$ to the next voter $V_2$. As before, $V_2$ also makes similar operation to his received ballot state so that $|A_2\rangle$ is obtained. The process is repeated until the final voter casts his vote and the state $|A_K\rangle$ is obtained, after which he returns the particle to the tallyman. On the other hand, the agent also returns his holding system $p_i$ to the tallyman. By calculating the received entangled state, the tallyman may get the yes vote number of every candidates $B_n$ ($n = 0, \cdots, N-1$) as following operation. With respect to the eigenvalue of every state vector, the tallyman determines the value of the tally from the expectation $\langle A_K|\hat{T}_n|A_K\rangle = M_n$, where $\hat{T}_n = n|T_n\rangle\langle T_n|$ is the corresponding multiparticle tally operator for

$$|T_n\rangle = \frac{1}{\sqrt{N}}\sum_{j=0}^{N} \exp(i\theta_n)|j, N-1-j\rangle. \quad (5)$$

Consequently, after all the particles are translated to the tallyman, he will count the tallies of every candidates. The circuit of the traveling ballot system is shown in Fig. 1.

During the voting procedure, no particle carries any information about the votes being cast. The vote information is carried in the correlations between the particles, so that the anonymity of voting procession is insured. This also protects the privacy of the votes from every voter.

Now we consider the multi-object voting approach. Assume more than one objects are entitled to be cast by voters in protocol, such as the traveling ballot scheme. After using multi-object search operator $Q_m$ to act on $|A\rangle_V$ for times of $r_m = \text{round}\{\frac{1}{\sqrt{N}}[1+O(\frac{N}{m})]\}$, every voter may obtain the desired states $|\tau_1\rangle, \cdots, |\tau_m\rangle$ with probability

$$P_m = \cos^2(r_m\phi - \mu), \quad \phi = \sin^{-1}\left(2\sqrt{m(N-m)}\right) \quad \text{and} \quad \mu \approx \frac{\phi}{2} \quad \text{for} \quad m \ll N.$$ And then, the voter $V_k$ applies an operator $M^{(k)}$ on his selected states:

$$M^{(k)}|A\rangle_{k} = \frac{1}{\sqrt{N}}\left(\sum_{j=1}^{m} \exp(i\theta_{\tau_j})|\tau_j, N-1-\tau_j\rangle + \sum_{k\neq \tau_j}^{N} |k, N-1-k\rangle\right). \quad (6)$$

Finally, each of candidate tallies may be counted by the tallyman. The anonymous voting for multiple objects among the great deal of candidates can be applied in a number of different scenarios, such as network election and so on. In the correlations between the particles, the quantum state contains no information about how individuals voted, and the entangled state shared between at least two sites. Because of the physical properties, only collective features of the set of votes are calculated and made public, such as the tally of yes and no votes, so that the ballot information can be kept secret.

If two separated ballot agents separately have attack for the scheme, then this attack will be detected with one half of the time. Because any change of states will be made public, cheating attempt by the ballot agents must be detected on average. Subsequently, the qubit system is evidently disturbed. If the voters take attacking together and compare the projections onto phase states, then the total particle number of the attack should be altered on average with a probability $\frac{1}{N}$. As the agent does not have access to the site $V$ at any point in this operation, in the traveling ballot scheme, he hence can only see the mixed state

$$\text{Tr}_V(|A_K\rangle\langle A_K|) = \frac{1}{N}\sum_{n=0}^{N-1} \frac{1}{N}|n\rangle\langle n|.$$ \quad (7)

Likewise, the voters who do not have access to the site $T$ can just see a mixed state too. If the tallyman has access to both modes at site $T$, the states $|N-1-l, l\rangle$ form an orthonormal basis for an $N$-dimensional subspace for $0 \leq l \leq N - 1$. To obtain the tally, the tallyman should find the expectation value of the tally operator. The tallyman can access the tally number only if he is in possession of all particles. The voting procession of individual voters is kept secret from both the tallyman and the other voters while the particles are shared between the ballot sites.

