Security analysis and improvements on a semi-quantum electronic voting protocol

Qiu Shujing[1], Xin Xiangjun[1], Zheng qian[1], Li Chaoyang[1], Li Fagen[2]
[1] College of Software Engineering, Zhengzhou University of Light Industry, Zhengzhou 450002, China
[2] School of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu 611731, China
*Corresponding author. Xin Xiangjun; Email: xin_xiang_jun@126.com

Abstract. Recently, Qiu et al. proposed a semi-quantum voting scheme based on the ring signature (International Journal of Theoretical Physics, 60: 1550–1555(2021)), in which the signer and verifier only need measure the received particles with Z-basis and perform some classical simple encryption/decryption operations on the classical message. Although their scheme is very efficient, it cannot resist against the eavesdropping attacks and forgery attack. In this paper, first, the eavesdropping attacks on Qiu et al.'s scheme are proposed. Second, we show the forgery attack on their scheme.

Keywords： Electronic voting scheme; Quantum ring signature; Eavesdropping attack; Forgery attack

1 Introduction

Electronic voting is gaining importance in the modern world. However, the security of traditional electronic voting heavily depends on solving complex mathematical problems, which may be easily solved by the quantum technologies [1, 2]. Quantum computers have an incredible computing power that poses a significant threat to established electronic voting protocols. In contrast, quantum voting is more secure as it uses the principles of quantum mechanics. The unclonability and quantum entanglement of quantum states ensure the privacy and security of voting, making any potential interference easier to be detected. Therefore, designing efficient and secure quantum voting protocols is currently a significant issue.

In 2005, Christandl et al. introduced a quantum anonymous transmission protocol that uses anonymous entanglement technology to protect the sender's identity [3]. Moreover, in the same year, Vaccaro et al. introduced a quantum voting protocol based on quantum entanglement technology, which was very helpful in protecting the privacy of voters [4]. In 2006, Hillery et al. proposed a quantum voting protocol to prevent voter cheating. This protocol required each voter should submit multiple votes [5]. Later, Hillery et al. proposed the traveling ballot protocol and distributed ballot protocol, which made significant contributions to the development of quantum voting protocols [6]. These protocols acted as fundamental components, inspiring a growing number of researchers. For instance, Li et al. introduced an anonymous electronic voting protocol that used quantum entanglement to enable voting across multiple candidates [7]. To address the challenge posed by dishonest voters and vote counters, Horoshko et al. proposed a quantum voting protocol that featured anonymous detection [8]. In addition, Jiang et al. developed a two-valued quantum voting protocol using entangled states of continuous variables [9]. However, these protocols have an intricate voting process, which can be problematic for large-scale voting. To overcome this issue, Wang et al. introduced a quantum voting protocol based on quantum teleportation specifically designed for large-scale voting [10]. Subsequently, Tian et al. introduced a

quantum voting protocol based on four-qubit entangled states, demonstrating increased reliability and efficiency compared to previous protocols [11]. Thapliyal et al. further improved the security of Tian et al.'s protocol by incorporating quantum cryptographic switch technology [12]. Wang et al. presented a self-technology quantum voting approach to avoid security risks associated with third-party vote counting [13]. To improve voting function and efficiency, Qin et al. proposed a quantum voting protocol based on GHZ-like states [14]. Li et al. proposed a quantum voting protocol based on eight-qubit entangled states to reduce the complexity of the voting process by utilizing only Bell state measurements and single-particle measurements [15]. Jiang et al. proposed a solution to the difficulty of preparing entangled states by incorporating orthogonal product states into the quantum voting protocol [16]. Liu et al. proposed a more efficient quantum voting protocol by utilizing BB84 states and introducing a trusted third-party center [17]. Li et al. greatly improved the practicality of the protocol by proposing a quantum voting scheme that uses single-particle states only [18].

A later proposed quantum e-voting system used a ring signature as an encrypted vote, which could be verified by the ring members without revealing the identity of the signer [19]. To generate and verify a ring signature, the signer and the verifier should have the ability of preparing or verifying various kinds of single qubits. They also should be able to perform the complicated quantum Fourier transform operations.

In the quantum voting protocols discussed above, it was necessary for all participants to be fully quantum ones, with the ability of preparing and measuring different types of qubits. Some protocols even required the ability to perform complex quantum operations.

