Int J Theor Phys (2018) 57:2657–2664
https://doi.org/10.1007/s10773-018-3787-2

A Trusted Third-Party E-Payment Protocol Based on Quantum Blind Signature Without Entanglement

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

Received: 4 January 2018 / Accepted: 25 May 2018 / Published online: 4 June 2018

Abstract In this paper, we present a trusted third-party e-payment protocol which is designed based on quantum blind signature without entanglement. The security and verifiability of our scheme are guaranteed by using single-particle unitary operation, quantum key distribution (QKD) protocol and one-time pad. Furthermore, once there is a dispute among the participants, it can be solved with the assistance of the third-party platform which is reliant.

Keywords Third-party e-payment protocol · Quantum blind signature · Single-particle unitary operation

1 Introduction

With the rapid development of e-business, the third-party e-payment, as one of the basic links of e-business development, has become the way that people are familiar with and

✉ Jian-Zhong Zhang
1416655910@qq.com

Xi Guo
872552325@qq.com

Shu-Cui Xie
xieshucui@163.com

[1] School 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

accepted. The key to building an efficient and secure electronic cash payment system is to design a favorable cryptogram protocol.

Since Chaum [1] proposed the concept of electronic cash, kinds of e-cash schemes [2–8] based on signature techniques, have been presented. The current e-cash systems depend mainly on classical signature schemes, whose securities are based on complex mathematic problems, such as factorization problem, discrete logarithm problem. However, these problems will be solved easily as the quantum computer is growing quickly. Fortunately, in the quantum information processing and computation, quantum cryptography can provide unconditionally secure communication based on the laws of physics, especially with the no-cloning theorem [9].

Inspired by the properties, some scholars have proposed a few e-payment schemes based on quantum signatures [10–14]. In 2010, an e-payment protocol based on group signature was proposed to solve the conditional security problem by Wen et al. [10]. The disadvantage of this protocol is that the system was only applied within the same banks. Then, they presented also a new inter-bank protocol based on quantum proxy blind signature which could not only protect user's anonymity but also implement among different banks in 2013 [11]. But Cai et al. [12] indicated that the scheme is insure because purchase information could be tampered by the dishonest merchant. In 2014, an online banking system based on quantum cryptography communication is proposed by Zhou et al. [13]. They used two sets of GHZ states to ensure safety in this paper. In 2016, Yang et al. [14] presented a third-party e-payment protocol based on quantum group blind in which message of signer could be protected.

To the best of our knowledge, previous schemes use entanglement states to finish transaction. To simplify the operation, a trusted third-party e-payment protocol which adopts quantum blind signature without entanglement is proposed. Compared with classical e-payment protocols, our scheme can provide unconditional security which is a outstanding characteristic of quantum cryptography. Meanwhile, in the process of payment, the payment message has been blinded by owner of information, which can keep other people from obtaining it except verifier. To achieve it, quantum key distribution (QKD) protocol [15–17] and quantum Z gate are adopted in our scheme. Furthermore, the proposed scheme not only can resist the attacks by inserting decoy photons but also be applied in different banks. In addition, this scheme can be realized easily since we only use single-particle states. Therefore, it will have a good application value in current condition.

The rest of this paper is organized as follows. In Section 2, we introduce the basic theories of quantum Z gate. In Section 3, we present the detail content of third-party e-payment protocol. In Section 4, we give an example to describe this scheme. The security is analyzed in Section 5. Finally, we draw conclusions.

2 Basic Theory

In this section, we introduce basic theory that will be used in the later section.

2.1 Quantum Z Gate

Quantum Z gate is expressed as

$$Z = |0\rangle\langle 0| - |1\rangle\langle 1|. \tag{1}$$

It is used to transform for single quantum bit($\{|+X\rangle, |-X\rangle\}$ and $\{|+Y\rangle, |-Y\rangle\}$ refer to two different bases), such as

$$\begin{aligned}
Z|+X\rangle &= \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = |-X\rangle,\\
Z|-X\rangle &= \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = |+X\rangle,\\
Z|+Y\rangle &= \frac{1}{\sqrt{2}}(|0\rangle - i|1\rangle) = |-Y\rangle,\\
Z|-Y\rangle &= \frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle) = |+Y\rangle.\\
(|+X\rangle &= \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), |-X\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle),\\
|+Y\rangle &= \frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle), |-Y\rangle = \frac{1}{\sqrt{2}}(|0\rangle - i|1\rangle))
\end{aligned}$$

