www.nature.com/scientificreports

SCIENTIFIC REPORTS

OPEN

A simple quantum voting scheme with multi-qubit entanglement

Peng Xue[1,2] & Xin Zhang[1]

Received: 17 February 2017
Accepted: 3 July 2017
Published online: 08 August 2017

We propose a simple quantum voting scenario with a set of pairs of particles in a multi-particle entangled state. This scenario is suitable for large scale general votings. We also provide a proof of security of our scheme against the most general type of attack by generalizing Shor and Preskill's proof of security of the other schemes.

Cryptography is the art of rendering a message unintelligible to any unauthorized party. Over one century, many applications of classical cryptography have been discovered. One of the most outstanding applications is secure voting. Classical secret voting protocols have been investigated by many researchers from both the practical and theoretical points of view[1–9]. Let us briefly review the goal of a secure voting scheme. Usually, a classical secure voting scheme requires the following conditions: 1 Only the votes of the authorized voters can be taken into account; 2 Every interested voter must vote exactly once. Voting more than once can not be accepted by the administrator and other voters; 3 No one can control other voters' opinions about the issues to be voted upon; 4 No one can duplicate the votes of the other voters from being detected by the administrator and other voters. For any classical voting scheme, the electronic votes can be easily duplicated; 5 No one can change the votes of the other voters from being detected by the administrator and the other voters; 6 Every voter can confirm that her/his vote is taken into account by the administrator. In addition, sometimes, secret ballot is needed.

Unfortunately, security of classical cryptography is based on the unproven complexity of calculating certain functions, such as the difficulty of factoring large integers. However, the recent work in quantum computation[10] shows that quantum computers can, at least in principle, factor much faster than classical computers, which means that classical cryptography is already insecure.

The security of quantum cryptography is based on the fundamental postulate of quantum physics that "every measurement perturbs a system". Indeed, passive monitoring of transmitted signals is strictly forbidden in quantum mechanics. The "quantum no-cloning theorem[11, 12]" indicates that it is impossible to make an exact copy if an unknown quantum state.

It is known that for some tasks such as bit commitment, quantum mechanics can not help[13, 14]. However for others, such as quantum voting, a number of novel quantum protocols have been developed[7, 15–22]. Quantum cryptography brings an entirely new way of solving the secure voting problem.

In this paper, we propose a simple quantum voting scheme for world environments with the following conditions: (a) This protocol involves voters and an administer who also plays a role as a counter, and a scrutinizer. If the issue of votes are controlled by a single administrator, sh/he may add extra votes as she/he wished. To overcome this problem, the whole election should be monitored by a scrutinizer in our protocol; (b) The six conditions required in classical secure voting are satisfied in our protocol; (c) The computations among voters are independent without the requirement of any global computation and a voter only has to communicate with the scrutinizer and finally sends his vote to the counter (administrator). So this protocol is suitable for large scale general elections; (d) Its security is guaranteed by the fundamental postulate of quantum physics; (e) The physical requirements of the scheme well fit the current experimental technique. The validity of the result is base on the assumption that one of the administrator and scrutinizer is absolutely trusted at least.

Results

Suppose that Alice is one of the voters, and there are an administrator named Bob and a scrutinizer named Carol which are equal in status and supervise each other's performance. If one of them wants to cheat in the election, it can be detected by the other. Carol prepares M pairs of particles in Greenbergee-Horne-Zeilinger (GHZ) type of maximally entangled state

[1]Department of Physics, Southeast University, Nanjing, 211189, China. [2]State Key Laboratory of Precision Spectroscopy, East China Normal University, Shanghai, 200062, China. Correspondence and requests for materials should be addressed to P.X. (email: gnep.eux@gmail.com)

