Article

Two Quantum Proxy Blind Signature Schemes Based on Controlled Quantum Teleportation

Qiming Luo [1]**, Tinggui Zhang** [1,2,*]**, Xiaofen Huang** [1,2] **and Naihuan Jing** [3,4]

1   School of Mathematics and Statistics, Hainan Normal University, Haikou 571158, China
2   Key Laboratory of Data Science and Smart Education, Ministry of Education, Hainan Normal University, Haikou 571158, China
3   Department of Mathematics, North Carolina State University, Raleigh, NC 27695, USA
4   College of Sciences, Shanghai University, Shanghai 200444, China
*   Correspondence: tinggui333@163.com

Abstract: We present a scheme for teleporting an unknown, two-particle entangled state with a message from a sender (Alice) to a receiver (Bob) via a six-particle entangled channel. We also present another scheme for teleporting an unknown one-particle entangled state with a message transmitted in a two-way form between the same sender and receiver via a five-qubit cluster state. One-way hash functions, Bell-state measurements, and unitary operations are adopted in these two schemes. Our schemes use the physical characteristics of quantum mechanics to implement delegation, signature, and verification processes. Moreover, a quantum key distribution protocol and a one-time pad are adopted in these schemes.

Keywords: quantum teleportation; quantum signature; proxy signature; blind signature

PACS: 03.67.-a; 02.20.Hj; 03.65.-w

1. Introduction

Following the in-depth development of quantum key distribution (QKD) [1–3], various quantum cryptographic protocols have been developed, such as the quantum secure direct communication [4–7], quantum private query [8–10], quantum secret sharing [11–13], quantum multiparty secure computations [14,15], quantum authentication [16–18], quantum signature [19], and others. To ensure the safety of quantum cryptographic protocols, some attacking strategies on quantum cryptography protocols have been proposed, such as intercepted-resend [20,21], entanglement-swapping [22,23], teleportation [24], dense-coding [25–27], channel-loss [28], denial-of-service [29,30], correlation-extractability [31,32], trojan-horse [33,34], information-leakage [35], collusive attacks [36], and others. These effective attack strategies helped the design of new quantum cryptography schemes that are more secured.

In recent years, many different quantum signature schemes have been proposed for different application environments, including (but not limited to) quantum blind [37,38], quantum proxy [39,40], quantum multiple [41,42], quantum group [43,44], and others. In 2013, Zhang et al. proposed a secure quantum group signature scheme based on the Bell state [45], and they also presented the cryptanalysis of the quantum group signature protocol [46]. These signature schemes can be applied to e-commerce or other related fields.

The digital signature, which was independently introduced by Diffe [47] and Merkle [48], has been an important branch of cryptography. Digital signatures constitute a very important research topic in classic cryptography as it has many applications in real life. The security of classical signature schemes is based on complex mathematical problems, such as factorization and discrete logarithm problems. However, classic signatures are becoming increasingly vulnerable as quantum algorithms develop further. Fortunately,

in quantum information processing and computation, quantum cryptography can provide secure communication based on quantum mechanics, especially when based on the no-cloning theorem. Inspired by these properties, some progress has been achieved in the field of quantum signatures [49–51].

Proxy signatures, which allow the original signer to authorize the proxy signer to sign messages on his behalf, plays a key role in cryptography. Since Mambo et al. [52] proposed the concept of the proxy signature in 1996, some signature schemes have been proposed. Wang et al. [53] proposed a one-time proxy signature scheme without decoherence. Yang et al. [54] subsequently indicated that this scheme could not meet the security requirements of non-forgery and nonrepudiation. However, Wang et al. [55] showed in 2015 that this conclusion was not appropriate. Recently, Cao et al. [39,56] presented two quantum proxy signature schemes based on some genuine six- and five-qubit entangled states. However, Zhang et al. [57] suggested that receivers could forge valid signatures. In 2015, Tian et al. [58] presented a quantum multi-proxy blind signature scheme based on four-qubit entangled states with fewer resources.

The blind signature is a special digital signature that can protect the anonymity of the message owner to ensure privacy. In blind signatures, the message owner can always obtain the real signature of his message, even if the signer knows nothing about the content of his signature. Blind signatures can be classified into weak and strong blind signatures based on whether the signer can track the message owner. Chaum proposed the first blind signature scheme in 1983 based on the complexity of factoring large integers [59]. However, it was easily broken with the emergence of quantum computers. In 2010, Su et al. [38] presented a weak blind quantum signature scheme based on a two-state vector formalism. They used EPR pairs to implement the signature process, and applied the characteristics of the two-state vector form to implement the verification scheme. In recent years, quantum signature schemes have received extensive attention.

In this study, we propose two quantum proxy blind signature schemes based on controlled quantum teleportation. The first scheme takes advantage of the correlation of the maximal EPR and four-qubit entangled states, Bell-state measurements (BMs), $\{|0\rangle, |1\rangle\}$ basis measurements, Hadamard operation, quantum-key distribution, and unitary operations. In this scheme, two particles are delivered to the original signer, Alice. The proxy signers Charlie and David hold one particle each. The remaining two particles are distributed to the verifier, Bob. The second scheme is bidirectional, taking advantage of the correlation of the five-qubit cluster state, BMs, $\{|+\rangle, |-\rangle\}$ basis measurements, quantum-key distribution, and unitary operations. In this scheme, two particles are delivered to the original signer and verifier, Alice. The proxy signer Charlie holds one particle. The other two particles are distributed to the verifier and original signer, Bob. We used the quantum key distribution and a one-time pad to guarantee the unconditional security and signature anonymity. It is shown to be unconditionally secured, i.e., may not be forged or modified in any way by the receiver or attacker. In addition, it may neither be disavowed by the signatory, nor denied by the receiver.