Its matrix representation is

$$Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}. \tag{2}$$

2.2 Quantum Key Generation and Distribution

Alice shares a secret key K_{AB1} with Bob1 and the trusted third-party Trent shares secret keys K_{TA} with Alice, K_{TB1} with Bob1, K_{TC} with Charlie. These secret keys' length is n and they are distributed via quantum key distribution (QKD) protocol [15–17] to ensure security. Then, Trent operates K_{TA}, K_{TB1} and K_{TC} by adding mod 2 and obtains key K.

$$K = K_{TA} \oplus K_{TB1} \oplus K_{TC}.$$

3 Trusted Third-Party E-Payment Protocol

Our e-payment system involves five roles as follows.

(1) Alice: payor;
(2) Bob1: Alice's agent bank;
(3) Charlie: payee;
(4) Bob2: Charlie's agent bank;
(5) Trent: the trusted third-party e-payment platform.

When Alice wants to give payment to Charlie, she will ask Trent to distribute secret keys. Then, she starts to carry through payment. Firstly, after receiving Alice's message, Trent will inform Bob1 to transmit money to himself. At the same time, Bob1 can deduct the corresponding quantity from Alice's account. Secondly, Charlie will verify the validity of message and send message to Trent. Finally, if all participants have no dispute, Trent will transmit these money to Bob2.

The brief procedure of our payment has been illustrated in Fig. 1.

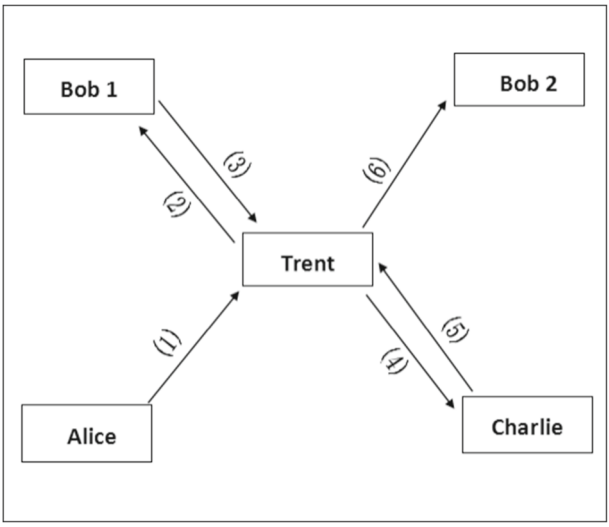

Fig. 1 The model of third-party e-payment

3.1 Initial Phase

Step1: Alice divides her payment information into two parts: $m1$, involving the amount that Alice should pay; $m2 = \{m2(1), m2(2), \cdots, m2(i), \cdots, m2(n)\}(m2(i) \in \{00, 01, 10, 11\})$, meaning compact which is shared between Alice and Charlie before payment. If the length of compact is a odd number, they appoint to add a number 0 at the end of it.

Alice produces quantum sequence $M = \{M(1), \cdots, M(i), \cdots, M(n)\}$ according to message $m2$ as follows.

$$M(i) = \begin{cases} |+X\rangle, & if \quad m2(i) = 00 \\ |-X\rangle, & if \quad m2(i) = 01 \\ |+Y\rangle, & if \quad m2(i) = 10 \\ |-Y\rangle, & if \quad m2(i) = 11 \end{cases}, 1 \le i \le n. \tag{3}$$

Nobody knows this encoded rule expect Alice and Charlie.

Step2: Alice performs unitary operations on her quantum sequence M according to her secret key K_{TA} as follows. If $K_{TA}(i)$ is equal to 0, Alice does nothing on $M(i)$. If $K_{TA}(i)$ is equal to 1, Alice performs Z gate operation on $M(i)$.

$$M1(i) = \begin{cases} IM(i), & if \quad K_{TA}(i) = 0 \\ ZM(i), & if \quad K_{TA}(i) = 1 \end{cases}, 1 \le i \le n. \tag{4}$$

Then she obtains a new quantum sequence $M1$.

