OPTICAL REVIEW Vol. 15, No. 5 (2008) 219–223

Quantum Anonymous Voting Systems Based on Entangled State

Yuan LI and Guihua ZENG

Department of Electronic Engineering, Shanghai Jiaotong University, Laboratory of Coding and Communication Security, Shanghai 200240, China

(Received May 12, 2008; Accepted June 16, 2008)

Based on quantum entanglement, secure anonymous ballot systems are introduced to realize voting among numerous candidates in this paper. By searching individuals, each voter may cast a vote for his desired candidates of which number may be more than one. Therefore, the system based on the proposed algorithm may be applied voting among many candidates, such as a network ballot with the development of a quantum network. Finally, the security of the present scheme is investigated.

Key words: quantum voting system, multi-object ballot, quantum entangled states, quantum network, security and anonymity

1. Introduction

Practically, a ballot system always has some applications such as for election and so on. An universally verifiable voting scheme should be one which is open to authentication by all interrelated parties. In the scheme, each legitimate user can vote just once for a candidate and no one can learn any intermediate result. A reliable voting scheme should hence be a private, secure and verifiable scheme. In a classical secret ballot scheme the secrecy is generally protected by making use of one-time pads which are shared between all pairs of voters,[1] otherwise, the security is vulnerable. As a resource in quantum communication, quantum entanglement which has unique properties and primary features in quantum theory, is the subject of much studies.[2,3] 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.[4] By means of a series of single qubit measurements that are performed on an initial state of a highly entangled cluster state, Raussendorf *et al.*, showed the universal quantum computation.[5] Motivated by these developments in quantum entanglement, we investigate its application in quantum voting with the relation between entanglement and quantum phase transition.[6,7] In quantum information, the security and anonymity in quantum ballot system are based on quantum mechanics. Some researchers have focused on quantum voting scheme,[8–10] such that proposed in ref. 8 of a traveling ballot protocol, in which voting and surveying processes are initially explored. These previous papers focus mainly on the case of a candidate and the voting on a single ballot object. However, on some occasions, such as the electronic balloting or the select on of more prevalent books in network, people want to vote for their desired individuals among numerous candidates and a single voter may cast for individuals more than one. This motivates us to seek application of an appropriate ballot system, such as quantum network voting. Quantum network plays a key role in quantum information processing.[11] A general network may be characterized by a quantum state shared by different nodes. With the development of a quantum network, the realization of voting in such a network becomes possible. For instance, a set of quantum repeaters can be considered as a simple quantum network where the goal is to establish quantum communication over long distances. Therefore, the traveling voting scheme proposed in ref. 8 may be realized with a one-dimensional quantum network based on quantum repeaters.

Generally, two authorities in a ballot system are addressed to complete the voting scheme, one called the agent who prepares the ballot states and one called the tallyman who counts the votes. The quantum system with two authorities ensures the privacy of each vote and the anonymity of each voter, thus it increases security of the voting scheme. In the voting process, the ballot should include the voter's identity, by secretly marking it during or prior to the vote. Each participate is designated on the every ballot objects only to caste a vote. To each vote, the voter has to decide between yes or no. After all votes have been casted, the tally of every candidates can be determined by counting by the tallyman, and read directly from his computation basis states. In this paper, we describe quantum systems of anonymous voting using two different methods in quantum networks. In the present system, an agent first prepares entangled-particle system pairs (or pair) to assure the ballot secrecy and sends them to voters by different methods. After receiving the list of candidates from the agent, each voter decide his choice (maybe more than one), and then casts his vote to them. Finally, the tallyman counted the vote for all candidates. In the voting process, the identities of the participants are always kept private to outsides, although the total of the votes is made public. Therefore, users of the ballot protocol can anonymously find the winning individuals with low computational complexity. This paper is arranged as follows. We devote §2 to the description of systems, which includes two approaches, the traveling ballot system and the distributed ballot system. In the next section, security against some attack strategies is analyzed. Finally, conclusions are drawn in §4.

2. General Descriptions of Quantum Anonymous Voting Scheme

In this section, we will describe the design of the voting systems in detail. By making use of an entangled state of particles, each voter may cast his or her ballot using the traveling ballot system or the distributed ballot system. In this process, voters first search and decide on their desired candidates and then cast them corresponding votes which may be yes or no. Following the completion of the anonymous voting, all of the ballots are sent to the designated tallyman who counts them by measuring the multiparticle state and is thereby able to determine the total number of votes for each candidates.

