Int J Theor Phys (2018) 57:1612–1621
https://doi.org/10.1007/s10773-018-3688-4

Improvement of a Quantum Proxy Blind Signature Scheme

Jia-Lei Zhang[1] · Jian-Zhong Zhang[1] · Shu-Cui Xie[2]

Received: 24 October 2017 / Accepted: 2 February 2018 / Published online: 26 February 2018

Abstract Improvement of a quantum proxy blind signature scheme is proposed in this paper. Six-qubit entangled state functions as quantum channel. In our scheme, a trust party Trent is introduced so as to avoid David's dishonest behavior. The receiver David verifies the signature with the help of Trent in our scheme. The scheme uses the physical characteristics of quantum mechanics to implement message blinding, delegation, signature and verification. Security analysis proves that our scheme has the properties of undeniability, unforgeability, anonymity and can resist some common attacks.

Keywords Proxy blind signature · Quantum cryptography · Controlled quantum teleportation · Six-qubit entangled state

1 Introduction

Digital signature is an essential ingredient of classical cryptography and has been employed in various applications. Unfortunately, most existing classical signature schemes whose security depends on the difficulty of solving some hard mathematical problems were threatened by quantum computation [1]. Therefore, researchers turn to investigate its quantum

✉ Jian-Zhong Zhang
1416655910@qq.com

Jia-Lei Zhang
295533745@qq.com

Shu-Cui Xie
xieshucui@163.com

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

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

counterpart with the hope that quantum signature can become an alternative to classical signature and provide unconditional security.

Proxy signature, as an importation cryptographic primitive was firstly introduced in 1996. In a proxy signature scheme, it allows a proxy signer to sign on behalf of an original signer. Since Mambo M et al. proposed a quantum digital signature protocol [2], many efforts have been made on it and lots of schemes have been presented [3–10]. In 2002, Barnum [11] proposed a quantum signature scheme and it was proved to be unconditionally secure. A quantum digital signature scheme based on quantum one-way function was proposed by Gottesman and Chuang [12]. Zeng et al. [13, 14] presented arbitrated quantum signature (AQS) schemes based on a three-qubit Greenberger-Horne-Zeilinger (GHZ) state. Two arbitrated quantum signature schemes with message recovery were proposed by Lee et al. [15]. Recently, Cao et al. presented two quantum proxy signature schemes [16, 17] based on genuine six-qubit entangled state and five-qubit entangled state, respectively.

Chaum [18] first proposed a blind signature scheme. In blind signature schemes, the message anonymity could be guaranteed. When signed, the message is disguised to ensure privacy. In other words, it allows a signatory to sign a message for a user in such a way that she can not learn the content of the message. In 2008, Wen et al. proposed a weak blind signature scheme based on quantum cryptography [19]. Afterwards, a quantum blind signature protocol using GHZ states was proposed by Wang et al. [20].

In this paper, we put forward improvement of a quantum proxy blind signature scheme based on genuine six-qubit entangled state. Our scheme allows a proxy signer Peter to finish the signature on behalf of the original signers Bob and Charlie, which may have applications in e-payment system, e-government, e-business and so on. For instance, elects in the network, a legal person simultaneously was appointed by the two legal representative to replace them to carry on the signature. We use quantum key distribution protocol, quantum one-time pad and other quantum properties to guarantee the unconditional security and signature message anonymity. Compared with the scheme Ref. [16, 21], a trust party Trent is proposed in this paper so as to avoid receiver David's dishonest behavior. Compared to [22], our scheme adopts the GHZ-state measurement, Bell-state measurement which are easier to implement under current technology and experimental conditions. In addition, the messages may not be forged or modified in any way by the receiver or attacker.

2 Preliminary Theory of Controlled Quantum Teleportation

The quantum proxy blind signature is based on controlled teleportation. In this section, we will introduce the controlled teleportation. A genuine six-qubit entangled state [23] as quantum channel. It is given by

$$\begin{aligned}|\xi\rangle_{123456} = \tfrac{1}{4}(&|000000\rangle - |000011\rangle + |111100\rangle - |111111\rangle \\ &+|001100\rangle + |001111\rangle + |110000\rangle + |110011\rangle \\ &+|011001\rangle - |011010\rangle + |100101\rangle - |100110\rangle \\ &+|010101\rangle + |010110\rangle + |101001\rangle + |101010\rangle)_{123456}.\end{aligned} \tag{1}$$

Alice is a sender, she owns particles (2,5), the controllers Bob and Charlie hold particles (1,3) and particle 6, respectively. The verifier David holds particle 4.

