A Novel Quantum Proxy Blind Signature Scheme

Wei Guo[1] · Shu-Cui Xie[2] · Jian-Zhong Zhang[1]

Received: 10 September 2016 / Accepted: 8 February 2017 / Published online: 22 February 2017

Abstract A novel quantum proxy blind signature scheme is proposed. In this scheme, a special type of non-maximally entangled three-qubit state is introduced as a quantum channel, which can realize perfect teleportation. The message sender U blinds his message by means of preparing two groups of non-orthogonal single-photon states. According to the original signer Charlie's delegation message, the proxy signer Alice generates a corresponding signature. The arbitrator Trent can help the receiver Bob verify the signature, and also prevent Bob from doing any damage. The above-mentioned advantages make this scheme different from some existing schemes. It is showed that our scheme has the properties of undeniability, unforgeability, blindness, untraceability. Moreover, it is free from intercept-resend attack.

Keywords Quantum cryptography · Quantum signature scheme · Proxy signature · Blind signature

1 Introduction

With the combination of information theory and quantum mechanics, quantum information has been developed into a novel interdisciplinary subject in recent years. Quantum cryptography, as an emerging and rapidly developing subdiscipline, has become a hot research topic in the field of quantum information. In contrast to the security of classical public key cryptography, the security of quantum cryptography is based on the principle of

✉ Jian-Zhong Zhang
crypto-guo.0328@snnu.edu.cn

[1] College of Mathematics and Information Science, Shaanxi Normal University, Xi'an, 710119, China

[2] College of Science, Xi'an University of Posts and Telecommunications, Xi'an, 710121, China

quantum mechanics instead of computational complexity. Nowadays, many protocols have been presented in quantum cryptography, such as quantum key distribution [1–3], quantum encryption algorithm[4, 5], quantum secure authentication[6, 7], quantum secret sharing [8–10], quantum secure direct communication, quantum signature scheme, etc. Most notably, it has been proved that quantum key distribution protocol is unconditionally secure in both theoretical researches and experimental works.

Different from the quantum key distribution protocol which is used to set up a random secret key between two parties, a quantum secure direct communication is a protocol whose aim is to transmit important information directly. Deng et al. [11] proposed a two-step quantum direct communication protocol using the Einstein-Podolsky-Rosen (EPR) pair block. Then they also proposed a secure direct communication with a quantum one-time pad [12]. In their scheme, a batch of single photons was used directly to encode a secret message. A deterministic secure communication without using entanglement was presented by Cai et al. [13], the security of their scheme is based on the security proof of BB84 protocol. Wang et al. [14] put forward a multiparty controlled quantum secure direct communication using Greenberger-Horne-Zeilinger (GHZ) state.

In recent years, much more attention has been paid to quantum signature scheme, which is one of the most important ingredients of quantum cryptography. An arbitrated quantum signature (AQS) scheme based on a three-particle GHZ state was proposed by Zeng et al. [15]. Since then, many arbitrated quantum signature schemes [16–19] have been put forward. More recently, Wen et al. [20–22] presented different kinds of quantum signature schemes based on quantum teleportation.

Chaum [23] first proposed a blind signature scheme. It allows a signer to sign a message without knowing the content of the message. A weak blind signature scheme based on the characteristic of EPR pairs was presented by Wen et al. [24]. However, Naseri [25] showed that their scheme does not complete the task of a blind signature fairly. A fair quantum blind signature was proposed by Wang et al. [26], which is composed of a signing protocol and a link-recovery protocol. Afterwards, He et al. [27] investigated the scheme and pointed out that it can not satisfy the property of unforgeability. Wang et al. [28] proposed a quantum blind signature protocol using GHZ states. A quantum partially blind signature was presented by Cai et al. [29] to protect the signer's legitimate interest.

The concept of proxy signature was first introduced by Mambo, Usuda and Okamoto in 1996 [30]. It allows a proxy signer to sign a message on behalf of an original signer in the case that the original signer is not present because of business trip, illness or other limits. A quantum proxy signature scheme based on controlled quantum teleportation was proposed by Cao et al. [31]. A genuinely entangled five-qubit state was used in their scheme, which is not easier generated than the non-maximally entangled state in experimental condition. Zhou et al. [32] presented a quantum proxy signature scheme with public verifiability. But they must use the operation of quantum states comparison which increases the implementation complexity.

In a practical application, an original signer needs to delegate a proxy signer to sign a message because he is not present. Meanwhile, the anonymity of the message needs to be guaranteed. For example, in an e-payment system, a customer provides a merchant with an e-currency to purchase some goods, but the e-currency should be signed blindly by an agent whose signing authority is delegated by a bank. However, all these schemes mentioned above can not fulfill the task. In this paper, a novel quantum proxy blind signature scheme is proposed to conquer this problem.

