Journal of Computers Vol. 28, No. 5, 2017, pp. 220-227
doi:10.3966/199115992017102805020

# A Secure Quantum Voting Protocol with Rich Roles

Xiaohua Liu[1*], Xiaojun Wen[1], Xincan Fan[1] and Junbin Fang[2]

[1] School of Computer Engineering, Shenzhen Polytechnic, Shenzhen, Guangdong, 518055, China.
Uoa18@163.com, szwxjun@sina.com, horsefxc@szpt.edu.cn

[2] Department of Optoelectronic Engineering, Jinan University, Guangzhou, Guangdong, 510632, China.
junbinfang@gmail.com

Received 25 October 2016; Revised 13 June 2017; Accepted 26 June 2017

Abstract. According to the actual demand of artificial vote in real life, the paper proposes a secure voting protocol based on quantum secret sharing. In the protocol, the four particles of each group of four-GHz-state are delivered to the voter Alice, the verifier Bob, the signatory and internal auditor Charlie and external auditor Trent respectively. Alice measures the particles of her own to vote her message out implicitly, and then Charlie, Bob, and Trent complete the rest signature, verification and audit work by measuring their own particles. Compared with previous protocols, the roles in the protocol are comprehensive and they can be substantially involved in voting related activities. In particular, the use of complex quantum fingerprint function is avoided, so the protocol is easy to implement technically.

Keywords: blind signature, quantum voting, unconditional security

## 1 Introduction

The main drawback of the traditional voting method is inefficient, it requires voters to the polling station to vote, and their voting information may be seen by people nearby in this case, it will cause psychological stress even to produce ideas of following the crowd to part of voters, because of this, the traditional voting method should be replaced by electronic voting method.

The strict definition of electronic voting is based on cryptography, through the network to complete the vote, and the secure electronic voting scheme should meet the following basic characteristics: legitimacy, anonymity, fairness, integrity and non - repeatability.

The industry has done a lot of researches on electronic voting method, and put forward some classic voting protocols [1], but most of these protocols are based on computational complexity problem such as large number factorization problem, discrete logarithm problem, quadratic residue problem etc. [2], however, these problems will gradually become unsafe in the background of attacker's computing resources increasing, so the classic electronic voting protocols will be eliminated sooner or later. Fortunately, the application of quantum physics in the field of cryptography can overcome the problems classic voting protocols faced, because the security of quantum cryptography is based on the inherent physical properties of quantum state rather than computational complexity, the quantum key distribution protocols such as BB84 and B92 have been strictly proved to be unconditionally secure [3].

The key technology used in electronic voting method is blind signature and group signature technology [2, 4]. At present, the researches on blind signature and group signature of quantum cryptography are not too many, there are some results such as WEN's [5-6]. Li and Zeng introduced two kinds of quantum voting mechanism through the use of quantum entanglement to ensure that anonymous voting can be achieved in different situations [7]. Li and Zeng uses two non-coupling quantum links and a polling state to transfer the votes among different votes to propose a quantum network voting mechanism with anonymity and security [8], after the voting is over, the voting state will be sent to the authorities for counting and publishing. Naseri, Gong, Houshmand and Matin proposed a new anonymous survey

* Corresponding Author

protocol with authentication based on the three GHz state and quantum ultra-dense coding [9]. Wen, Tian and Niu, Wen and Cai presented a strong blind signature protocol based on the principle of quantum secret sharing [10-11], the protocol indeed implements the signature's blindness and the message owner's untraced ability, and its security is not affected by the computing resources owned by the attacker, so it can be used in electronic voting. The main flaw of this protocol is that the audit is ex post facto, the possible fraud cannot be found immediately. In addition, the protocol uses quantum fingerprint function which is difficult technically to prevent fraud, so it is difficult to implement. Wen et al. aiming at the deficiency of the literature [10], adjusted the quantum voting model, and introduced a variety of roles in the voting, among them, Alice is the voter, Charlie is the signer (and the internal auditor), Bob is the verifier, Trent is the external auditor, Bob and Charlie belong to the ballot management center, the division of labor is closer to real life, so it's easy to be adopted in reality. In addition, the audit is immediate rather than ex post facto, accordingly, the quantum fingerprint function [12] can be discarded so that the protocol can be implemented more easily.

