Int J Theor Phys (2017) 56:1241–1248
DOI 10.1007/s10773-016-3266-6

An E-payment Protocol Based on Quantum Multi-proxy Blind Signature

Ai-Xia Shao[1] · Jian-Zhong Zhang[1] · Shu-Cui Xie[2]

Received: 1 September 2016 / Accepted: 27 December 2016 / Published online: 7 January 2017

Abstract Based on quantum multi-proxy blind signature, a new E-payment protocol is proposed in this paper. Adopting the techniques of quantum key distribution, one-time pad and quantum proxy blind signature, our E-payment protocol could protect user's anonymity as the traditional E-payment systems do, and also have unconditional security which the classical E-payment systems cannot provide. Additionally, the quantum operation can be transmitted successfully with the probability 1, which can make the protocol reliable and practical.

Keywords E-payment protocol · Quantum multi-proxy blind signature · Four-particle cluster state · Unitary operation

1 Introduction

Nowadays, E-commerce is in a period of rapid development and choosing an appropriate model of payment is very important for E-commerce transaction. Since Chaum [1] proposed the concept of E-cash, many researchers have dedicated to study E-cash system and

✉ Jian-Zhong Zhang
1021672987@qq.com

Ai-Xia Shao
1018844066@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

proposed a number of E-cash payment schemes [2–6]. Compared with other payment methods, E-cash has the properties of anonymity and off-line transferability and is becoming an ideal method of payment. The current E-payment system is mainly based on blind signature and group signature to achieve.

Digital signature is one of the most important components of modern cryptography, which serves as a basic module to design cryptography protocols [7]. Blind signature is a special kind of digital signature [8–12] in which the message anonymity could be guaranteed. In blind signature schemes, the message owner could always get the authentic signature of his own message even though the signer knows nothing about the content that he signed, quantum blind signature is supposed to provide unconditionally secure. Quantum blind signature has many applications like electronic voting systems and electronic payment systems, so it attracts widespread attention [13–15]. In 2010, Wen and Nie proposed an E-payment system based on quantum blind and group signature, employing two third trusted party instead of one to enhance the systems robustness [16]. In succession, Wen et al proposed an inter-bank E-payment protocol based on quantum proxy blind signature (named WCF protocol hereafter) [17]. However, Cai et al. [18] showed that the dishonst merchant can succeed to change the purchase information of the customer in this protocol.

In this paper, we propose an E-payment protocol based on quantum multi-proxy blind signature. In our system, quantum key distribution and one-time pad are adopted in order to guarantee unconditional security. Compared with previous E-payment systems and quantum signature schemes, we have made the following contributions. To the best of our knowledge, we are the first to apply quantum multi-proxy blind signature. The property of quantum multi-proxy blind signature could protect the anonymity of E-payment systems, while the quantum protocol could guarantee unconditional security. Moreover, different from existing quantum signature schemes, our protocol only need Bell-measurement, it can be implemented easily with the current experimental conditions.

2 Preliminary Theory

2.1 Multi-Proxy Blind Signature

Proxy signature allows a designated person, called proxy signer, to sign on behalf of an original signer. Proxy signatures are widely used in the fields of grid computing, mobile agent, mobile communications, e-commerce etc. [19, 20]. As for blind signature, the message owner could get the authentic signature for his own message, but not reveal the specific content of the message. In some cases, such as an inter-bank trading system, both the property of proxy signature and that of blind signature were required for application and security concern, so multi-proxy blind signature was proposed.

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

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

Suppose that Alice and Bob share a Bell state

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

where

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

Due to the entanglement characteristic of EPR pairs, after Alice has measured particle A, particle B will collapse to the same state as particle A. Thus, if Alice and Bob choose the same base $B_z = \{|0\rangle, |1\rangle\}$ or $B_x = \{|+\rangle, |-\rangle\}$ to measure their particles respectively, they will get the similar results. For example, if both Alice and Bob choose base B_z 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.

2.2 Controlled Quantum Teleportation

The quantum multi-proxy blind signature is based on controlled teleportation. In this section, we will introduce the controlled teleportation using four-particle cluster state as quantum channel. It is given by

$$|\xi\rangle_{1234} = \frac{1}{2}(|0000\rangle + |0011\rangle + |1100\rangle - |1111\rangle)_{1234}. \tag{3}$$

The sender Alice owns particles 4, the controller Charlie owns particles (2, 3) and the particle 1 belongs to the receiver Bob.