Conclusive transfer is more valuable than simple state transfer with the same fidelity. A single spin-1/2 quantum chain could not be used for conclusive transfer, because any measurement would destroy the unknown quantum state that is being transferred$^{[12]}$. We consider that the simplest quantum chain for conclusive transfer is a system consisting of two uncoupled quantum chains (1) and (2) which are between the users for traveling ballot state. Define a general finite quantum network graph $G = \{V(G), E(G)\}$, where $V(G)$ is the finite set of its vertices and $E(G)$ is the set of its edges. A source state sender, i.e., the agent, is located to the first spin from $G$. Quantum ballot state transfer over a network is similar to the quantum random walk problem. To a one-dimensional chain, the Hamiltonian in single-particle subspace can be written as

$$H_G = \sum_{j=0}^{N+1} \omega_j(\sigma^x_j\sigma^x_{j+1} + \sigma^y_j\sigma^y_{j+1}), \quad (8)$$

where $\omega_j$ is the time-independent coupling constant, $\sigma_j$ is a Pauli matrix. Denote two Hamiltonians $H^{(1)}$ and $H^{(2)}$ of a network $G$ as well as two Hilbert spaces $\mathcal{H}_1$ and $\mathcal{H}_2$ likes $\mathcal{H}_G$. The tallyman also needs the abil-
ity to perform single-qubit measurements. The relevant sector of the Hilbert space is spanned by the states \(|n^{(\lambda)}⟩ = |00\cdots00⟩^{(\lambda)}\) for \(0 \leq n \leq N + 1\) (\(\lambda = 1, 2\)), which represents a state of the chain where the \(n\)th spin is prepared in \(|1⟩\) and the other \(N + 1\) ones in \(|0⟩\). Set the initial state of two systems after time \(\tau_0\) as

\[|φ(\tau_0)⟩ = \sum_{n=0}^{N} f_{n,0}(\tau_0)|s(n)⟩, \tag{9}\]

where \(|s(n)⟩ = α₁|0⟩^{(1)} ⊗ |n⟩^{(2)} + β₁|n⟩^{(1)} ⊗ |0⟩^{(2)}\) is the \(n\)th superposition of excitations in both systems, and \(|s(0)⟩ = |s(1)⟩\). Furthermore, the dynamics restricted to this subspace can be expressed in terms of the \(r\)th and \(s\)th transition amplitudes as

\[f_{r,s}(t) = (r^{(\lambda)}e^{iH^{(\lambda)}t}|s⟩^{(\lambda)}, \quad r, s = 0, \cdots, N; \quad \lambda = 1, 2. \tag{10}\]

The state in Eq. (9) after time \(\tau_1\) can be written as

\[|φ(\tau_1)⟩ = \sum_{n=0}^{N} f_{n,1}(\tau_1)|s(n)⟩. \tag{11}\]

Denote a family of searching operators \(\{Q_n, n = 1, \cdots, N\}\). In terms of the Grover algorithm, employing \(Q_1\) on state \(|φ(\tau_1)⟩\) for times of \(r\), \(V_1\) can obtain the ballot state \(|s(1)⟩\) with the possibility near 1 at his own voting site. To ascertain whether the found element is state \(|s(1)⟩\), \(V_1\) may resort to an ancilla state \(|\eta_1⟩\) in a register \(R_1\) which is held by himself. With a Boolean function and measuring the ancilla state in register \(R_1\), the voter \(V_1\) may finally obtain the ballot state \(|s(1)⟩\). Then, it determines that wether or not to cast his vote on the state \(|s(N_1)⟩\). \(V_1\) applies phase shifting operation \(V_1 = \exp(\i N \delta_1)|N⟩|n⟩ = n|n⟩\) and an amount \(\delta_1 = 2r u_1/(N + 1)\) with \(u_1 = 0, 1\), on the ballot state. If the candidate is not his desired one, \(u_1\) takes 0, i.e., he does not cast vote, otherwise, \(u_1\) takes 1. After the voting of the first voter, the state becomes

\[|V_1⟩ = V_1 f_{N,1}(\tau_1)|s(1)⟩ + \sum_{n\neq 1}^{N} f_{n,1}(\tau_1)|s(n)⟩ = \exp(iN \delta_1) f_{N,1}(\tau_1)|s(1)⟩ + \sum_{n\neq 1}^{N} f_{n,1}(\tau_1)|s(n)⟩. \tag{12}\]

Whereafter, the traveling ballot state in Eq. (12) is transferred to the next voter \(V_2\). Because the resulting state of every spin is a mixed state, the voter \(V_2\) cannot trace off any voting information of \(V_1\) with his obtained state from \(V_1\). Then, he performs a vote in a similar manner with the phase shifting angle \(\delta_2\) on state \(|s(2)⟩\) at his voting note, and the corresponding ballot state \(|V_2⟩\) may be obtained. Finally, the last voter \(V_N\) may get the traveling state cast by \(N - 1\) pre-voters in quantum chains. Similarly, if he does not cast a vote to this candidate, the ballot state should be equal to the state that cast by the voter \(V_{N-1}\). Otherwise, the ballot state by searching and ascertaining, finally becomes

\[|V_N⟩ = \sum_{n=0}^{N} \exp(\i N \delta_n) f_{n,N}(\tau_N)|s(n)⟩. \tag{13}\]

For counting the tally of ballot state, the voter \(V_N\) then translates the ballot state cast by all voters to another authority (i.e., the tallyman). Similarly, tallyman can determine the corresponding tallies cast by voters.