$\boldsymbol{b_l}$	$\boldsymbol{B_{bl}^2}$	$\boldsymbol{C_{bl}^3}$	$\boldsymbol{\vert\psi\rangle_f = I^1 \otimes B_{b_l}^2 \otimes C_{b_l}^3 \vert\psi\rangle_i}$
0	I	I	$\frac{1}{\sqrt{2}}(\vert000\rangle \pm \vert111\rangle)$
1	I	σ_x	$\frac{1}{\sqrt{2}}(\vert001\rangle \pm \vert110\rangle)$
2	σ_z	I	$\frac{1}{\sqrt{2}}(\vert000\rangle \mp \vert111\rangle)$
3	σ_z	σ_x	$\frac{1}{\sqrt{2}}(\vert000\rangle \mp \vert111\rangle)$
4	σ_x	I	$\frac{1}{\sqrt{2}}(\vert010\rangle \pm \vert001\rangle)$
5	σ_x	σ_x	$\frac{1}{\sqrt{2}}(\vert011\rangle \pm \vert100\rangle)$
6	$-i\sigma_y$	I	$\frac{1}{\sqrt{2}}(\vert010\rangle \mp \vert101\rangle)$
7	$-i\sigma_y$	σ_x	$\frac{1}{\sqrt{2}}(\vert011\rangle \mp \vert100\rangle)$

Table 1. Here, initially the particles 1, 2 and 3 are in the GHZ state $|\psi\rangle_i = \frac{1}{\sqrt{2}}(|000\rangle \pm |111\rangle$ which is determined by the result of the GHZ measurement on the rest qubits 4, 5 and 6. After a certain operation, the three qubits will be in the final state $|\psi\rangle_f$ if σ_x, σ_y and σ_z are Pauli operators.

$$\begin{aligned} |\varphi\rangle &= \frac{1}{\sqrt{2}}(|000000\rangle + |111111\rangle) \\ &= \frac{1}{(2\sqrt{2})}(|000\rangle + |111\rangle)_{123}(|000\rangle + |111\rangle)_{456} \\ &\quad + \frac{1}{(2\sqrt{2})}(|000\rangle - |111\rangle)_{123}(|000\rangle - |111\rangle)_{456}. \end{aligned} \tag{1}$$

Particles 1 is sent to Bob, particles 2 and 3 are sent to Alice and particles 4, 5 and 6 are left for Carol herself. Alice receives the particles from Carol and encodes her opinion on the vote, which is represented in binary notation as $a \in \{000, 001, \ldots, 111\}$, by performing the operation $B_b \otimes C_c$ corresponding to $b = g(a)$ on them (See Table 1), where $g(x)$ is bijection.

Remarkably, in order to keep the votes from being duplicated, the voters perform the voting process with probability $1 - \varepsilon$ and the detecting process with probability ε, where $0 < \varepsilon < 1$.

Suppose there are n candidates to be voted, which are coded in binary notation. In the voting process, Alice sends the two resulting particles (three bits of information) representing her opinion on vote to Bob every time. This kind of communication has be done for N times in all. Then the vote from Alice can be represented as $\upsilon = (\sum_{l=1}^{N} a_l) \bmod n$.

The voters, administrator and scrutinizer are connected by a quantum channel and a classical public channel. They follow the below procedures.

1 With probability $1 - \varepsilon$, Alice performs the voting process. She randomly chooses a coding scheme g: $\{0, 1, \ldots, 7\} \rightarrow \{B_0 \otimes C_0, B_1 \otimes C_1, \ldots, B_7 \otimes C_7\}$.

Suppose this is the l th part of opinion on her vote. She encodes the value by performing the operation corresponding to $b_l = g(a_l)$ on the particles 2 and 3. Even if there is any eavesdropper Eve who tries a "man-in the middle" attack[23] to duplicate the vote finds out which operation Alice has performed, she still does not know her message. The coding scheme g acts as a secret key used by Alice. Here, there are eight unitary operations $B_{b_l} \otimes C_{b_l}$ (seeing Table 1) on the particles 2 and 3. This process is similar to the scheme of densecoding using multiparticle quantum channel[24].

Then, she sends the resulting particles 2 and 3 to the administrator Bob.

2 At the same time, Carol makes a GHZ measurement on the particles 4, 5 and 6 and announces the result over the public channel. Then, she sends the particle 6 to Alice, and the rest particles are left for herself.

3 Bob receives Particles 2 and 3 and measures the three qubits resulting in the final state $|\psi\rangle_f$ if along the GHZ basis. According to the result of Carol's measurement, he learns the form of the operation $B_{b_l} \otimes C_{b_l}$ (that is b_l), but not the three bits of information representing one part of Alice's opinions about the issues to be voted upon.