To simplify the quantum protocol, Boyer et al. [20] introduced the concept of semi-quantum protocol. In this type of the protocol, there was one quantum party, while the other participants were “classical” parties. The quantum party was required to have the ability of performing complex quantum operations and preparing and measuring different types of qubits, while the classical parties were only required to perform the below simple operations:

(1) Preparing qubits $|0\rangle$ and $|1\rangle$ and measuring qubits with Z-basis;

(2) Reflecting or reordering the received qubits.

These requirements can simplify the quantum protocol, allowing classical parties to communicate with quantum parties without the need for complicated quantum devices. The classical participants can utilize simple devices, such as reflectors, Z-basis measurement devices, and delay devices to communicate quantum information with the other parties.

Recently, by calling the quantum secure direct communication protocol (QSDCP), Xu proposed a semi-quantum voting protocol that is based on the three-particle GHZ state and introduced the semi-quantum concept [21]. This protocol is more practical than previous ones as the voters only need classical capabilities to participate, which significantly reduces the need for various quantum resources and complex quantum operations. Qiu et al. introduced a new semi-quantum voting protocol that used a ring signature to sign votes [22]. In their protocol, to generate/verify a quantum ring signature on a vote, the signer/verifier only need to perform the simple Z-basis measurement and XOR operation, which made their protocol very efficient. Their system has the properties of semi-quantum protocol. However, according to our analysis, their protocol has some issues on correctness and security. In this paper, we investigated the correctness of Qiu et al.’s protocol.

What is more, we demonstrate that even if their protocol is correct, the protocol is vulnerable to eavesdropping and forgery attacks.

The following sections of this paper are as follows: Section 2 presents a review of Qiu et al.'s quantum voting protocol which uses the ring signature; Section 3 focus on analyzing the correctness of Qiu et al.'s protocol; Section 4 shows the security analysis of Qiu et al.'s protocol and demonstrates the eavesdropping attacks and forgery attack; Finally, in the last section, we present our conclusions.

2 Review of Qiu et al.'s semi-quantum voting protocol

In Qiu's quantum voting protocol, the generalized GHZ state is used. The generalized GHZ state can be expressed as

$$\left|\Psi\right\rangle = \frac{1}{\sqrt{2}}\left(\left|0\right\rangle^{\otimes n} + \left|1\right\rangle^{\otimes n}\right).$$

Assume there are n classical ring users. A trusted quantum third party(TQTP) is employed to distribute the GHZ particles to the n classical ring users. As one classical user of the ring, Alice will generate a ring signature on the vote, which can be verified by the rest n-1 users. Assume Alice is the first user.

2.1 Initialization

Step 1. TQTP shares the private keys K_a, K_b, …, K_n with the n users in the ring by performing the secure semi-quantum key distribution protocol, respectively.

Step 2. When Alice signs a vote in the ring, she informs TQTP. Then, TQTP prepares n generalized GHZ states $\left|\Psi_1\right\rangle$, $\left|\Psi_2\right\rangle$,…, $\left|\Psi_n\right\rangle$. Let $\left|\Psi_i^j\right\rangle$ denote the j-th sub-system of the i-th generalized GHZ states $\left|\Psi_i\right\rangle$. For i=1, 2, …, n, TQTP sends $\left|\Psi_i^j\right\rangle$ to the j-th user(j=1, 2, …, n).

2.2 Voting phase

Step 3. After Alice receives the n particles from TQTP, she encrypts the vote V with the private key K_a and gets V_{Ka}.

Step 4. Alice computes the message digest $M=H(V_{Ka})$, where H is a hash function and the length of M is n.

Step 5. Alice measures all the $\left|\Psi_i^1\right\rangle$ (i=1, 2, …, n) with Z-basis and gets $K_s=\{a_1, a_2, \ldots, a_n\}$. If the measurement result of $\left|\Psi_i^1\right\rangle$ is $\left|0\right\rangle$ ($\left|1\right\rangle$), a_i=0(a_i=1).

Step 6. Alice calculates $S= K_s \oplus M$. Then, Alice sends the ring signature (M, S, V_{Ka}) to TQTP.