The rest of this paper is organized as follows. In Section 2, a basic theory of controlled quantum teleportation is introduced. In Section 3, we describe the novel quantum proxy blind signature scheme in detail. The security analysis and discussion are given in Section 4. Finally, conclusions are drawn in Section 5.

2 Preliminary Theory

The novel quantum proxy blind signature scheme is based on controlled teleportation. In this section, the controlled teleportation is introduced by using a special form of non-maximally entangled three-qubit state. It is generally admitted that the generation and storage of maximally entangled states are not easily realized in a practical application because of noise, decoherence, etc. Thus, the utilization of non-maximally entangled states is becoming increasingly important. To guarantee perfect teleportation, we choose the following special state as quantum channel

$$|\phi\rangle_{123} = \frac{1}{\sqrt{2}}(\sin\theta|000\rangle - \cos\theta|011\rangle + \cos\theta|110\rangle + \sin\theta|101\rangle)_{123}, \qquad (1)$$

where $\theta \neq \frac{k\pi}{2}$ $(k \in \mathbb{Z})$.

As showed in Fig. 1, this controlled teleportation involves the following three partners: a sender Alice, a controller Charlie and a receiver Bob. Alice owns particle 1, Charlie holds particle 2 and particle 3 belongs to Bob. Suppose that an arbitrary single-qubit state to be teleported in Alice's hands has the form

$$|\varphi\rangle_m = (\alpha|0\rangle + \beta|1\rangle)_m, \qquad (2)$$

where α , β are unknown amplitudes that satisfy $|\alpha|^2 + |\beta|^2 = 1$. So the joint state of the total system is

$$\begin{aligned} |\psi_0\rangle &= |\varphi\rangle_m \otimes |\phi\rangle_{123} = (\alpha|0\rangle + \beta|1\rangle)_m \otimes \\ &\quad \frac{1}{\sqrt{2}}(\sin\theta|000\rangle - \cos\theta|011\rangle + \cos\theta|110\rangle + \sin\theta|101\rangle)_{123}. \end{aligned} \qquad (3)$$

If the controller Charlie agrees the two parties of communication to achieve their teleportation, he first sends his particle 2 through a Hadamard gate, obtaining

$$\begin{aligned} |\psi_1\rangle &= (\alpha|0\rangle + \beta|1\rangle)_m \otimes \frac{1}{2}(\sin\theta|000\rangle + \sin\theta|010\rangle - \cos\theta|001\rangle + \cos\theta|011\rangle \\ &\quad + \cos\theta|100\rangle - \cos\theta|110\rangle + \sin\theta|101\rangle + \sin\theta|111\rangle)_{123} \\ &= (\alpha|0\rangle + \beta|1\rangle)_m \otimes \frac{1}{2}[(\sin\theta|00\rangle - \cos\theta|01\rangle + \cos\theta|10\rangle + \sin\theta|11\rangle)_{13}|0\rangle_2 \\ &\quad (\sin\theta|00\rangle + \cos\theta|01\rangle - \cos\theta|10\rangle + \sin\theta|11\rangle)_{13}|1\rangle_2]. \end{aligned} \qquad (4)$$

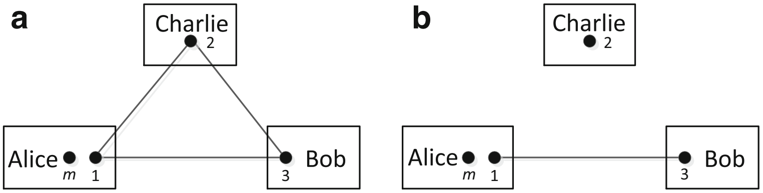


Fig. 1 **a**: Alice wants to teleport the state $|\varphi\rangle$ in particle m to Bob, the particles 1, 2, 3 are entangled. **b**: Charlie agrees the two parties to achieve their teleportation by performing operations on particle 2

Then he measures his particle 2 with the basis $\{|0\rangle, |1\rangle\}$, and records the measurement result as R_C, then sends it to Alice. After that, the system of Alice and Bob will collapse into the state $|\psi_2\rangle$ or $|\psi_3\rangle$ which depends on $R_C = 0$ or $R_C = 1$, where

$$|\psi_2\rangle = (\alpha|0\rangle + \beta|1\rangle)_m \otimes \frac{1}{\sqrt{2}}(\sin\theta|00\rangle - \cos\theta|01\rangle + \cos\theta|10\rangle + \sin\theta|11\rangle)_{13}, \quad (5)$$

$$|\psi_3\rangle = (\alpha|0\rangle + \beta|1\rangle)_m \otimes \frac{1}{\sqrt{2}}(\sin\theta|00\rangle + \cos\theta|01\rangle - \cos\theta|10\rangle + \sin\theta|11\rangle)_{13}. \quad (6)$$

Afterwards, Alice carries out the following steps according to R_C received from Charlie (See Fig. 2).