## 2 Basic Principle

The four particle GHZ entangled state we used in this protocol is a maximally entangled state, take $B_z = \{|0\rangle, |1\rangle\}$ as the basic vectors, its quantum state can be expressed as

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle_a |0\rangle_b |0\rangle_c |0\rangle_t + |1\rangle_a |1\rangle_b |1\rangle_c |1\rangle_t), \tag{1}$$

where the subscript a, b, c and t show that the corresponding particles are owned by Alice, Bob, Charlie and Trent respectively.

Define the coordinate system $\mathrm{H_x}$ in the two dimensional Hilbert space, its corresponding basis vectors are $B_x = \{|+x\rangle, |-x\rangle\}$. Express the base vectors $B_x$ using the base vectors $B_z$, we have

$$|+x\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), |-x\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle); \tag{2}$$

On the contrary, the base vectors $B_z$ can be expressed using the base vectors $B_x$ according to the formula 2,

$$|0\rangle = \frac{1}{\sqrt{2}}(|+x\rangle + |-x\rangle), |1\rangle = \frac{1}{\sqrt{2}}(|+x\rangle - |-x\rangle). \tag{3}$$

According to the formula 3, we have

$$|0\rangle_a = \frac{1}{\sqrt{2}}(|+x\rangle_a + |-x\rangle_a), |1\rangle_a = \frac{1}{\sqrt{2}}(|+x\rangle_a - |-x\rangle_a) \tag{4}$$

Substitute formula 4 into formula 1, then GHZ four particle entangled state can be expressed as

$$|\psi\rangle = (\frac{1}{\sqrt{2}}|+x\rangle_a)[\frac{1}{\sqrt{2}}(|0\rangle_b |0\rangle_c |0\rangle_t + |1\rangle_b |1\rangle_c |1\rangle_t)] + (\frac{1}{\sqrt{2}}|-x\rangle_a)[\frac{1}{\sqrt{2}}(|0\rangle_b |0\rangle_c |0\rangle_t - |1\rangle_b |1\rangle_c |1\rangle_t)] \tag{5}$$

The above formula shows that if the measurement result of Alice is $|+x\rangle$, then the GHZ four-state will collapse to the following state

$$|\psi\rangle' = \frac{1}{\sqrt{2}}(|0\rangle_b |0\rangle_c |0\rangle_t + |1\rangle_b |1\rangle_c |1\rangle_t). \tag{6}$$

If the measurement result is $|-x\rangle$, then the GHZ four-state will collapse to the following state

$$|\psi\rangle' = \frac{1}{\sqrt{2}}(|0\rangle_b|0\rangle_c|0\rangle_t - |1\rangle_b|1\rangle_c|1\rangle_t). \quad \textbf{(7)}$$

Substitute formula 3 into formula 6, then the GHZ three-state can be expressed as follows

$$|\psi\rangle' = \frac{1}{2}[(|+x\rangle_b|+x\rangle_c + |-x\rangle_b|-x\rangle_c)|+x\rangle_t + (|+x\rangle_b|-x\rangle_c + |-x\rangle_b|+x\rangle_c)|-x\rangle_t], \quad \textbf{(8)}$$

It is showed that there is a quantum correlation between particle b, c and t, and we can combine the measurement results of particle c and b to determine the quantum state of particle t. For example, Charlie and Bob adopt the orthogonal measurement method $\sigma_x^B \otimes \sigma_x^C$ ($\sigma_x = |+x\rangle\langle+x| + |-x\rangle\langle-x|$ in this formula) to measure their own particles together, if the measurement results are the same, then it indicates that the quantum state of particle t must be $|+x\rangle$. If the measurement results are opposite, then it indicates that the quantum state of particle t must be $|-x\rangle$. The quantum correlations between the particles b, c and t are shown in Table 1.

**Table 1.** The quantum correlations between the particles b, c and t

| If $\|+x\rangle_a$ | $\|+x\rangle_c$ | $\|-x\rangle_c$ |
|---|---|---|
| $\|+x\rangle_b$ | $\|+x\rangle_t$ | $\|-x\rangle_t$ |
| $\|-x\rangle_b$ | $\|-x\rangle_t$ | $\|+x\rangle_t$ |

Formula 8 and Chart 1 demonstrate the quantum correlation between particles b, c, and t when particle a is measured as $|+x\rangle_a$.