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

$$|\varphi\rangle_M = \frac{1}{\sqrt{2}}(|0\rangle + b|1\rangle)_M, \tag{2}$$

in which b=1 and b=−1 is corresponding to $M(i)$=1 and $M(i)$=0, respectively.

The mixed state $|\Psi\rangle_{M123456}$ of the whole system is given by

$$|\Psi\rangle_{M123456} = |\varphi\rangle_M \otimes |\xi\rangle_{123456} = \frac{1}{\sqrt{2}}(|0\rangle + b|1\rangle)_M \otimes |\xi\rangle_{123456}. \tag{3}$$

The controlled quantum teleportation works in the following process. The frame of teleportation is shown in Fig. 1.

1) Alice makes a GHZ-state measurement on her particles (M,2,5), and sends her measurement outcomes to Bob, Charlie and David via secure quantum channels. The GHZ-state measurement can collapse the state of particles (1,3,4,6) into one of the following eight states

$$\begin{aligned}
\langle Z^{\pm}_{M25}|\Psi\rangle_{M123456} = & \tfrac{1}{2\sqrt{2}}(|0000\rangle + |0110\rangle + |1011\rangle + |1101\rangle \\
& \mp b|1111\rangle \pm b|1001\rangle \mp b|0100\rangle \pm b|0010\rangle)_{1346}, \\
\langle H^{\pm}_{M25}|\Psi\rangle_{M123456} = & \tfrac{1}{2\sqrt{2}}(-|1111\rangle + |1001\rangle - |0100\rangle + |0010\rangle \\
& \pm b|0000\rangle \pm b|0110\rangle \pm b|1011\rangle \pm b|1101\rangle)_{1346}, \\
\langle S^{\pm}_{M25}|\Psi\rangle_{M123456} = & \tfrac{1}{2\sqrt{2}}(-|0001\rangle + |0111\rangle - |1010\rangle + |1100\rangle \\
& \pm b|1110\rangle \pm b|1000\rangle \pm b|0101\rangle \pm b|0011\rangle)_{1346}, \\
\langle T^{\pm}_{M25}|\Psi\rangle_{M123456} = & \tfrac{1}{2\sqrt{2}}(|1110\rangle + |1000\rangle + |0101\rangle + |0011\rangle \\
& \mp b|0001\rangle \pm b|0111\rangle \mp b|1010\rangle \pm b|1100\rangle)_{1346}.
\end{aligned} \tag{4}$$

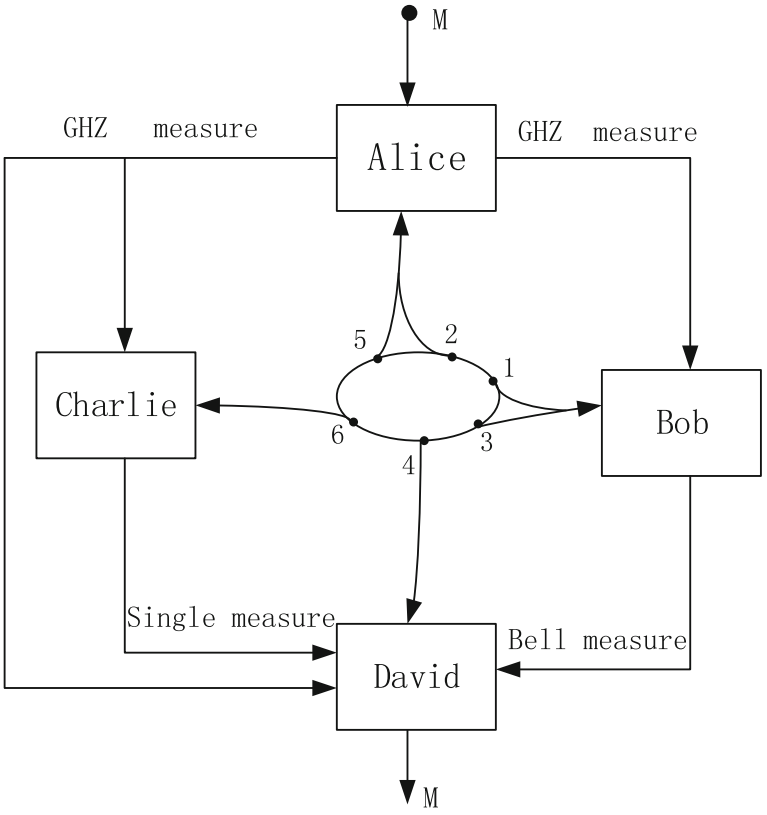

Fig. 1 The model of controlled quantum teleportation

The eight GHZ states of 3-qubit are

$$\begin{aligned} |Z^{\pm}\rangle &= \tfrac{1}{\sqrt{2}}(|000\rangle \pm |111\rangle), \\ |H^{\pm}\rangle &= \tfrac{1}{\sqrt{2}}(|011\rangle \pm |100\rangle), \\ |S^{\pm}\rangle &= \tfrac{1}{\sqrt{2}}(|001\rangle \pm |110\rangle), \\ |T^{\pm}\rangle &= \tfrac{1}{\sqrt{2}}(|010\rangle \pm |101\rangle). \end{aligned} \tag{5}$$

