Postprint of Identity Authentication Protocol Based on Bell State Entanglement Swapping

Authors: Xiong Jinxin, Fang Jie, Chang Yan, Zhang Shibin

Date: 2018-05-02T00:00:00+00:00

Abstract

A novel quantum identity authentication protocol is proposed that employs Bell states as the transmission carrier and utilizes Bell state entanglement swapping and Bell basis measurements to authenticate communication users. In the transmission process of two Bell states, no unitary transformations are required; information transmission can be realized solely through Bell basis measurements and bitwise XOR operations. The quantum carrier operations throughout the entire process are simple and easy to implement. Furthermore, the correctness of this protocol has been verified.

Full Text

Quantum Identity Authentication Protocol Based on Bell States and Entanglement Swapping

Xiong Jinxin[1], **Fang Jie**[2]†, **Chang Yan**[1], **Zhang Shibin**[1] 1. School of Cybersecurity, Chengdu University of Information Technology, Chengdu 610225, China 2. Sichuan Institute of Computer Science, Chengdu 610041, China

Abstract: This paper proposes a novel quantum identity authentication protocol that employs Bell states as the transmission carrier and utilizes Bell state entanglement swapping and Bell basis measurement to authenticate communicating users. During the transmission of two Bell states, no unitary transformations are required; information transmission can be achieved solely through Bell basis measurements and bitwise XOR operations. The quantum carrier operations are simple and easy to implement throughout the entire process. Furthermore, the correctness of this protocol has been verified.

Keywords: quantum identity authentication; entanglement swapping; Bell basis measurement

0 Introduction

Classical methods are traditionally used for mutual identity authentication. However, anti-jamming channels are difficult to implement in communication, and classical identity authentication protocols struggle to achieve unconditional security. Since Bennett and Brassard proposed the quantum key distribution (QKD) protocol (known as BB84) [1], which opened the field of quantum cryptography, researchers have developed numerous quantum cryptographic protocols to meet various needs and address emerging information security issues. These 主要包括 quantum secret sharing (QSS) [2,3], quantum secure direct communication (QSDC) [4,5], and quantum identity authentication (QIA) [6~13].

Quantum communication represents one of the most important applications in the quantum domain and has achieved continuous theoretical and experimental breakthroughs in recent years. However, in quantum communication networks, illegal users may impersonate legitimate users, compromising the security of quantum communication systems. In quantum communication, a malicious attacker impersonating a legitimate user can distribute keys and conduct secret communications with other users—that is, they can send forged information to legitimate users or steal secret information from them. Simultaneously, in quantum key distribution protocols, establishing anti-jamming channels or using classical identity authentication methods makes it difficult to effectively prevent impersonation attacks. Especially when an attacker has certain technical capabilities to access the quantum and classical communication channels of both parties, the probability of man-in-the-middle attacks during communication increases significantly. Therefore, this protocol performs quantum identity authentication on both communicating users during quantum key distribution or quantum secure direct communication, thereby preventing man-in-the-middle attacks in quantum secure communication without requiring the establishment of anti-jamming channels or classical identity authentication in the communication channel. This design can also be applied to smart card systems for identification purposes [12,13]. Different smart cards have different IDs, and different Bell state particles are prepared according to these IDs to complete smart card identity authentication through quantum identity authentication. The uncertainty principle and quantum no-cloning theorem guarantee unconditional security for the authentication.

Current quantum identity authentication schemes fall into three categories: The first category comprises point-to-point quantum identity authentication schemes. In 2014, Yuan et al. [6] proposed an entanglement-free single-particle quantum identity authentication scheme based on the ping-pong technique. In 2016, Ma et al. [7] proposed a continuous-variable quantum identity authentication protocol based on quantum teleportation using two-mode squeezed vacuum states and coherent states, which effectively verifies user identity using newly defined fidelity parameters. The second category combines identity authentication with quantum key distribution, achieving both simultaneously during key transmission. In 2017, Ma et al. [8] proposed a novel bidirectional identity

authentication scheme based on measurement-device-independent quantum key distribution (MDI-QKD), which uses Bell states as carriers to achieve identity authentication and key distribution in a single round. The third category comprises quantum identity authentication schemes in networks. Yang et al. [9] proposed a multiparty quantum identity authentication protocol based on GHZ states, where multiple users can be authenticated simultaneously by a trusted third party. In 2013, Yang et al. [10] further proposed a (t,n) threshold multiparty identity authentication scheme based on GHZ states. In 2014, Zhang et al. [11] proposed a wireless communication network identity authentication scheme based on quantum teleportation.

