Postprint of a Verifiable-Third-Party Quantum Secret Information Fair Exchange Protocol

Authors: Shao Tingting, ZHANG Shibin, Chang Yan

Date: 2018-12-13T00:00:00+00:00

Abstract

To realize information exchange between communicating parties, we propose a verifiable-third-party quantum secret information fair exchange protocol. In this protocol, a third party prepares a GHZ state and sends two of its particles to the communicating parties respectively. Each party performs Pauli operations on their received particles and then sends them back to the third party; the third party measures the new GHZ state and publishes the measurement results, based on which the communicating parties can infer each other' s secret information. Analysis demonstrates that this protocol can achieve fair exchange of secret information between the communicating parties, authenticate the identity of the third party, with the third party being responsible for particle distribution and measurement but unable to obtain the secret information. The protocol can detect eavesdropping and simultaneously resist intercept-resend attacks, man-in-the-middle attacks, and participant attacks.

Full Text

Preamble

Third-Party Verifiable Quantum Secret Information Equal Exchange Protocol

Shao Tingting, Zhang Shibin†, Chang Yan (School of Cybersecurity, Chengdu University of Information Technology, Chengdu 610225, China)

Abstract: To realize information exchange between two communicating parties, this paper proposes a verifiable third-party quantum secret information equal exchange protocol. In this protocol, a third party prepares GHZ states and sends two particles from each state to the communicating parties respectively. The two parties perform Pauli operations on their received particles and return them to the third party. The third party measures the resulting GHZ

states and publishes the measurement outcomes, enabling both parties to deduce each other' s secret information based on the announced results. Analysis demonstrates that this protocol achieves equal exchange of secret information between the two parties, allows authentication of the third party' s identity, and ensures that while the third party distributes and measures particles, it cannot obtain the secret information. The protocol can detect eavesdropping and resist interception-resend attacks, man-in-the-middle attacks, and participant attacks.

Keywords: quantum communication; secret information; GHZ state; equal exchange; verifiable third party

0 Introduction

Classical cryptographic systems have become relatively mature over time and are widely applied across various domains to protect information security. However, the security of classical cryptosystems faces significant challenges with the proposal of quantum algorithms [**?**, **?**] and the development of quantum computers [**?**]. In 1969, Wiesner first proposed using quantum effects to protect information in his paper "Conjugate Coding" [**?**]. Quantum communication possesses two fundamental characteristics: unconditional security and detectability of eavesdropping. Unconditional security means that even an adversary with unlimited computational resources cannot break the cryptosystem. Detectability of eavesdropping means that when communication channels between users are disturbed, the presence of interference can be detected based on the uncertainty principle. In recent years, quantum communication has achieved a series of remarkable research results [**?**, **?**], primarily including quantum key distribution (QKD) [**?**, **?**], quantum secret sharing (QSS) [**?**, **?**], quantum private query (QPQ) [**?**, **?**], and quantum secure direct communication (QSDC) [**?**, **?**].

In real-world scenarios, when two users each possess a piece of secret information —where User 1 wants to obtain User 2' s secret while User 2 wants to obtain User 1' s secret—they can acquire more information through secret information exchange. However, in previous communication protocols, this process typically involves User 1 first sending secret information to User 2, who only transmits their own secret after confirming receipt. This approach risks User 2 obtaining User 1' s secret but deceiving User 1 by sending false information, leaving User 1 with fake secrets while their own information has already been compromised. To eliminate this risk, this paper designs a novel verifiable third-party quantum secret information equal exchange protocol.

In this protocol, the third party first prepares GHZ states and sends two particles to each communicating party. Although a third party is introduced, its identity can be verified to reduce dependency. Upon receiving the particles, the communicating parties encode their secret information onto them using Pauli operations before returning them to the third party, who then performs joint measurements on the resulting GHZ states and publishes the outcomes. Both

parties can deduce each other' s secret information based on these published results. The protocol enables simultaneous acquisition of each other' s secrets, achieving equal exchange and preventing either party from deceiving the other. Analysis shows that the third party' s identity can be verified to ensure its trustworthiness, while the protocol also provides eavesdropping detection and resistance against interception-resend attacks, man-in-the-middle attacks, and participant attacks.