2) If Bob and Charlie agree Alice and David to complete their teleportation, Bob performs a Bell-state measurement on his particles (1,3). Charlie performs single particle measurement on his particle 6 based on $\{|0\rangle, |1\rangle\}$. Suppose that Alice's measurement result is $|T^{-}\rangle_{M25}$, the Bell-state measurement on Bob's particles (1,3) will collapse the quantum state of particles (4,6) into one of the following states

$$\begin{aligned} \left\langle \phi_{13}^{\pm} | T_{M25}^{-} | \Psi \right\rangle_{M123456} &= \tfrac{1}{2}(|11\rangle + b|01\rangle \pm |10\rangle \mp b|00\rangle)_{46}, \\ \left\langle \psi_{13}^{\pm} | T_{M25}^{-} | \Psi \right\rangle_{M123456} &= \tfrac{1}{2}(|01\rangle - b|11\rangle \pm |00\rangle \pm b|10\rangle)_{46}. \end{aligned} \tag{6}$$

Suppose that Bob's measurement result is $|\phi^{+}\rangle_{13}$, the single particle measurement on Charlie's particle 6 in the basis $\{|0\rangle, |1\rangle\}$ will collapse the particle 4 into one of the following states

$$\begin{aligned} \left\langle 0_6 | \phi_{13}^{+} | T_{M25}^{-} | \Psi \right\rangle_{M123456} &= \tfrac{1}{\sqrt{2}}(|1\rangle - b|0\rangle)_4, \\ \left\langle 1_6 | \phi_{13}^{+} | T_{M25}^{-} | \Psi \right\rangle_{M123456} &= \tfrac{1}{\sqrt{2}}(|1\rangle + b|0\rangle)_4. \end{aligned} \tag{7}$$

The four Bell states of 2-qubit are

$$|\phi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle), |\psi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle). \tag{8}$$

Bob and Charlie send their measurement results to David through secure quantum channels.

3) According to Alice's, Bob's and Charlie's measurement outcomes, David imposes an appropriate unitary operation U_4 on particle 4 to successfully reconstruct the original unknown quantum state $|\varphi\rangle_M$. For instance, if Alice's measurement outcome is $|T^{-}\rangle_{M25}$, Bob's and Charlie's measurement outcomes are $|\phi^{+}\rangle_{13}$ and $|1\rangle_6$, respectively, David's operation on particle 4 is σ_x. For other cases, the relationship between Alice's, Bob's, Charlie's measurement results and David's operation are shown in Table 1.

Alice successfully transmits the unknown quantum state $|\varphi\rangle_M$ to the receiver David under Bob's and Charlie's control.

3 Improvement of Quantum Proxy Blind Signature Scheme

The proposed quantum proxy blind signature scheme includes the following several phases. Alice is the massage owner; Bob and Charlie are the original signers, they delegate a proxy signer Peter to sign message instead of them; David is the verifier; Trent is the trust party.

3.1 Initializing Phase

Step 1 Alice holds a string of n-bit (information bits) which carry the messages to be signed:

$$M = \{M(1), M(2), \cdots, M(n)\} = \{M(i), i = 1, 2, \cdots, n\}. \tag{9}$$

Table 1 The relationship between Alice's, Bob's, Charlie's measurement results and David's operation

