Int J Theor Phys (2014) 53:419–425
DOI 10.1007/s10773-013-1826-6

A Quantum Proxy Weak Blind Signature Scheme

Hai-Jing Cao · Yan-Yan Zhu · Peng-Fei Li

Received: 29 April 2013 / Accepted: 7 September 2013 / Published online: 19 September 2013

Abstract We present a weak blind signature scheme based on a genuinely entangled six qubits state. Different from classical blind signature schemes and current quantum signature schemes, our quantum weak blind signature scheme could guarantee not only the unconditionally security but also the anonymity of the message owner. To achieve that, quantum key distribution and one-time pad are adopted in our scheme. Our scheme has the characteristics of classical security and quantum security.

Keywords Proxy weak blind signature · Controlled teleportation · Bell-state measurement

1 Introduction

Proxy signature, as an importation cryptographic primitive, was firstly introduced in 1996 [1]. In a proxy signature scheme, an original signer can authorize another person, called proxy signer, to issue signatures on behalf of himself/herself. However, the common digital signature can not satisfy the special needs in the deep-seated application of E-commerce and E-government [2, 3]. Quantum digital signature is a technique which can ensure the security requirements for integrity of message, proof of origin or disavowal signature can be performed using the counter-intuitive properties of quantum mechanics. Since Mambo M et al. proposed a quantum digital signature protocol [1], many efforts have been made on it and lots of schemes have been presented [4–14]. In 2002, Zeng and Christoph proposed an arbitrated quantum signature scheme based on Greenberger-Horne-Zeilinger states [4]. Li et al. [11] presented an arbitrated quantum signature scheme using two-particle entangled Bell states. Moreover, Wen et al. [15, 16] have proposed some multi-signature schemes.

Blind signature is a special digital signature in which the message owner's anonymity could be protected to ensure privacy. In blind signature, the message owner could always

Project supported by the National Natural Science Foundation of China (Grant No 11305100).

H.-J. Cao (✉) · Y.-Y. Zhu · P.-F. Li
Physics Department, Shanghai University of Electric Power, Shanghai 201300, China
e-mail: caohj@shiep.edu.cn

get the authentic signature of his own message even though the signatory knows nothing about the content that he signed. Blind signature could be classified into weak blind signature and strong blind signature according to whether or not the signatory can trace the message owner. Chaum [17] proposed the first blind signature scheme in 1983 based on the complexity of factoring large integers. However, it could be easily broken with the emergence of quantum computers. Hence, researchers have show increasing interests in quantum signature schemes.

In this paper, we put forward a proxy weak blind signature scheme based on controlled quantum teleportation. The scheme uses the genuinely entangled six qubit state as quantum channel. We use quantum key distribution and one-time pad to guarantee the unconditional security and signature anonymity. It is shown to be unconditionally secure, 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 may it be deniable by the receiver.

2 Preliminary Theory

Different from classical blind signature scheme, the quantum blind signature scheme is based on the theory below. The four Bell states of 2-qubit are

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

Suppose that Alice and Bob share a quantum state in one of the Bell states

$$|\phi^{+}\rangle_{AB} = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{AB} = \frac{1}{\sqrt{2}}(|++\rangle + |--\rangle)_{AB}, \tag{2}$$

where

$$|+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}, \qquad |-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}.$$

Due to the entanglement characteristic of EPR pairs, after Alice having measured particle A, particle B will collapse to the same state as particle A. Thus, if Alice and Bob choose the same base $Bz = \{|0\rangle, |1\rangle\}$ or $Bx = \{|+\rangle, |-\rangle\}$ to measure their particles respectively, they will get the similar results. For example, if both Alice and Bob choose base Bz and Alice gets $|0\rangle$, then Bob's measuring result must be $|0\rangle$ too. However, after Alice's measurement, if Bob chooses a different base from Alice, Bob will get a random result.

Based on the above theory, we will detail the scheme of quantum weak blind signature and its verification in the following sections.