---

1 Basic Principles

The four Pauli matrices are as follows:

Performing the four Pauli operations on and yields the following results:

The eight GHZ states are as follows:

---

2 Protocol Description

Alice possesses secret information $X = (x_1, x_2, ..., x_n)$ and Bob possesses secret information $Y = (y_1, y_2, ..., y_n)$, where each x_i and y_i corresponds to two binary bits. Alice and Bob wish to exchange their secret information through the following protocol:

a) Alice and Bob notify the third party, who prepares $|\Psi_a\rangle_{123} = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$ states. All particle 1s form sequence S_1, all particle 2s form sequence S_2, and all particle 3s form sequence S_3. The third party retains sequence S_1, randomly inserts decoy particles $|0\rangle$, $|1\rangle$, $|+\rangle$, $|-\rangle$ into sequences S_2 and S_3, then sends them to Alice and Bob respectively.

b) Upon receiving the particles, Alice and Bob perform eavesdropping detection. The third party announces the positions and measurement bases of the decoy particles: Z-basis for $|0\rangle$ or $|1\rangle$, and X-basis for $|+\rangle$ or $|-\rangle$. Alice and Bob extract the corresponding particles and measure them in the X or Z basis. If the error rate exceeds the threshold, they abort the communication; otherwise, they proceed to step c).

c) The third party's identity is authenticated. Alice and Bob randomly designate m particles and their positions, requiring the third party to measure them in the X basis and announce the results via a classical channel. Alice and Bob then measure their corresponding particles in the X basis. If the third party correctly prepared the GHZ states, the relationship should hold: when the third party announces $|\Psi_a\rangle$ state, Alice and Bob' s measurement results are identical; when $|\Psi_b\rangle$ state is announced, their results are opposite. Successful verification proceeds to step d).

d) Alice performs one of four Pauli operations on n particles based on her secret information X: σ_{00} for "00" , σ_{01} for "01" , σ_{10} for "10" , and σ_{11} for "11" . After performing these operations, Alice forms new sequence S_2'. Similarly, Bob forms new sequence S_3' based on his secret information Y.

e) Alice randomly inserts decoy particles $|0\rangle$, $|1\rangle$, $|+\rangle$, $|-\rangle$ into sequence S_2' and sends it to the third party. Bob does the same with sequence S_3'.

f) After receiving the particles from Alice and Bob, they announce the positions and measurement bases of their decoy particles (same method as step b). The third party extracts the decoy particles to obtain S_2' and S_3', then performs joint GHZ measurements with their own sequence S_1. The measurement results are shown in Table 1 , and the third party publishes the measured GHZ states.

g) Alice can deduce Bob' s secret information Y' based on the third party' s published measurement results and Table 1. Similarly, Bob can deduce Alice' s secret information X'. Alice publishes $X' \oplus X$ via a classical channel, and Bob publishes $Y' \oplus Y$. If both published values match, it confirms the third party is not cheating, and Alice obtains Bob' s secret Y while Bob obtains Alice' s secret X.

3.1 Protocol Correctness Analysis

If communicating parties Alice and Bob wish to exchange secret information, the third party prepares GHZ state $|\Psi_a\rangle_{123} = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$, sending particle 2 to Alice and particle 3 to Bob. Based on their secret information, Alice and Bob perform Pauli operations on their particles and return them to the third party, who measures the resulting states and publishes the outcomes. As shown in Table 1, Alice can deduce Bob's secret information from the published results combined with her own secret, and Bob can similarly deduce Alice's secret. The simplified protocol flowchart is shown in Figure 1 [Figure 1: see original paper].