Alice's result	Bob's and Charlie's resluts	David's operation	Bob's and Charlie's resluts	David's operation
$\|Z^+\rangle_{M25}$	$\|\phi^+\rangle_{13}\|0\rangle_6$	I_4	$\|\phi^+\rangle_{13}\|1\rangle_6$	$(\sigma_z)_4$
	$\|\phi^-\rangle_{13}\|0\rangle_6$	I_4	$\|\phi^-\rangle_{13}\|1\rangle_6$	$(-\sigma_z)_4$
	$\|\psi^+\rangle_{13}\|0\rangle_6$	$(i\sigma_y)_4$	$\|\psi^+\rangle_{13}\|1\rangle_6$	$(\sigma_x)_4$
	$\|\psi^-\rangle_{13}\|0\rangle_6$	$(i\sigma_y)_4$	$\|\psi^-\rangle_{13}\|1\rangle_6$	$(-\sigma_x)_4$
$\|Z^-\rangle_{M25}$	$\|\phi^+\rangle_{13}\|0\rangle_6$	$(\sigma_z)_4$	$\|\phi^+\rangle_{13}\|1\rangle_6$	I_4
	$\|\phi^-\rangle_{13}\|0\rangle_6$	$(\sigma_z)_4$	$\|\phi^-\rangle_{13}\|1\rangle_6$	$(-I)_4$
	$\|\psi^+\rangle_{13}\|0\rangle_6$	$(\sigma_x)_4$	$\|\psi^+\rangle_{13}\|1\rangle_6$	$(i\sigma_y)_4$
	$\|\psi^-\rangle_{13}\|0\rangle_6$	$(\sigma_x)_4$	$\|\psi^-\rangle_{13}\|1\rangle_6$	$(-i\sigma_y)_4$
$\|H^+\rangle_{M25}$	$\|\phi^+\rangle_{13}\|0\rangle_6$	$(\sigma_x)_4$	$\|\phi^+\rangle_{13}\|1\rangle_6$	$(-i\sigma_y)_4$
	$\|\phi^-\rangle_{13}\|0\rangle_6$	$(\sigma_x)_4$	$\|\phi^-\rangle_{13}\|1\rangle_6$	$(i\sigma_y)_4$
	$\|\psi^+\rangle_{13}\|0\rangle_6$	$(-\sigma_z)_4$	$\|\psi^+\rangle_{13}\|1\rangle_6$	I_4
	$\|\psi^-\rangle_{13}\|0\rangle_6$	$(-\sigma_z)_4$	$\|\psi^-\rangle_{13}\|1\rangle_6$	$(-I)_4$
$\|H^-\rangle_{M25}$	$\|\phi^+\rangle_{13}\|0\rangle_6$	$(i\sigma_y)_4$	$\|\phi^+\rangle_{13}\|1\rangle_6$	$(-\sigma_x)_4$
	$\|\phi^-\rangle_{13}\|0\rangle_6$	$(i\sigma_y)_4$	$\|\phi^-\rangle_{13}\|1\rangle_6$	$(\sigma_x)_4$
	$\|\psi^+\rangle_{13}\|0\rangle_6$	$(-I)_4$	$\|\psi^+\rangle_{13}\|1\rangle_6$	$(\sigma_z)_4$
	$\|\psi^-\rangle_{13}\|0\rangle_6$	$(-I)_4$	$\|\psi^-\rangle_{13}\|1\rangle_6$	$(-\sigma_z)_4$
$\|S^+\rangle_{M25}$	$\|\phi^+\rangle_{13}\|0\rangle_6$	I_4	$\|\phi^+\rangle_{13}\|1\rangle_6$	$(-\sigma_z)_4$
	$\|\phi^-\rangle_{13}\|0\rangle_6$	$(-I)_4$	$\|\phi^-\rangle_{13}\|1\rangle_6$	$(-\sigma_z)_4$
	$\|\psi^+\rangle_{13}\|0\rangle_6$	$(-i\sigma_y)_4$	$\|\psi^+\rangle_{13}\|1\rangle_6$	$(\sigma_x)_4$
	$\|\psi^-\rangle_{13}\|0\rangle_6$	$(i\sigma_y)_4$	$\|\psi^-\rangle_{13}\|1\rangle_6$	$(\sigma_x)_4$
$\|S^-\rangle_{M25}$	$\|\phi^+\rangle_{13}\|0\rangle_6$	$(\sigma_z)_4$	$\|\phi^+\rangle_{13}\|1\rangle_6$	$(-I)_4$
	$\|\phi^-\rangle_{13}\|0\rangle_6$	$(-\sigma_z)_4$	$\|\phi^-\rangle_{13}\|1\rangle_6$	$(-I)_4$
	$\|\psi^+\rangle_{13}\|0\rangle_6$	$(-\sigma_x)_4$	$\|\psi^+\rangle_{13}\|1\rangle_6$	$(i\sigma_y)_4$
	$\|\psi^-\rangle_{13}\|0\rangle_6$	$(\sigma_x)_4$	$\|\psi^-\rangle_{13}\|1\rangle_6$	$(i\sigma_y)_4$
$\|T^+\rangle_{M25}$	$\|\phi^+\rangle_{13}\|0\rangle_6$	$(\sigma_x)_4$	$\|\phi^+\rangle_{13}\|1\rangle_6$	$(i\sigma_y)_4$
	$\|\phi^-\rangle_{13}\|0\rangle_6$	$(-\sigma_x)_4$	$\|\phi^-\rangle_{13}\|1\rangle_6$	$(i\sigma_y)_4$
	$\|\psi^+\rangle_{13}\|0\rangle_6$	$(\sigma_z)_4$	$\|\psi^+\rangle_{13}\|1\rangle_6$	I_4
	$\|\psi^-\rangle_{13}\|0\rangle_6$	$(-\sigma_z)_4$	$\|\psi^-\rangle_{13}\|1\rangle_6$	I_4
$\|T^-\rangle_{M25}$	$\|\phi^+\rangle_{13}\|0\rangle_6$	$(i\sigma_y)_4$	$\|\phi^+\rangle_{13}\|1\rangle_6$	$(\sigma_x)_4$
	$\|\phi^-\rangle_{13}\|0\rangle_6$	$(-i\sigma_y)_4$	$\|\phi^-\rangle_{13}\|1\rangle_6$	$(\sigma_x)_4$
	$\|\psi^+\rangle_{13}\|0\rangle_6$	I_4	$\|\psi^+\rangle_{13}\|1\rangle_6$	$(\sigma_z)_4$
	$\|\psi^-\rangle_{13}\|0\rangle_6$	$(-I)_4$	$\|\psi^-\rangle_{13}\|1\rangle_6$	$(\sigma_z)_4$