Case 1: If $R_C = 0$, Alice sends her particles m and 1 through a CNOT gate (particle m is control qubit, particle 1 is target qubit), obtaining

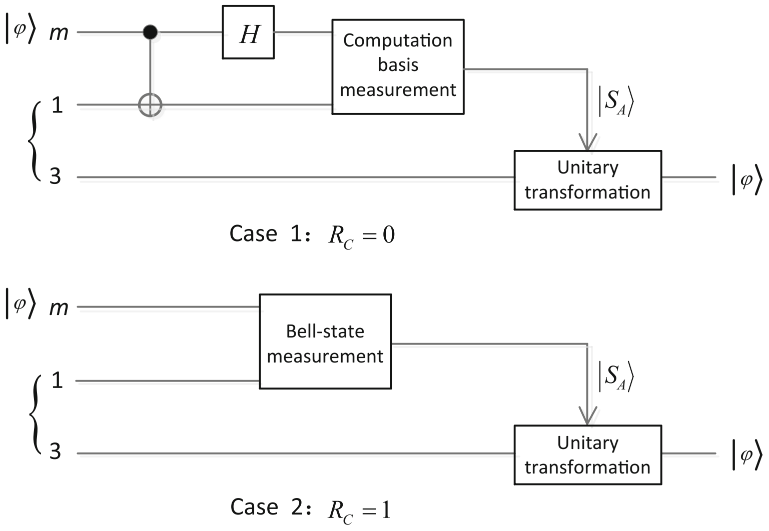
$$\begin{aligned}|\psi_{21}\rangle \;=\; &\frac{1}{\sqrt{2}}[\alpha|0\rangle_m(\sin\theta|00\rangle - \cos\theta|01\rangle + \cos\theta|10\rangle + \sin\theta|11\rangle)_{13}\\ &+\beta|1\rangle_m(\sin\theta|10\rangle - \cos\theta|11\rangle + \cos\theta|00\rangle + \sin\theta|01\rangle)_{13}]. \quad (7)\end{aligned}$$

Then she performs a Hadamard gate on her particle m, obtaining

$$\begin{aligned}|\psi_{22}\rangle \;=\; &\frac{1}{2}[\alpha(|0\rangle + |1\rangle)_m(\sin\theta|00\rangle - \cos\theta|01\rangle + \cos\theta|10\rangle + \sin\theta|11\rangle)_{13}\\ &+\beta(|0\rangle - |1\rangle)_m(\sin\theta|10\rangle - \cos\theta|11\rangle + \cos\theta|00\rangle + \sin\theta|01\rangle)_{13}]. \quad (8)\end{aligned}$$

This state can be regrouped in the following form

$$\begin{aligned}|\psi_{22}\rangle \;=\; &\frac{1}{2}\{|00\rangle_{m1}[(\alpha\sin\theta + \beta\cos\theta)|0\rangle + (\beta\sin\theta - \alpha\cos\theta)|1\rangle]_3\\ &+|01\rangle_{m1}[(\alpha\cos\theta + \beta\sin\theta)|0\rangle + (\alpha\sin\theta - \beta\cos\theta)|1\rangle]_3\\ &+|10\rangle_{m1}[(\alpha\sin\theta - \beta\cos\theta)|0\rangle - (\alpha\cos\theta + \beta\sin\theta)|1\rangle]_3\\ &+|11\rangle_{m1}[(\alpha\cos\theta - \beta\sin\theta)|0\rangle + (\alpha\sin\theta + \beta\cos\theta)|1\rangle]_3\}. \quad (9)\end{aligned}$$



Case 1: $R_C = 0$

Case 2: $R_C = 1$

Fig. 2 The operations carried out by Alice in two cases

Alice uses a two-qubit computation basis to measure her particles m and 1, and records the measurement result as $|S_A\rangle$, where $|S_A\rangle \in \{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$. Then Alice transmits R_C and $|S_A\rangle$ to Bob.

Case 2: If $R_C = 1$, the state $|\psi_3\rangle$ can be re-written as follows

$$\begin{aligned}|\psi_3\rangle = \frac{1}{2}\{&|\phi^+\rangle_{m1}[(\alpha\sin\theta - \beta\cos\theta)|0\rangle + (\alpha\cos\theta + \beta\sin\theta)|1\rangle]_3\\ &|\phi^-\rangle_{m1}[(\alpha\sin\theta + \beta\cos\theta)|0\rangle + (\alpha\cos\theta - \beta\sin\theta)|1\rangle]_3\\ &|\psi^+\rangle_{m1}[(\beta\sin\theta - \alpha\cos\theta)|0\rangle + (\alpha\sin\theta + \beta\cos\theta)|1\rangle]_3\\ &|\psi^-\rangle_{m1}[-(\beta\sin\theta + \alpha\cos\theta)|0\rangle + (\alpha\sin\theta - \beta\cos\theta)|1\rangle]_3\},\end{aligned} \quad (10)$$

the (10) involves the following four Bell states

$$|\phi^\pm\rangle = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle), \;\; |\psi^\pm\rangle = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle). \quad (11)$$

Alice performs a Bell-state measurement on her particles m and 1, then records the measurement result as $|S_A\rangle$, where $|S_A\rangle \in \{|\phi^+\rangle, |\phi^-\rangle, |\psi^+\rangle, |\psi^-\rangle\}$. After that, Alice transfers R_C and $|S_A\rangle$ to Bob.