Similarly, substitute formula 3 into formula 7, then the GHZ three-state can be expressed as follows

$$|\psi\rangle' = \frac{1}{2}[(|+x\rangle_b|+x\rangle_c + |-x\rangle_b|-x\rangle_c)|-x\rangle_t + (|+x\rangle_b|-x\rangle_c + |-x\rangle_b|+x\rangle_c)|+x\rangle_t], \quad \textbf{(9)}$$

Formula 9 demonstrates the quantum correlation between particles b, c, and t when particle a is measured as $|-x\rangle$ by Alice. We can combine the measurement results of particle c and b to determine the quantum state of particle t also. For example, Charlie and Bob adopt the orthogonal measurement method $\sigma_x^B \otimes \sigma_x^C$ to measure their own particles together, if the measurement results are the same, then it indicates that the quantum state of particle t must be $|-x\rangle$. If the measurement results are opposite, then it indicates that the quantum state of particle t must be $|+x\rangle$. The quantum correlations between the particles b, c and t are shown in Table 2.

**Table 2.** The quantum correlations between the particles b, c and t

| If $\|-x\rangle_a$ | $\|+x\rangle_c$ | $\|-x\rangle_c$ |
|---|---|---|
| $\|+x\rangle_b$ | $\|-x\rangle_t$ | $\|+x\rangle_t$ |
| $\|-x\rangle_b$ | $\|+x\rangle_t$ | $\|-x\rangle_t$ |

## 3 Protocol Description

### 3.1 Protocol Initialization

**Step 1.** Charlie prepares entangled particle of GHZ four-state sequences. Charlie prepares Q (Q>N) groups GHZ four-state entangled particles whose quantum state is $|\psi\rangle_{abct}$ represented as $\{|\psi(1)\rangle_{abct},|\psi(2)\rangle_{abct},...,|\psi(i)\rangle_{abct},...,|\psi(Q)\rangle_{abct}\}$, in which:

$$|\psi(i)\rangle_{abct}=\frac{1}{\sqrt{2}}(|0_{a_i}\rangle|0_{b_i}\rangle|0_{c_i}\rangle|0_{t_i}\rangle+|1_{a_i}\rangle|1_{b_i}\rangle|1_{c_i}\rangle|1_{t_i}\rangle),i=1,2,...,Q \quad \textbf{(10)}$$

**Step 2.** Charlie distributes the GHZ particles. For each group of four particles, Charlie leaves the particle $c_i$ to himself, and then distributes the particle $a_i$, $b_i$ and $t_i$ to Alice, Bob and Trent respectively.

**Step 3.** Detect the security of the quantum channel. In order to prevent intercept-resend attack or man-in-middle attack, it is necessary to detect the security of quantum channel. First, Charlie randomly selects $Q-N$ particles from his own particles, and randomly selects $+x$ direction or $-x$ direction to measure them, then he publicly announces the number of these particles in the sequence and the measurement results. Subsequently, Alice, Bob and Trent in turn measure the particles of the same number of their own in $+x$ direction or $-x$ direction. Four people compare the measurement results publicly. If the relationship of these results satisfy the basic principle, then there is no such situation of intercept-resend attack or man-in-middle attack. Then, the remaining N groups of four entangled particles are shared by communication four people, thus a secure quantum channel is established between Alice, Bob, Charlie and Trent.

**Step 4.** Distribute quantum keys between Trent and Bob, as well as between Charlie and Trent securely. Distribute and share the $N-bit$ quantum key $K_{tb}$ and $K_{tc}$ respectively between Trent and Bob, as well as between Trent and Charlie based on the famous BB84 protocol, where $N$ is the number of bits of information contained in each standard ballot.