This paper presents an identity authentication protocol based on Bell state entanglement swapping. In this protocol, two users only need to prepare Bell states according to their binary identity strings, perform particle swapping, conduct Bell basis measurements, and execute bitwise XOR operations to authenticate each other' s identities. Therefore, compared with the continuous-variable quantum identity authentication protocol based on quantum teleportation proposed by Ma et al. [7], although this protocol cannot achieve key updating during identity authentication, it eliminates the need for third-party involvement and parameter definition, reducing protocol complexity. Compared with the identity authentication scheme based on measurement-device-independent quantum key distribution proposed by Ma et al. [8], this protocol does not require complex quantum control techniques, lowering the system execution requirements and improving protocol practicality. Moreover, this protocol is easily implementable under current technological conditions.

1 Preliminary Knowledge

The four Bell states can be expressed as follows:

$$|\phi^+\rangle_{12} = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$
$$|\phi^-\rangle_{12} = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$$
$$|\psi^+\rangle_{12} = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$$
$$|\psi^-\rangle_{12} = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$

Entanglement swapping is a phenomenon where entanglement is transferred between particles. If two Bell states are both in $|\phi^+\rangle$ state, the following equation holds:

$$|\phi^+\rangle_{12}\otimes|\phi^+\rangle_{34} = \frac{1}{2}\left(|\phi^+\rangle_{13}|\phi^+\rangle_{24} + |\phi^-\rangle_{13}|\phi^-\rangle_{24} + |\psi^+\rangle_{13}|\psi^+\rangle_{24} + |\psi^-\rangle_{13}|\psi^-\rangle_{24}\right)$$

If particles 1 and 3 are measured in the Bell basis, particles 2 and 4 become entangled. For example, if the measurement result of particles 1 and 3 is $|\phi^+\rangle_{13}$, then the state of particles 2 and 4 becomes $|\phi^+\rangle_{24}$. The relationship is shown in equation (3).

Through derivation, any two Bell states exhibit the relationship shown in equation (3). Based on this equation, it is easy to deduce that any two Bell states, after entanglement swapping, will be in one of the four Bell states with equal probability of 1/4. Ignoring phase, the entanglement swapping of any two Bell states is shown in Table 1 .

If we use 00 to represent $|\phi^+\rangle$, 01 to represent $|\phi^-\rangle$, 10 to represent $|\psi^+\rangle$, and 11 to represent $|\psi^-\rangle$, then the binary representations of the two Bell states before entanglement swapping are $c_{1c}2$ and $c_{3c}4$, and the binary representations of the two Bell state particles after entanglement swapping are $c_{1c}3$ and $c_{2c}4$. From Table 1, we can conclude that after entanglement swapping, the two Bell states are in $|\phi^+\rangle$ with probability 1/4, in $|\phi^-\rangle$ with probability 1/4, in $|\psi^+\rangle$ with probability 1/4, and in $|\psi^-\rangle$ with probability 1/4.

Let $ID_A = \{C_1^A, C_2^A, ..., C_n^A\}$ be Alice' s binary identity string and $ID_B = \{C_1^B, C_2^B, ..., C_n^B\}$ be Bob' s binary identity string. Alice and Bob share ID_A and ID_B. Alice prepares particle sequence S_A^{ID} according to ID_A, and Bob prepares particle sequence S_B^{ID} according to ID_B. The preparation rule is: if the current bit of the identity string is 00, prepare the particle in $|\phi^+\rangle$; if 01, prepare in $|\phi^-\rangle$; if 10, prepare in $|\psi^+\rangle$; if 11, prepare in $|\psi^-\rangle$.

The binary relationship corresponding to entanglement swapping of any two Bell states is shown in Table 2 .

2 Protocol

This protocol achieves identity authentication functionality, and when one party publishes their measurement results, it does not cause leakage of either party' s identity information.

2.1 Protocol Content

a) Alice' s binary identity string is $ID_A = \{C_1^A, C_2^A, ..., C_n^A\}$, and Bob' s binary identity string is $ID_B = \{C_1^B, C_2^B, ..., C_n^B\}$. Alice and Bob share ID_A and ID_B.

b) Alice prepares particle sequence S_A^{ID} according to ID_A, and Bob prepares particle sequence S_B^{ID} according to ID_B. The preparation rule is: if the current bit of the identity string is 00, prepare the particle in $|\phi^+\rangle$; if 01, prepare in $|\phi^-\rangle$; if 10, prepare in $|\psi^+\rangle$; if 11, prepare in $|\psi^-\rangle$.

c) Alice sends all the first particles of the Bell states to Bob, while Bob sends all the second particles of the Bell states to Alice. After particle exchange, Alice possesses particle sequence $S_A^{ID'}$ and Bob possesses particle sequence