Step 2 Quantum Key Distribution : Alice shares a secret key K_{AD} with David, a secret key K_{AP} with Peter, a secret key K_{AT} with the trust party Trent, respectively. Bob and Charlie share a secret key K_{PBC} with Peter. All secret keys are distributed through QKD protocols, which have been proved to be unconditionally secure [24–26].

Step 3 Quantum Channel Setup: David produces n six-qubit entangled states as in (1), he gives particles (2,5) to Peter, particles (1,3) to Bob and particle 6 to Charlie, David holds particle 4.

3.2 Blind the Message Phase

Alice blinds the message M and gets $M' = \{M'(1), M'(2), \cdots, M'(n)\}(M'(i) \in \{0, 1\}, i = 1, 2, \cdots, n)$. The method of blinding and encoding message are as follows.

(a) The $M'(i)$ is decided by the ith bit of K_{AD}. Alice obtains $M'(i)$ as following

$$M'(i) = K_{AD}^{i} \oplus M(i), i = 1, 2, \cdots, n. \tag{10}$$

(b) Alice produces n quantum states: $\{|\varphi_1\rangle_{M'}, |\varphi_2\rangle_{M'}, \cdots, |\varphi_n\rangle_{M'}\}(|\varphi_i\rangle_{M'} = \frac{1}{\sqrt{2}}(|0\rangle + b(i)|1\rangle), i = 1, 2, \cdots, n)$. Where $b(i)$=1 and $b(i)$=−1 is corresponding to $M'(i)$=1 and $M'(i)$=0, respectively. The secret key K_{AD} is shared by Alice and David, the length of K_{AD} is large enough. Since K_{AD} is distributed via QKD protocols [24–26] so that it is unknown to other people except Alice and David.

This message blinding and coding rule is only known to Alice and David, and other people do not know it.

3.3 Authorizing and Signing Phase

In our scheme, the quantum one-time pad [27] is adopted to guarantee the transmit secure.

Step 1 Alice sends $E_{K_{AP}}\{|\varphi_i\rangle_{M'}\}$ to Peter. Peter decrypts $E_{K_{AP}}\{|\varphi_i\rangle_{M'}\}$ with the key K_{AP} to get $|\varphi_i\rangle_{M'}$, then he performs the GHZ-state measurement on particles (M',2,5) and records his measurement results as α_P, where α_P is Peter's signature of the blind message M'. Then he encrypts α_P with key K_{PBC} to get the message $E_{K_{PBC}}\{\alpha_P\}$ and sends it to Bob and Charlie as his proxy request.

Step 2 After Bob and Charlie received the message $E_{K_{PBC}}\{\alpha_P\}$. If they agree to delegate Peter to sign messages instead of them, they will help Peter and David to complete the controlled teleportation. Bob performs the Bell-state measurement on particles (1,3) and records the measuring result as α_B. Charlie performs single particle measurement on particle 6 in the basis $\{|0\rangle, |1\rangle\}$ and records the measuring results as α_C. Then they encrypt α_B and α_C with the key K_{PBC} to get the message $E_{K_{PBC}}\{\alpha_B, \alpha_C\}$ and send it to Peter as their proxy authorization. If Bob and Charlie do not agree Peter to sign messages for them, they will not allow Peter and David to perform their teleportation.

Step 3 After Peter received the message $E_{K_{PBC}}\{\alpha_B, \alpha_C\}$, he decrypts it with key K_{PBC} to get the messages α_B and α_C. Then Peter encrypts α_B, α_C, α_P with key K_{AP} to get his signature $E_{K_{AP}}\{\alpha_B, \alpha_C, \alpha_P\}$ and sends it to Alice.