### 3.2 Voting Stage

Voter Alice holds particle $a_i$, $i=1,2,...,N$. Alice's voting information M is a standard vote, it's n bit binary sequence as previously mentioned. That is:

$$M=\{m(1),m(2),...,m(i),...,m(N)\},i=1,2,...,N,m(i)\in\{0,1\} \quad \textbf{(11)}$$

Alice measures the particles in her own hand according to the value of $m(i)$, but she does not publish the measurement results.

$$\text{The measurement direction of Alice}=\begin{cases}+x,m(i)=0\\-x,m(i)=1\end{cases}$$

Taking $+x$ direction measurement as an example, the specific measurement tools can be used to make the particle collapse to the $|+x\rangle$ state, then the measurement result is $|+x\rangle$, the other direction is similar. After completion of the voting, the GHZ four state $|\psi\rangle_{abct}$ collapses into a GHZ three state $|\psi\rangle'_{bct}$, the three state $|\psi\rangle'_{bct}$ already contains the voting information M.

### 3.3 Signature, Verification and Audit Stage

**Step 1.** Because both Bob and Charlie belong to the ballot management center, so they are qualified for jointly measuring the particles of their own in the base $B_x=\{|+x\rangle,|-x\rangle\}$. The implementation of the joint measurement covers Charlie's signature of the voting message. The results of this joint measurement have four combinations, as shown in Table 3.

**Table 3.** The results of this joint measurement have four combinations

| The measurement result of $c_i$ | $\|+x\rangle$ | $\|+x\rangle$ | $\|-x\rangle$ | $\|-x\rangle$ |
|---|---|---|---|---|
| The measurement result of $b_i$ | $\|+x\rangle$ | $\|-x\rangle$ | $\|+x\rangle$ | $\|-x\rangle$ |
| The joint measurement result cb(i) | 00 | 01 | 10 | 11 |

The joint measurement results for all particles ( $b_i$ s and $c_i$ s ) are expressed as:

$$CB = \{cb(1), cb(2), ..., cb(i), ..., cb(N)\}, i = 1, 2, ..., i, ..., N \quad \textbf{(12)}$$

CB information are jointly owned by both Charlie and Bob, thus Charlie achieves the effective supervision of Bob.

**Step 2.** Charlie encrypts CB information using One-Time Pad Algorithm and key $K_{tc}$, then he gets $E_{k_{tc}}(CB)$, subsequently Charlie sends $E_{k_{tc}}(CB)$ to the external auditor Trent.

**Step 3.** The external auditor Trent measures the particle $t_i$ of his own using base $B_x = \{|+x\rangle, |-x\rangle\}$, the measurement result is expressed as

$$t(i) = \begin{cases} 0, |t_i\rangle = |+x\rangle \\ 1, |t_i\rangle = |-x\rangle \end{cases},$$

The measurement result of all of particle $t_i$ are expressed as

$$T = \{t(1), t(2), ..., t(i), ..., t(N)\}, i = 1, 2, ..., N . \quad \textbf{(13)}$$

Trent encrypts T information using One-Time Pad Algorithm and key $K_{tb}$, then he gets $E^2_{k_{tb}}(T)$, subsequently Trent sends $E^2_{k_{tb}}(T)$ to the verifier Bob.

**Step 4.** Bob decrypts $E^2_{k_{tb}}(T)$ received from Trent using key $K_{tb}$, then he gets the T information.

**Step 5.** Verifier Bob can figure out the blind vote information $M'$ of Alice's according to T, CB and the four particle association rules described in the basic principle, and then he can calculate the voting information M of Alice's easily.

**Step 6.** Bob announces the M and CB information publicly.

**Step 7.** Charlie is a signatory, and he is an internal auditor at the same time. Charlie checks the CB information, if he finds out that the CB information announced by Bob is wrong, then he will refuse to accept the election result M, if he finds out that the CB information announced by Bob is correct, then the process continues.

**Step 8.** The external auditor Trent audits the quantum correlations between M, CB, and T information according to quantum correlation rules described in the basic principle, if the correlation meets the rules, then the audit result is passed, the results of the vote are accepted.

Fig. 1 as follows shows part of the interactive processes in the protocol.

## 4 Security Analysis and Discussion

### 4.1 Protocol Can Satisfy the Security of Electronic Voting

This quantum voting protocol satisfies the security requirements of the traditional electronic voting protocol.

**The legitimacy and the blindness of the signature.** In this protocol, Charlie signs for the voting information by measuring, thus ensures the legitimacy of the voting information. But he is unable to know the details of the Alice's vote when he signs, so Charlie's signature is blind.