After receiving R_C and $|S_A\rangle$, Bob needs to perform an appropriate unitary transformation on particle 3 in order to reconstruct the teleported state $|\varphi\rangle$. The corresponding relationship between the measurement results and Bob's unitary transformations is summarized in Table 1. Thus, the arbitrary single-qubit state $|\varphi\rangle$ has been perfectly teleported from the sender Alice to the receiver Bob under Charlie's control.

Table 1 The relationship between measurement results and Bob's unitary transformations

Charlie's measurement results	Alice's measurement results	Bob's unitary transformations
0	$\|00\rangle$	$U_1 = \begin{pmatrix}\sin\theta & -\cos\theta\\ \cos\theta & \sin\theta\end{pmatrix}$
0	$\|01\rangle$	$U_2 = \begin{pmatrix}\cos\theta & \sin\theta\\ \sin\theta & -\cos\theta\end{pmatrix}$
0	$\|10\rangle$	$U_3 = \begin{pmatrix}\sin\theta & -\cos\theta\\ -\cos\theta & -\sin\theta\end{pmatrix}$
0	$\|11\rangle$	$U_4 = \begin{pmatrix}\cos\theta & \sin\theta\\ -\sin\theta & \cos\theta\end{pmatrix}$
1	$\|\phi^+\rangle$	$U_5 = \begin{pmatrix}\sin\theta & \cos\theta\\ -\cos\theta & \sin\theta\end{pmatrix}$
1	$\|\phi^-\rangle$	$U_6 = \begin{pmatrix}\sin\theta & \cos\theta\\ \cos\theta & -\sin\theta\end{pmatrix}$
1	$\|\psi^+\rangle$	$U_7 = \begin{pmatrix}-\cos\theta & \sin\theta\\ \sin\theta & \cos\theta\end{pmatrix}$
1	$\|\psi^-\rangle$	$U_8 = \begin{pmatrix}-\cos\theta & \sin\theta\\ -\sin\theta & -\cos\theta\end{pmatrix}$

It should be noted that the teleported state $|\varphi\rangle$ is an arbitrary single-qubit state, so the following four states are suitable for the aforementioned teleportation.

$$|x_{\pm}\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle), \quad |y_{\pm}\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm \mathrm{i}|1\rangle). \tag{12}$$

3 Quantum Proxy Blind Signature Scheme

As showed in Fig. 3, the proposed quantum proxy blind signature scheme involves the following five participants: a message sender U, an original signer Charlie, a proxy signer Alice, a receiver (verifier) Bob and a trusted arbitrator Trent. Our scheme consists of four phases: initializing phase, delegating phase, signing phase, and verifying phase.

3.1 Initializing Phase

Step 1: Charlie sets up n non-maximally entangled three-qubit states as showed in (1).

Step 2: Afterwards, Charlie takes first particles, second particles and third particles from these states to form the ordered sequences Q_1, Q_2 and Q_3, respectively. To guarantee the security of distribution, Charlie generates some decoy particles which are critical for statistical analysis of eavesdropping. Each decoy particle is randomly selected from $\{|0\rangle, |1\rangle, |x_+\rangle, |x_-\rangle\}$. Then Charlie randomly inserts these decoy particles into Q_1 to form a new sequence Q_1'. Similarly, Q_3' can be constructed in the same method. It should be paid attention to that Charlie must record the insertion positions and original states of the decoy particles in order to detect the eavesdropping. Finally, he distributes Q_1' and Q_3' to Alice and Bob, respectively, and leaves Q_2 to himself.

Step 3: After confirming that Alice (Bob) has received the sequence Q_1' (Q_3'), Charlie announces the insertion positions and the corresponding measurement bases. Alice (Bob) measures the decoy particles according to Charlie's announcement, then tells Charlie her (his) measurement outcomes. After comparing the measurement outcomes with the original states, Charlie can detect the existence of eavesdroppers. If there is no eavesdroppers or the probability of being eavesdropped is lower than a presupposed threshold, the rest steps of this protocol can be continued. Otherwise, they abort this communication and restart. Hence, the three participants have securely shared n non-maximally entangled three-qubit states.