3 Controlled Quantum Teleportation

Borras et al. [18], introduced a genuinely entangled six qubits state It is given by

$$\begin{aligned}|\xi_6\rangle = \frac{1}{4}[&|000\rangle(|0\rangle|\phi_+\rangle + |1\rangle|\psi_+\rangle) + |001\rangle(|0\rangle|\psi_-\rangle - |1\rangle|\phi_-\rangle)\\ &+ |010\rangle(|0\rangle|\psi_+\rangle - |1\rangle|\phi_+\rangle) + |011\rangle(|0\rangle|\phi_-\rangle + |1\rangle|\psi_-\rangle)\\ &+ |100\rangle(-|0\rangle|\psi_-\rangle - |1\rangle|\phi_-\rangle) + |101\rangle(-|0\rangle|\phi_+\rangle + |1\rangle|\psi_+\rangle)\\ &+ |110\rangle(|0\rangle|\phi_-\rangle - |1\rangle|\psi_-\rangle) + |111\rangle(|0\rangle|\psi_+\rangle + |1\rangle|\phi_+\rangle)].\end{aligned} \tag{3}$$

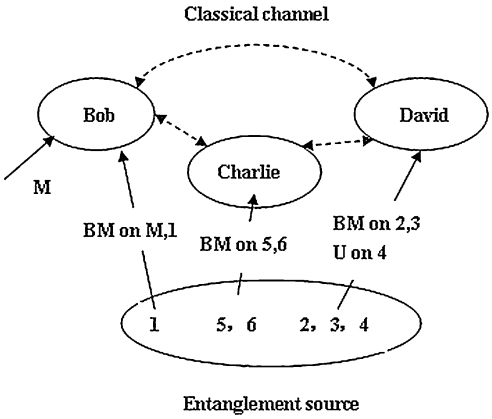

Fig. 1 Model of controlled quantum teleportation (BM and U behalf of Bell-state measurement and unitary operation, respectively)

Bob holds particle 1, Charlie owns particles (5, 6), and particles (2, 3, 4) are belong to David. The model of controlled quantum teleportation is shown in Fig. 1.

Suppose that the quantum state of particle M carrying messages in Bob is

$$|\psi\rangle_M = (\alpha|0\rangle + \beta|1\rangle)_M \tag{4}$$

where the coefficients α and β are unknown and satisfy $|\alpha|^2 + |\beta|^2 = 1$.

The state $|\Psi\rangle_{M123456}$ of the whole system composed of particles M and particles $(1, 2, 3, 4, 5, 6)$ is given by

$$|\Psi\rangle_{M123456} = |\psi\rangle_M \otimes |\xi_6\rangle_{123456} = (\alpha|0\rangle + \beta|1\rangle)_M \otimes |\xi_6\rangle_{123456} \tag{5}$$

(1) If Charlie agrees that Bob and David perform their quantum teleportation, he will perform Bell-state measurement on his particles (5, 6). Then he informs Bob and David his measuring results through the classical channel. The Bell-state measurement can collapse the quantum state $|\Psi\rangle_{M123456}$ into the following states

$$\begin{aligned}
\langle\phi_+^{56}|\Psi\rangle_{M123456} &= \frac{1}{4\sqrt{2}}(\alpha|0\rangle + \beta|1\rangle)_M(|0000\rangle - |0101\rangle - |1010\rangle + |1111\rangle)_{1234} \\
\langle\phi_-^{56}|\Psi\rangle_{M123456} &= \frac{1}{4\sqrt{2}}(\alpha|0\rangle + \beta|1\rangle)_M(-|0011\rangle + |0110\rangle - |1001\rangle + |1100\rangle)_{1234} \\
\langle\psi_+^{56}|\Psi\rangle_{M123456} &= \frac{1}{4\sqrt{2}}(\alpha|0\rangle + \beta|1\rangle)_M(|0001\rangle + |0100\rangle + |1011\rangle + |1110\rangle)_{1234} \\
\langle\psi_-^{56}|\Psi\rangle_{M123456} &= \frac{1}{4\sqrt{2}}(\alpha|0\rangle + \beta|1\rangle)_M(|0010\rangle + |0111\rangle - |1000\rangle + |1101\rangle)_{1234}.
\end{aligned} \tag{6}$$

(2) Bob performs Bell-state measurement on particles $(M, 1)$. He informs David his measuring results through the classical channel. Suppose that Charlie's measuring result is $|\psi_-^{56}\rangle$, the Bell-state measurement will collapse the quantum state of particles $M, 1, 2, 3, 4$ into the following states

$$\begin{aligned}
\langle\phi_\pm^{M1}|\psi_-^{56}|\Psi\rangle_{M123456} &= \frac{1}{8}(\alpha|010\rangle + \alpha|111\rangle \mp \beta|000\rangle \pm \beta|101\rangle)_{234} \\
\langle\psi_\pm^{M1}|\psi_-^{56}|\Psi\rangle_{M123456} &= \frac{1}{8}(-\alpha|000\rangle + \alpha|101\rangle \pm \beta|010\rangle \pm \beta|111\rangle)_{234}.
\end{aligned} \tag{7}$$