In the following, we will analyze the present protocols against some attacks. We firstly concern an eavesdropping strategy that consists in applying a coherent attack on a qubit sequence of finite length. Here, we use an uncertainty principle due to Hall that sets a limit on the sum of voters’ and Eve’s information when both groups measure the same quantum system.

Assume the Eve who is not one of the participants in scheme implements the entangled state attack strategy, namely, Eve takes an attack strategy by applying an arbitrary operation \(U_{VE}\) on the ballot state \(|A⟩\). Then, his intervention can be detected by the agent, which implies that Eve cannot change the ballot results of voters without being detected. In fact, suppose Eve tries to attack the scheme by entangling his own particle as an ancilla with the ballot state \(|A⟩\). Without loss of generality, in quantum anonymous traveling ballot scheme we consider that Eve wants to change the ballot result of the voter \(V_k\). Eve entangles her state \(|E⟩_k\) with \(V_k\)’s ballot state in quantum network. Correspondingly, the complex state of \(|V_k⟩\) and \(|E⟩_k\) can be denoted by \(|V⟩_{VTE} = |V_k⟩ ⊗ |E⟩_k\).

At the voting site of \(V_k\), unitary operation \(U_{VE}^{(k)}\) applied by Eve on \(|V⟩_{VTE}\) yields

\[U_{VE}^{(k)}|V⟩_{VTE} = \frac{1}{\sqrt{N}} \sum_{n=0}^{N-1} |n, N - 1 - n⟩|E_n⟩_k, \tag{14}\]

where \(|E_n⟩ : n = 0, \cdots, N - 1\) is a set of Schmidt base. After voted by \(V_k\), the ballot state should be

\[|T_{E_k}⟩ = M_k|U_{VE}^{(k)}|\Phi⟩_{VTE} = \sum_{n=0}^{N} \exp(\i a_k \theta_n)|n, N - 1 - n⟩|E_n⟩_k. \tag{15}\]

Denote the state held by tallyman after voted as \(|A''⟩\). By computing \(⟨A''|T_{E_k}|A''⟩\), where the form of \(T_{E_k}\) is similar to Eq. (5), the tallyman may get that the total tally is changed. The tallyman then sends the states to corresponding voters for detecting the destroyed votes. Therefore, no matter that \(V_k\) casts or not to \(|A⟩\), the result always may be detected by the voters, which implies that Eve cannot intervene the procession of ballot.

Actually, denote that \(\hat{V}\) and \(\hat{E}\) are voters’ and Eve’s measurement operators applied on the particles sent from the agent, then

\[I_{AV_k} + I_{AE} \leq 2 \log_2\left(N \max_{k,j} |⟨v_k|e_k⟩|\right), \tag{16}\]

where \(|v_k⟩\) and \(|e_k⟩\) are the eigenstates of \(\hat{V}_k\) and \(\hat{E}\), respectively. The inequality holds with \(I_{AV_k}\) and \(I_{AE}\) being...
information on the qubit without knowledge of the basis chosen by the agent. Because voters and Eve may get the same average information when measuring the different basis, one obtains the possible upper bound on $I_{AV}$ for a given $I_{AV}$, by assuming that Eve measures an observable $E$ complementary to $V_k$, i.e., $I_{AV} + I_{AE} \leq 2 \log_2 N$ for $\langle \langle \nu_k | \rho_{AV} \rangle \rangle = N^{-1/2}, \forall k, j$. In order to ensure the security of scheme with a nonzero rate, it should be satisfied that $I_{AV} > I_{AE}$. So, it may be introduced that $I_{AB} > (\log_2 N)/2$ is a sufficient condition against coherent attacks for large number of candidates.

Furthermore, we consider another general attack strategy, i.e., individual eavesdropping based on the use of a quantum cloning machine for qubits, that $K$ systems are used in the distributed ballot scheme. This strategy may be detected in quantum distributed ballot scheme.