2. Controlled Quantum Teleportation of the First Scheme

Our multiproxy blind signature scheme is based on the controlled quantum teleportation that uses the maximal EPR state and maximal four-qubit entangled states as its quantum channel. It is given by

$$
\begin{aligned}
|\psi\rangle_{3456} &= \frac{1}{2\sqrt{2}}(|0000\rangle - |0111\rangle + |1001\rangle - |1110\rangle \\
&\quad + |0110\rangle + |0001\rangle + |1111\rangle + |1000\rangle)_{3456},
\end{aligned}
\tag{1}
$$

$$
|\psi\rangle_{78} = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{78}.
\tag{2}
$$

Suppose that the quantum state of particle carrying message in Alice is

$$|\phi\rangle_{12} = (\alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle)_{12}, \tag{3}$$

where the unknown coefficients α, β, γ and δ satisfy $|\alpha|^2 + |\beta|^2 + |\gamma|^2 + |\delta|^2 = 1$.

This controlled quantum teleportation scheme involves the following four partners: the sender (Alice), two controllers (Charlie and David), and the receiver (Bob). Alice holds particles (1,2,3,7), Bob holds particles (6,8), and Charlie and David own particles 4 and 5. Therefore, the quantum state $|\Psi\rangle$ of the entire system composed of particles (1,2,3,4,5,6,7,8) is as follows

$$|\Psi\rangle = |\phi\rangle_{12} \otimes |\psi\rangle_{3456} \otimes |\psi\rangle_{78}. \tag{4}$$

The steps of the controlled quantum teleportation are as follows (the detailed process is described in reference [60]).

(1) Alice performs BMs on particles (1,3) and (2,7). These are 16 possible outcomes.
(2) Alice sends her measurement outcomes to Bob through a secure quantum channel. Bob then performs a corresponding unitary operation on particles (6,8).
(3) If Charlie and David agree with Alice and Bob to complete their teleportation process, they perform the Hadamard operation on their particles, respectively. Subsequently, they perform a $\{|0\rangle, |1\rangle\}$ based measurement on their particles. They then send their measurement outcomes to Bob through a secure quantum channel.
(4) When the two measurements are the same, Bob will obtain the quantum state transferred from Alice. When the two measurements are different, Bob just needs to apply the unitary operation σ_x on particle 6, whereupon the same receiver obtains the quantum state transferred from Alice.

3. Quantum Multiproxy Blind Signature Scheme

In our scheme, the participants are defined as follows.

(i) Alice: the original signer; (ii) Bob: the message receiver; (iii) Charlie and David: two proxy signer; and (iiii) Trent: the message verifier and trusted party.

The detailed procedure of our scheme can be described as follows.

3.1. Initial Phase

(i) QKD. Alice shares the secret key K_{AB} with Bob. In addition, Bob establishes the secret keys K_{BC} with Charlie and K_{BD} with David. Moreover, Trent shares the secret keys K_{TA} with Alice, K_{TB} with Bob, K_{TC} with Charlie, and K_{TD} with David. These distribution tasks can be fulfilled via QKD protocols, which have been proved to be unconditionally safe.
(ii) Quantum Channel Establishment. Bob produces $t + l$ quantum states $|\psi\rangle_{3456}$ and $|\psi\rangle_{78}$. He sends particles (3,7) to Alice, particle 4 to Charlie, and particle 5 to David, leaving particles (6,8) to himself.
(iii) To ensure security of the quantum channel, Bob arranges eavesdropping checks.

3.2. Blinding the Message Phase

(i) Alice converts her message m into an N-bit sequence and records $m = \{m(1), m(2), \dots, m(j), \dots, m(N)\}$. Subsequently, Alice sends the binary sequence m to Trent.
(ii) Alice transforms m to $H(m)$ by using a Hash function, where $H: \{0, 1\}^N \to \{0, 1\}^n (N \gg n)$, and Trent also knows the Hash function H. She then blinds the message based on $M(i) = K_{TA} \oplus m(i), i = 1, 2, \dots, n$, where $\oplus$ is the XOR operation. She can identify an appropriate Hash function, such that n is an even umber. Let $l = \frac{n}{2}$.
(iii) Alice produces $\frac{n}{2}$ quantum states $|\phi\rangle_{12} = (\alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle)_{12}$, denoted as $|\phi\rangle_{12}(1), |\phi\rangle_{12}(2), \dots, |\phi\rangle_{12}(\frac{n}{2})$. If $m(i) = 00, |\phi\rangle_{12} = |00\rangle$; If $m(i) = 01, |\phi\rangle_{12} = |01\rangle$; if $m(i) = 10, |\phi\rangle_{12} = |10\rangle$; if $m(i) = 11, |\phi\rangle_{12} = |11\rangle$.