Protocol Example: Suppose Alice' s secret information is "001011" and Bob' s is "110011" . They notify the third party to prepare $|\Psi_a\rangle_{123}$ states. All particle 2s (randomly interspersed with decoy particles) are sent to Alice, and all particle 3s (with decoys) to Bob. After eavesdropping detection confirms channel security, they verify the third party' s identity.

Alice and Bob randomly designate particle positions and require the third party to measure in the X basis. When the third party announces $|\Psi_a\rangle$ state, Alice and Bob's X-basis measurements yield identical results; when $|\Psi_b\rangle$ is announced, their results are opposite. After verification, they encode their secrets: Alice performs σ_{00}, σ_{01}, σ_{11} operations on particle 2s; Bob performs σ_{11}, σ_{00}, σ_{11} on particle 3s. They insert decoy particles and send the sequences to the third party.

Upon receipt and eavesdropping check, the third party extracts decoys and

performs GHZ measurements on all particle 1s combined with the returned particles. Publishing the result $|\Psi_h\rangle$, Alice obtains "110011" and Bob obtains "001011" according to Table 1. Alice computes $110011 \oplus 001011 = 111000$ and publishes it; Bob computes $001011 \oplus 110011 = 111000$ and publishes it. The identical published values confirm no deception or attack occurred, and the equal exchange of secret information is successfully realized.

3.2 Security Analysis Model

The quantum secret information equal exchange protocol enables two users to securely exchange information. As shown in Figure 2 [Figure 2: see original paper], potential attackers during the exchange include third-party attacks (involving incorrect GHZ state preparation or false announcement of results), man-in-the-middle or intercept-resend attacks during communication, and participant attacks.

3.2.1 Third-Party Attacks

The third party performs two critical functions: correctly preparing GHZ states and accurately publishing joint measurement results after Alice and Bob's Pauli operations.

The third party prepares $|\Psi_a\rangle_{123}$ states and distributes particles 2 and 3 to Alice and Bob. Any attempt to prepare fake GHZ states to disrupt the exchange will be detected during identity verification. In the protocol implementation, Alice and Bob randomly select particles for verification after receiving particles 2 and 3. They require the third party to measure in the X basis and announce results via a classical channel. If the third party correctly prepared the GHZ states, announcing $|\Psi_a\rangle$ should yield identical measurement results for Alice and Bob, while announcing $|\Psi_b\rangle$ should yield opposite results. Satisfying these conditions confirms proper GHZ state preparation; otherwise, deception is indicated.

If the third party attempts to block the exchange through false signal attacks —measuring S_2' and S_3' with their S_1 sequence but publishing fake GHZ states to mislead Alice and Bob—they would cause Alice to obtain false secret Y' and Bob to obtain false secret X'. Alice would deduce Y' and Bob would deduce X' from the fake announcements. If $Y' \neq Y$ and $X' \neq X$, the published values of $Y' \oplus Y$ and $X' \oplus X$ would differ, revealing the deception. However, the third party cannot accurately obtain Alice and Bob' s secrets. For instance, upon obtaining $|\Psi_h\rangle$ from Table 1, the third party cannot determine whether Alice and Bob performed operations "00" or "11" . As the number of binary bits increases, the probability of the third party obtaining correct information diminishes.

3.2.2 Man-in-the-Middle or Intercept-Resend Attacks

When channels are insecure, man-in-the-middle or intercept-resend attacks may occur. After Alice and Bob receive particles, they perform channel security detection based on the third party' s announced decoy particle positions. They extract and measure these particles in the X or Z basis. An attacker choosing the wrong measurement basis will disturb the particles. If measurement results differ from the inserted decoy states, it indicates a potential attack, prompting the third party to distribute new GHZ states. The return process after Pauli operations also requires eavesdropping detection. Alice and Bob can verify attack presence by checking whether their published $X' \oplus X$ and $Y' \oplus Y$ values match. If an attacker is present, Alice' s obtained information Y' would not be Bob' s true secret Y, and Bob' s X' would not be Alice' s true secret X, causing the XOR results to differ. This analysis demonstrates the protocol' s effectiveness against man-in-the-middle and intercept-resend attacks.