Consider the case of single ballot system of certain voter $V_k$. Eve mainly investigates how to make an individual eavesdropping attack with a cloner to a single ballot site. Eve employs a unitary operator

$$U_{s,t} = \sum_{n=0}^{N-1} \exp(it\theta_n) |n + s\rangle \langle n|$$

(17)

for $s, t = 0, \cdots, N - 1$ to obtain a cloner of the ballot system $|A\rangle_{V_k}$, where the subscripts $s, t$ denote the shift error and phase error respectively. Let amplitudes $a_{s,t}$ with $\sum_{s=0}^{N-1} |a_{s,t}|^2 = 1$ be the characteristics of cloner. In terms of cloning transformations, the gotten state is

$$|A_E\rangle_{V_k} = \sum_{n=0}^{N-1} a_{s,t} U_{s,t} |n\rangle_{V_k} |B_{s,-t}\rangle_{E,E'},$$

(18)

where $E$ and $E'$ are Eve’s clone and the cloning machine, respectively, while $|B_{s,-t}\rangle_{E,E'}$ is a set of orthonormal maximally entangled states of the two-particle system

$$|B_{s,t}\rangle_{E,E'} = \frac{1}{\sqrt{N}} \sum_{n=0}^{N-1} \exp(it\theta_n) |n\rangle_{E} |n + s\rangle_{E'}.$$

(19)

Tracing the output joint state of Eq. (18) over $EE'$ held by the tallyman implies that the agent’s state $|A\rangle_{V_k}$ is transformed into the mixture at voting sites,

$$\rho_{V} = \sum_{s,t=0}^{N-1} |a_{s,t}|^2 U_{s,t} |A_E\rangle_{V_k} \langle A_E| U_{s,t}^\dagger.$$  

(20)

Thus, after the state $|A\rangle_{V_k}$ underwent an operator $U_{s,t}$, the error probability is $|a_{s,t}|^2$. To any ballot state $|n\rangle$ in the computational basis, if the voter $V_k$ does not cast vote to any candidates, the phase errors clearly do not play any role in the above mixture since $U_{s,t} |n\rangle = \exp(it\theta_n) |n + s\rangle$. So, the voters’ fidelity can be expressed as

$$F = \langle \langle \nu_k | \rho_{AV} \rangle \rangle = \sum_{s=0}^{N-1} |a_{s,t}|^2.$$  

The dual of computational basis $|n\rangle$ of candidate for $n = 0, \cdots, N - 1$, where $F$ is Fourier transform. If $V_k$ casts a vote to the voting sites, then after the voting, Eve may get $U_{s,t} |\tilde{n}\rangle = \exp(it\theta_{n+s}) |\tilde{n} + s\rangle$. So, the shift errors ($s \neq 0$) do not play any role and the voters’ fidelity becomes $\tilde{F} = \langle \langle \nu_k | \tilde{\rho}_{AV} \rangle \rangle = \sum_{s=0}^{N-1} |a_{s,0}|^2$. For the cloner to copy equally well the states of both cases, Eve chooses a proper $N \times N$ amplitude matrix. The amplitude matrix may result in a cloning fidelity $F_E$ for Eve. Maximizing Eve’s optimal fidelity $F_E$ for a given value of $V_k$’s fidelity $F$ yields the optimal cloner. Let us see how Eve can maximize her information on the ballot state. To the ballot state $|n\rangle$, it is clear from Eq. (18) that Eve can obtain voter’s shift error $s$ simply by performing a partial Bell measurement on $EE'$. In order to infer the agent’s state, Eve must distinguish among $N$ nonorthogonal states regardless of the measured value of $s$. Denote $I_{AV}$ the corresponding mutual information between the agent and voter $V_k$. By taking an optimal fidelity $F_E$, Eve’s information $I_{AE}$ consequently may be obtained. However, if the agent, voter $V_k$, and Eve share many independent realizations of a probability distribution, and then with the great of candidates in the present scheme, it is sufficient that $I_{AV} > I_{AE}$ for every voter $V_k$. Therefore, the introduced ballot scheme is security in the network election specially.

In conclusion, we have introduced the quantum traveling ballot scheme for ensuring the anonymous voting in different scenarios. With all the information about the votes contained in the correlations between the particles, the quantum state contains no information about how individuals voted. Because of the physical properties, only collective features of the set of votes are calculated and open, such as the tally of yes and no votes, so that the ballot information can be kept secret. After all votes have been made, the vote tally can be determined by a collective measurement.

This work was supported by the National Natural Science Foundation of China under Grant No. 60773085.

References