3.3. Authorizing and Signing Phases

In our scheme, we used a one-time pad as the encryption algorithm to ensure unconditional security.

(i)   If Alice agrees with Charlie and David as her proxy signers to sign the message, she will help to perform controlled teleportation. Alice performs the BMs on particles (1,3) and (2,7) and records the measurement outcomes as S_A. She then encrypts S_A with the key K_{AB} to obtain the secret message $E_{K_{AB}}\{S_A\}$. Alice sends the message $E_{K_{TA}}\{S_A\}$ to Trent via the quantum channel. Similarly, Alice sends the message $E_{K_{AB}}\{S_A\}$ to Bob via the quantum channel.

(ii)   After Bob has received the message $E_{K_{AB}}\{S_A\}$, he decrypts it with his K_{AB} to obtain the message S_A. Bob then performs corresponding unitary operations on particles (6,8). After this, he encrypts S_A with the keys K_{BC} and K_{BD} to obtain the secret messages $E_{K_{BC}}\{S_A\}$ and $E_{K_{BD}}\{S_A\}$, respectively. Bob sends the messages $E_{K_{BC}}\{S_A\}$ and $E_{K_{BD}}\{S_A\}$ to Charlie and David, respectively, via the quantum channel.

(iii)   After Charlie and David have received the messages $E_{K_{BC}}\{S_A\}$ and $E_{K_{BD}}\{S_A\}$, they decrypt it with their keys K_{BC} and K_{BD} to obtain the message S_A. They then perform the Hadamard operation on their particles. Subsequently, they perform a $\{|0\rangle,|1\rangle\}$ based measurement on their particles, and they note the measurement outcomes as $S_C = \{c(1), c(2), \ldots c(i), \ldots, c(\frac{n}{2})\}$ and $S_D = \{d(1), d(2), \ldots d(i), \ldots, d(\frac{n}{2})\}$. Charlie then encrypts $\{S_A, S_C\}$ with the use of the key K_{BC} to obtain the secret message $S_1 = E_{K_{BC}}\{S_A, S_C\}$, and David also encrypts $\{S_A, S_D\}$ with the key K_{BD} to obtain the secret message $S_2 = E_{K_{BD}}\{S_A, S_D\}$. They send the messages S_1 and S_2 to Bob as the proxy authorization. Similarly, they send $\{S_A, S_C\}$ and $\{S_A, S_D\}$ to Trent by K_{TC} and K_{TD}.

3.4. Verifying Phases

(i)   Bob receives the messages S_A, S_C and S_D by using the keys K_{BC} and K_{BD} to decrypt S_1 and S_2. If S_A in the proxy signature does not match that sent by Alice, the signature verification process will be terminated, and the signature will be declared invalid. Otherwise, the process continues based on the following steps.

(ii)   According to S_C and S_D, Bob performs an appropriate unitary operation on particle 6 to replicate the unknown state $|\phi\rangle_{12}$ which carries the messages. He then sends the state $|\phi\rangle_{12}$ to Trent.

(iii)   Trent encodes the quantum state $|\phi\rangle_{1'2'}$ to obtain the message M'. If $M' = M$, he confirms a series of signatures and messages (m, S_C, S_D). Otherwise, Trent rejects it.

4. Security Analysis and Discussion of the First Scheme

In this section, we will demonstrate that our scheme meets the following security requirements in accordance with reference [57].

4.1. Message Blindness

Alice blinded the message m to M. Proxy signers Charlie and David could not obtain the contents of the messages because Alice used hash functions and XOR operations to blind them. Therefore, Charlie and David could not know the content of the information she signed.

4.2. Impossibility of Denial

In this scheme, we prove that Alice cannot refuse her delegation, and Charlie and David cannot refuse their signatures. If the signature is verified, the signer cannot reject its signature or message for the following reasons: (1) the signature is encrypted by the key, and (2) the entangled states have stable coherence among particles. Only by measuring their own particles can they achieve teleportation. All keys are distributed based on the QKD protocol, which has been unconditionally proved. All messages are sent through

secure quantum channels. Therefore, Alice cannot refuse her delegation, nor can Charlie and David refuse their signatures.

4.3. Impossibility of Forgery

Firstly, we assume that Trent is completely credible. We can prove that Charlie and David cannot forge Alice's signature. In our scheme, trusted Trent can prevent these attacks. Suppose Charlie tries to forge Alice's signature. Even if he knows the key, he cannot forge any signature because Charlie's forgery attack will be detected by Trent. Similarly, David could not input Alice's signature for Charlie's signature. In other words, internal attackers cannot forge their signatures.

Secondly, we assumed that there was an external attacker (Eve). Eve cannot obtain the secret key. Therefore, she cannot forge the signatures of Alice, Charlie, and David. We assumed that Eve could obtain the secret key randomly and generate a valid signature with the probability $\frac{1}{2^n}$ tending to zero when n tends to infinity. At the same time, we realized the eavesdropping detection function in the construction stage of the quantum channel. Therefore, the signing process will only continue when the channel is secure; otherwise, the signing process will terminate. Therefore, Eve cannot forge their signatures.