2.3 Verification phase

Step 7. After getting (M, S, V_{Ka}), TQTP chooses another ring number Bob, who shared the key K_b with TQTP, to verify the ring signature. Assume Bob is the second ring member. TQTP

encrypts S with key K_b and gets S_{kb}. After that, TQTP sends S_{kb} to Bob.

Step 8. After receiving S_{kb}, Bob decrypts it with the shared key K_b and gets S. Then, Bob measures all the received $\left|\Psi_i^2\right\rangle$ (i=1, 2, …, n) with Z-basis and gets $K_s' = \{a_1', a_2', \cdots, a_n'\}$. If the measurement result of $\left|\Psi_i^2\right\rangle$ is $\left|0\right\rangle$ ($\left|1\right\rangle$), $a_i' = 1$ ($a_i' = 0$). Bob calculates $V_{K_b} = K_s' \oplus S$. Then, Bob encrypts V_{K_b} with K_b and gets S'_{K_b}. At last, he sends S'_{K_b} to TQTP.

Step 9. When receiving S'_{K_b}, TQTP decrypts S'_{K_b} with the shared key K_b and obtains V_{K_b}. Then, he checks whether $V_{K_b} = M$. If $V_{K_b} = M$, TQTP decrypts V_{Ka} by the shared key K_a and gets the voting result. Otherwise, TQTP repeats Step 8 and sends S to the other two ring users Charlie and Emily. At last, he gets V_{kc} and V_{ke} as well. If V_{Kc}=V_{Ke}=M, this means Bob is dishonest. TQTP continues to decrypt V_{ka} with the key K_a and gets the voting result. Or it means that Alice's vote has been tampered.

3 Correctness analysis of Qiu et al.'s protocol

In this section, we analyze the correctness of Qiu et al.'s protocol. We prove that the encrypted vote cannot be correctly verified.

In fact, in Step 6, we know that S= $K_s \oplus M$. In Step 8, it follows $V_{K_b} = K_s' \oplus S$. According to the entanglement of the generalized GHZ state and the decryptions of Step 5 and Step 8, it follows that $K_s' \oplus K_s = (1,1,\cdots,1)$. Therefore, it follows that $V_{K_b} \neq M$. Then, the valid (M, S, V_{Ka}) cannot pass the verification. This means TQTP can never successfully check the validity of the signed vote. Therefore, Qiu et al.'s protocol lacks correctness.

4 Security analysis of Qiu et al.'s protocol

In this section, we prove that Qiu et al.'s protocol is insecure against the eavesdropping attacks and forgery attack.

4.1 Eavesdropping attacks

In this section, we show two kinds of eavesdropping attacks, entanglement-measurement attack and intercept-measurement attack.

In the entanglement-measurement attack, the adversary tries to entangle the quantum channel with some auxiliary particle so that he can get some information by measuring his auxiliary particle.

In the intercept-measurement attack, the adversary intercepts the transmitted quantum particle and measures it so that he can get some information about the quantum particle. Then, the adversary resends the measured particle to the receiver. He may also intercept the classical message transmitted on the classical channel.

4.1.1 Entanglement-measurement attack

In this section, we demonstrate that an adversary outside the ring can eavesdrop on the quantum channel to get the session key K_s by performing the entanglement-measurement attack.

For example, in Step 2, when TQTP sends $\left|\Psi_i^1\right\rangle$ (i=1, 2, …, n) to the Alice, the adversary outside the ring can prepare an auxiliary particle e_i with initial state $\left|0\right\rangle_{e_i}$. Then, the adversary performs the controlled NOT operation such that $\left|\Psi_i^1\right\rangle$ and $\left|0\right\rangle_{e_i}$ are the controlled state and target state, respectively. Thus, we can get the

$$\left|\Psi_i'\right\rangle = \frac{1}{\sqrt{2}}\left(\left|0\right\rangle^{\otimes n} \otimes \left|0\right\rangle_{e_i} + \left|1\right\rangle^{\otimes n} \otimes \left|1\right\rangle_{e_i}\right) \left(i = 1, 2, \cdots, n\right). \tag{1}$$

During the voting phase, the adversary can measure each auxiliary particle e_i(i=1, 2, …, n) with Z-basis. If the measurement result of e_i is $\left|0\right\rangle$ ($\left|1\right\rangle$), the adversary set x_i=0(x_i=1). Thus, the adversary can get X={x_1, x_2, …, x_n}. According to the entanglement of $\left|\Psi_i'\right\rangle$, it follows that X=K_s. Therefore, by eavesdropping on the quantum channel between TQTP and the ring user Alice, the adversary can get the session key K_s.

