Int J Theor Phys
DOI 10.1007/s10773-017-3464-x

A Third-Party E-Payment Protocol Based on Quantum Group Blind Signature

Jian-Zhong Zhang[1] · Yuan-Yuan Yang[1] · Shu-Cui Xie[2]

Received: 26 April 2017 / Accepted: 26 June 2017

Abstract A third-party E-payment protocol based on quantum group blind signature is proposed in this paper. 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 can not provide. To achieve that, quantum key distribution, one-time pad and quantum group blind signature are adopted in our scheme. Furthermore, if there were a dispute, the manager Trent can identify who tells a lie.

Keywords Third-party E-payment · Quantum group blind signature · Four-qubit entangled state · Unconditional security

1 Introduction

Nowadays, with the rapid development of internet, E-commerce is favored by the majority of individuals for its convenience and speeding. Hence, choosing an appropriate model of payment is very important for E-commerce transaction. E-cash has the properties of anonymity and off-line transferability. Since Chaum first proposed the concept of E-cash [1], many researchers turned to research E-cash system and proposed a number of

✉ Jian-Zhong Zhang
1416655910@qq.com

Yuan-Yuan Yang
1191617739@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

Published online: 04 July 2017

E-cash payment schemes [2–6]. The current E-payment system is mainly based on group and blind signature to design.

To ensure scheme's unconditional security, quantum signature was introduced by combining classical cryptography and quantum theory. Recently, the application of quantum signature in E-payment also attracted some attention. An E-payment system based on quantum group and blind signature was proposed by Wen and Nie, employing two-third trusted party instead one to enhance the system's robustness [7]. In succession, Wen et al. proposed an inter-bank E-payment protocol based on quantum proxy blind signature [8]. However, Cai et al. [9] pointed that the dishonest merchant can succeed to change the purchase information of the customer in this protocol. Recently, Chou et al. [10] proposed an efficient novel online shopping mechanism based on quantum communication. However, Huang et al. [11] pointed that the controller is able to eavesdrop the secret information of the sender. Zhou et al. proposed an online banking system based on quantum cryptography communication [12].

In this paper, we propose a third-party E-payment protocol based on quantum group blind signature. Quantum key distribution and one-time pad are adopted in our scheme in order to guarantee unconditional security. This is the first time to propose a third-party quantum E-payment scheme, which not only supports the E-payment among different banks but also enhances the transaction credibility and improves the success of business rate. The property of group blind signature could protect the anonymity of E-payment systems, while the quantum signature could guarantee unconditional security. Our scheme only need Bell-measurement, it can be easily implemented with the current experimental conditions.

2 Preliminary Theory

2.1 Group Blind Signature

Group signature [13] allows a member to sign a message on behalf of the group and no one knows who signed it except group manager. As for blind signature [14, 15], the message owner could get the authentic signature for his own message, but not reveal the specific content of the message. Both the property of group and blind signature are required for application and security concern in E-payment systems, so group blind signature was proposed.

Different from classical signature scheme, our quantum group 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 Charlie share a Bell-state

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

where

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

Due to the entanglement property of EPR pairs, after Alice measures particle A, particle C will collapse to the same state as particle A. Thus, if Alice and Charlie choose the same base $B_z = \{|0\rangle, |1\rangle\}$ or $B_x = \{|+\rangle, |-\rangle\}$ to measure their particles respectively, they will get

the same results. For example, if both Alice and Charlie choose the base B_x and Alice gets $|+\rangle$, then Charlie's measurement result must be $|+\rangle$. However, after Alice's measurement, if Charlie chooses a different base from Alice, Charlie will get a random result.

2.2 Controlled Quantum Teleportation

The quantum group blind signature is based on controlled quantum teleportation. In this section, we will introduce the controlled teleportation using four-qubit entangled state [16] as quantum channel. It is given by

$$|\xi\rangle_{1234} = \frac{1}{2}(|0000\rangle + |0110\rangle + |1001\rangle - |1111\rangle)_{1234}. \tag{3}$$

Trent owns particles (3,4), particle 1 and particle 2 belong to Bob1 and Charlie, respectively.

Suppose that the quantum state of particle M carrying the message by Bob1 is the following form

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

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

The combining state $|\Psi\rangle_{M1234}$ of the whole system be 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 are given in the following.