5. Controlled Quantum Teleportation of the Second Scheme

Our two-way proxy blind signature scheme is based on controlled quantum teleportation that uses the five-qubit cluster state as its quantum channel. It is given by,

$$|\phi\rangle_{12345} = \frac{1}{2}(|00000\rangle + |00111\rangle + |11101\rangle + |11010\rangle). \tag{5}$$

Suppose that the quantum state of the particle-carrying message for Alice is

$$\begin{aligned} |\phi\rangle_A &= (\alpha|0\rangle + \beta|1\rangle)_A, \\ |\phi\rangle_B &= (\gamma|0\rangle + \delta|1\rangle)_B, \end{aligned} \tag{6}$$

where the unknown coefficients α, β, γ and δ satisfy $|\alpha|^2 + |\beta|^2 = 1$ and $|\gamma|^2 + |\delta|^2 = 1$.

This controlled quantum teleportation involves the following three partners: the sender and receiver Alice, sender and receiver Bob, and the controller Charlie. Alice holds particles (1,5,A), Bob holds particles (2,3,B), and Charlie owns particle 4. Thus, the quantum states $|\Psi\rangle$ of the entire system takes the following form

$$|\Psi\rangle = |\phi\rangle_B \otimes |\phi\rangle_A \otimes |\phi\rangle_{12345}. \tag{7}$$

The steps of the controlled quantum teleportation are as follows (the detailed process is described in reference [61]).

(1) Alice performs BMs on particles (A,1) and Bob performs BMs on particles (B,3), respectively. These are 16 types of possible outcomes.

(2) Alice sends her measurement outcomes to Bob and Charlie through the secured quantum channel. Bob sends his measurement outcomes to Alice and Charlie.

(3) If Charlie agrees with Alice and Bob to complete their two-way teleportation processes, he performs a $\{|+\rangle, |-\rangle\}$ based measurement on particle 4. He then sends his measurement outcomes to Alice and Bob through the secured quantum channel.

(4) Bob performs a corresponding unitary operation on particle 2, whereupon Bob receives the quantum state transferred from Alice. The same applies for Alice who receives the quantum state for particle 5 transferred from Bob.

6. Quantum Two-Way Proxy Blind Signature Scheme

In our scheme, participants are defined as follows:

(i) Alice and Bob: the original signers; (ii) Charlie: the proxy signer; and (iii) Trent: the message verifier and the trusted party.

The detailed procedure of our scheme is as follows.

6.1. Initial Phase

(i) QKD. Alice shares the secret key K_{AB} with Bob and shares the secret key K_{AC} with Charlie. In addition, Bob establishes the secret key K_{BC} with Charlie. Moreover, Trent shares the secret keys K_{TA} with Alice, K_{TB} with Bob, and K_{TC} with Charlie. These distribution tasks can be fulfilled via QKD protocols, which have been proven to be unconditionally secured.

(ii) Quantum Channel Establishment. Bob produces $p + q$ quantum states $|\phi\rangle_{12345}$. He sends particles (1,5) to Alice, particle 4 to Charlie, and leaves particles (2,3) to himself.

(iii) To ensure the security of the quantum channel, Bob arranges eavesdropping checks.

6.2. Blinding the Message Phase

(i) Alice converts the message m' into a K-bit sequence and records $m' = \{m'(1), m'(2), \ldots, m'(j), \ldots, m'(K)\}$. Subsequently, Alice sends the binary sequence m' to Trent. Similarly, Bob converts the message m'' into an R-bit sequence and records $m'' = \{m''(1), m''(2), \ldots, m''(j), \ldots, m''(R)\}$. Subsequently, Bob sends the binary sequence m'' to Trent.

(ii) Alice converts m' to $H'(m')$ by using the Hash function, where H', $\{0,1\}^K \rightarrow \{0,1\}^q (K \gg q)$, and Trent also knows the Hash function H'. She then blinds the message by $M'(i) = K_{TA} \oplus m'(i), i = 1, 2, \ldots, q$, where $\oplus$ is the XOR operation. Similarly, Bob converts m'' to $H'(m'')$ by using the Hash function, where $H': \{0,1\}^K \rightarrow \{0,1\}^q (K \gg q)$. He then blinds the message by $M''(i) = K_{TB} \oplus m''(i), i = 1, 2, \ldots, q$.

(iii) Alice produces q quantum states $|\phi\rangle_A = (\alpha|0\rangle + \beta|1\rangle)_A$, denoted as $|\phi\rangle_A(1), |\phi\rangle_A(2), \ldots, |\phi\rangle_A(q)$. Similarly, Bob produces q quantum states $|\phi\rangle_B = (\gamma|0\rangle + \delta|1\rangle)_B$, denoted as $|\phi\rangle_B(1), |\phi\rangle_B(2), \ldots, |\phi\rangle_B(q)$.

6.3. Authorizing and Signing Phase

In our scheme, we used the one-time pad as the encryption algorithm to ensure unconditional security.

(i) If Alice agrees that Charlie can act as her proxy signer to sign the message, she will help the execution of controlled teleportation. Alice performs the BM on particles (A,1) and records the measured outcomes as S_A. She then encrypts S_A with the keys K_{AB} and K_{AC} to obtain the secret messages $E_{K_{AB}}\{S_A\}$ and $E_{K_{AC}}\{S_A\}$. Alice sends the messages $E_{K_{AB}}\{S_A\}$ to Bob and $E_{K_{AC}}\{S_A\}$ to Charlie via the quantum channel. Similarly, If Bob agrees that Charlie can act as his proxy signer to sign the message, he will help the execution of controlled teleportation. Bob performs the BM on particles (B,3) and records the measuring outcomes as S_B. He then encrypts S_B with the keys K_{AB} and K_{BC} to obtain the secret messages $E_{K_{AB}}\{S_B\}$ and $E_{K_{BC}}\{S_B\}$. Bob sends the messages $E_{K_{AB}}\{S_B\}$ to Alice and $E_{K_{BC}}\{S_B\}$ to Charlie via the quantum channel.