4.1.2 Intercept-measurement attack

In this section, we demonstrate that an adversary outside the ring can eavesdrop on the quantum channel get the session key K_s by performing the intercept-measurement attack.

For example, when TQTP sends $\left|\Psi_i^1\right\rangle$ (i=1, 2, …, n) to Alice, the adversary intercepts all the $\left|\Psi_i^1\right\rangle$ and measures them with Z-basis. According to the measurement results, the adversary can get the session key K_s. After that, the adversary resends the measured $\left|\Psi_i^1\right\rangle$ (i=1, 2, …, n) to Alice.

Another very simple example is that the adversary may intercept (M, S, V_{Ka}) sent from Alice to Trent. Then, the adversary simply calculates $K_s = S \oplus M$. If necessary, he resends (M, S, V_{Ka}) to Trent. In this case, the adversary can also get the session key K_s.

4.2 Forgery attack

In this section, we show that an adversary Ad can forge the ring signature during the voting phase.

Assume that during some voting phase, the ring member Alice generates the ring signature (M, S, V_{Ka}) on the vote V. Then, she sends (M, S, V_{Ka}) to TQTP. The adversary Ad intercepts (M, S, V_{Ka}), keeps a copy of (M, S, V_{Ka}), and resends (M, S, V_{Ka}) to TQTP.

By using the (M, S, V_{Ka}), Ad can forge a new ring signature.

Assume that in another voting phase, the ring member Alice generates a new ring signature (M', S', V'_{Ka}) on the new vote V'. Then, she tries to send (M', S', V'_{Ka}) to TQTP. However, the adversary Ad intercepts (M', S', V'_{Ka}). What is more, by performing the eavesdropping attack

discussed in section 4.1, Ad can obtain the session key K_s' used during this voting phase. Then, Ad calculates $S'' = K_s' \oplus M$. It is easy to verify that (*M*, *S''*, V_{Ka}) is a valid ring signature on the vote *V*. At last, Ad sends (*M*, *S''*, V_{Ka}) to TQTP. It is clear that (*M*, *S''*, V_{Ka}) can passes the verification phase. This means that Ad can forge the signed vote.

Acknowledgements

This work is supported by the National Natural Science Foundation of China (Grant No.62272090) and the Key Scientific Research Project of Colleges and Universities in Henan Province (Grant No.22A413010).

CRediT authorship contribution statement

The correctness and security analyzed were presented by Xin Xiangjun and Qiu Shujng, and the manuscript was written by Xin Xiangjun and Qiu Shujng as well. The manuscript was reviewed by Zheng qian, Li Chaoyang and Li Fagen. All authors read and approved the final manuscript.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

The manuscript has no associated data.

References

[1] Shor, P.W.: Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM J. Comput. 26(5), 1484–1509 (1997)

[2] Huang, Y., Su, Z., Zhang, F., et al.: Quantum algorithm for solving hyper elliptic curve discrete logarithm problem. Quantum Inf. Process. 19, 62 (2020)

[3] Christandl, M., Wehner, S.: Quantum anonymous transmissions. Roy B. (eds) Advances in Cryptology-ASIACRYPT 2005 3788, 217–235 (2005)

[4] Vaccaro, J.A., Spring, J., Chefles, A.: Quantum protocols for anonymous voting and surveying. Phys.Rev. A 75(1), 012333 (2005)

[5] Hillery, M., et al.: Towards quantum-based privacy and voting. Phys. Lett. A 349(1-4), 75–81(2006)

[6] Hillery, M.: Quantum voting and privacy protection: first steps. Int. Soc. Opt Eng. https://doi.org/10.1117/2.1200610.0419 (2006)

[7] Li, Y., Zeng, G.H.: Quantum anonymous voting systems based on entangled state. Opt. Rev. 15(5), 219–223 (2008)