(3) According to Charlie's and Bob's measuring outcomes, David performs Bell-state measurement on particles (2, 3). If Charlie's and Bob's measuring results are $|\psi_{-}^{56}\rangle$ and $|\phi_{+}^{M1}\rangle$, respectively, the Bell-state measurement will collapse the quantum state of particles 2, 3, 4 into the following states

$$\begin{aligned}\langle\phi_{\pm}^{23}|\phi_{+}^{M1}|\psi_{-}^{56}|\Psi\rangle_{M123456} &= \frac{1}{8\sqrt{2}}(-\beta|0\rangle \pm \alpha|1\rangle)_4 \\ \langle\psi_{\pm}^{23}|\phi_{+}^{M1}|\psi_{-}^{56}|\Psi\rangle_{M123456} &= \frac{1}{8\sqrt{2}}(\alpha|0\rangle \pm \beta|1\rangle)_4.\end{aligned} \tag{8}$$

David operates appropriate unitary operation U_{exa} on particle 4 to successfully reconstruct the original unknown quantum state.

For example, when particle 4 is in the state of Eq. (8), the unitary operation are

$$U_1 = \pm|0\rangle_4\langle 1| - |1\rangle_4\langle 0|, \qquad U_2 = |0\rangle_4\langle 0| \pm |1\rangle_4\langle 1|. \tag{9}$$

Bob successfully transmits the unknown quantum state $|\psi\rangle_M$ to the receiver David.

4 Quantum Proxy Weak Blink Signature Scheme

To clarify our quantum weak blind signature scheme, three characters are defined as follows:

(1) Alice is defined as the customer who blinds the payment messages into the blinded messages, and sends the blinded messages to the businessman.

(2) Bob is defined as the representative of the bank Charlie, who signs the blinded messages to make a blind signature.

(3) David is defined as the businessman, who receives and verifies the payment messages, its signature and blind signature.

4.1 Initializing phase

(4.1.1) Message transformation. Alice transforms the message m into an n-bit sequence as $m = \{m(1), m(2), \ldots, m(i), \ldots, m(n)\}$ $(i = 1, 2, \ldots, n)$.

(4.1.2) Quantum key distribution. Alice, Bob and Charlie share secret key $K_{AD}(2n\text{-bit})$, $K_{BD}(3n\text{-bit})$ and $K_{CD}(n\text{-bit})$ with David, respectively. Bob shares secret key $K_{BC}(n\text{-bit})$ with Charlie. To ensure unconditional security, let us suppose that all keys are distributed via QKD protocols [19–22].

(4.1.3) Entangled states generation. Bob generates n EPR pairs such that

$$|\psi_i\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{a_i b_i} \tag{10}$$

where a_i and b_i denote the ith two entangled particles.

David generates $2n$ entangled six qubits state $|\xi_6\rangle$.

(4) In each EPR pair, Bob sends particle a_i to Alice while leaving particle b_i to himself. In every entangled six qubits state, David sends particle 1 to Bob, particles (5, 6) to Charlie, and holds particles (2, 3, 4).

4.2 Blind the message phase

(4.2.1) Alice measures her particle sequence according to message m. If $m(i) = 0$, she measures a_i on the base $B_z = \{|0\rangle, |1\rangle\}$. If $m(i) = 1$, she chooses the base $B_x = \{|+\rangle, |-\rangle\}$. Alice records the measuring results as $m'(i) = \{m'(1), m'(2), \ldots, m'(i), \ldots, m'(n)\}(m'(i) \in$

$\{|0\rangle, |1\rangle |+\rangle, |-\rangle\}$). The four states $|0\rangle, |1\rangle |+\rangle, |-\rangle$ could be encoded into two classical bits, for example

$$|0\rangle \to 00, \quad |1\rangle \to 01, \quad |+\rangle \to 10, \quad |-\rangle \to 11 \tag{11}$$

Thus, the message m (n-bit) has been blinded into m' ($2n$-bit).