Suppose that the quantum state of particle M carrying message in Alice 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 $|\Psi\rangle_{M1234}$ of whole system composed of particles M and (1, 2, 3, 4) is given by

$$|\Psi\rangle_{M1234} = |\psi\rangle_M \otimes |\xi\rangle_{1234} = (\alpha|0\rangle + \beta|1\rangle)_M \otimes |\xi\rangle_{1234}. \tag{5}$$

The details of the controlled teleportation are as follows.

1) Alice performs a Bell-state measurement on particles M and 4. The measurement can collapse the state of particles (1, 2, 3) into one of the following states

$$\begin{aligned} \langle\phi^{\pm}_{M4}|\Psi\rangle_{M1234} &= \frac{1}{2\sqrt{2}}(\alpha|000\rangle + \alpha|110\rangle \pm \beta|001\rangle \mp \beta|111\rangle)_{123}, \\ \langle\psi^{\pm}_{M4}|\Psi\rangle_{M1234} &= \frac{1}{2\sqrt{2}}(\alpha|001\rangle - \alpha|110\rangle \pm \beta|000\rangle \pm \beta|110\rangle)_{123}. \end{aligned} \tag{6}$$

Alice sends her measurement outcomes to Charlie and Bob.

2) If Charlie agrees Alice and Bob to perform their teleportation, Charlie performs a Bell-state measurement on his particles (2, 3). Suppose that Alice's measurement result is $|\phi^+\rangle_{M4}$, The measurement will collapse the state of particle 1 into one of the following states

$$\begin{aligned} \langle\phi^{\pm}_{23}|\phi^{+}_{M4}|\Psi\rangle_{M1234} &= \tfrac{1}{4}(\alpha|0\rangle \mp \beta|1\rangle)_1, \\ \langle\psi^{\pm}_{23}|\phi^{+}_{M4}|\Psi\rangle_{M1234} &= \tfrac{1}{4}(\beta|0\rangle \pm \alpha|1\rangle)_1. \end{aligned} \tag{7}$$

3) According to Alice's and Charlie's measurement outcomes, Bob operates one of four unitary operations $(I, \sigma_z, \sigma_x, i\sigma_y)$ on particle 1 to reconstruct the unknown quantum state $|\psi\rangle_M$. For example, assume Alice's measurement result is $|\phi^+\rangle_{M4}$ and Charlie's measurement result is $|\phi^+\rangle_{23}$, respectively, Bob's operation on particle 1 is σ_z. For other cases, the relationship between Alice's, Charlie's measurement outcomes and Bob's operation is listed in Table 1.

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

Alice's measurement outcome	Charlie's measurement outcome	Bob's operation
$\|\phi^+\rangle_{M4}$	$\|\phi^+\rangle_{23}$	$(\sigma_z)_1$
$\|\phi^+\rangle_{M4}$	$\|\phi^-\rangle_{23}$	I_1
$\|\phi^+\rangle_{M4}$	$\|\psi^+\rangle_{23}$	$(\sigma_x)_1$
$\|\phi^+\rangle_{M4}$	$\|\psi^-\rangle_{23}$	$(i\sigma_y)_1$
$\|\phi^-\rangle_{M4}$	$\|\phi^+\rangle_{23}$	I_1
$\|\phi^-\rangle_{M4}$	$\|\phi^-\rangle_{23}$	$(\sigma_z)_1$
$\|\phi^-\rangle_{M4}$	$\|\psi^+\rangle_{23}$	$(i\sigma_y)_1$
$\|\phi^-\rangle_{M4}$	$\|\psi^-\rangle_{23}$	$(\sigma_x)_1$
$\|\psi^+\rangle_{M4}$	$\|\phi^+\rangle_{23}$	$(i\sigma_y)_1$
$\|\psi^+\rangle_{M4}$	$\|\phi^-\rangle_{23}$	$(\sigma_x)_1$
$\|\psi^+\rangle_{M4}$	$\|\psi^+\rangle_{23}$	I_1
$\|\psi^+\rangle_{M4}$	$\|\psi^-\rangle_{23}$	$(\sigma_z)_1$
$\|\psi^-\rangle_{M4}$	$\|\phi^+\rangle_{23}$	$(\sigma_x)_1$
$\|\psi^-\rangle_{M4}$	$\|\phi^-\rangle_{23}$	$(i\sigma_y)_1$
$\|\psi^-\rangle_{M4}$	$\|\psi^+\rangle_{23}$	$(\sigma_z)_1$
$\|\psi^-\rangle_{M4}$	$\|\psi^-\rangle_{23}$	I_1

3 Quantum E-payment Protocol

To clarify our quantum E-payment protocol, 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) $U_j(j = 1, 2, \cdots, t)$ is defined as the representative of the bank Charlie, who signs the blinded messages to make a blind signature.

