Security analysis on an electronic voting scheme based on a quantum ring signature

Xin Xiangjun[1], Qiu Shujing[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 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. According to the security analysis, it follows that, when desiring the quantum ring signature scheme, we should carefully analysis its security against eavesdropping attacks and forgery under chosen message attack.

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

1 Introduction

Internet makes us closer and closer. Every day, we enjoy the amusement that the Internet brings us. We exchange the messages and information with our relatives and colleagues. However, all of the enjoyment and information exchange over Internet are built on the security of the Internet, which may be threatened by various attacks. For example, an adversary may intercept the transmitted messages and modify them. Then he sends disturbed messages to the receiver. The adversary may also impersonate someone to send a message to the desired receiver.

As one of the important technologies of information security, digital signature [1] is widely used to authenticate the exchanged messages. It can be used to verify the integrality of the received messages, and to check where the messages come from. Now, the digital signature technologies have been used in various fields including the e-commerce and e-voting system.

The security of most mathematical signatures relies on the difficulty of the assumptions such as factoring large composite number and computing discrete logarithm. However, Shor et al. showed that these assumptions may be broken by the delicate quantum algorithms [2-3]. This means all the digital signatures based on the mathematical assumptions may be broken by the quantum adversary in the future.

In response to the growing challenges of the quantum adversary, Gottesman and Chuang [4] introduced the concept of quantum signature. The quantum signature has the similar functions as the mathematical signature. However, the security quantum signature depends on some basic quantum theories rather than the unproved mathematical hypothesis. Therefore, the quantum signature can be theoretically secure against the quantum adversary. Therefore, since the introduction of the quantum signature, various quantum signatures for different applications have

been proposed. For example, the arbitrated quantum signature scheme [5-10] was proposed so that the identity of the signer could be authenticated and the disputation among the signer and the verifier can be solved by the trusted arbitrator. The quantum proxy signature scheme [11-12] was proposed so that the message could be signed by the proxy signer authorized by the message owner. The quantum designated verifier signature scheme [13-16] was proposed such that only the designated verifier could check the validity of the signed message. The quantum blind signature scheme [17-20] was proposed so that the signer could sign some message without knowing its contents. Quantum ring signature protocol [21-24] was proposed such that some ring member could sign a message on behalf of all the ring members without disclosing the true signer's identity. The property of unconditional anonymity of the quantum ring signature makes it is very useful in the application of electronic voting [22, 23]. In this paper, we focus our research to the quantum ring signature.

In general, a quantum ring signature should have the following properties [21-24]:

(1) Correctness: When the signer generates a correct signature, the verifier can verify its validity by the using the verification equation.

(2) Anonymity: Once some member of the ring signs a message, the adversary can judge the identity of the true signatory with probability 1/*n*, even the signing keys of all the possible signers in the ring are disclosed, where *n* is the count of the possible signers.

(3) No tampering: If a signature is tampered, it can hardly pass the verification.

(4) Unforgeability: Any user outside the ring can hardly generate the forgery of the ring signature.

(5) Non-repudiation: Once a ring signature is correctly generated and verified, its validity cannot be refused.

In 2019, Qu et al. [21] proposed the first quantum ring signature protocol. Their scheme was based on the single qubits without using any entangled quantum states and quantum swap test. It was required that the participants of the protocol should have the quantum ability of preparing and measuring the quantum states selected in Z-basis and X-basis. In [23], a quantum e-voting system was proposed. In this system, the encrypted vote was a ring signature, which could be verified by the ring members without disclosing the identity of the signer. In this system, 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 have the ability of performing the complicate quantum Fourier transform operations. In [24], Xiong et al. proposed a novel quantum ring signature protocol without using entangled states. In their scheme, the participants should have the ability of performing the quantum Hadamard operations. They also should have the ability of preparing and measuring the quantum states selected in Z-basis and X-basis.

In all the quantum ring signature protocols discussed above, it was required that the participants should be the full quantum ones, who should have the ability of preparing and measuring different kinds of qubits, and some protocols also required that the participants should have the ability of performing complicate quantum operations.

To simplify the quantum protocol, Boyer et al.[25] introduced the concept of semi-quantum protocol. In this kind of the protocol, there was one quantum party, while the other participants were "classical" parties. In the semi-quantum protocol, the quantum party has the ability of performing complicate quantum operations and preparing and measuring different kinds of qubits,

while the classical parties only need the simple ability of performing the following 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 greatly simplify the quantum protocol such that the classical parties can finish the message communication with the quantum parties without being equipped with complicated quantum devices. The classical participants can finish the quantum information communication with the other parties by the simple devices such as reflector, Z-basis measurement device and delay device.

In 2021, Qiu et al. [2] proposed a new quantum signature protocol based on GHZ state. In their protocol, to generate/verify a quantum ring signature, the signer/verifier only need perform the Z-basis measurement and simple XOR operation, which made their protocol very efficient. Their system has the properties of semi-quantum protocol. However, according to our analysis, their protocol lacks of correctness and security. In this paper, we analyze the correctness of Qiu et al.'s protocol. What is more, we demonstrate that even if their protocol is correct, the protocol cannot resist against the eavesdropping attacks and forgery attack.

In the following, we organize the rest paper as follows. In section 2, we simply review Qiu et al.'s quantum voting system, in which the ring signature is used. In section 3, we analyze the correctness of Qiu et al.'s protocol. In section 4, we analyze the security of Qiu et al.'s protocol and demonstrate the eavesdropping attacks and forgery attack. In the last section, we present the conclusions.

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

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

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

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, B_b, …, K_n with the n users in the ring by performing the secure semi-quantum key distribution protocol[25] , respectively.