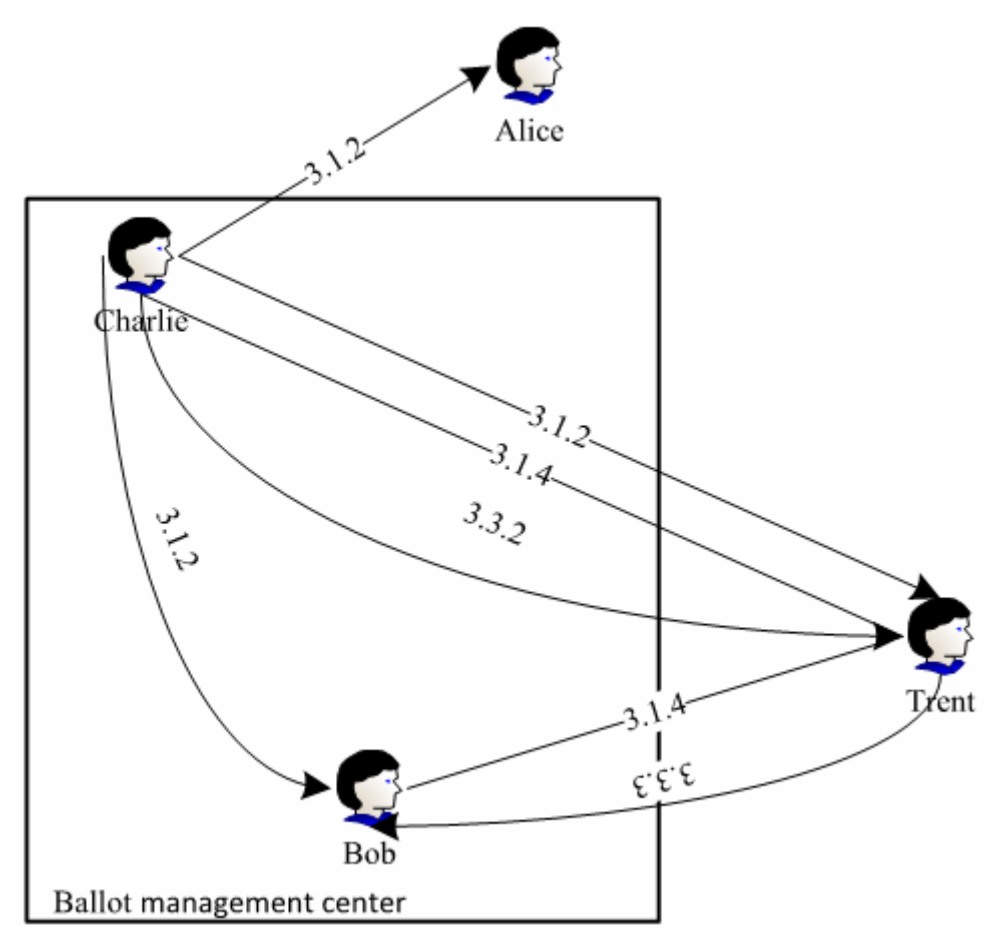


**Fig. 1.** The interactive processes in the protocol

**Anonymity.** Electronic voting must take steps to make it impossible for anyone to connect the voters with their votes. In this protocol, Alice sends voting information out then exit immediately by measuring a particle in the GHZ-four-state, because she did not leave any personal characteristics in voting information, so Alice cannot be traced.
**Fairness.** In this protocol, Bob needs to use external auditor Trent's measuring result to verify the voting results, this balances the power of the Bob to ensure the fairness of the vote.
**Integrity.** All particles in this voting protocol will be measured, once the particle of a party has not been measured, he immediately realizes the fault with the counting and the counting process is not complete.
**Non-repeatability.** In this protocol, a person who has been proved to be a legal voter can only receive a single particle, so no one can repeat to vote.

### 4.2 Protocol Can Prevent Fraud

Bob, Charlie and Trent can only get part of the secret information, so their measurements are blind, they cannot completely determine the final results of the vote. The results obtained by Bob's verification will be immediately subject to internal and external audit, the abnormal results of the vote will be found even if the forgery exists.