(4.2.2) Alice encrypts m' with the key K_{AD} to get the secret message M, which is defined as

$$M = E_{K_{AD}}\left\{m'(1), m'(2), \ldots, m'(i), \ldots, m'(n)\right\} \tag{12}$$

Since both m' and K_{AD} are $2n$-bit, we adopt one-time pad as the encryption algorithm to guarantee the unconditional security.

(4.2.3) Alice sends the secret message M to the verifier David through the classical channel.

(4.2.4) Alice asks Bob to perform blind signature on message m'.

4.3 Authorizing phase

(4.3.1) After Bob receives Alice's signature ask, he ask the original signer Charlie to grant him to perform proxy signature on the message.

(4.3.2) Charlie receives particles $(5, 6)$ in $|\xi_6\rangle$ which David sends. If he agrees Bob as his proxy to sign the message, he will allow Bob and David to perform their controlled teleportation. Charlie performs the Bell-state measurement on particles $(5, 6)$ and records the measuring results as S_C. Then he encrypts S_C with the key K_{BC} to get the secret message $E_{K_{BC}}\{S_C\}$. He sends $E_{K_{BC}}\{S_C\}$ to Bob as granting secret key. If Charlie does not agree Bob to sign message for him, he will not allow Bob and David to perform their teleportation.

(4.3.3) Charlie encrypts S_C with the key K_{CD} to get the secret message $E_{K_{CD}}\{S_C\}$. He sends $E_{K_{CD}}\{S_C\}$ to David for verification signature.

4.4 Signing the blind message phase

After Bob has received the message $E_{K_{BC}}\{S_C\}$, he decrypts it with his key K_{BC} to get the message S_C. Bob performs the Bell-state measurement on particles (b_i,1) and records the measuring results as S_B. Bob encrypts S_B and S_C with the key K_{BD} to get the secret message $E_{K_{BD}}\{S_B, S_C\}$. Bob sends message $E_{K_{BD}}\{S_B, S_C\}$ to David, that is, Bob finishes the proxy signature of the blind signature m'.

4.5 Verifying phase

David first verifies Bob's proxy identity, then verifies Bob's proxy blind signature.

(4.5.1) David receives the secret message M from Alice, then decrypts it with his key K_{AD} to get the blind message m'. The odd number of blind message m' is the original message m.

(4.5.2) David receives the secret message $E_{K_{CD}}\{S_C\}$ from Charlie, then decrypts it with the key K_{CD} to get message S'_C. On the other hand, he receives the proxy blink signature $E_{K_{BD}}\{S_B, S_C\}$ from Bob, then decrypts it with the key K_{BD} to get messages S_B and S_C.

(4.5.3) David verifies Bob's proxy identity: when $S'_C = S_C$, Bob is authentic proxy and David will excuse the following operations to verify Bob's proxy blink signature. Otherwise he will end the agreement.

(4.5.4) According to the messages S_B and S_C, David performs the Bell-state measurement on particles $(2, 3)$. Based on all the measuring results, David operates appropriate unitary operation on particle 4 to successfully reconstruct the original unknown quantum state on particle 4.

(4.5.5) Based on the real messages David has obtained, David measures particle 4 on appropriate base according to the rule in (4.2.1). The measuring results could be encoded

into two classical bits according to Eq. (11). The encodes results is wrote as d. If $m' = d$, the proxy blink signature is valid, otherwise David will reject it.

5 Security Analysis and Discussion

In this section, we will give out that our weak blind signature scheme has the characteristics of classical security and quantum security.

(5.1) Classical security: the classical trick strategy fails

(5.1.1) The signature is weak blind

In our scheme, Bob is kept blind from the message content. However, measuring the particles is enough for Bob to sign the message. In E-payment system, the bank is not necessary to know the customer's transaction content, but he could sign the payment message for her. And the businessman could verify and accept the payment message signed by the bank.

(5.1.2) David can not forge messages or signatures

Bob is the representative of the bank Charlie, and they are totally credible in the scheme, usually. Suppose that the message receiver David is not honest, and attempt to forge Alice's message or Bob's and Charlie's signatures to get profits. Since David knows the shared secret keys between Alice, Bob, Charlie and himself, he would not be able to forge the messages, blind messages or signatures. If this disagreement happens, Alice will find David's behaviors. Bob and Charlie are able to measure their particles respectively to uncover David's trick.

In addition, David can not disavow his messages and his signatures. If he performs the controlled quantum teleportation, he will receive the signature and verify it.