Step3: In order to prevent truncation or middle attack, Alice selects t decoy photons from $\{|0\rangle, |1\rangle, |+X\rangle, |-X\rangle\}$ and inserts them randomly into $M1$ to obtain a new quantum sequence $M1'$. Then Alice sends $M1'$ and $E_{K_{AB1}}\{m1\}$ which is encrypted by using the one-time pad with the key K_{AB1} to Trent. Meanwhile, she writes down message of t decoy photons. Afterward, Alice informs Trent of the information including positions of selected qubits and corresponding particle states. With the information from Alice, Trent could determine error rate. If the error rate is more

than the threshold value, he will cancel this payment, or else, he will proceed to the next step.

3.2 Payment Phase

Step1: Trent removes these decoy photons according to information published by Alice and obtains the initial quantum sequence $M1$. Then, Trent encrypts $E_{K_{AB1}}\{m1\}$ with key K_{TB1} and gains $E_{K_{TB1}}\{E_{K_{AB1}}\{m1\}\}$. He also chooses t decoy photons from $\{|0\rangle, |1\rangle, |+X\rangle, |-X\rangle\}$ to get $M1''$ the same as Alice. After that, he sends $E_{K_{TB1}}\{E_{K_{AB1}}\{m1\}\}$ and $M1''$ to Bob1.

Step2: After Bob1 has received Trent's signature requirement, Trent and he adopt the decoy photon checking technique to guarantee the security of transmission. If there is a eavesdropper, they will give up this transmission. Or else, Bob1 will go on and obtain $M1$. Meanwhile, he will decrypt $E_{K_{AB1}}\{m1\}$ and perform unitary operation on $M1$ depending on his key K_{TB1} if he agrees Alice to trade in the third-party platform. Based on (4), if $K_{TB1}(i)$ is equal to 0, Bob1 does nothing on $M1(i)$. If $K_{TB1}(i)$ is equal to 1, Bob1 performs quantum Z gate operation on $M1(i)$ and gains quantum signature $M2$.

Then Bobl creates a unique number $N = \{N_1, N_2, \cdots, N_n\}$ whose length is n. According to N, he inserts $\left[\frac{n}{2}\right]$ additional particles into $M2$.

1) The rule that he generates them as follows (A(i) denotes the ith additional particle).

$$A(i)\begin{cases} |0\rangle, & if \quad N_{2i-1}N_{2i} = 00 \\ |1\rangle, & if \quad N_{2i-1}N_{2i} = 01 \\ |+X\rangle, & if \quad N_{2i-1}N_{2i} = 10 \\ |-X\rangle, & if \quad N_{2i-1}N_{2i} = 11 \end{cases}, 1 \le i \le \left[\frac{n}{2}\right]. \tag{5}$$

2) The positions where these additional particles should insert are determined by the following way.

If $N_{2i-1} = 0\,\left(i = 1, 2\cdots, \left[\frac{n}{2}\right]\right)$, the ith additional particle is inserted in front of $M2(2i)\,\left(i = 1, 2\cdots, \left[\frac{n}{2}\right]\right)$. Otherwise, the additional particle is behind $M2(2i)\,\left(i = 1, 2\cdots, \left[\frac{n}{2}\right]\right)$. After that, he sends $E_{K_{TB1}}\{m1\}$, $E_{K_{TB1}}\{N\}$ and $M2'$ to Trent.

Step3: After Trent has received Bob1's message, he decrypts $E_{K_{TB1}}\{N\}$ and measures these additional particles according to N. Then, he verifies whether the measurement results are consistent with the generation rules and determines whether there exists eavesdropping. If there exists eavesdropping, Trent will inform other participants abort the scheme. Otherwise, he discards these additional particles and obtains $M3$. At the same time, Trent also inserts t decoy photons into $M3$ to detect eavesdropping and get $M3'$. After that, he sends $M3'$ and $K_{TC}\{m1\}$ to Charlie.

Step4: Similarly, after receiving Trent's message $M3'$ and $K_{TC}\{m1\}$, Charlie carries out some operations and obtains $M4$ and $m1$. Then, based on compact $m2$ which is shared with Alice, he measures quantum sequence $M4$ on appropriate bases according to the rule by the step1 in Section 3.1. The measurement results could be wrote as $m2'$. If $m2' = m2$, the signature is valid, otherwise, Charlie will reject it.

Step5: If there is no dispute, Charlie will inform Trent to send message to Bob2, meanwhile Bob2 could receive the proper amount from Trent.