Assume there are K voters $V_1, \ldots, V_K$, N ballot items $B_0, \ldots, B_{N-1}$ and two authorities, i.e., an agent and a tallyman. Let N^2-dimensional space $\mathcal{H} = \mathcal{H}_V \otimes \mathcal{H}_T$ be Hilbert space, where $\mathcal{H}_V$ and $\mathcal{H}_T$ are N-dimensional subspaces. Assume $\{|0\rangle, \ldots, |N-1\rangle\}$ is a set of computational orthonormal basis states, i.e., $\langle i|j\rangle = \delta_{ij}$, $i, j \in \{0, 1, \ldots, N-1\}$. Let an entangled state in space $\mathcal{H}$ be

$$|\mathcal{A}\rangle = \frac{1}{\sqrt{N}} \left(\sum_{n=0}^{N-1} |n, N-n-1\rangle \right) = U(|\mathcal{A}\rangle_V \otimes |\mathcal{A}\rangle_T), \quad (1)$$

which is carried by particle pair (p_v, p_t) for $p_v \in \mathcal{H}_V$, $p_t \in \mathcal{H}_T$, where $|n, N-n-1\rangle = |n\rangle_{\mathcal{V}} \otimes |N-n-1\rangle_T$ and U is entanglement state generation operator. After the operation is completed, we will introduce two approaches for voting, the anonymous traveling ballot system and the distributed ballot system.

2.1 Quantum anonymous traveling ballot system

In the traveling ballot system, the main idea is that the voters cast their votes with the traveling ballot state. The agent distributes ballot state carried by p_v to the first voter V_1. Receiving the particle from the agent, V_1 determines the candidate for whom he wishes to cast his vote. If he does not vote for any one among these candidates, then V_1 sends p_v to the next voter. Otherwise, let τ be the desired candidate for whom he wants to cast his vote. In terms of the generalized Grover algorithm,[12] $|\mathcal{A}\rangle_V$ may be expressed as $|\mathcal{A}\rangle_V = \sin\phi|\alpha\rangle + \cos\phi|\beta\rangle$, where $\phi = \arcsin(1/\sqrt{N})$, and $|\alpha\rangle = |\tau\rangle$, $|\beta\rangle = (1/\sqrt{N}) \sum_{n \neq \tau} |n\rangle$. Employing a searching operator Q on state $|\mathcal{A}\rangle_V$ for times of $r = \text{round}[(\pi/2)\sqrt{N}]$, V_1 may obtain the desired state $|\tau\rangle$ with a passibility near 1. To ascertain wether 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 $f(x)$: $\{0, \ldots, N-1\} \to \{0, 1\}$, ultimately V_1 can obtain his desired state with respect to the following state

$$|\tau'\rangle = Q^r(|\mathcal{A}\rangle_{V_1}|q\rangle) = |\beta\rangle|q \oplus f(\tau)\rangle. \quad (2)$$

Namely, by measuring the ancilla state in register R_1, V_1 can judge whether or not he has found the desired state $|\tau\rangle$.

In the following, he will cast his vote for candidate τ. Denote phase shifting operator acted by V_k as $\mathcal{M}_n^{(k)} = \exp(i\theta_n)$, where $\theta_n = 2n\pi/N$. State $|\tau\rangle$ after V_1 casted his vote becomes

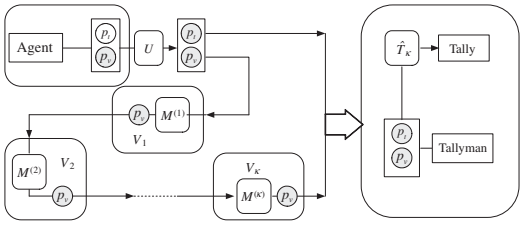

Fig. 1. Quantum circuit system of anonymous traveling described ballot scheme. The white ball in the above figure denotes a vacant state carried by p_t, the black ball is carried by p_v being cast by voters, and U is an entanglement state generation unitary operator.

$$|V_1\rangle = \mathcal{M}_\tau^{(1)}|\tau\rangle = \exp(i\theta_\tau)|\tau\rangle. \quad (3)$$