### 4.3 Protocol Is Secure Against Quantum Attack

After establishing a secure quantum channel, Alice's vote information eventually passes to the verifier Bob through Entanglement properties between GHZ four particles, this result will not be intercepted or tampered with by an attacker. The intermediate measurement results transferred between Trent and Charlie and between Trent and Bob are encrypted by One-Time Pad Algorithm, they are secure, too.

### 4.4 Unconditional Security of the Protocol

In order to guarantee the unconditional security of the protocol, the security of the protocol should be independent of the computing resources owned by attacker.

**Unconditional security of key distribution.** In this protocol, the quantum key $K_{tb}$ shared by Trent and Bob and the quantum key $K_{tc}$ shared by Trent and Charlie are distributed by BB84 protocol, this has proved to be unconditionally secure.

**Unconditional security of encryption algorithm.** The One-Time Pad Algorithm used to encrypt information between Trent and Bob as well as between Trent and Charlie has been shown to be unconditionally secure.

**Unconditional security of transmission channels.** In this protocol, in the process of voting, signature, verification and audit, the instantaneous transfer of information in the quantum channel is realized by measuring the entangled state of GHZ four-particle. According to the principle of quantum mechanics, the transmission is not limited by time and distance, and will not be blocked by any obstacle.

## 5 Conclusion

In the scene we designed, the voting activity is initiated by the ballot management center. After the voter casts the ballot, the ballot is signed by the signer, and then verified by the verifier. In order to guarantee the credibility of the vote, we innovatively introduce the external supervisor to take the external supervision as a real link of the voting activity. So we introduce the quartet when the protocol is implemented, namely, the voter Alice, the verifier Bob, the signer and internal auditor, Charlie, and the external auditor, Trent. As the title of this paper says, this voting protocol's participants have rich roles. In this paper, according to the election activities depicted above, we propose a new quantum voting model which is easy to implement. In this model, we introduce internal audit and external audit simultaneously, and external auditor participates in the measurement. In order to achieve unconditional security, we fulfill the protocol by using the entanglement properties of four particle GHZ state. The protocol is secure and reliable, especially it does not require complicated quantum fingerprint function.

## Acknowledgements

The work is supported by the Guangdong Provincial Natural Science Foundation (Grant No. 2016A030313023), and the Shenzhen Basic Research Project (Grant No. JCYJ20160322114027138).

## References

[1] J. Jan, C. Tai, A secure electronic voting protocol with IC cards, Journal of Systems and Software 39(2)(1997) 93-101.

[2] C.I. Fan, C.L. Lei, Efficient blind signature scheme based on quadratic residues, Electronic Letters 32(9)(1996) 811-813.

[3] P.W. Shor, J. Preskill, Simple proof of security of the BB84 quantum key distribution protocol, Physical Review Letters 85(2)(2000) 441-444.

[4] D. Chaum, E. Heyst, Group signature, in: Proc. Advances in Cryptology –Eurocrypt'91, 1992.

[5] X. Wen, X. Niu, L. Ji, Y. Tian, A weak blind signature scheme based on quantum cryptography, Optics Communications 282(4) (2008) 666-669.

[6] X. Wen, Y. Tian, X. Niu, A group signature scheme based on quantum teleportation, Physica Scripta 81(2010) 055001-055005.

[7] Y. Li, G. Zeng, Quantum anonymous voting systems based on entangled state, Optical Review 15(5)(2008) 219-223.

[8] Y. Li, G. Zeng, Anonymous quantum network voting scheme, Optical Review 19(3)(2012) 121-124.

[9] M. Naseri, L.H. Gong, M. Houshmand, L.F. Matin, An anonymous surveying protocol via Greenberger-Horne-Zeilinger

states, International Journal of Theoretical Physics 55(10)(2016) 4436-4444.

[10] X. Wen, Y. Tian, X. Niu,. A strong blind quantum signature protocol based on secret sharing, ACTA ELECTRONICA SINICA 38(3)(2010) 720-724.

[11] X. Wen, X. Cai, Secure quantum voting protocol, Journal of Shandong University(Natural Science) 46(9)(2011) 9-13.

[12] H. Buhrman, R. Cleve, J. Watrous, R. Wolf, Quantum fingerprinting, Physical Review Letters 87(2001) 167902-167904.