Step 4 Alice decrypts $E_{K_{AP}}\{\alpha_B, \alpha_C, \alpha_P\}$ with key K_{AP} to get the messages α_B, α_C, α_P. She encrypts these messages with key K_{AD} and K_{AT} to get $E_{K_{AD}}\{M', \alpha_B, \alpha_C, \alpha_P\}$ and $E_{K_{AT}}\{M', \alpha_B, \alpha_C, \alpha_P\}$, then she sends $E_{K_{AD}}\{M', \alpha_B, \alpha_C, \alpha_P\}$ to David and sends $E_{K_{AT}}\{M', \alpha_B, \alpha_C, \alpha_P\}$ to Trent, respectively.

3.4 Verifying Phase

Step 1 After David received the message $E_{K_{AD}}\{M', \alpha_B, \alpha_C, \alpha_P\}$ from Alice, he decrypts it with the key K_{AD} to get the messages $M', \alpha_B, \alpha_C, \alpha_P$.

Step 2 Trent decrypts message $E_{K_{AT}}\{M', \alpha_B, \alpha_C, \alpha_P\}$ with key K_{AT} to get messages M^* and $\alpha_B^*, \alpha_C^*, \alpha_P^*$. Then Trent announces his messages M^* and $\alpha_B^*, \alpha_C^*, \alpha_P^*$. David compares his messages with Trent's messages, if M'=M^*, α_B=α_B^*, α_C=α_C^*, α_P=α_P^*, he will declare

that the process is valid and continue the following verify process. Then David performs appropriate unitary operation on particle 4 to replicate the teleported unknown state $|\varphi\rangle_{M'}$ which carries messages.

Step 3 According to coding rule (b) in 3.2, David obtains $\{M''(1), M''(2), \cdots, M''(n)\}$ via measuring $\{|\varphi_1\rangle_{M'}, |\varphi_2\rangle_{M'}, \cdots, |\varphi_n\rangle_{M'}\}$ in the basis $\{|+\rangle, |-\rangle\}$, where $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. Then he gets message M'' and compares it with M'. if M'=M'', David accepts the message M' and the signature. Otherwise, David rejects it.

Step 4 David unblinds M' with key K_{AD} according to the rule by (a) in 3.2 to get the message M. The message M has been signed. David confirms the signature (M, α_B, α_C, α_P).

4 Security Analysis and Discussion

4.1 Impossibility of Disavowal

Firstly, we show that it is impossible for Bob and Charlie to disavow their delegation. According to (3.4.1) in 3.4, David decrypts message $E_{K_{AD}}\{M', \alpha_B, \alpha_C, \alpha_P\}$ with key K_{AD} to get Bob's and Charlie's proxy authorization α_B, α_C. The receiver David can verify signature with the help of Trent. All keys are distributed via QKD protocols, which have been proved unconditionally secure and all messages are sent through the secure quantum channel. Hence, Bob and Charlie can not deny their delegation once David accepts the signature.

Secondly, we show that it is impossible for Peter to disavow his signature. From Section 3.4 in Section 3.4, the receiver David can get Peter's proxy request and verify signature with the help of the trust party Trent. Then Peter can not deny that he indeed has signed the message.

Thirdly, David can not disavow he has received the signature. It is obvious that David knows the secret key K_{AD} and can obtain the signature by Section 3.4 in Section 3.4. Moreover, the process of the verifying indicates he has received it. Suppose David deny he has received the signature, the sender Alice requests the trust party Trent to resolve the disagreement. The receiver David needs Trent's help in the process of signature verification so that Trent can confirm that David has received the signature. Hence David can not deny his receipt of the signature.

4.2 Impossibility of Forgery

In our scheme, those who attempt to forge message and signature would definitely be detected.

Firstly, we show that it is impossible for David to forge Peter's signature. If David wants to forge Peter's signature, as David needs the trust party Trent's help in the verifying process and David knows the secret key K_{AD} shared between Alice and David, so David's forge attacks will be detected by Trent and Alice. Then, David would not be able to forge the message and signature. David's cheat will be perceived through Peter, Bob and Charlie measuring their particles, respectively. Similarly, Alice will face the same situation like David. In other words, the trick insider attackers not be able to forge Peter's signature.

Secondly, suppose that an attacker or eavesdropper Eve forge Peter's signature. However, he not be able to know the secret key K_{AP} shared between Alice and Peter, so he can not send message encrypted by K_{AP}, in other words, it is impossible for Eve to forge Peter's signature. If an attacker Eve intends to forge Peter's signature, he must get the information

about K_{AP}. Assume that Eve guesses K_{AP} randomly, then he can produce the valid signature with the probability at most $\frac{1}{2^n}$, which vanishes zero if n is large enough. So Eve can forge Peter's signature with a negligible probability. Therefore, Eve can not forge Peter's signature.