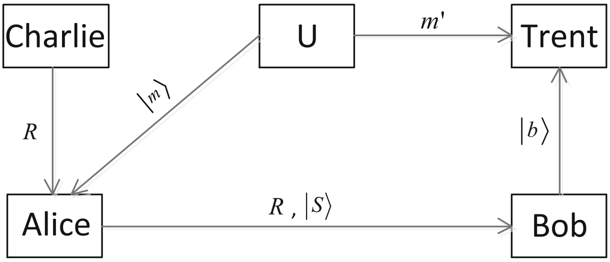


Fig. 3 Schematic diagram of transmission when Alice signs a message

3.2 Delegating Phase

Step 1: Charlie performs Hadamard gates on his particles of sequence Q_2, then he measures the particles under the basis $\{|0\rangle, |1\rangle\}$ and records measurement results as

$$R = (R_1, R_2, \cdots, R_n), \tag{13}$$

where every $R_i \in \{0, 1\}(i = 1, 2, \cdots, n)$. Then Charlie sends R to the proxy signer Alice by using the quantum secure direct communication (QSDC) protocol such as the ones in [11–13].

Step 2: After being notified that Alice has obtained the delegation message R, Charlie confirms that the delegation is accomplished. Otherwise, the delegation is failed.

3.3 Signing Phase

Step 1: If the sender U's message needs to be signed, then U transforms his message into an n-bit message string $m = (m_1, m_2, \cdots, m_n)$.

Step 2: Afterwards, U blinds the message m into a quantum state $|m\rangle$ in the following way. Here, we only give out the blinding process of the i-th message bit m_i, and other ones can also be blinded in the same manner.

(1) If $m_i = 0$, U blinds it into $|x_+\rangle$ or $|x_-\rangle$ with equal probability 1/2.

(2) Otherwise, the message m_i will be randomly blinded into $|y_+\rangle$ or $|y_-\rangle$.

After that, the n-bit message m has been blinded into n-qubit $|m\rangle$ which has the form $|m\rangle = (|m_1\rangle, |m_2\rangle, \cdots, |m_n\rangle)$, where every $|m_i\rangle \in \{|x_+\rangle, |x_-\rangle, |y_+\rangle, |y_-\rangle\}$ $(i = 1, 2, \cdots, n)$. Here, let two classical bits 00 (01,10,11) correspond to the quantum state $|x_+\rangle$ $(|x_-\rangle, |y_+\rangle, |y_-\rangle)$, which is only known to U and the arbitrator Trent. Thus, the blinded message $|m\rangle$ could be encoded into $2n$ classical bits m', which has the form

$$m' = (m'_1, m'_2, \cdots, m'_n). \tag{14}$$

Step 3: Then U transmits $|m\rangle$ to the proxy signer Alice. To guarantee the security of quantum channel between U and Alice, they also use the technique of eavesdropping check similar to the method shown in 3.1. Then U transfers m' to Trent using the QSDC protocols in [11–13].

Step 4: After the second eavesdropping check, Alice obtains the blinded message $|m\rangle$, then Alice signs it according to Charlie's delegation message R. For example, if $R_i = 0$, Alice first sends $|m_i\rangle$ and the i-th particle of Q_1 through a CNOT gate ($|m_i\rangle$ is control qubit, the i-th particle of Q_1 is target qubit), then he sends $|m_i\rangle$ through a Hadamard gate. Afterwards, Alice uses a two-qubit computation basis to measure the two particles and obtains $|S_i\rangle$, where $|S_i\rangle \in \{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$. If $R_i = 1$, Alice directly performs a Bell-state measurement on $|m_i\rangle$ and the i-th particle of Q_1, then obtains $|S_i\rangle$, where $|S_i\rangle \in \{|\phi^+\rangle, |\phi^-\rangle, |\psi^+\rangle, |\psi^-\rangle\}$. Therefore, Alice gets her proxy blind signature $|S\rangle$ about the blinded message $|m\rangle$, where $|S\rangle$ has the form

$$|S\rangle = (|S_1\rangle, |S_2\rangle, \cdots, |S_n\rangle). \tag{15}$$

Step 5: By using the QSDC protocols in [11–13], Alice sends R to Bob. To ensure the security of transmission, Alice transmits $|S\rangle$ to Bob using the similar strategy as showed in 3.1.

3.4 Verifying Phase

Step 1: Bob receives R from Alice. After the third eavesdropping check, Bob obtains Alice's proxy blind signature $|S\rangle$.

Step 2: According to R and $|S\rangle$, Bob gets $|b\rangle$ by performing appropriate unitary transformations listed in Table 1 on his particles of sequence Q_3, where $|b\rangle = (|b_1\rangle, |b_2\rangle, \cdots, |b_n\rangle)$. Then Bob transmits $|b\rangle$ to the arbitrator Trent. To check the security of channel between Bob and Trent, they use the same strategy as described in 3.1.