1) Bob1 performs a Bell-state measurement on his particles (M,1), and sends his measurement outcome to Trent via secure quantum channel. The Bell-state measurement can collapse the state of particles (2,3,4) into one of the following four states

$$\begin{aligned}\langle\phi^{\pm}_{M1}|\Psi\rangle_{M1234} &= \frac{1}{2}(\alpha|000\rangle + \alpha|110\rangle \pm \beta|001\rangle \mp \beta|111\rangle)_{234},\\ \langle\psi^{\pm}_{M1}|\Psi\rangle_{M1234} &= \frac{1}{2}(\alpha|001\rangle - \alpha|111\rangle \pm \beta|000\rangle \pm \beta|110\rangle)_{234}.\end{aligned} \tag{6}$$

2) Trent performs a Bell-state measurement on his particles (3,4). Suppose that Bob1's measurement result is $|\phi^+\rangle_{M1}$, the Bell-state measurement on Trent's particles (3,4) will collapse the state of particle 2 into one of the following four states

$$\begin{aligned}\langle\phi^{\pm}_{34}|\phi^+_{M1}|\Psi\rangle_{M1234} &= \frac{1}{\sqrt{2}}(\alpha|0\rangle \mp \beta|1\rangle)_2,\\ \langle\psi^{\pm}_{34}|\phi^+_{M1}|\Psi\rangle_{M1234} &= \frac{1}{\sqrt{2}}(\beta|0\rangle \pm \alpha|1\rangle)_2.\end{aligned} \tag{7}$$

Trent sends his measurement result to Charlie through secure quantum channel.

4) According to Bob1's and Trent's measurement outcomes, Charlie imposes an appropriate unitary operation on particle 2, so that he can reconstruct the original state $|\psi\rangle_M$. The unitary operations are pauli operators ($I, \sigma_z, \sigma_x, i\sigma_y$)

$$I = \begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}, \sigma_z = \begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}, \sigma_x = \begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}, i\sigma_y = \begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix}.$$

Assume that Bob1's and Trent's measurement results are $|\phi^+\rangle_{M1}$ and $|\phi^+\rangle_{34}$, respectively, Charlie's operation on particle 2 is σ_z. For other cases, the relationship between Bob1's, Trent's measurement outcomes and Charlie's operation are listed in Table 1.

3 The Third-party Quantum E-payment Protocol

3.1 Protocol Description

Suppose that Trent is a group manager who is the trusted third-party, both Alice(customer) and Charlie(merchant) register as members of the group. Bob1 is Alice's agent bank, while Bob2 is Charlie's agent bank. Alice trades with Charlie in the third-party payment platform. In the process of trading, banks can not know the content of transactions, that is, the confidentiality of the trading are ensured. The receiver Charlie verifies the signature's validation without knowing who gives the message, that is, the customer's anonymity is protected. If there were a dispute, the group manager Trent can identify who tells a lie.

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

3.2 Initial Phase

Step1: Alice, Bob1 and Bob2 share secret key K_{AT}, K_{B_1T} and K_{B_2T} with Trent, respectively. All these keys are distributed via QKD protocols [17–19], which have been proved unconditional security.

Step2: Trent generates n EPR pairs

$$|\psi_i\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{A_iT_i}, i = 1, 2, \cdots, n. \tag{8}$$

In each EPR pair, Trent sends particle A_i to Alice while leaving T_i for himself.

Table 1 The relationship between Bob1's, Trent's measurement outcomes and Charlie's operation