After V_1 completes his voting, the ballot state $|\mathcal{A}\rangle_V$ can be expressed as

$$|\mathcal{A}_1\rangle = \frac{1}{\sqrt{N}} \left(\sum_{n \neq \tau} |n, N-1-n\rangle + |V_1\rangle|N-1-\tau\rangle \right). \quad (4)$$

Then, V_1 sends $|\mathcal{A}_1\rangle$ to the next voter V_2. As described before, V_2 also similarly handle his received ballot state so that $|\mathcal{A}_2\rangle$ is obtained. The process is repeated until the final voter casts his vote and state $|\mathcal{A}_K\rangle$ is obtained, after which he returns the ballots to the tallyman. The agent also returns p_t to tallyman. By calculating the entangled state carried by received particle state, the tallyman will obtain the number of yes vote of every candidate $B_n (t = 0, \ldots, N-1)$. With respect to the eigenvalue of each state vector, the tallyman determines the total tally from the expectation $\langle \mathcal{A}_K|\hat{T}_n|\mathcal{A}_K\rangle = M_n$, where $\hat{T}_n = n|T_n\rangle\langle T_n|$, is the corresponding multipartite tally operator for

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

Consequently, after all the ballots have be translated to the tallyman, he will count the votes for each candidate. The circuit of the traveling ballot system is shown in Fig. 1.

2.2 Quantum anonymous distributed ballot system

In contrast to the traveling ballot system, in the anonymous distributed ballot system, all voters and the agent share a multipartite entangled state in a quantum multiuser channel. This system makes use of $(K+1)$-particle entangled state, in which the agent holds one particle and the voters hold the remainder. Each of the K voters receives one particle and performs an operation on it corresponding to his or her vote. Then, all of the particles (the voters' and the agent's) are sent to the tallyman, who measures the multi-particle state system and is thereby able to determine the tally for each candidate. As the information about the votes is contained in the correlations between the particles, the quantum state realizes no information about how individuals voted.

The agent also first prepares originally a multiparty ballot state system in register R_1 as $|\mathcal{A}'\rangle = |\mathcal{A}\rangle^{\otimes K}$, where $|\mathcal{A}\rangle$ is the state system in eq. (1), i.e., $|\mathcal{A}'\rangle$ is carried by K entangled pairs $(p_{v_1}, p_{t_1}), \ldots, (p_{v_K}, p_{t_K})$. Then, the agent distributes

particles $p_{v_1},\ldots,p_{v_K}$ to voters $V_1,\ldots,V_K$ respectively, and remains the left particles. Similarly, each voter V_k ($k=1,\ldots,K$) can quickly find his desired candidate employing quantum algorithm as before, and determine that whether or not to cast a vote for that individual, i.e., transforming $\mathcal{M}^{(k)}$ to state $|\mathcal{A}\rangle$. All voters cast their respective votes at their unique assigned voting sites. The voting can be formalized as mapping $\mathcal{M}^{(1)}\otimes\cdots\otimes\mathcal{M}^{(K)}\rightarrow\mathcal{M}=\bigotimes_{k=1}^{K}\mathcal{M}^{(k)}$. Consequently, the initial state cast by K voters becomes

$$|V\rangle=\mathcal{M}|\mathcal{A}'\rangle=\left(\bigotimes_{k=1}^{K}\mathcal{M}^{(k)}|\mathcal{A}\rangle_{V_k}\right)|\mathcal{A}\rangle_T$$
$$=\frac{1}{\sqrt{N}}\sum_{n=0}^{N-1}\exp(i\Delta_K)|n,\ldots,n,K(N-n-1)\rangle, \quad (6)$$

where $\Delta_K=\sum_{k=1}^{K}i\theta^{(k)}$, and $|n,\ldots,n,K(N-n-1)\rangle=|n\rangle_{V_1}\cdots|n\rangle_{V_K}|K(N-n-1)\rangle_T$ for K voting sites $V_1,\ldots,V_K$ and an authority site. After all entangled particles of the voters and the agent are translated to the tallyman, the tallyman can determine the corresponding tallies cast by voters in terms of the eigenvalues.