Step 3: After the fourth eavesdropping check, Trent obtains $|b\rangle$. Once Trent receives m' from U, he can obtain the original message m by extracting the odd number bits of m'. After that, Trent measures $|b\rangle$ according to m. For instance, if $m_i = 0$, Trent uses the basis $\{|x_+\rangle, |x_-\rangle\}$ to measure $|b_i\rangle$; if $m_i = 1$, he measure it with the basis $\{|y_+\rangle, |y_-\rangle\}$. Then he encodes the measurement results into b by using the same method as U used. After that, Trent obtains b which has the form

$$b = (b_1, b_2, \cdots, b_n). \tag{16}$$

Now, Trent compares b with m', if $b = m'$, then he tells Bob that $|S\rangle$ is valid proxy blind signature signed by Alice; otherwise, he rejects it.

4 Security Analysis and Discussion

In this section, we will show that our scheme satisfies the properties of undeniability, unforgeability, blindness, untraceability, and it can resist intercept-resend attack.

4.1 Undeniability

Firstly, we show that it is impossible for Alice to deny her signature. According to the Step 4 in 3.3, Alice must use Charlie's delegation message R, the sequence Q_1 and the blinded message $|m\rangle$ to generate her proxy blind signature $|S\rangle$. But, it is difficult for any other people to get the sequence Q_1 because it is transmitted by using the eavesdropping check. Therefore, Alice can not deny her signature.

Secondly, Bob can not deny receiving the signature $|S\rangle$. The reason is that Bob needs Trent's further verification and his willingness to verify the signature implies he has received it. Besides, Zou et al. [33] pointed out that, in some existing AQS schemes [15, 34], the receiver Bob can tell a lie to deny the integrality of the signature successfully without being detected. However, in our scheme, it is clear that the eventual verification is carried out by Trent so Bob has no chance to do that. Therefore, Bob can not deny the integrality of the signature $|S\rangle$ and our scheme can resist the attack proposed in [33, 35].

4.2 Unforgeability

Another security issue will be discussed, i.e., the impossibility of forgery by both dishonest internal attackers and malicious external ones. Firstly, it is impossible for Bob to forge Alice's signature. According to the Step 4 in 3.3, Bob can not generate the correct signature $|S\rangle$ without the sequence Q_1. However, the photon sequence is transmitted by using the technique of eavesdropping check, so anyone can not obtain it except for Alice. Hence, Bob can not forge Alice's signature. Similarly, the same situation will appear in front of U. In a word, the dishonest internal attackers can not forge Alice's signature.

Secondly, we consider the forgery made by the external attacker Eve. As demonstrated above, Eve can not forge Alice's signature under the condition that he has no information about Charlie's delegation message R, the sequence Q_1 and the blinded message $|m\rangle$. Therefore, if Eve attempts to forge Alice's signature successfully, he needs to obtain the aforesaid elements. However, it is impossible, because the elements are transmitted in secure ways. Therefore, Eve can not forge Alice's signature.

Thirdly, Zhang et al. [36] noted that the receiver Bob can forge a valid signature for his benefit without being detected. This is because Bob is the only verifier of the signature and this gives him sufficient opportunities to forge the signature. To prevent the security loophole, the validity of the signature should be verified by Bob and other participants. In view of this point, we introduce an arbitrator Trent to help Bob verify the signature. So Bob has no chance to forge the signature using the similar method showed in [36].

4.3 Blindness

According to the Step 2 in 3.3, the message $m = (m_1, m_2, \cdots, m_n)$ has been blinded into $|m\rangle = (|m_1\rangle, |m_2\rangle, \cdots, |m_n\rangle)$ by the message sender U, where every $|m_i\rangle \in \{|x_+\rangle, |x_-\rangle, |y_+\rangle, |y_-\rangle\}$. If Alice tries to determine the blinded message $|m\rangle$ after receiving it from U, the only way is to perform measurements. If Alice randomly selects basis $\{|x_+\rangle, |x_-\rangle\}$ or $\{|y_+\rangle, |y_-\rangle\}$ to measure $|m\rangle$, then the probability that she can determine it is $\frac{1}{2^n}$, which will vanish zero if n is large enough. Thus, Alice can not learn the blinded message $|m\rangle$, so the original message m is unknown to her. Therefore, the proxy signer Alice can not know the content of the message m when she signs it.

4.4 Untraceability

In our scheme, although the message owner U does not unblind the signature $|S\rangle$, the proxy signer Alice can not trace him. More specifically, the signature $|S\rangle$ consists of nonorthogonal two-qubit states, so Alice can not identify it. Hence, Alice can not trace the message m when one of message-signature pairs $(m, |S\rangle)$ is published. Therefore, our scheme has the property of untraceability and could be applied to an e-payment system.

4.5 Impossibility of Intercept-resend Attack

Firstly, if an adversary Eve intercepts the quantum state $|m\rangle'$ composed of $|m\rangle$ and some decoy particles, then he resends another quantum state to Alice. However, this trick will be detected by the security check between U and Alice. Besides, although Eve obtains the quantum state $|m\rangle'$, he can not extract the blinded message $|m\rangle$, since he does not know the insertion positions of the decoy particles. Similarly, this trick is invalid for the quantum state $|S\rangle$ and $|b\rangle$. Therefore, our scheme can resist intercept-resend attack [37, 38].