4 In the meantime of Step 1, with probability ε, Alice performs the detecting process. She measures the particle 2 along the orthogonal basis $\{| + \rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), | - \rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\}$. The particles 1 and 3 will be in one of the two EPR states $|\Phi\pm\rangle = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle)$ with the same probability determined by both of the results of the measurement of Carol and Alice. Alice randomly chooses one out of the rectilinear $(\{|0\rangle, |1\rangle\})$ and orthogonal bases and measures particle 3 along it. Then she announces the two results of her measurement and the basis she has chosen.

5 If Bob has received the information over the public channel (not the particles), he will also perform the detecting process. He measures his particle 1 along the same basis and detects the correlations of the particles 1, 2 and 3. For example, if Carol measure the particles 4, 5 and 6 and gets the state $|\psi\rangle_{456} = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)_{456}$, the rest particles 1, 2 and 3 will be in the same state $|\psi\rangle_{123} = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)_{123}$. If the result of Alice's measurement

$\|\psi\rangle_{456}$ ($\|\psi\rangle_{123}$)	$\frac{1}{\sqrt{2}}(\|000\rangle + \|111\rangle)$	$\frac{1}{\sqrt{2}}(\|000\rangle + \|111\rangle)$	$\frac{1}{\sqrt{2}}(\|000\rangle + \|111\rangle)$	$\frac{1}{\sqrt{2}}(\|000\rangle + \|111\rangle)$
result 1 (Alice)	$\frac{1}{\sqrt{2}}(\|0\rangle - \|1\rangle)$	$\frac{1}{\sqrt{2}}(\|0\rangle - \|1\rangle)$	$\frac{1}{\sqrt{2}}(\|0\rangle - \|1\rangle)$	$\frac{1}{\sqrt{2}}(\|0\rangle - \|1\rangle)$
$\|\phi\rangle_{13}$	$\|\Phi^-\rangle$	$\|\Phi^-\rangle$	$\|\Phi^-\rangle$	$\|\Phi^-\rangle$
basis(Alice)	$\{\|0\rangle, \|1\rangle\}$	$\{\|0\rangle, \|1\rangle\}$	$\{\|+\rangle, \|-\rangle\}$	$\{\|+\rangle, \|-\rangle\}$
result 2 (Alice)	$\|0\rangle$	$\|1\rangle$	$\|+\rangle$	$\|-\rangle$
result 3 (Bob)	$\|0\rangle$	$\|1\rangle$	$\|-\rangle$	$\|+\rangle$

Table 2. Example of the detecting process. Here $\{|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\}$ represents the + $|\Phi^-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$.

is $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$, the results of correlation detection are shown in Table 2. If the number of the mismatches r (here, mismatch means the results of Alice and Bob are not correlated), the error rate of the channel is estimated as $e = (r)/(m)$ (m is the number of the pairs of particles used to detect the security of the quantum channel).

$$m = \varepsilon M. \tag{2}$$

Note that the test samples m are sufficiently large, the estimated error rates e should be rather accurate. Now they demand that $e < e_{max}$ where e_{max} is a prescribed maximally tolerable error rate. In our scheme, after Alice measures her particles with the orthogonal basis, the detection process is equal to that of a modified EPR scheme[25, 26]. Please see refs 26–28 for details. If the constraint is satisfied, it has been proved that the error rate of the signal is also small enough to allow the stabilizer code to correct. Then they proceed to the next steps. Otherwise, they re-start the whole procedure.

6 Then Alice announces the coding scheme g, that is the relation among a_l, b_l and the corresponding operations.

7 Bob calls out the vote, but the other voters apart from the scrutinizer do not know who has sent this vote.

8 Since Carol and Alice share another GHZ state $|\psi\rangle_{456}$, she can send a return receipt to Alice and make her to confirm her vote is taken into the results of the election. This step is achieved as Alice just has done. Carol performs the process to send receipt with probability $1 - \varepsilon$ as the modified densecoding using GHZ channel (seeing Steps 1 and 3). Or, she may perform the detecting process with ε to ensure the security of the channel (seeing Steps 5 and 6).