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

3.1 Initial Phase

Step1 The customer Alice holds a n-bit purchase message string (information bits) to be signed:

$$m = \{m(1), m(2), \cdots, m(n)\} = \{m(i), i = 1, 2, \cdots, n\}. \tag{8}$$

Step2 Alice, U_j and Charlie share secret keys K_{AB}, K_{BU_j} and K_{BC} with Bob, respectively. All these keys are distributed via QKD protocols, which have been proved unconditionally secure [21–23].

Step3 U_j generates n EPR pairs such that

$$|\psi_i\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{A_iB_i}. \tag{9}$$

where A_i and B_i denote the ith two entangled particles. In every EPR pair, U_j sends particle A_i to the customer Alice while leaving B_i to himself. Bob generates tn entangled four particle cluster states as showed in (3), he gives particle 4 to U_j, particles (2, 3) to the bank Charlie and he holds particle 1.

3.2 Blind the Purchase Message Phase

Step1 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 $m' = \{m'(1), m'(2), \cdots, m'(i) \cdots, m'(n)\}(m'(i) \in \{|0\rangle, |1\rangle, |+\rangle, |-\rangle\})$. The four states $|0\rangle, |1\rangle, |+\rangle, |-\rangle$ could be encoded into two classical bits as following

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

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

Step2 Alice encrypts m'' with the key K_{AB} to get the secret message M, which is denoted as

$$M = E_{K_{AB}}\{m''(1), m''(2), \cdots, m''(i) \cdots, m''(n)\}. \tag{11}$$

We adopt one-time pad as the encryption algorithm to guarantee the unconditional security. Alice sends the secret message M to the businessman Bob through the classical channel.

3.3 Authorizing and Signing Phase

Step1 To distinguish each proxy signers, Alice creates a unique serial number, which is denoted as SN and transfers it to a quantum state sequence $|SN\rangle$ in the basis $\{|0\rangle, |1\rangle\}$. Then she sends $|SN_j\rangle$ to U_j.

Step2 After U_j received $|SN_j\rangle$, he performs a Bell-state measurement on particles B_i and 4. He combines the resulting records with his serial number as $\beta_{U_j} = (\alpha(i)_{B_i4}, i = 1, 2, \cdots, n, |SN_j\rangle)(\alpha(i)_{B_i4} \in |\phi^+\rangle, |\phi^-\rangle, |\psi^+\rangle, |\psi^-\rangle)$, where β_{U_j} is $U_j's$ individual signature of message. U_j sends $S_{U_j} = E_{K_{BU_j}}\{\beta_{U_j}\}$ to Bob, and β_{U_j} to Charlie as his request.

Step3 If the bank Charlie agrees U_j to sign the message on behalf of himself, he will help U_j and the businessman Bob to complete the controlled teleportation. Charlie performs a Bell-state measurement on his particles (2, 3) and combines the records with $|SN_j\rangle$ as $\beta_{Cj} = (\beta(i)_{23}, i = 1, 2, \cdots, n, |SN_j\rangle)(\beta(i)_{23} \in |\phi^+\rangle, |\phi^-\rangle, |\psi^+\rangle, |\psi^-\rangle)$. Then Charlie sends $S_{Cj} = E_{K_{BC}}\{\beta_{Cj}\}$ to Bob.

3.4 Verifying Phase

Step1 Bob receives the secret message M from Alice, then he decrypts it with the key K_{AB} to get the blind message m''.

Step2 Bob decrypts messages S_{U_j} and S_{Cj} with keys K_{BU_j} and K_{BC} to get the signature β_{U_j} and the message β_{Cj}, respectively. According to β_{U_j} and β_{Cj}, Bob performs a corresponding unitary operation on particle 1 to successfully reconstruct the unknown state on particle 1. The relationship between $U_j's$, Charlie's measurement results and Bob's operation is listed in Table 1. (We replace Alice's measurement results which is listed in Table 1 with $U_j's$).