5 Conclusion

In this paper, we have proposed a novel quantum proxy blind signature scheme. It is shown that, the original signer Charlie can delegate his signing authority to the proxy signer Alice by performing Hadamard gates and single-qubit measurements. The sender U produces two groups of nonorthogonal single-photon states to blind his message. According to Charlie's delegation message, Alice implements corresponding operations to generate her signature. The receiver Bob performs appropriate unitary transformations to obtain $|b\rangle$, and sends it to Trent. After receiving $|b\rangle$, Trent first measures it, then he can easily verify the signature by a comparison. In addition, we have given the security analysis and discussion in detail.

This scheme has some advantages. Firstly, we use the QSDC protocol to guarantee the secure transmission of classical message while other schemes [22, 39, 40] use one-time pad to do it. However, these schemes are easily cracked by the intercept-resend attack [38, 41, 42]. Secondly, differing from some existing signature schemes [31, 43] using maximally entangled state, we replace it with non-maximally entangled state which is easier generated than the former. Thirdly, the proxy signer Alice's signature depends on Charlie's delegation message, which is different from the related schemes [31, 43, 44] whose different delegation messages correspond to one kind of signature. Fourthly, the sender U prepares two groups of nonorthogonal single-photon states to guarantee the anonymity of his message, which is easily realized than the generation of entangled state [24, 28] with present technology. Fifthly, the arbitrator Trent can keep the receiver Bob from denying and forging the signature [33, 35, 36], so the security of this scheme has been enhanced. Finally, the proposed scheme is secure and it combines proxy signature with blind signature, so it has a more wide application.

Acknowledgments This work was supported by the National Natural Science Foundation of China (Grant Nos. 61273311 and 61402275), the Natural Science Basic Research Plan of Shaanxi Province of China (Grant No. 2015JM6263), the Special Foundation for Basic Research Funding of the Central Higher Education of China (Grant No. GK201402004).

References

1. Bennett, C.H., Brassard, G.: Quantum Cryptography: Public Key Distribution and Coin Tossing. In: Proceedings of IEEE International Conference on Computers Systems and Signal Processing, Bangalore, India, pp. 175–179 (1984)
2. Ekert, A.K.: Quantum cryptography based on Bell's theorem. Phys. Rev. Lett. **67**, 661–663 (1991)
3. Bennett, C.H.: Quantum cryptography using any two nonorthogonal states. Phys. Rev. Lett. **68**, 3121–3124 (1992)
4. Boykin, P.O., Boychowdhury, V.: Optimal encryption of quantum bits. Phys. Rev. A **67**, 042317 (2003)
5. Oppenheim, J., Horodecki, M.: How to reuse a one-time pad and other notes on authentication, encryption, and protection of quantum information. Phys. Rev. A **72**, 042309 (2005)
6. Wang, T.Y., Wen, Q.Y., Zhu, F.C.: Secure authentication of classical messages with single photons. Chin. Phys. B **18**, 3189–3192 (2009)
7. Wang, T.Y., Wen, Q.Y., Zhu, F.C.: Secure authentication of classical messages with decoherence-free states. Opt. Commun. **282**, 3382–3385 (2009)
8. Hillery, M., Bužek, V., Berthiaume, A.: Quantum secret sharing. Phys. Rev. A **59**, 1829–1834 (1999)
9. Chen, X.B., Niu, X.X., Zhou, X.J., Yang, Y.X.: Multi-party quantum secret sharing with the single-particle quantum state to encode the information. Quantum Inf. Process. **12**, 365–380 (2013)
10. Dehkordi, M.H., Fattahi, E.: Threshold quantum secret sharing between multiparty and multiparty using Greenberger-Horne-Zeilinger state. Quantum Inf. Process. **12**, 1299–1306 (2013)
11. Deng, F.G., Long, G.L., Liu, X.S.: Two-step quantum direct communication using the Einstein-podolsky-Rosen pair block. Phys. Rev. A **68**, 042317 (2003)
12. Deng, F.G., Long, G.L.: Secure direct communication with a quantum one-time pad. Phys. Rev. A **69**, 052319 (2004)
13. Cai, Q.Y., Li, B.W.: Deterministic secure communication without using entanglement. Chin. Phys. Lett. **21**, 601–603 (2004)
14. Wang, J., Zhang, Q., Tang, C.J.: Multiparty controlled quantum secure direct communication using Greenberger-Horne-Zeilinger state. Opt. Commun. **266**, 732–737 (2006)