4 An Example: the Trusted Third-Party Payment Scheme

For the sake of clearness, we will give an example to describe our scheme. Assumed the channel is safe and the compact which is shared between Alice and Charlie is wrote as $m2 = 01100011$ (8 qubit), and the shared keys are wrote as $K_{TA} = 0110$, $K_{TB1} = 1100$, $K_{TC} = 0001$ and $K = K_{TA} \oplus K_{TB1} \oplus K_{TC} = 1011$. For simplify, we skip the quantum key distribution process and the transmission process of the payment account $m1$. The main process is showed as follows.

Step1: Following the rule of step 1 and step 2 of Section 3.1, firstly, Alice needs to prepare a four-qubit quantum sequence $M = \{|-X\rangle, |+Y\rangle, |+X\rangle, |-Y\rangle\}$ according to content of compact $m2 = 01100011$. Then, she uses her key $K_{TA} = 0110$ and performs Z gate operations on M to get $M1 = \{|-X\rangle, |-Y\rangle, |-X\rangle, |-Y\rangle\}$. (If $K_{TA(i)} = 0$, she does nothing on $M(i)$, else, she performs Z gate operations.)

Step2: After Bobl has received Alice's message $M1$, he performs Z gate operation on $M1$ and obtains $M2 = \{|+X\rangle, |+Y\rangle, |-X\rangle, |-Y\rangle\}$ according to his key $K_{TB1} = 1100$. The operation process also follows the rule of step 2 of Section 3.1.

Step3: When receiving Bob1's message $M2$, Trent carries out some operations and gains $M3 = \{|-X\rangle, |+Y\rangle, |+X\rangle, |+Y\rangle\}$ according to his key $K = 1011$, as Bob1 does.

Step4: Similarly, Charlie can also gain $M4 = \{|-X\rangle, |+Y\rangle, |+X\rangle, |-Y\rangle\}$. Then, he measures his quantum sequence $M4$ on appropriate bases according to compact $m2$. If $m2(i) = 00$ or $m2(i) = 01$, he selects base $\{|+X\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), |-X\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\}$. Else, he selects base $\{|+Y\rangle = \frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle), |-Y\rangle = \frac{1}{\sqrt{2}}(|0\rangle - i|1\rangle)\}$ if $m2(i) = 10$ or $m2(i) = 11$. Then, he can rebuilt the content of compact $m2' = 01100011$.

The result is showed in Table 1.

5 Scheme Properties and Security Analysis

5.1 Blind Property

In our scheme, Bob1 is blind from the content of compact. Because he neither has encoded rule (3) which is shared between Alice and Charlie nor selects appropriate bases $\{|+Y\rangle, |-Y\rangle\}$ or $\{|+X\rangle, |-X\rangle\}$ to measure quantum sequence. Assumed Bob1 attempts to gain

Table 1 The result of the third-party e-payment

$m2$	01	10	00	11
$\|M\rangle$	$\|-X\rangle$	$\|+Y\rangle$	$\|+X\rangle$	$\|-Y\rangle$
Alice($\|M1\rangle$)	$\|-X\rangle$	$\|-Y\rangle$	$\|-X\rangle$	$\|-Y\rangle$
Bob1($\|M2\rangle$)	$\|+X\rangle$	$\|+Y\rangle$	$\|-X\rangle$	$\|-Y\rangle$
Trent($\|M3\rangle$)	$\|-X\rangle$	$\|+Y\rangle$	$\|+X\rangle$	$\|+Y\rangle$
Charlie($\|M4\rangle$)	$\|-X\rangle$	$\|+Y\rangle$	$\|+X\rangle$	$\|-Y\rangle$
The recuperative information $m2'$	01	10	00	11

the information $m2$, he will choose $\{00, 01, 10, 11\}$ randomly. Then he can get it with the probability $(1/4)^n$ which is negligible if n is large enough. As a result, the agency bank Bob1 can not get content of compact in the process of transaction.

5.2 Unforgeability

The third-party e-payment platform is trusty in our scheme. Those who want to forge would be detected. Obviously, Bob1's signature on compact is generated by the key K_{TB1}. Meanwhile, $M2'$ is composed of $M2$ and some additional particles which are generated according to N. Supposed that internal participant Alice is dishonest and wants to counterfeit the signatory of Bob1 to own his benefit, the only way to finish it is obtaining Bob1's secret key K_{TB1}, however, it is impossible. In addition, they can't forge the signature even if Alice collaborates with Charlie. Because all secret keys are distributed via quantum key distribution (QKD) protocol [15–17] which has proved unconditional security.