(ii) After Charlie has received the messages $E_{K_{AC}}\{S_A\}$ and $E_{K_{BC}}\{S_B\}$, he decrypts them with their keys K_{AC} and K_{BC} to obtain the messages S_A and S_B. Charlie then performs a $\{|+\rangle, |-\rangle\}$ based measurement on particle 4, and he notes the measured outcome as $S_C = \{c(1), c(2), \ldots c(i), \ldots, c(q)\}$. Charlie encrypts $\{S_A, S_C\}$ with the use of the key K_{BC} to obtain the secret message $S_1 = E_{K_{BC}}\{S_A, S_C\}$, and also encrypts $\{S_B, S_C\}$ with the use of the key K_{BC} to obtain the secret message $S_2 = E_{K_{BC}}\{S_B, S_C\}$. He then sends the messages S_1 to Bob and S_2 to Alice as the proxy authorization. Similarly, Charlie sends $\{S_A, S_C\}$ and $\{S_B, S_C\}$ to Trent by using K_{TA} and K_{TB}, respectively.

6.4. Verifying Phases

(i) Bob receives the messages S_A, S_C by using the key K_{BC} to decrypt S_1. If S_A in the proxy signature does not match that sent by Alice, the signature verification process will be terminated, and the signature will be declared invalid. Otherwise, continue with the steps which follow (ii and iii). Similarly, Alice receives the messages S_B, S_C

by using the key K_{AC} to decrypt S_2. If S_B in the proxy signature does not match that sent by Bob, the signature verification process will be terminated, and the signature will be declared invalid. Otherwise, continue in accordance with the following steps.

(ii) According to S_A and S_C, Bob performs an appropriate unitary operation on particle 2 to replicate the unknown state $|\phi\rangle_{A'}$ which carries messages. Similarly, according to S_B and S_C, Alice performs an appropriate unitary operation on particle 5 to replicate the unknown state $|\phi\rangle_{B'}$ which carries messages. Alice and Bob then sends the states $|\phi\rangle_{B'}$ and $|\phi\rangle_{A'}$ to Trent.

(iii) Trent encodes the quantum state $|\phi\rangle_{A'}$ and obtains the message M'''. He then compares it with M'. If $M''' = M'$, he confirms a series of signatures and messages (m, S_A, S_C). Otherwise, Trent rejects it. Similarly, Trent encodes the quantum state $|\phi\rangle_{B'}$, obtains the message M'''' and compares it with M''. If $M'''' = M''$, he confirms a series of signatures and messages (m, S_B, S_C). Otherwise, Trent rejects it.

7. Security Analysis and Discussion of the Second Scheme

In this section, we will demonstrate that our scheme meets the following security requirements.

7.1. Message Blindness

Alice blinded the message m' to M', and Bob blinded the message m'' to M''. Proxy signer Charlie was unable to obtain the contents of the message because Alice and Bob used hash functions and XOR operations to blind messages. Therefore, Charlie cannot know the contents of the information he signed.

7.2. Impossibility of Denial

We verified that Alice and Bob could not refuse their delegations, nor could Charlie refuse his signature. If the signature is verified, the signer cannot reject its signature or message. This is due to the following factors: (1) the signature is encrypted by the key, and (2) the entangled states have stable coherence among particles. Teleportation can be achieved only by measuring their own particles. All keys are distributed through the QKD protocol, which has been unconditionally proven. All messages are sent through secure quantum channels. Therefore, Alice and Bob cannot deny their authorization, and Charlie cannot refuse his signature.

7.3. Impossibility of Forgery

Firstly, we can prove that Charlie cannot forge Alice's or Bob's signatures because trusted Trent can prevent these attacks in our scheme. Suppose that Charlie tries to forge Alice's signature. Even if he knows the key, he cannot forge any signature because Charlie's forgery attack will be detected by Trent. Likewise, Charlie cannot forge Bob's signature. In other words, internal attackers cannot forge signatures.

Secondly, we assumed that there was an external attacker (Eve). Eve cannot obtain the secret key. Therefore, she cannot forge their signatures. We also assumed that Eve could obtain the secret key randomly and generate a valid signature with the probability $\frac{1}{2^n}$ tending to zero when n tends to infinity. At the same time, we realized the eavesdropping detection function in the construction stage of the quantum channel. Therefore, the signing process will only continue when the channel is secure; otherwise, the signing will terminate. Therefore, Eve cannot forge their signatures.