Thirdly, Refs. [16, 17, 28] has shown that the receiver David can forge a valid signature for his own benefit without being detected. There we will give a thorough analysis and indicates that our scheme be safe from this counterfeit. Suppose that David have obtained M'=M'', he wants to modify them such that $(M')^*$=$(M'')^*$ because $(M')^*$ is beneficial to him. Then David claims that $|S\rangle$ is valid signature about the message $(M')^*$. However, it is impossible, because when Alice knows it, she requires the trust party Trent to solve the controversy by making a comparison between $(M')^*$ and M^*, if $(M')^* \neq M^*$, then the behavior of David will be detected.

4.3 Message's Blindness

In this scheme, the message M has been blinded by the sender Alice into $M' = \{M'(1), M'(2), \cdots, M'(n)\}(M'(i) \in \{0, 1\}, i = 1, 2, \cdots, n)$ according to blinding rule (a) in 3.2. The signatory Peter can get $E_{K_{AP}}\{|\varphi_i\rangle_{M'}\}$ from Alice, then he decrypts it with key K_{AP} to get the message $|\varphi_i\rangle_{M'}$ and signs the message by measuring his particles, he does not know the content of the message. Firstly, if Peter attempts to determine the message M, the only way is to get the information about K_{AD}. However, it is impossible, because the secret key is distributed via QKD protocols which have been proved unconditionally secure [24–26].

Secondly, even if Peter does know the secret key K_{AD}, the message blinding rule in 3.2 is secret to him. If Peter guesses the message blinding rule randomly, then he can determine it with the probability at most $\frac{1}{2^n}$, which will approximate zero if n is large enough. As a result, the proxy signatory Peter can not know the content of the message that he has signed. Hence, this scheme has the property of blindness.

4.4 The Proxy Property

In our scheme, the original signatory Bob and Charlie can give the proxy signatory Peter the proxy authorization by correlation of the controlled teleporation. Meanwhile, Peter can generate the valid signature.

4.5 Impossibility of Some Attacks

In this portion, we show that our scheme can resist some attacks. On the one hand, this scheme can resist the man-in-the-middle attack. Assume that Eve, an attacker, can fabricate Peter send signature to Alice or fabricate Alice send messages to David. However, the message M or signature is encrypted by the secret key. Because of the unconditional security of both quantum key distribution and one-time pad algorithm, it is impossible for Eve to manipulate the message or fabricate Peter's signature.

On the other hand, this scheme can resist intercept-resend attack. Suppose that Eve, an attacker, know well the signature protocol, and intercept the particles that transmitted from David to Peter, Bob and Charlie, respectively. Suppose Eve manipulate the message M or M' by means of resending his own particles instead of the original particles, however, the behavior will be detected by David because Eve unavoidably destroyed the correlation of particles in the quantum states.

5 Conclusion

In this paper, we present improvement of a quantum proxy blind signature scheme which uses genuine six-qubit entangled state as quantum channel. Compared with previous work Refs. [17], our scheme has the property of blindness. At the same time, the unconditional security is guaranteed by the quantum key distribution [24–26], quantum one-time pad and encryption algorithm. Different from the quantum signature proposed in Refs. [16, 17, 21, 29], our scheme introduces a trust party Trent to prevent David from forging a valid signature.

In addition, the message keeps the blind over the whole signature process in this scheme. Compared with the related scheme Refs. [16, 21], the introduction of the trust party Trent makes our scheme achieves a higher security. Moreover, this scheme adopts the GHZ-state measurement, Bell-state measurement and single particle measurement which are feasible to implement with current technologies and experimental conditions. Therefore, our scheme has a more extensive application value.

Acknowledgements This work is supported by the National Natural Science Foundation of China (Grant No. 61402275, 61402015, 61273311), the Natural Science Foundation of Shaanxi Province (Grant No. 2015JM6263, 2016JM6069), and the Fundamental Research Funds for the Central Universities(Grant No. GK201402004).