Step3 Based on the real message the businessman Bob has obtained, Bob measures particle 1 on appropriate base according to the rule by the step1 in 3.2. The measuring results could be encoded into two classical bits according to (10). The results are wrote as $c(j)$. If $c(j) = m''$, the proxy signature is valid, otherwise, Bob will reject it.

Step4 Bob collects $\{S_{U_j}, j = 1, 2, \cdots, t\}$ and gets the messages $\{c(j), j = 1, 2, \cdots, t\}$, if $c(j) = c(j+1) = m''(j = 1, 2, \cdots, t-1)$, he will confirm the signature and generate the final signature $S = \{S_{U_1}, S_{U_2}, \cdots, S_{U_t}\}$, else terminates the process.

4 Security Analysis and Discussion

Inspired by some articles [24–26], we have carried out the security analysis and discussion from the following aspects.

4.1 Message's Blindness

In our scheme, the payment message m has been translated by Alice into m', where every $m'(i) \in \{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$. If U_j attempts to obtain the message m', the only way is to perform measurements. However, U_j can not know Alice choose which base to measure her particle A_i, so U_j can not learn the message m', thus, he also can not deduce the original message m from it. Therefore, each proxy signatory knows nothing about the message that he has signed. That is, our scheme has the property of blindness.

4.2 Impossibility of Denial

In our scheme, we show that the bank Charlie can not disavow his delegation and U_j can not deny his signature. According to Step 2 in 3.4, businessman Bob decrypts messages S_{Cj} and S_{U_j} with key K_{BC} and key K_{BU_j} can get Charlie's authorization, $U_j^{\prime}s$ proxy request and his serial number SN_j, respectively. All keys are distributed via QKD protocols, which have been proved unconditionally secure and all messages are sent through the secure quantum channel. Hence, Charlie can not deny his delegation and U_j can not deny his signature.

4.3 Impossibility of Forgery

Firstly, we show that it is impossible for the dishonest insider attackers to forge U_j's signature. Suppose that the businessman Bob is not honest, and attempts to forge customer's message or U_j's signature. Since Bob knows the shared secret keys between customer Alice and himself, he would not be able to forge the message, blind message or signatures. If this disagreement happens, Alice will find Bob's behaviors. U_j and Charlie are able to measure their particles respectively to uncover Bob's trick. Similarly, Alice and $U_i(i \neq j)$ can not forge U_j's signature. In a word, the dishonest insider attackers can not forge signature.

Secondly, we discuss the forgery made by the outsider attacker Eve. As analyzed above, it is impossible for Eve to forge U_j's signature under the condition that he has no knowledge of the secret key K_{BU_j}. Therefore, if Eve aims to forge U_j's signature successfully, the only way is to get the information about K_{BU_j}. However, it is impossible, because the secret key is generated by the QKD protocol which has been proved unconditionally secure. Hence, Eve can not forge U_j's signature.

4.4 Unconditional Security

Our scheme ensures security from the following three aspects. First, the protocol BB84 is adopted for quantum key distribution; Second, we employ one-time pad to encrypt; Third, our protocol is based on the secure quantum channel, which has instantaneous transmission not restricted by distance, time or obstacles, all of these are proved to be unconditional secure.

5 Conclusion

Combined with the actual demand for E-payment, in this paper, we proposed an E-payment protocol based on quantum multi-proxy blind signature. Compared with previous works, our protocol can realize the customer blind the payment messages into the blinded messages, which can protect the payment messages. Furthermore, our protocol is based on four-particle cluster state with less resource and as the key techniques of our protocol only rely on the Bell-measurement, which can make the protocol reliable and practical.

Additionally, in our scheme the Bell state $|\phi^{+}\rangle_{AB}$ can be replaced by the other three Bell states, the E-payment protocol can be finished and proved secure.(We will not repeat the details of the protocol).