(5.1.3) The message owner can be traced

Alice sends message M to David. Since M includes the secret key which is only known by Alice and David, Alice can not disavow her message M. Once some disagreement happens, according to the parameters of messages and secret keys, combined with the measuring results of particles, the referee can trace the message owner and judge whether the E-payment is valid or not.

(5.2) The quantum security: the quantum attack strategy fails

Our scheme can resist intercept-resend attacks. Suppose that Eve is an adversary who knows well the signature protocol, and captures the particles that Bob sent to Alice. If Eve tampers the message m or blind message m', by replacing the original particles with her own particles, she will inevitably destroy the correlation of particles in the quantum states and be detected by David.

Our scheme can also resist the man-in-the-middle attacks. Suppose Eve counterfeit Alice and Bob and send simultaneously particles and message M (or signature S) to Charlie. Due to the unconditional security of both quantum key distribution and one-time pad algorithm, it is impossible for Eve to either tamper the message M or counterfeit signing the message S. This is because that the message M is encrypted by the quantum secret key K_{AD} and the signature S is encrypted by K_{BD} and K_{CD}.

6 Conclusions

In this paper, we presented a quantum proxy multi-signature scheme based on genuinely entangled six qubits state. Different from previous quantum signature scheme in classical cryptography, the security of our scheme is guaranteed by the quantum one-time pad and quantum key distribution [23–25]. Hence, it is unconditionally secure.

References

1. Mambo, M., Usuda, K., Okamoto, E.: IEICE Trans. Fundam., E **79**(A(9)), 1338–1353 (1996)
2. Wang, T.Y., Cai, X.Q., Zhang, J.Z.: Comput. Eng. Appl. **33**(15), 155–157 (2007)
3. Cao, F., Cao, Z.F.: Inf. Sci. **179**(3), 292–302 (2009)
4. Zeng, G.H., Christoph, K.: Phys. Rev. A **65**, 042312 (2002)
5. Lee, H., Hong, C., Kim, H.J., et al.: Phys. Lett. A **321**, 295 (2004)
6. Wang, J., Zhang, Q., Tang, C.J.: Proceedings of the Eighth International Conference on Advanced Communication Technology, p. 1375. IEEE, New York (2006)
7. Curty, M., Lutkenhaus, N.: Phys. Rev. A **77**, 046301 (2008)
8. Yang, Y.G.: Chin. Phys. B **17**, 415 (2008)
9. Wen, X.J., Niu, X.M., Ji, L.P., et al.: Opt. Commun. **282**, 666–669 (2009)
10. Cao, Z.J., Markowitch, O.: Int. J. Quantum Inf. **7**, 1205 (2009)
11. Li, Q., Chan, W.H., Long, D.Y.: Phys. Rev. A **79**, 054307 (2009)
12. Yang, Y.G., Zhou, Z., Teng, Y.W., et al.: Eur. Phys. J. D **61**, 773–778 (2011)
13. Wu, Y.H., Zhai, W.D., Cao, W.Z., et al.: Int. J. Theor. Phys. **50**(7), 325–331 (2011)
14. Yin, X.R., Ma, W.P., Liu, W.Y.: Int. J. Quantum Inf. **10**, 1250041 (2012)
15. Wen, X.J., Liu, Y., Sun, Y.Z.: Z. Naturforsch. A **62**, 147–151 (2007)
16. Wen, X.J., Liu, Y., Sun, Y.: Chin. J. Electron. **17**, 340–344 (2008)
17. Chaum, D.: Proc. CRYPTO **82**, 199 (1983)
18. Borras, A., Majtey, A.P., Plastino, A.R., et al.: Eprint, arXiv:0806.0779 [quant-ph]
19. Hughes, R., Morgan, G., Peterson, C.: J. Mod. Opt. **47**(2–3), 533 (2000)
20. Deng, F.G., Long, G.L.: Phys. Rev. A **70**(1), 012311 (2004)
21. zhou, y.y., Li, X.Q., Zhou, X.J.: Chin. J. Quantum Electron. **27**(5), 565–572 (2010)
22. Wu, Z.B., Chen, G.: Chin. J. Quantum Electron. **26**(5), 560–564 (2009)
23. Shor, P.: Phys. Rev. Lett. **85**(2), 441 (2000)
24. Mayers, D.: J. ACM **48**(3), 351 (2001)
25. Deng, F.G., Long, G.L.: Phys. Rev. A **69**(5), 052319 (2004)