Step 2. When Alice signs a vote in the ring, she informs TQTP. Then, TQTP prepares n generalized GHZ states $|\Psi_1\rangle$, $|\Psi_2\rangle$,…, $|\Psi_n\rangle$. Let $|\Psi_i^j\rangle$ denote the j-th sub-system of the i-th generalized GHZ states $|\Psi_i\rangle$. For i=1, 2, …, n, TQTP sends $|\Psi_i^j\rangle$ 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 valid vote. Therefore, Qiu et al.'s protocol lacks of 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 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}) and resends it to TQTP.

By using the intercepted (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.

5. Conclusions

Qiu et al.'s quantum voting scheme is based on the ring signature. Their scheme is very efficient because the ring members are all classical participants, who only need perform the simple measurement with Z-basis. Unfortunately, their scheme lacks of correctness. What is more, the security analysis shows that their scheme is insecure against eavesdropping attack and forgery attack as well.

The quantum ring signature is very useful in the quantum voting scheme so that the ring members can vote without disclosing their identities. However, this paper shows that in the quantum voting system based on ring signature, the security of the system relies on the security of the quantum channel and the ring signature. Therefore, it is very important to protect the quantum channel from being disturbed by the adversary. We can insert the decoy particles into the quantum channel so as to check eavesdropping and protect the quantum channel. On the other hand, the ring signature should be desired carefully so that it is secure against forgery attack.

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).

Declarations

Conflicts of Interest: All the authors declare that they have no conflict of interest.

Author Contributions: 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 Li Chaoyang and Li Fagen. All authors read and approved the final manuscript.

Data availability statement

My manuscript has no associated data.

References

[1] Diffie W., Hellman M.: New direction in cryptography [J]. IEEE Tran. Inf. Theor., 22, 644-654(1976)

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

[3] Huang, Y., Su, Z., Zhang, F., et al.: Quantum algorithm for solving hyperelliptic curve discrete logarithm problem. Quantum Information Processing 19(2), 62(2020)

[4] Gottesman, D., Chuang, I.: Quantum digital signatures. arXiv: quant-ph/0105032 (2001)

[5] Zeng, G. H., Keitel, C. H.: Arbitrated quantum-signature scheme. Physical Review A 65(4), 042312 (2002)

[6] Xin, X, Ding, L., Zhang, T, et al.: Provably secure arbitrated-quantum signature, Quantum Information Processing, 21(12), 390(2022)

[7] Xin, X., Ding, L., Yang, Q., et al.: Efficient chain-encryption-based quantum signature scheme with semi-trusted arbitrator. Quantum Information Processing, 21(7), 246(2022)

[8] Ding, L., Xin, X., Yang, Q., et al.: Security analysis and improvements of XOR arbitrated quantum signature-based GHZ state. Modern Physics Letters A, 37(2), 2250008 (2022)

[9] He, Q., Xin, X., Yang, Q.: Security analysis and improvement of a quantum multi-signature protocol. Quantum Information Processing 20(1), 26 (2021)

[10] Jiang, D. H., Xu, Y. L., Xu, G. B.: Arbitrary quantum signature based on local indistinguishability of orthogonal product states. International Journal of Theoretical Physics 58(3), 1036-1045 (2019)

[11] Zheng, T., Chang, Y., Yan, L. L, et al.: Semi-quantum proxy signature scheme with quantum walk-based teleportation. International Journal of Theoretical Physics 59(10), 3145-3155 (2020)

[12] Xin, X., Yang, Q., Li, F.: Quantum proxy signature with provable security. Modern Physics Letters A 35(24), 2050197(2020)

[13] Zhang, Y., Xin, X., Li F.: Secure and efficient quantum designated verifier signature scheme. Modern Physics Letters A 35(18), 2050148 (2020)

[14] Xin X., Ding L., Li C., et al.: Quantum public-key designated verifier signature. Quantum Information Processing, 21(1), 33(2022)

[15] Zhang, L., Zhang, J., Xin, X., et al.: Quantum designated verifier signature scheme with semi-trusted third-party. International Journal of Theoretical Physics 62(8), 166 (2023)

[16] Zhang, L., Zhang, J., Xin, X., et al: Quantum designated verifier signature without third party. Quantum Information Processing 22(12), 452 (2023)

[17] Chen, B., Yan L.: Quantum and semi-quantum blind signature schemes based on entanglement swapping. International Journal of Theoretical Physics 60(10), 4006–4014 (2021)

[18] Cao, J., Xin, X., Li, C., et al.: Security analysis and improvement of a blind semi-quantum signature. International Journal of Theoretical Physics 62(4), 87 (2023)

[19] Liu, G., Ma, W. P., Cao, H., et al.: A novel quantum group proxy blind signature scheme based on five-qubit entangled state. International Journal of Theoretical Physics 58(6), 1999–2008 (2019)

[20] Xia, C., Li, H., Hu, J.: A semi-quantum blind signature protocol based on five-particle GHZ state. European Physical Journal Plus 136(6), 633(2021)

[21] Qu, W., X., Zhang, Y., Liu, H., W., et al.: Multi-party ring quantum digital signatures. Journal of the Optical Society of America B-Optical Physics 36(5), 1335–1341 (2019)

[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] Xiong, Z., H., Yin, A., H.: Single particle electronic voting scheme based on quantum ring signature. Modern Physics Letters A, 37(26), 2250174 (2022)

[24] Xiong, Z.,H., Yin, A., H.: A novel quantum ring signature scheme without using entangled states. Quantum Inf. Process. 21(4), 140 (2022)

[25] Boyer, M., Kenigsberg, D., Mor, T.: Quantum key distribution with classical Bob [J]. Phys. Rev. Lett. 99(14), 140501 (2007)