$S_B^{ID'}$. Alice performs Bell basis measurement on $S_A^{ID'}$, at which point the particles in Bob' s possession become correspondingly entangled. Bob performs Bell basis measurement on $S_B^{ID'}$, completing the entanglement swapping.

d) The measurement results are represented in binary bits. The representation rule is: use 00 to represent $|\phi^+\rangle$, 01 to represent $|\phi^-\rangle$, 10 to represent $|\psi^+\rangle$, and 11 to represent $|\psi^-\rangle$.

e) If Alice wants to authenticate Bob' s identity, she only needs to notify Bob through the classical channel to publish C'_{B_k}, and then verify according to equation (4). If the equation holds, Bob is proven legitimate. If Bob wants to authenticate Alice' s identity, steps a)~d) must be repeated, and Bob notifies Alice through the classical channel to publish C'_{A_k}. If equation (4) holds, Alice is proven legitimate.

The identity authentication process is shown in Figure 1 [Figure 1: see original paper].

2.2 Protocol Example

a) Alice' s binary identity string is $ID_A = 11110100$, and Bob' s binary identity string is $ID_B = 11100010$. Alice and Bob share ID_A and ID_B.

b) Alice prepares particle sequence S_A^{ID} according to ID_A, and Bob prepares particle sequence S_B^{ID} according to ID_B. The preparation rule is: if the current bit of the identity string is 00, prepare the particle in $|\phi^+\rangle$; if 01, prepare in $|\phi^-\rangle$; if 10, prepare in $|\psi^+\rangle$; if 11, prepare in $|\psi^-\rangle$.

c) Alice sends all the first particles of the Bell states to Bob, while Bob sends all the second particles of the Bell states to Alice. After particle exchange, Alice possesses particle sequence $S_A^{ID'}$, and Bob possesses particle sequence $S_B^{ID'}$. Alice performs Bell basis measurement on $S_A^{ID'}$, at which point $S_B^{ID'}$ becomes correspondingly entangled. Bob performs Bell basis measurement on $S_B^{ID'}$, completing the entanglement swapping.

d) The measurement results are represented in binary bits. The representation rule is: use 00 to represent $|\phi^+\rangle$, 01 to represent $|\phi^-\rangle$, 10 to represent $|\psi^+\rangle$, and 11 to represent $|\psi^-\rangle$.

e) If Alice wants to authenticate Bob' s identity, she only needs to notify Bob through the classical channel to publish C'_{B_k}. Alice calculates $ID_A \oplus C'_{A_k} = ID_B \oplus C'_{B_k}$ for verification. If the equation holds, Bob is proven to be a legitimate user. Similarly, if Bob wants to authenticate Alice' s identity, he repeats the process of particle preparation and exchange, then notifies Alice through the classical channel to publish C'_{A_k}. This method achieves identity authentication functionality.

3 Security Analysis

3.1 Impersonation Attack

Eve attempts to impersonate Bob without knowing ID_B. Since Eve does not know ID_B, she randomly prepares a Bell state particle sequence S_E^{ID}. Alice sends all the first particles of the Bell states to Bob, while Eve sends all the first particles of her Bell states to Alice. After particle exchange, Alice possesses particle sequence $S_A^{ID'}$, and Eve possesses particle sequence $S_E^{ID'}$. Alice performs Bell basis measurement on $S_A^{ID'}$, while Eve performs Bell basis measurement on $S_E^{ID'}$, completing the entanglement swapping. Subsequently, Alice represents her measurement results in binary as C'_{A_k}, and Eve represents her measurement results in binary as C'_{E_k}. If Alice attempts to authenticate Bob' s identity, Eve publishes C'_{E_k}, and Alice verifies according to equation (4). Since $ID_A \oplus C'_{A_k} \neq ID_B \oplus C'_{E_k}$, Eve cannot pass the identity authentication. Therefore, Eve cannot impersonate Bob without knowing ID_B. Similarly, Eve cannot impersonate Alice.

Eve may attempt an intercept-resend attack to obtain ID_A or ID_B. If Eve intercepts particles sent by Alice or Bob, it prevents the completion of entanglement swapping, causing equation (4) to fail during identity authentication between Alice and Bob, and the authentication cannot pass. Similarly, Eve' s intercept-resend attack cannot obtain ID_A or ID_B, and identity authentication will fail.