Assume the corresponding multipartite tally operator to eq. (6) is given by

$$|\hat{T}_n\rangle=\sum_{n=0}^{N-1}n|T_n\rangle\langle T_n|, \quad (7)$$

where

$$|T_n\rangle=\frac{1}{\sqrt{N}}\sum_{j=0}^{N-1}\exp(ij\theta_n)|j,\ldots,j,K(N-j-1)\rangle. \quad (8)$$

Consequently, the tallies of all candidates may be counted from the expectation $\langle V|\hat{T}_n|V\rangle=M_n$. The circuit of the distributed ballot system is shown in Fig. 2.

Next, we consider the case of casting more than one ballot for a candidate, e.g., $m>1$ candidates are entitled to be cast by a voter. After using the multi-object search operator $Q^{(m)}$ to act on $|\mathcal{A}\rangle$ for times of

$$r_m=\text{round}\left\{\frac{\pi}{4}\sqrt{\frac{N}{m}}\left[1+\mathcal{O}\left(\frac{m}{N}\right)\right]\right\}, \quad (9)$$

each voter may also obtain the his desired states $|\tau_1\rangle,\ldots,|\tau_m\rangle$ with probability $P_m=\cos^2(r_m\phi-\mu)$, where $\phi=\sin^{-1}(2\sqrt{m(N-m)}/N)$ and $\mu\approx\pi/2$ for $m\ll N$. Then, voter V_k applies ballot operator $\mathcal{M}^{(k)}=\prod_{j=1}^{m}\mathcal{M}_j$ on his selected state

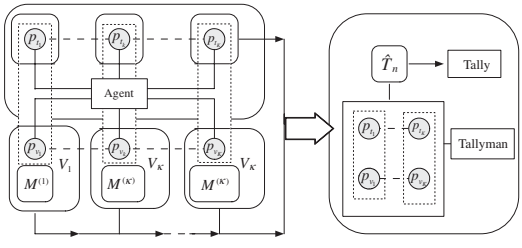

Fig. 2. Quantum circuit system of anonymous distributed ballot scheme.

$$|V_k\rangle=\mathcal{M}^{(k)}|\mathcal{A}\rangle_{V_k}$$
$$=\prod_{j=1}^{m}\mathcal{M}_j|\mathcal{A}\rangle_{V_k}\frac{1}{\sqrt{N}}\left(\sum_{j=1}^{m}\exp(i\theta_{\tau_j})|\tau_j,N-1-\tau_j\rangle\right.$$
$$\left.+\sum_{n\neq\tau_j}^{N}|n,N-1-n\rangle\right). \quad (10)$$

The final tally of each candidate also may be counted by the tallyman as before. Namely, employing tally-counting operator $\hat{T}_n$ into $\langle V_k|\hat{T}_{nk}|V_k\rangle=M_{nk}$, one may get the tally of candidate B_n cast by V_k, where

$$|T_{nk}\rangle=\frac{1}{\sqrt{N}}\sum_{j=0}^{N-1}\exp(ij\theta_n)|j\rangle_{V_k}|N-j-1\rangle_T. \quad (11)$$

Ultimately, the total tally of B_n will be revealed by $M_n=\langle V|\hat{T}_n|V\rangle$ for $\hat{T}_n=\bigotimes_{k=1}^{K}\hat{T}_{nk}$. With respect to the character of present anonymous distributed voting system, it may be applied in scenarios with many candidates, such as network election.

Because of the physical properties, only collective features of the set of votes are calculated and made public, that is the tally of yes and no votes, so that the ballot information can be kept secret. In the correlations between the entangled pairs, the quantum state hence contains no information about how individuals voted. If the two separated ballot authorities separately have attack for the scheme, then this attack will be detected one half of the time. After detecting the attack, the qubit system should be immediately returned to the voter following the action by tallyman for further confirmation. If the voters take attack together and compare the projections onto phase states, then the total particle number the attack should be altered on average with probability $(N-1)/N$.

3. Security Analysis

In this section, we will analyze the present protocols against some attacks. We are first concerned with an eavesdropping strategy that consists of applying a coherent attack on a qudit sequence of finite length. Here, we use an uncertainty principle by Hall that puts a limit on the sum of voters' and Eve's information when both groups measure the same quantum system.