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

References

1. Chaum, D.: Blind signature for untraceable payments. Advances in cryptology. In: Proceeding of Crypto82, pp. 199–203. Springer, New York (1983)
2. Chaum, D., Heyst, E.: Group Signatures, Advances in Cryptology-Eurocrypt91. LNCS 547, pp. 257–265. Springer, Berlin (1991)
3. Maitland, G., Boyd, C.: Fair Electronic Cash Based on a Group Signature Scheme, ICICS 2001, LNCS 2229, pp. 461–465. Springer, Berlin (2001)
4. Canard, S., Traor J.: On Fair E-cash Systems Based on Group Signature Schemes, ACISP 2003, LNCS 2727, pp. 237–248. Springer, Berlin (2003)
5. Traor, J.: Group Signatures and Their Relevance to Privacy-Protecting Offline Electronic Cash Systems, ACISP99 LNCS 1587, pp. 228–243. Springer, Berlin (1999)
6. Qiu, W., Chen, K., Gu, D.: A New Off-Line Privacy Protecting E-Cash System with Revocable Anonymity, ISC 2002, LNCS 2433, pp. 177–190. Springer, Berlin (2002)
7. William, S.: Cryptography and Network Security: Principles and Practice, 2nd edn. Prentice Hall, New York (2003)
8. Harn, L.: Cryptanalysis of the blind signature based on the discrete logarithm. Electron. Lett. **31**(14), 1136–1137 (1995)
9. Fan, C., Lei, C.: Efficient blind signature scheme based on quadratic residues. Electron. Lett. **32**(9), 811–813 (1996)
10. Lysyanskaya, A., Ramzan, Z.: Group blind digital signature: a scalable solution to electronic cash. In: Proceedings of the 2nd Financial Cryptography Conference (1998)
11. Mohammed, E., Emarah, A.E., El-Shennawy, K.: A blind signature scheme based on elgamal signature. In: EURO-COMM 2000. Information Systems for Enhanced Public Safety and Security, pp. 51–53. IEEE/AFCEA (2000)

12. Chien, H., Jan, J., Tseng, Y.: Eighth international conference on parallel and distributed systems (ICPADS01) 44 (2001)
13. Xu, R., Huang, L., Yang, W., He, L.: Quantum group blind signature scheme without entanglement. Opt. Commun. **284**, 3654 (2011)
14. Yin, X.R., Ma, W.P., Liu, W.Y.: A blind quantum signature scheme with chi-type entangled states. Int. J. Theor. Phys. **51**, 455–461 (2012)
15. Tian, J.H., Zhang, J.Z., Li, Y.P.: A voting protocol based on the controlled quantum operation teleportation. Int. J. Thero. Phys. **55**(5), 2303–2310 (2016)
16. Wen, X.J., Nie, Z.: An E-payment system based on quantum blind and group signature. Physica Scripta. **82**(6), 5468–5478 (2010)
17. Wen, X.J., Chen, Y.Z., Fang, J.B.: An inter-bank E-payment protocol based on quantum proxy blind signature. Quantum. Inf. Process. **12**(1), 549–558 (2013)
18. Cai, X.Q., Wei, C.Y.: Cryptanalysis of an inter-bank E-payment protocol based on quantum proxy blind signature. Quantum. Inf. Process. **12**(4), 1651–1657 (2013)
19. Wang, T.Y., Cai, X.Q., Zhang, J.Z.: Off-line e-cash system with multiple banks based on elliptic curve. Comput. Eng. Appl. **33**(15), 155–157 (2007)
20. Cao, F., Cao, Z.F.: A secure identity-based proxy multi-signature scheme. Inf. Sci. **179**(3), 292–302 (2009)
21. Shor, P.W., Preskill, J.: Simple proof of security of the BB84 quantum key distribution protocol. Phys. Rev. Lett. **85**(2), 441–444 (2000)
22. Mayers, D.: Unconditional security in quantum cryptography. J. Assoc.: Comput. Math **48**(1), 351–406 (2001)
23. Inamon, H., Lutkenhaus, N., Mayers, D.: Unconditional security of practical quantum key distribution. Eur. Phys. J. D **41**(3), 599–627 (2007)
24. Xia, Z.H., Wang, X.H., Zhang, L.G.: A Privacy-preserving and Copy-deterrence Content-based Image Retrieval Scheme in Cloud Computing[J]. 1–1 (2016)
25. Wang, T.Y., Wei, Z.L.: Analysis of forgery attack on one-time proxy signature and the improvement. Int. J. Theor. Phys. **55**, 743–745 (2016)
26. Guo, P., Wang, J., Geng, X.H.: A variable threshold-value authentication for wireless mesh networks. Journal of Internet Technology **15**(6), 929–936 (2014)