What's more, if the external attacker Eve tries to forge Bob1's signature, on the one hand, he needs to elude additional particles' checking, on the other hand, he should know secret key K_{TB1} and M, otherwise, Trent will expose his forgery by step 3 in Section 3.2. Therefore, the forgery of Bob1's signature is impossible for everyone.

5.3 Undeniability

During the phase of signature verifying, Charlie can use his key K_{TC} and initial compact $m2$ to rebuild a new compact $m2'$ if Alice and Bob1 faithfully implements the trade procedure and no eavesdropper exists. If the content of compact is valid, he will accept it and inform Trent to finish payment. Once Charlie attempts to disavow the receipt of signature, Trent can expose him. Similarly, Bob1 can not disavow his signature either.

5.4 Unconditional Security

Firstly, we employ BB84 protocol [15] which is proved to be unconditional security to distribute keys. Secondly, the payment amount is encrypted by one-time pad algorithm [18]. Finally, we adopt the decoy photon checking technique and insert some additional particles to achieve the transmissive security. Therefore our scheme is unconditional security.

6 Conclusion

With a detailed security analysis, we show that the proposed scheme meets all the characteristics of quantum blind signature [19–24]. Furthermore, the proposed scheme can resist internal and external attack by taking advantage of the special encoded rules and quantum key distribution protocol (QKD) [15–17]. In addition, as described in [10–14, 25], most of the previous signatures' operations are complex. However, in our scheme, all participants only need to employ single-particle quantum Z gate operations in the process of payment, which make the scheme more practical and convenient than them.

Acknowledgements 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-Crypto 82, pp. 199–203. Springer, New York (1982)
2. Chaum, D., Heyst, E.: Group Signatures. Advances in Cryptology-Eurocrypt'91. 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. 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)
8. Lysyanskaya, A., Ramzan, Z.: Group Blind Digital Signatures: a Scalable Solution to Electronic Cash. FC'98, LNCS 1465, pp. 184–197. Springer, Berlin (1998)
9. Fan, L., Zhang, K.J., Qin, S.J., et al.: A novel quantum blind signature scheme with four-particle GHZ states. Int. J. Theor. Phys. **55**(2), 1–8 (2015)
10. Wen, X.J., Nie, Z.: An e-payment system based on quantum blind and group signature. Phys. Scr. **82**(6), 5468–5478 (2010)
11. 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)
12. 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)
13. Zhou, R.G., Li, W., Huan, T.T., et al.: An online banking system based on quantum cryptography communication. Int. J. Theor. Phys. **53**(7), 1–14 (2014)
14. Yang, Y.Y., Zhang, J.Z., Xie, S.C.: A third-party e-payment protocol based on quantum group blind signature. Int. J. Theor. Phys. **56**(9), 2981–2989 (2017)
15. Shor, P.W., Preskill, J.: Simple proof of security of the BB84 quantum key distribution protocol. Phys. Rev. Lett. **85**(2), 441–444 (2000)
16. Mayers, D.: Unconditional security in quantum cryptography. J. Assoc.: Comput. Math. **48**(1), 351–406 (2001)
17. Inamon, H., Lutkenhaus, N., Mayers, D.: Unconditional security of practical quantum key distribution. Eur. Phys. J. D. **41**(3), 599–627 (2007)
18. Boykin, P.O., Roychowdhury, V.: Optimal encryption of quantum bits. Phys. Rev. A **67**(4), 645–648 (2003)
19. 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**(12), 5216–5224 (2016)
20. 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)
21. Zeng, C., Zhang, J.Z., Xie, S.C.: A quantum proxy blind signature based on genuine five-qubit entangled state. Int. J. Theor. Phys. **56**(6), 1762–1770 (2017)
22. Harn, L.: Cryptanalysis of the blind signature based on the discrete logarithm. Electron. Lett. **31**(14), 1136–1137 (1995)
23. Xu, R., Huang, L., Yang, W., et al.: Quantum group blind signature scheme without entanglement. Opt. Commun. **284**(14), 3654–3658 (2011)
24. Xu, G.B., Wen, Q.Y., Gao, F., et al.: Novel multiparty quantum key agreement protocol with GHZ states. Quantum. Inf. Process. **13**(12), 2587–2594 (2014)
25. Shao, A.X., Zhang, J.Z., Xie, S.C.: An E-payment protocol based on quantum multi-proxy blind signature. Int. J. Theor. Phys. **56**(4), 1–8 (2017)