8. Conclusions

In this study, we proposed two quantum proxy blind signature schemes based on controlled quantum teleportation. We presented a scheme for teleporting an unknown two-particle entangled state with a message from a sender (Alice) to a receiver (Bob) via a six-particle entangled channel. Additionally, we presented a scheme for teleporting an unknown, one-particle entangled state with a message passed in both directions be-

tween a sender (Alice) and a receiver (Bob) via a five-qubit cluster state. Our scheme used a one-way Hash function and XOR operations to blind the message. The security of the proposed schemes are guaranteed by the quantum one-time pad and quantum key distribution, which are different from the previous signature schemes in classical cryptography. In addition, compared with the existing quantum signature schemes, our schemes have some advantages. Firstly, unlike the quantum blind signature scheme, both schemes arranged eavesdropping checks to ensure security. Secondly, the first scheme used quantum teleportation to transmit two unknown qubit states, and were effective. Thirdly, owing to the maximum connectivity of cluster states and the persistence of entanglement, the second scheme was more secure. Fourthly, our scheme adopted BM and single-event measurements, which are easy to realize based on the existing technology and experimental conditions. Therefore, our scheme had a better security profile and could be applied to e-payment, e-commerce, e-voting, and other application scenarios.

However, the following problems still exist in quantum teleportation. (1) In quantum-teleportation experiments, the first step requires the preparation of the quantum channel (which is essentially the preparation of the quantum entangled state); the technology for preparing the multiparticle entangled state needs to be improved. (2) Moreover, when conducting quantum teleportation, the measurement of quantum states is a mandatory step, for which a high-precision measuring instrument is required. (3) Finally, when realizing the teleportation of quantum states, the particles need to pass through the quantum entanglement channel; during the process of transmission, various interference phenomena will occur. In other words, the teleportation process needs to be perfected to keep particles from being affected by external interference or physical factors in the process of transmission. The most prominent problem is the security problem after the combination of quantum teleportation and quantum signature. In the signature, we must prevent outside interferences, the infliction of harm on internal actors, and more importantly, the leakage of information. We believe that these problems can be overcome with further investigations.

Author Contributions: Methodology, N.J.; Project administration, T.Z.; Writing original draft, Q.L.; Writing review & editing, X.H. All authors have read and agreed to the published version of the manuscript.

Data Availability Statement: Data sharing not applicable to this article as no datasets were generated or analyzed during the current study.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Bennett, C.H. Quantum key distribution and coin tossing. In Proceedings of the International Conference on Computers, Bangalore, India, 9–12 December 1984.
2. Gobby, C.; Yuan, Z.L.; Shields, A.J. Quantum Key Distribution over 122km of Standard Telecommunication Fiber. *Appl. Phys. Lett.* **2004**, *84*, 3762–3764. [CrossRef]
3. Gao, F.; Guo, F.Z.; Wen, Q.Y. Quantum Key Distribution without Alternative Measurements and Rotations. *Phys. Lett. A* **2006**, *349*, 53–58. [CrossRef]
4. Lin, S.; Wen, Q.Y.; Zhu, F.C. Quantum Secure Direct Communication with χ-Type Entangled States. *Phys. Rev. A* **2008**, *78*, 064304. [CrossRef]
5. Long, G.L.; Liu, X.S. Theoretically efficient high-capacity quantum-key-distribution scheme. *Phys. Rev. A* **2002**, *65*, 032302. [CrossRef]
6. Wang, J.; Zhang, Q.; Tang, C.J. Quantum Secure Direct Communication Based on Order Rearrangement of Single Photons. *Phys. Lett. A* **2006**, *358*, 256–258. [CrossRef]