Eve attempts to deduce ID_A and ID_B from the published C'_{A_k} or C'_{B_k}. In step c), Eve has particle sequences $S_A^{ID'}$ and $S_B^{ID'}$, each randomly in one of four maximally mixed states with probability 1/4: $\{|\phi^+\rangle, |\phi^-\rangle, |\psi^+\rangle, |\psi^-\rangle\}$. In step d), Alice and Bob represent their measurement results as C'_{A_k} and C'_{B_k}. In step e), the published C'_{A_k} and C'_{B_k} are binary representations of the four maximally mixed states after entanglement swapping, each occurring with probability 1/4. These have no correlation with ID_A and ID_B. During the identity authentication process, Eve cannot deduce any information about ID_A and ID_B from one party' s published results. Therefore, publishing C'_{A_k} or C'_{B_k} during protocol execution does not cause leakage of ID_A and ID_B, which can be reused.

3.2 Security of ID_A and ID_B

Since ID_A and ID_B are secretly shared between communicating parties beforehand, illegal users do not know ID_A and ID_B. If Eve attempts to guess ID_A or ID_B, let ID_A and ID_B be binary strings of length $2n$. The probability of Eve correctly guessing ID_A or ID_B is $1/4^n$. As long as the length of ID_A or ID_B is sufficiently long, the probability of Eve guessing correctly approaches zero. Consequently, Eve cannot pass identity authentication at all.

The protocol proposed in this paper not only prevents illegal users from impersonating legitimate users but also ensures the security of ID_A and ID_B.

4 Conclusion

This paper proposes an identity authentication protocol based on Bell state entanglement swapping. In this protocol, both parties only need to prepare two groups of particle sequences according to their binary identity strings following specified rules. Then Alice sends the first particles of her prepared Bell state sequence to Bob, and Bob sends the second particles of his prepared Bell state sequence to Alice. Both parties perform Bell basis measurements on their respective particles, and finally represent the measurement results in binary. Alice or Bob can complete one-way identity authentication by publishing the corresponding binary representation. Throughout the identity authentication process, the transmission of Bell states requires no unitary transformations; information transmission can be achieved solely through Bell state measurements and bitwise XOR operations. In practical applications, the implementation of this protocol only depends on the accurate preparation of Bell states and reliable Bell state measurements. Finally, security analysis of the protocol demonstrates that it can resist impersonation attacks. During protocol execution, one party publishing C'_{A_k} or C'_{B_k} does not cause leakage of ID_A and ID_B, which can be reused.

References

[1] Bennett C H, Brassard G. Quantum cryptography: public key distribution and coin tossing [C]// Proc of IEEE International Conference on Computers Systems and Signal Processing. 1984: 175-179.

[2] Bell B A, Markham D, Herrera-Martí D A, et al. Experimental demonstration of graph-state quantum secret sharing [J]. Nature Communications, 2014, 5: 5480.

[3] Mishra S, Shukla C, Pathak A, et al. An integrated hierarchical dynamic quantum secret sharing protocol [J]. International Journal of Theoretical Physics, 2015, 54 (9): 1-12.

[4] Chang Y, Xu C X, Zhang S B, et al. Quantum secure direct communication and authentication protocol with single photons [J]. Chinese Science Bulletin, 2013, 58 (36): 4571-4576.

[5] Li J, Guo X J, Song D, et al. Improved quantum "ping-pong" protocol based on extended three-particle GHZ state [J]. China Communications, 2012, 9 (1): 111-116.

[6] Yuan H, Liu Y M, Pan G Z, et al. Quantum identity authentication based on ping-pong technique without entanglements [J]. Quantum Information Processing, 2014, 13 (11): 2535-2549.

[7] Ma H, Huang P, Bao W, et al. Continuous-variable quantum identity authentication based on quantum teleportation [J]. Quantum Information Processing, 2016, 15 (6): 2605-2620.

[8] Ma S Q, Zhu C H, Pei C X. A practical identity authentication scheme for measurement-device-independent quantum key distribution [C]// Proc of Computer, Information and Telecommunication Systems. 2017: 274-278.

[9] Yang Y G, Wen Q Y. Economical multiparty simultaneous quantum identity authentication based on greenberger–horne–zeilinger states [J]. Chinese Physics B, 2009, 18 (8): 3233-3237.

[10] Yang Y G, Wang H Y, Jia X, et al. A quantum protocol for (t, n)-threshold identity authentication based on greenberger-horne-zeilinger states [J]. International Journal of Theoretical Physics, 2013, 52 (2): 524-530.

[11] 张沛, 周小清, 李智伟. 基于量子隐形传态的无线通信网络身份认证方案 [J]. 物理学报, 2014, 63 (13): 19-24.

[12] Wang D, He D, Wang P, et al. Anonymous two-factor authentication in distributed systems: certain goals are beyond attainment [J]. IEEE Trans on Dependable and Secure Computing, 2015, 12 (4): 428-442.

[13] Wang D, Wang P. Two birds with one stone: two-factor authentication with security beyond conventional bound [J]. IEEE Trans on Dependable and Secure Computing, 2016, PP (99): 1-22.

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