15. Zeng, G.H., Keitel, C.H.: Arbitrated quantum-signature scheme. Phys. Rev. A **65**, 042312 (2002)
16. Curty, M., Lütkenhaus, N.: Comment on Arbitrated quantum-signature scheme. Phys. Rev. A **77**, 046301 (2008)
17. Zeng, G.H.: Reply to Comment on Arbitrated quantum-signature scheme. Phys. Rev. A **78**, 016301 (2008)
18. Lee, H., Hong, C., Kim, H., Lim, J., Yang, H.J.: Arbitrated quantum signature scheme with meesage recovery. Phys. Lett. A **321**, 295–300 (2004)
19. Wang, J., Zhang, Q., Liang, L.M., Tang, C.J.: Comment on: Arbitrated quantum signature scheme with meesage recovery. Phys. Lett. A **347**, 262–263 (2005)
20. Wen, X.J., Liu, Y.: A realizable quantum sequential multi-signature scheme. Acta Electron. Sin. **35**, 1079–1083 (2007)
21. Wen, X.J., Liu, Y., Zhou, N.R.: Realizable quantum broadcasting multi-signature scheme. Int. J. Mod. Phys. B **22**, 4251–4259 (2008)
22. Wen, X.J., Tian, Y., Ji, L.P., Niu, X.M.: A group signature scheme based on quantum teleportation. Phys. Scr. **81**, 055001 (2010)
23. Chaum, D.: Blind Signature for Untraceable Payments. In: Advances in Cryptology Proceedings of Crypto'82, pp. 199–203. Springer-Verlag (1983)
24. Wen, X.J., Niu, X.M., Ji, L.P., Tian, Y.: A weak blind signature scheme based on quantum cryptography. Opt. Commun. **282**, 666–669 (2009)
25. Naseri, M.: A weak blind signature based on quantum cryptography. Int. J. Phys. Sci. **6**, 5051–5053 (2011)
26. Wang, T.Y., Wen, Q.Y.: Fair quantum blind signatures. Chin. Phys. B **19**, 060307 (2010)
27. He, L.B., Huang, L.S., Yang, W., Xu, R.: Cryptanalysis of fair quantum blind signatures. Chin. Phys. B **21**, 030306 (2012)
28. Wang, M.M., Chen, X.B., Yang, Y.X.: A blind quantum signature protocol using the GHZ states. Sci. China Phys. Mech. **56**, 1636–1641 (2013)
29. Cai, X.Q., Niu, H.F.: Partially blind signature based on quantum cryptography. Int. J. Mod. Phys. B **26**, 1250163 (2012)
30. Mambo, M., Usuda, K., Okamoto, E.: Proxy signatures: Delegation of the power to sign messages. IEICE Trans. Fundam. **E79-A**, 1338–1354 (1996)
31. 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. **53**, 3095–3100 (2014)
32. Zhou, J.X., Zhou, Y.J., Niu, X.X., Yang, Y.X.: Quantum proxy signature with public verifiability. Sci. China Phys. Mech. Astron. **54**, 1828–1832 (2011)
33. Zou, X., Qiu, D.W.: Security analysis and improvements of arbitrated quantum signature schemes. Phys. Rev. A **82**, 042325 (2010)
34. Li, Q., Chan, W.H., Long, D.Y.: Arbitrated quantum signature scheme using Bell states. Phys. Rev. A **79**, 054307 (2009)
35. Hwang, T., Luo, Y.P., Chong, S.K.: Comment on Security analysis and improvements of arbitrated quantum signature schemes. Phys. Rev. A **85**, 056301 (2012)
36. Zhang, K.J., Jia, H.Y.: Cryptanalysis of a quantum proxy weak blind signature scheme. Int. J. Theor. Phys. **54**, 582–588 (2015)
37. Su, Q., Li, W.M.: Improved group signature scheme based on quantum teleportation. Int. J. Theor. Phys. **53**, 1208–1216 (2014)
38. 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. **101**, 208901 (2008)
39. Tian, Y., Chen, H., Ji, S.F., Han, Z.P., Lian, H.G., Wen, X.J.: A broadcasting multiple blind signature scheme based on quantum teleportation. Opt. Quant. Electron. **46**, 769–777 (2014)
40. Wen, X.J., Liu, Y., Sun, Y.: Quantum multi-signature protocol based on teleportation. Z. Naturforsch. A **62a**, 147–151 (2007)
41. Zuo, H.J., Zhang, K.J., Song, T.T.: Security analysis of quantum multi-signature protocol based on teleportation. Quantum Inf. Process **12**, 2343–2353 (2013)
42. Zhang, W., Qiu, D.W., Zou, X.F.: Improvement of a quantum broadcasting multiple blind signature scheme based on quantum teleportation. Quantum Inf. Process **15**, 2499–2519 (2016)
43. Cao, H.J., Zhu, Y.Y., Li, P.F.: A quantum proxy weak blind signature scheme. Int. J. Theor. Phys. **53**, 419–425 (2014)
44. Cao, H.J., Yu, Y.F., Song, Q., Gao, L.X.: A quantum proxy weak blind signature scheme based on controlled quantum teleportation. Int. J. Theor. Phys. **54**, 1325–1333 (2015)