References

1. Shor, P.W.: Inproceedings of the 35th annual IEEE symposium on foundations of computer science, pp 124–134 (1994)
2. Mambo, M., Usuda, K., Okamoto, E.: Proxy signatures for delegating signing operation. In: Proceedings of the 3rd ACM Conference on Computer and Communications Security, pp. 48–57, New Delhi (1996)
3. Wen, X.J., Liu, Y., Zhang, P.Y.: Digital multi-signature protocol based on teleportation. Wuhan Univ. J. Nat. Sci. **12**(1), 29–32 (2007)
4. Wen, X.J., Liu, Y., Zhou, N.R.: Secure quantum telephone. Opt. Commun. **275**(1), 278–282 (2007)
5. Li, Q., Chan, W.H., Long, D.Y.: Arbitrated quantum signature scheme using Bell states. Phys. Rev. A **79**(5), 054307 (2009)
6. Wang, T.Y., Wei, Z.L.: One-time proxy signature based on quantum cryptography. Quantum Inf. Process. **11**(2), 455–463 (2012)
7. Zhang, K.J., Zhang, W.W., Li, D.: Improving the security of arbitrated quantum signature gainst the forgery attack. Quantum Inf. Process. **12**(8), 2655–2699 (2013)
8. Zou, X.F., Qiu, D.W.: Attack and improvements of fair quantum blind signature schemes. Quantum Inf. Process. **12**(6), 2071–2085 (2013)
9. Wang, T.Y., Cai, X.Q.: Security of a sessional blind signature based on quantum cryptograph. Quantum Inf. Process. **13**(8), 1677–1685 (2014)
10. Wang, T.Y., Cai, X.Q., Ren, Y.L., et al.: Security of quantum digital signatures for classical messages. Sci. Rep. **5**, 9231 (2015)
11. Barnum, H., Crepeau, C., Gottesman, D., et al.: In: Proceedings of the 43th annual IEEE symposium on foundations of computer science, pp. 449–458 (2002)
12. Gottesman, D., Chuang, I.L.: Quantum digital signature arXiv:quant-ph/0105032v2 (2001)
13. Zeng, G.H., Keitel, C.H.: Arbitrated quantum-signature scheme. Phys. Rev. A **65**, 042312 (2002)
14. Zeng, G.H.: Reply to Comment on Arbitrated quantum-signature scheme. Phys. Rev. A **78**, 016301 (2008)
15. Lee, H., Hong, C., Kim, J., et al.: Arbitrated quantum signature scheme with message recovery. Phys. Lett. A **321**, 295–300 (2004)
16. Cao, H.J., Wang, H.S., Li, P.F.: Quantum proxy multi-signature scheme using genuinely entangled six-qubits state. Int. J. Theor. Phys. **52**(4), 1188–1193 (2013)

17. Cao, H.J., Huang, J., Yu, Y.F., et al.: A quantum proxy signature scheme based on genuine five-qubit entangled state. Int. J. Theor. Phys. **53**(9), 3095–3100 (2014)
18. Chaum, D.: Blind signature for untraceable payments. Advances in cryptology. In: Proceeding of Crypto82, pp. 199–203. Springer, New York (1983)
19. Wen, X.J., Niu, X.M., Ji, L.P.: A weak blind signature scheme based on quantum cryptography. Opt. Commun. **282**(4), 666–669 (2008)
20. 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)
21. Shao, A.X., Zhang, J.Z., Xie, S.C.: A quantum multi-proxy multi-blind-signature scheme based on genuine six-qubit entangled state. Int. J. Theor. Phys. **55**, 5216–5224 (2016)
22. Yang, Y.Y., Xie, S.C., Zhang, J.Z.: An Improved Quantum Proxy Blind Signature Scheme Based on Genuine Seven-Qubit Entangled State. Int. J. Theor. Phys. **56**(7), 2293–2302 (2017)
23. Zhu, H.P.: Quantum state sharing of an arbitrary single-Atom state by using a genuine six-atom entangled state in cavity QED. Int. J. Theor. Phys. **52**(5), 1588–1592 (2013)
24. Shor, P.W., Preskill, J.: Simple proof of security of the BB84 quantum key distribution protocol. Phys. Rev. Lett. **85**(2), 441–444 (2000)
25. Mayers, D.: Unconditional security in quantum cryptography. J. Assoc.: Comput. Math. **48**(1), 351–406 (2001)
26. Inamon, H., Lutkenhaus, N., Mayers, D.: Unconditional security of practical quantum key distribution. Eur. Phys. J. D **41**(3), 599–627 (2007)
27. Guo, W., Zhang, J.Z., Li, Y.P., et al.: Multi-proxy strong blind quantum signature scheme. Int. J. Theor. Phys. **55**(8), 3524–3536 (2016)
28. Zhang, K.J., Jia, H.Y.: Cryptanalysis of a quantum proxy weak blind signature scheme. Int. J. Theor. Phys. **54**, 582–588 (2015)
29. Tian, J.H., Zhang, J.Z., Li, Y.P.: A quantum multi-proxy blind signature scheme based on genuine four-qubit entangled state. Int. J. Theor. Phys, 55(2) 809–816 (2015)