7. Xia, Y.; Song, H.S. Controlled Quantum Secure Direct Communication Using a Non-Symmetric Quantum Channel with Quantum Superdense Coding. *Phys. Lett. A* **2007**, *364*, 117–122. [CrossRef]
8. Gao, F.; Liu, B.; Huang, W.; Wen, Q.Y. Postprocessing of the Oblivious Key in Quantum Private Query. *IEEE J. Sel. Top. Quantum Electron.* **2015**, *3*, 98–108. [CrossRef]
9. Wei, C.Y.; Wang, T.Y.; Gao, F. Practical Quantum Private Query with Better Performance in Resisting Joint-Measurement Attack. *Phys. Rev. A* **2016**, *93*, 042318. [CrossRef]
10. Wei, C.Y.; Cai, X.Q.; Liu, B. A Generic Construction of Quantum-Oblivious-Key-Transfer-Based Private Query with Ideal Database Security and Zero Failure. *IEEE Trans. Comput.* **2018**, *67*, 2–8. [CrossRef]
11. Chen, X.B.; Niu, X.X.; Zhou, X.J.; Yang, Y.X. Multi-Party Quantum Secret Sharing with the Singleparticle Quantum State to Encode the Information. *Quantum Inf. Process.* **2013**, *12*, 365–380. [CrossRef]
12. Hillery, M.; Buzek, V.; Berthiaume, A. Quantum Secret Sharing. *Phys. Rev. A* **1999**, *59*, 1829. [CrossRef]
13. Bogdanski, J.; Rafiei, N.; Bourennane, M. Experimental Quantum Secret Sharing Using Telecommunication Fiber. *Phys. Rev. A* **2008**, *78*, 062307. [CrossRef]
14. Li, X.H.; Zhou, P.; Li, C.Y.; Zhou, H.Y.; Deng, F.G. Efficient Symmetric Multiparty Quantum State Sharing of an Arbitrary M-Qubit State. *J. Phys. At. Mol. Opt. Phys.* **2006**, *39*, 1975. [CrossRef]
15. Loukopoulos, K.; Browne, D.E. Secure Multiparty Computation with a Dishonest Majority via Quantum Means. *Phys. Rev. A* **2010**, *81*, 062336. [CrossRef]
16. Fujiwara, A. Quantum Channel Identification Problem. *Phys. Rev. A* **2001**, *63*, 042304. [CrossRef]
17. Lee, H.; Lim, J.; Yang, H.J. Quantum Direct Communication with Authentication. *Phys. Rev. A* **2006**, *73*, 042305. [CrossRef]
18. Curty, M.; Santos, D.J. Quantum Authentication of Classical Messages. *Phys. Rev. A* **2001**, *64*, 062309. [CrossRef]
19. Zhang, H.Y.; Zhang, L.; Zhang, K.J. A New Quantum Proxy Signature Model Based on a Series of Genuine Entangled States. *Int. J. Theor. Phys.* **2019**, *58*, 591–604. [CrossRef]
20. Gao, F.; Guo, F.Z.; Wen, Q.Y.; Zhu, F.C. Comment on Experimental Demonstration of a Quantum Protocol for Byzantine Agreement and Liar Detection. *Phys. Rev. Lett.* **2008**, *101*, 208901. [CrossRef]
21. Chen, X.B.; Yang, S.; Xu, G.; Su, Y.; Yang, Y.X. Cryptanalysis of the Quantum State Sharing Protocol Using Four Sets of W-Class States. *Int. J. Quantum Inf.* **2013**, *11*, 1350010. [CrossRef]
22. Zhang, Y.S.; Li, C.F.; Guo, G.C. Comment on Quantum Key Distribution without Alternative Measurements. *Phys. Rev. A* **2001**, *63*, 036301. [CrossRef]
23. Gao, F.; Qin, S.J.; Wen, Q.Y.; Zhu, F.C. A Simple Participant Attack on the Bradler-Dusek Protocol. *Quantum Inf. Comput.* **2007**, *7*, 329–334. [CrossRef]
24. Gao, F.; Wen, Q.Y.; Zhu, F.C. Teleportation Attack on the QSDC Protocol with a Random Basis and Order. *Chin. Phys. B.* **2008**, *17*, 3189.
25. Gao, F.; Qin, S.J.; Guo, F.Z.; Wen, Q.Y. Dense-Coding Attack on Three-Party Quantum Key Distribution Protocols. *IEEE J. Quantum Electron.* **2011**, *47*, 630–635.
26. Hao, L.; Li, J.L.; Long, G.L. Eavesdropping in a Quantum Secret Sharing Protocol Based on Grover Algorithm and its Solution. Science China Physics. *Mech. Astron.* **2010**, *53*, 491–495. [CrossRef]
27. Qin, S.J.; Ga, F.; Wen, Q.Y.; Zhu, F.C. Improving the Security of Multiparty Quantum Secret Sharing Against an Attack with a Fake Signal. *Phys. Lett. A* **2006**, *357*, 101–103. [CrossRef]
28. Wojcik, A. Eavesdropping on the Ping-Pong Quantum Communication Protocol. *Phys. Rev. Lett.* **2003**, *90*, 157901. [CrossRef] [PubMed]
29. Cai, Q.Y. The Ping-Pong Protocol Can Be Attacked without Eavesdropping. *Phys. Rev. Lett.* **2003**, *91*, 109801. [CrossRef] [PubMed]
30. Gao, F.; Guo, F.Z.; Wen, Q.Y.; Zhu, F.C. Consistency of Shared Reference Frames Should Be Reexamined. *Phys. Rev. A* **2008**, *77*, 014302. [CrossRef]
31. Gao, F.; Qin, S.J.; Wen, Q.Y.; Zhu, F.C. Cryptanalysis of Multiparty Controlled Quantum Secure Direct Communication Using Greenberger-Horne-Zeilinger State. *Opt. Commun.* **2010**, *283*, 192–195. [CrossRef]
32. Gao, F.; Lin, S.; Wen, Q.Y.; Zhu, F.C. A Special Eavesdropping on One-Sender Versus N-Receiver QSDC Protocol. *Chin. Phys. Lett.* **2008**, *25*, 1561.
33. Gisin, N.; Fasel, S.; Kraus, B.; Zbinden, H.; Ribordy, G. Trojan Horse Attacks on Quantum Key Distribution Systems. *Phys. Rev. A* **2006**, *73*, 022320. [CrossRef]
34. Deng, F.G.; Li, X.H.; Zhou, H.Y.; Zhang, Z.J. Improving the Security of Multi-party Quantum Secret Sharing Against Trojan Horse Attack. *Phys. Rev. A* **2005**, *72*, 044302. [CrossRef]
35. Gao, F.; Guo, F.Z.; Wen, Q.Y.; Zhu, F.C. Revisiting the Security of Quantum Dialogue and Bidirectional Quantum Secure Direct Communication. *Sci. China Ser. Phys. Mech. Astron.* **2008**, *51*, 559–566. [CrossRef]
36. Wang, T.Y.; Wen, Q.Y.; Zhu, F.C. Cryptanalysis of Multiparty Quantum Secret Sharing with Bell States and Bell Measurements. *Opt. Commun.* **2011**, *284*, 1711–1713. [CrossRef]
37. Cai, X.Q.; Niu, H.F. Partially Blind Signature Based on Quantum Cryptography. *Int. J. Mod. Phys. B* **2012**, *26*, 1250163. [CrossRef]
38. Su, Q.; Huang, Z.; Wen, Q.Y.; Li, W.M. Quantum Blind Signature Based on Two-State Vector Formalism. *Opt. Commun.* **2010**, *283*, 4408–4410.