Theorem: Assume Eve who is not one of the participants in the scheme implements the entangled state attack strategy, namely, Eve takes an attack strategy by applying an arbitrary operation U_{VE} on ballot state $|\mathcal{A}\rangle$. His intervention can then be detected by the agent, which implies that Eve can not change the ballot results of voters without being detected.

Proof: Suppose Eve tries to attack the scheme by entangling his own particle as an ancilla with the ballot state $|\mathcal{A}\rangle$. Without loss of generality, in the quantum anonymous traveling ballot scheme we consider that Eve wants to change the ballot result of voter V_k. Eve entangles her state $|E\rangle_k$ with V_k's ballot state in the quantum network. Correspondingly, the complex state of $|V_k\rangle$ and $|E\rangle_k$ can be denoted by $|V\rangle_{\text{VTE}}=|V_k\rangle\otimes|E\rangle_k$. At the voting site of V_k, unitary operation $U_{\text{VE}}^{(k)}$ applied by Eve on $|V\rangle_{\text{VTE}}$ yields

$$U_{\mathrm{VE}}^{(k)}|V\rangle_{\mathrm{VTE}} = \frac{1}{\sqrt{N}}\sum_{n=0}^{N-1}|n, N-1-n\rangle|E_n\rangle_k, \qquad (12)$$

where $\{E_n\colon n = 0, \ldots, N-1\}$ is a set of the Schmidt base. After voting by V_k, the ballot state should be

$$\begin{aligned}|T_{E_k}\rangle &= \mathcal{M}_k|U_{\mathrm{VE}}^{(k)}|\Phi\rangle_{\mathrm{VTE}} \\ &= \sum_{n=0}^{N}\exp(ia_k\theta_n)|n, N-1-n\rangle|E_n\rangle_k. \end{aligned} \qquad (13)$$

Denote $|\mathcal{A}''\rangle$ as the state held by the tallyman after voting. By computing $\langle\mathcal{A}''|\hat{T}_{E_k}|\mathcal{A}''\rangle$, where the form of $\hat{T}_{E_k}$ is similar to eq. (7), the tallyman may see that the total tally is changed. He then sends the states to corresponding voters to detect the destroyed votes. Therefore, whether V_k or not casts to $|\mathcal{A}\rangle$, the result can always be detected by voters, which implies that Eve cannot intervene the procession of the ballot.

In fact, denote $\hat{V}$ and $\hat{E}$ as voters' and Eve's measurement operators applied to the particles sent from agent, then

$$I_{AV_k} + I_{\mathrm{AE}} \leq 2\log_2(N\max_{k,j}|\langle v_k|e_{kj}\rangle|), \qquad (14)$$

where $|v_k\rangle$ and $|e_{kj}\rangle$ 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 qudit without knowledge of the basis chosen by agent. Because voters and Eve may get the same average information when measuring the different basis, one obtains the possible upper bound on I_{AE} for a given I_{AV_k} by assuming that Eve measures an observable $\hat{E}$ complementary to $\hat{V}_k$, i.e., $I_{AV_k} + I_{\mathrm{AE}} \leq 2\log_2 N$, for $|\langle v_k|e_{kj}\rangle| = N^{-1/2}, \forall k, j$. In order to ensure the security of the scheme with a nonzero rate, it should be $I_{AV_k} > I_{\mathrm{AE}}$. So, it may be introduced that $I_{AB} > (\log_2 N)/2$ is a sufficient condition against coherent attacks for a large number of candidates.[13] Q.E.D.

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

Here we only consider the case of a single ballot system of certain voter V_k, and mainly investigates how Eve makes an individual eavesdropping attack with a cloner to a single ballot site. Eve employs an unitary operator

$$U_{s,t} = \sum_{n=0}^{N-1}\exp(it\theta_n)|n+s\rangle\langle n|, \qquad (15)$$

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

$$|\mathcal{A}_E\rangle_{V_k} = \sum_{n=0}^{N-1}a_{s,t}U_{s,t}|n\rangle_{V_k}|B_{s,-t}\rangle_{E,E'}, \qquad (16)$$

where E and E' at right in above equation 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 a two-particle system

$$|B_{s,t}\rangle_{E,E'} = \frac{1}{N}\sum_{n=0}^{N-1}\exp(it\theta_n)|n\rangle_E|n+s\rangle_{E'}. \qquad (17)$$