[8] Horoshko, D., Kilin, S.: Quantum anonymous voting with anonymity check. Phys. Lett. A 375(8), 1172–1175 (2011)

[9] Jiang, L., He, G.Q., Nie, D., Xiong, J., Zeng, G.H.: Quantum anonymous voting for continuous variables. Phys. Rev. A 85(4), 042309 (2012)
[10] Wang, Y.W., Wei, X.H., Zhu, Z.H.: Quantum voting protocols based on the non-symmetric quantum channel with controlled quantum operation teleportation (in Chinese). Acta Phys. Sin. 62(16), 160302 (2013)
[11] Tian, J.H., Zhang, J.Z., Li, Y.P.: A voting protocol based on the controlled quantum operation teleportation. Int. J. Theor. Phys. 55(5), 2303–2310 (2016)
[12] Thapliyal, K., Sharma, R.D., Pathak, A.: Analysis and improvement of Tian-Zhang-Li voting protocol based on controlled quantum teleportation. arXiv:1602.00791 [quant-ph] (2016)
[13] Wang, Q.L., et al.: Self-tallying quantum anonymous voting. Phys. Rev. A 94(2), 022333 (2016)
[14] Qin, J.Q., Shi, R.H., Zhang, R.: Quantum voting protocol based on controlled quantum secure direct communication(in Chinese). Chinese J. Quantum Electron. 35(5), 558–566 (2018)
[15] Li Y P, Zhou F, Wang T, et al. Novel quantum voting protocol with eight-qubit cluster entangled state. International Journal of Theoretical Physics, 2020, 59: 2671-2680.
[16] Jiang, D.H., Wang, J., Liang, X.Q., et al.: Quantum voting scheme based on locally indistinguishable orthogonal product states. Int. J. Theor. Phys. 59(2), 436–444 (2020)
[17] Liu, B.X., Jiang, D.H., Liang, X.Q., et al.: A novel quantum voting scheme based on BB84-state. Int. J. Theor. Phys. 60(4), 1339–1349 (2021)
[18] Li, Y.R., Jiang, D.H., Zhang, Y.H., et al.: A quantum voting protocol using single-particle states. Quantum Inf. Process. 20, 110 (2021)
[19] Xiong, Z., H., Yin, A., H.: Single particle electronic voting scheme based on quantum ring signature. Modern Physics Letters A, 37(26), 2250174 (2022)
[20] Boyer, M., Kenigsberg, D., Mor, T.: Quantum key distribution with classical Bob. Phys. Rev. Lett. 99(14), 140501 (2007)
[21] Xu, Y. P., Gao, D. Z., Liang, X. Q., et al. Semi-quantum voting protocol. International Journal of Theoretical Physics, 2022, 61(3): 78.
[22] Qiu, C., Zhang, S., B., Chang, Y., et al.: Electronic voting scheme based on a quantum ring signature. Int. J. Theor. Phys. 60(4), 1550–1555 (2021)
[23] Bennett, C. H., Brassard, G.: Quantum cryptography: public key distribution and coin tossing. Theor. Comput. Sci. 560, 7–11 (2014)
[24] Cai, Q.Y.: Eavesdropping on the two-way quantum communication protocols with invisible photons. Phys. Lett. A 351(1-2), 23-25 (2006)
[25] Gisin, N., Ribordy, G. G., Tittel, W., et al.: Quantum cryptography. Rev. Mod. Phys. 74(1), 145–195 (2002)
[26] Deng, F.G., Li, X.H., Zhou, H.Y., Zhang, Z.J.: Improving the security of multiparty quantum secret sharing against Trojan horse attack. Phys. Rev. A 72(4), 044302 (2005)
[27] Li, X. H., Deng, F. G., Zhou, H. Y.: Improving the security of secure direct communication based on the secret transmitting order of particles. Phys. Rev. A 74(5), 054302 (2006)
[28] Yang, C. W., Hwang, T., Luo, Y. P.: Enhancement on “Quantum blind signature based on two-state vector formalism”. Quantum Inf. Process. 12(1), 109-117 (2012)
[29] Hwang, T., Lee, K.C.: EPR quantum key distribution protocols with 100% qubit efficiency.

IET Inf. Secur. 1(1), 43–45 (2007)