Since the security of our protocol is proven in Step 5, here, we show a data analysis guarantees the security of this protocol against a "man-in the middle" strategy[23]. An eavesdropper Eve intercepts and catches the two particles from Carol and prepares another GHZ state $|\psi^e\rangle_{123} = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)_{123}$, and sends two particles to Alice. Then she catches the resulting qubits and makes a GHZ measurement on them to obtain the operation Alice has performed. She put the same operation on the initial particles which she has intercepted from Carol and sends them to Bob. Such an attack is called a "man-in-the-middle" attack.

If Eve is really smart she will try a man-in-the middle attack and duplicate the votes from the authorized voters. However, the voter will perform the detecting process with probability ε. So Eve has no chance to adapt her strategy. Then, an error rate is introduced showing the wrong type of correlation in the detecting process with probability $\frac{1}{4}$. That is with probability $\frac{1}{4}$ Eve is detected. Since the probability for a detecting process is ε, for M pairs of particles, there are m pairs of particles are used to detect the security of channel (seeing Eq. 2). If Eve attacks all the time, the probability that she will not be detected with probability P_d.

$$P_d = \left(\frac{3}{4}\right)^m. \tag{3}$$

which is goes to 0 as m is large enough.

Except for "man-in-the middle" attack, we will analyze the protocol against some other outsider's attack, such as "entangle-and-measure attack". Assume Eve applies the entangled state attack strategy. Namely, Eve takes an attack strategy by applying an arbitrary operation on her own ancillary state and the ballot state (particles 1, 2 and 3) which entangles the ancilla and the particles 1, 2, and 3. Her intervention can then be detected by the administrator Bob, which implies that Eve cannot change the ballot results of voters without being detected. Suppose Eve tries to attack the scheme by entangling her own particle as an ancilla with the ballot state. After voting, the administrator Bob may notice the entangled state which is shared with Alice previously is changed in Step 5. He then sends the states to corresponding voters to detect the destroyed votes. Therefore, whether or not Eve casts to the ballot state, the result can always be detected by voter Alice, which implies that Eve cannot intervene the procession of the ballot. Furthermore, the protocol can be further improved by introducing decoy state. To counter this attack, the decoy states are randomly inserted and when they are examined for security, the total detection probability of Eve is decreased by taking into account that the probability of generation of each decoy state.

There are still many questions that remain open and deserve further detailed investigation. Primarily, it is the analysis of the security of quantum voting against more sophisticated attacks, such as collaborating parties, the use of illegal voting operations, and cheating authorities that deserve further attention.

Discussion

Quantum secure voting could also be realized by using quantum key distribution. Each authorized voter encrypts her/his vote using quantum key, and sends it to the administrator who shares the key. Then, she/he decrypts the encrypted message and obtains the vote. Since this protocol needs a multi-party quantum key distribution between the administrator and each voter at first, it will bring vast waste of quantum resource. In our protocol, the voting is a deterministic process and does not need either a quantum key distribution or a teleportation compared to the previous protocols. There are one administrator and scrutinizer which supervise each other's performance and prevent other one from cheating. It is needed that one of them is absolutely trusted at least. We also prove that the protocol is secure against some outsider's attacks such as man-in-the-middle and entangle-and-measure attacks. Since the computations among voters are independent without the need of any global computation and every voter only has to communicate with the scrutinizer and finally sends his vote to the administrator, this protocol is suitable for large scale general elections and allows to be within the reach of current technology.