Tracing the output joint state of eq. (16) over EE' held by the tallyman, implies that the agent's state $|\mathcal{A}\rangle_{V_k}$ is transformed, at voting sites, into the mixture

$$\rho_V = \sum_{s,t=0}^{N-1}|a_{s,t}|^2U_{s,t}|\mathcal{A}_E\rangle_{V_kV_k}\langle\mathcal{A}_E|U_{s,t}^{\dagger}. \qquad (18)$$

Thus, after the state $|\mathcal{A}\rangle_{V_k}$ undergoes a $U_{s,t}$, the error probability is $|a_{s,t}|^2$. On any ballot $|n\rangle$ in the computational basis, if voter V_k does not cast a vote for any candidate, 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, voter fidelity can be expressed as

$$F = \langle n|\rho_{V_k}|n\rangle = \sum_{t=0}^{N-1}|a_{0,t}|^2. \qquad (19)$$

Denote $|\bar{n}\rangle = \mathcal{F}|n\rangle$ as the dual of computational basis $|n\rangle$ of a candidate for $n = 0, \ldots, N-1$, where $\mathcal{F}$ is Fourier transform. If V_k casts a vote to the voting sites, then after a vote is cast by voter V_k Eve may get $U_{s,t}|\bar{n}\rangle = \exp(it\theta_{n+s})|\overline{n+s}\rangle$. So, the shift errors ($s \neq 0$) do not play any role and voters' fidelity becomes

$$\bar{F} = \langle\bar{n}|\rho_{V_k}|\bar{n}\rangle = \sum_{s=0}^{N-1}|a_{s,0}|^2. \qquad (20)$$

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 then clear from eq. (16) that Eve can obtain voter's shift error s simply by performing a partial Bell measurement on EE'. In order to infer agent's state, Eve must distinguish between N nonorthogonal states regardless of the measured value of s. Denote I_{AV_k} the corresponding mutual information between agent and voter V_k. By taking a 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, then with the great of candidates in the present scheme, it is sufficient that $I_{AV_k} > I_{\mathrm{AE}}$ for each voter V_k. Therefore, the introduced ballot is secure especially in a network election. Similarly, the attack strategy on the whole distributed ballot system of K entangled pairs can also be analyzed.

4. Conclusions

In this paper, we have introduced two kinds of quantum ballot to ensure an anonymous ballot in different scenarios. With all the information about the votes contained in the correlations between the particle systems, 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 made public, 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. Because of the minimal complexity in searching for the desired objects among the great of candidates, the present protocol may be applied to network voting with the development of quantum networks.

Acknowledgments

This work was supported by the Natural Science Foundation of China (No. 60773085).

References

1) D. Chaum: Commun. ACM **24** (1981) 84.
2) C. H. Bennett, D. P. DiVincenzo, J. Smolin, and W. K. Wootters: Phys. Rev. A **54** (1996) 3824.
3) V. Coffman, J. Kundu, and W. K. Wootters: Phys. Rev. A **61** (2000) 052306.
4) E. Knill, R. LaYamme, and G. Milburn: Nature **409** (2001) 46.
5) R. Raussendorf, D. E. Browne, and H. J. Briegel: Phys. Rev. Lett. **68** (2003) 022312.
6) A. Osterloh, L. Amico, G. Falci, and R. Fazio: Nature (London) **416** (2002) 608.
7) G. Vidal, J. I. Latorre, E. Rico, and A. Kitaev: Phys. Rev. Lett. **90** (2003) 227902.
8) J. A. Vaccaro, J. Spring, and A. Chefles: Phys. Rev. A **75** (2007) 012333.
9) M. Hillery, M. Ziman, V. Buzek, and M. Bielikova: Phys. Lett. A **349** (2006) 75.
10) S. Dolev, I. Pitowski, and B. Tamir: quant-ph/0602087.
11) A. D. Boozer, A. Boca, R. Miller, T. E. Northup, and H. J. Kimble: Phys. Rev. Lett. **98** (2007) 193601.
12) G. L. Long: Phys. Rev. A **64** (2001) 022307.
13) J. N. Cerf, M. Bourennane, A. Karlsson, and N. Gisin: Phys. Rev. Lett. **88** (2002) 127902.