39. Cao, H.J.; Huang, J.; Yu, Y.F.; Jiang, X.L. A Quantum Proxy Signature Scheme Based on Genuine Five-Qubit Entangled State. *Int. J. Theor. Phys.* **2014**, *53*, 3095–3100. [CrossRef]

40. Zhou, J.X.; Zhou, Y.J.; Niu, X.X.; Yang, Y.X. Quantum Proxy Signature with Public Verifiability. *Sci. China Phys. Mech. Astron.* **2011**, *54*, 1828–1832. [CrossRef]

41. Wen, X.J.; Liu, Y. A Realizable Quantum Sequential Multi-Signature Scheme. *Acta Electron. Sin.* **2007**, *35*, 1079.

42. Wen, X.J.; Liu, Y.; Zhou, N.R. Realizable Quantum Broadcasting Multi-Signature Scheme. *Int. J. Mod. Phys. B* **2008**, *22*, 4251–4259. [CrossRef]

43. Wen, X.J.; Tian, Y.; Ji, L.P.; Niu, X.M. A Group Signature Scheme Based on Quantum Teleportation. *Phys. Scr.* **2010**, *81*, 055001. [CrossRef]

44. Xu, R.; Huang, L.S.; Yang, W.; He, L.B. Quantum Group Blind Signature Scheme without Entanglement. *Opt. Commun.* **2011**, *284*, 3654–3658. [CrossRef]

45. Zhang, K.J.; Song, T.T.; Zuo, H.J.; Zhang, W.W. A Secure Quantum Group Signature Scheme Based on Bell States. *Phys. Scr.* **2013**, *87*, 045012. [CrossRef]

46. Zhang, K.J.; Sun, Y.; Song, T.T.; Zuo, H.J. Cryptanalysis of the Quantum Group Signature Protocols. *Int. J. Theor. Phys.* **2013**, *52*, 4163–4173. [CrossRef]

47. Diffie, W.; Hellman, M. New directions in cryptography. *IEEE Trans. Inf. Theory* **1976**, *22*, 644. [CrossRef]

48. Merkle, R. *Authentication, and Public Key Systems*; Stanford University: Stanford, CA, USA, 1979.

49. Wang, T.Y.; Ma, J.F.; Cai, X.Q. The postprocessing of quantum digital signatures. *Quantum Inf. Process.* **2017**, *16*, 19. [CrossRef]

50. Wang, T.Y.; Cai, X.Q.; Zhang, R.L. Security of a sessional blind signature based on quantum cryptograph. *Quantum Inf. Process.* **2014**, *13*, 1677–1685. [CrossRef]

51. Du, H.; Wen, Q. Certificateless proxy multi-signature. *Inf. Sci.* **2014**, *276*, 21–30. [CrossRef]

52. Mambo, M.; Usuda, K.; Okamoto, E. Proxy signature: Delegation of the power to sign messages. *IEICE Trans. Fundam. A* **1996**, *79*, 1338–1354.

53. Wang, T.Y.; Wei, Z.L. One-time proxy signature based on quantum cryptography. *Quantum Inf. Process.* **2012**, *11*, 455–463. [CrossRef]

54. Yang, C.W.; Luo, Y.P.; Hwang, T. Forgery attack on one-time proxy signature and the improvement. *Quantum Inf. Process.* **2014**, *13*, 2007–2016. [CrossRef]

55. Wang, T.Y.; Wei, Z.L. Analysis of forgery attack on one-time proxy signature and the improvement. *Int. J. Theor. Phys* **2015**, *55*, 743–745. [CrossRef]

56. Cao, H.J.; Wang, H.S.; Li, P.F. Quantum proxy multi-signature scheme using genuinely entangled six qubits state. *Int. J. Theor. Phys.* **2013**, *52*, 1188–1193. [CrossRef]

57. Zhang, L.; Zhang, H.Y.; Zhang, K.J.; Wang, Q.L. The security analysis and improvement of some novel quantum proxy signature scheme. *Int. J. Theor. Phys.* **2017**, *56*, 1983–1994. [CrossRef]

58. Tian, J.H.; Zhang, J.Z.; Li, Y.P. A quantum multi-proxy blind signature scheme based on genuine fourqubit entangled state. *Int. J. Theor. Phys.* **2016**, *55*, 809–816. [CrossRef]

59. Chaum, D.; Rivest, R.L.; Sherman, A.T. Blind Signatures for Untraceable Payments. In *Advances in Cryptology*; Springer: Boston, MA, USA, 1983; pp. 199–203.

60. Peng, T. Research on Controlled Teleportation of Two-Particle and Three-Particle Entanglement. Master's Thesis, Huazhong University of Science and Technology, Wuhan, China, 2007.

61. Zheng, X.Y. Controlled two-way quantum teleportation based on five particle cluster state. *Chin. J. Quantum Electron.* **2016**, *33*, 177.