References

1. Fujioka, A., Okamoto, T. & Ohta, K. A practical secret voting scheme for large scale elections. *Lecture Notes in Computer Science (LNCS)* **718**, 244–251 (1992).
2. Lversen, K. R. Lecture Notes in Computer Science. *Advances in Cryptology: L'roc. of Crypt'91, LNCS* **576**, 405 (1991).
3. Nurmi, H., Salomaa, A. & Santean, L. Secrete ballot elections in computer networks. *Computers Security* **10**, 553–560 (1991).
4. Yao, A. L' *roc. 23rd Annual IEE Symp. on the Foundations of Computer Science* **23**, 160 (1982).
5. Chaum, D. Advances in Cryptology: L'roc. of EuroCrypt' 88. *LNCS* **330**, 177 (1988).
6. Wang, Q., Yu, C., Gao, F., Qi, H. & Wen, Q. Self-tallying quantum anonymous voting. *Phys. Rev. A* **94**, 022333 (2016).
7. Tian, J. H., Zhang, J. Z. & Li, Y. P. A voting protocol based on the controlled quantum operation teleportation. *Int. J. Theor. Phys.* **55**, 2303–2310 (2016).
8. Li, Y. & Zeng, G. H. Anonymous quantum network voting scheme. *Optical Review* **19**, 121C124 (2012).
9. Guo, Y., Feng, Y. Y. & Zeng, G. H. Quantum anonymous voting with unweighted continuous-variable graph states. *Quantum Information Processing* **15**, 3327C3345 (2016).
10. Shor, P. Proc. of 35th Annual Symposium on the Foundations of Computer Science. (IEEE Computer Society, Los Alamos), p. 124 (Extended Abstract). Full version of this paper appears in S. I. A. M. Journal on Computing. **26**, 1484 (1997).
11. Dieks, D. Communication by EPR devices. *Phys. Lett. A* **92**, 271–272 (1982).
12. Wootters, W. K. & Zurek, W. A single quantum cannot be cloned. *Nature (London)* **299**, 802–803 (1982).
13. Lo, H. K. & Chau, H. F. Is quantum bit commitment really possible? *Phys. Rev. Lett.* **78**, 3410 (1997).
14. Mayers, D. Unconditionally secure quantum bit commitment is impossible. *Phys. Rev. Lett.* **78**, 3414 (1997).
15. Horoshko, D. & Kilin, S. Quantum anonymous voting with anonymity check. *Phys. Lett. A* **375**, 1172–1175 (2011).
16. Bao, N. & Halpern, N. Y. Quantum voting and violation of Arrow's Impossibility Theorem. *arXiv: 1501.00458*.
17. Vaccaro, J. A., Spring, J. & Chefles, A. Quantum protocols for anonymous voting and surveying. *Phys. Rev. A* **75**, 012333 (2007).
18. Hillery, M., Zimanb, M., Bužekb, V. & Bielikovà, M. Towards quantum-based privacy and voting. *Phys. Lett. A* **349**, 75–81 (2006).
19. Jiang, L., He, G. Q., Nie, D., Xiong, J. & Zeng, G. H. Quantum anonymous voting for continuous variables. *Phys. Rev. A* **85**, 042309 (2012).
20. Li, Y. & Zeng, G. H. Quantum anonymous voting systems based on entangled state. *Opt. Rev.* **15**, 219C223 (2008).
21. Li, Y. & Zeng, G. H. Anonymous quantum network voting scheme. *Opt. Rev.* **19**, 121C124 (2012).
22. Thapliyal, K., Sharma, R. D. & Pathak, A. Protocols for quantum binary voting. *International Journal of Quantum Information.* **15**, 1750007 (2017).
23. Bostrom, K. Deterministic secure direct communication using entanglement. *Phys. Rev. Lett.* **89**, 187902 (2002).
24. Gorbachev, V. N., Trubilko, A. L., Zhiliba, A. I. & Yakovleva, E. S. Teleportation of entangled states and dense coding using a multiparticle quantum channel. *arXiv*: *quant-ph/0011124*.
25. Lo, H.-K. & Chau, H.-F. Unconditional security of quantum key distribution over arbitrarily long distance. *Science* **283**, 2050 (1999).
26. Shor, P. W. & Preskill, J. Simple proof of security of the BB84 quantum key distribution protocol. *Phys. Rev. Lett.* **85**, 441 (2000).
27. Lo, H. K., Chau, H.-F. & Ardehali, M. Efficient quantum key distribution scheme and a proof of its unconditional security. *J. of Cryptology* **18**, 133–165 (2005).
28. Xue, P., Li, C.-F. & Guo, G.-C. Conditional efficient multiuser quantum cryptography network. *Phys. Rev. A* **65**, 022317 (2002).

Acknowledgements

This work has been supported by the Natural Science Foundation of China under Grant Nos 11474049 and 11674056, the Natural Science Foundation of Jiangsu Province under Grant No. BK20160024, the Open Fund from Key Laboratory of Quantum Information, University of Science and Technology of China, Chinese Academy of Sciences, and the Open Fund from State Key Laboratory of Precision Spectroscopy, East China Normal University.

Author Contributions

P.X. developed the theory, analysed the results and wrote the paper. P.X. and X.Z. reviewed the manuscript.

Additional Information

Competing Interests: The authors declare that they have no competing interests.