3.2.3 Participant Attacks

Suppose Bob attempts to deceive Alice during communication by not performing Pauli operations according to his correct secret information Y. For example, if Alice' s secret is "01" and Bob' s is "00" , but Bob performs σ_{10} operations instead to steal Alice' s secret. After returning the manipulated particles to the third party, the measurement result $|\Psi_f\rangle$ would be published (instead of $|\Psi_a\rangle$ if Bob had operated correctly). Bob would deduce "10" from his secret "00" and Table 1, but cannot obtain Alice' s actual secret "01" through this attack method.

---

4 Conclusion

This paper proposes a verifiable third-party quantum secret information equal exchange protocol that enables equal exchange of secret information between communicating parties. The protocol prevents one party from deceiving the other to obtain secret information, allowing both parties to simultaneously acquire each other' s secrets through the third party' s announcements. The protocol verifies the third party' s identity, reducing dependency on it, while resisting man-in-the-middle attacks, intercept-resend attacks, and participant attacks to ensure secure and equal information exchange.

References

[1] Shor P W. Algorithms for quantum computation: discrete logarithms and factoring [C]//Proc of the 35th Annual Symposium on the Foundations of Computer Science. Washington DC: IEEE Computer Society, 1994: 124-134.

[2] Grover L K. A fast quantum mechanical algorithm for database search [C]//Proc of the 28th ACM Symposium on Theory of Computing. New York:

ACM Press, 1996: 212-219.

[3] Ladd T D, Jelezko F, Laflamme R, et al. Quantum computers [J]. Nature, 2010, 464(7285): 45-53.

[4] Wiesner S. Conjugate coding [J]. ACM SIGACT News, 1983, 15(1): 78-88.

[5] Gao Fei, Liu Bin, Wen Qiaoyan. Quantum position verification in bounded-attack-frequency model [J]. Science China: Physics, Mechanics & Astronomy, 2016, 59(11): 110311.

[6] Song Xueke, Zhang Hao, Ai Qing, et al. Shortcuts to adiabatic holonomic quantum computation in decoherence-free subspace with transitionless quantum driving algorithm [J]. New Journal of Physics, 2016, 18(2): 569-577.

[7] Curty M, Xu Feihu, Cui Wei, et al. Finite-key analysis for measurement-device-independent quantum key distribution [J]. Nature Communications, 2014, 5(4): 643-648.

[8] Wang Chao, Wang Shuang, Yin Zhenqian, et al. Experimental measurement-device-independent quantum key distribution with uncharacterized encoding [J]. Optics Letters, 2016, 41(23): 5596-5599.

[9] Qin Huawang, Dai Yuewei. Verifiable (t,n) threshold quantum secret sharing using d-dimensional Bell state [J]. Information Processing Letters, 2016, 116(5): 351-355.

[10] Gao Gan. Secure multiparty quantum secret sharing with the collective eavesdropping-check character [J]. Quantum Information Processing, 2013, 12(1): 55-68.

[11] Gao Fei, Liu Bin, Huang Wei, et al. Postprocessing of the oblivious key in quantum private query [J]. IEEE Journal of Selected Topics in Quantum Electronics, 2014, 21(3): 98-108.

[12] Wei Chunyan, Wang Tianyin, Gao Fei. Practical quantum private query with better performance in resisting joint-measurement attack [J]. Physical Review A, 2016, 93(4): 042318-042324.

[13] Patwardhan S, Moulick S R, Panigrahi P K. Efficient controlled quantum secure direct communication protocols [J]. International Journal of Theoretical Physics, 2016, 55(7): 3280-3288.

[14] Cao Zhengwen, Song Dan, Peng Jinye, et al. High security quantum secure direct communication protocol based on three-particle GHZ states [C]//Proc of IEEE International Conference on Nanotechnology. Piscataway, NJ: IEEE Press, 2017: 40-43.

Note: Figure translations are in progress. See original paper for figures.