Bob1's measurement outcome	Trent's measurement outcome	Charlie's operation
$\|\phi^+\rangle_{M1}$	$\|\phi^+\rangle_{34}$	$(\sigma_z)_2$
$\|\phi^+\rangle_{M1}$	$\|\phi^-\rangle_{34}$	I_2
$\|\phi^+\rangle_{M1}$	$\|\psi^+\rangle_{34}$	$(\sigma_x)_2$
$\|\phi^+\rangle_{M1}$	$\|\psi^-\rangle_{34}$	$(i\sigma_y)_2$
$\|\phi^-\rangle_{M1}$	$\|\phi^+\rangle_{34}$	I_2
$\|\phi^-\rangle_{M1}$	$\|\phi^-\rangle_{34}$	$(\sigma_z)_2$
$\|\phi^-\rangle_{M1}$	$\|\psi^+\rangle_{34}$	$(i\sigma_y)_2$
$\|\phi^-\rangle_{M1}$	$\|\psi^-\rangle_{34}$	$(\sigma_x)_2$
$\|\psi^+\rangle_{M1}$	$\|\phi^+\rangle_{34}$	$(i\sigma_y)_2$
$\|\psi^+\rangle_{M1}$	$\|\phi^-\rangle_{34}$	$(\sigma_x)_2$
$\|\psi^+\rangle_{M1}$	$\|\psi^+\rangle_{34}$	I_2
$\|\psi^+\rangle_{M1}$	$\|\psi^-\rangle_{34}$	$(\sigma_z)_2$
$\|\psi^-\rangle_{M1}$	$\|\phi^+\rangle_{34}$	$(\sigma_x)_2$
$\|\psi^-\rangle_{M1}$	$\|\phi^-\rangle_{34}$	$(i\sigma_y)_2$
$\|\psi^-\rangle_{M1}$	$\|\psi^+\rangle_{34}$	$(\sigma_z)_2$
$\|\psi^-\rangle_{M1}$	$\|\psi^-\rangle_{34}$	I_2

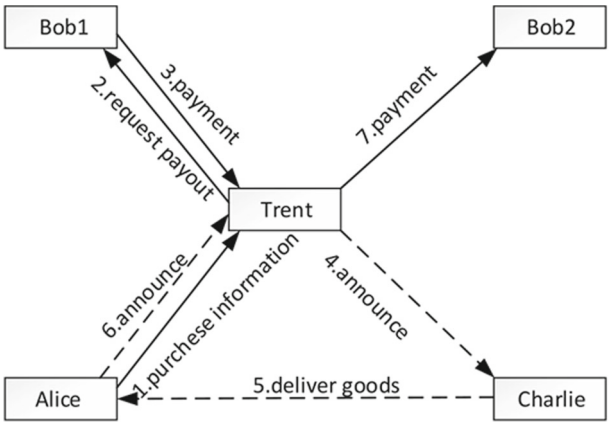

Fig. 1 The third-party quantum E-payment protocol

Step3: Charlie produces $t + n$ entangled four-qubit states as shown in (3) and distributes the particles (3,4) to Trent, the particle 1 to Bob1, and he holds particle 2. To ensure the channel is secure, they have to detect channel. Firstly, Trent randomly chooses t four-qubit entangled states and records their positions. Then, he performs two particles measurement on particles (3,4) basis in $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$. Trent announces measurement results and positions. Secondly, Bob1 and Charlie measure the corresponding particles basis in $\{|0\rangle, |1\rangle\}$. Then, Bob1 and Charlie announce their measurement results. If measurement results satisfy the correlation in Table 2, the safe channel sets up successfully.

3.3 Initialization Protocol

Step1: Alice divides her purchase information into two parts: $M1$, involving the amount that Alice ought to pay; $M2 = \{M2(1), M2(2), \cdots, M2(i), \cdots, M2(n)\}(M2(i) \in \{0, 1\})$, including Alice's purchase information which can not be seen by others. So Alice needs to blind the part $M2$.

Alice measures her particle sequence according to message $M2$. If $M2(i) = 0$, she measures A_i on the base $B_z = \{|0\rangle, |1\rangle\}$, if $M2(i) = 1$, she chooses the base $B_x = \{|+\rangle, |-\rangle\}$. Alice records the measurement results as M', $M' = \{M'(1), M'(2), \cdots, M'(i) \cdots, M'(n)\}(M'(i) \in \{|0\rangle, |1\rangle, |+\rangle, |-\rangle\})$. Here M' could be encoded into two classical bits M'' as following

$$|0\rangle \to 00, |1\rangle \to 01, |+\rangle \to 10, |-\rangle \to 11. \tag{9}$$

Therefore, the message $M2$ (n-bit) has been blinded into M'' ($2n$-bit).

Table 2 The measurement relationship between Bob1's, Trent's, and Charlie's results

Bob1's result	Trent's result	Charlie's result
$\|0\rangle_1$	$\|00\rangle_{34}$	$\|0\rangle_2$
$\|0\rangle_1$	$\|10\rangle_{34}$	$\|1\rangle_2$
$\|1\rangle_1$	$\|01\rangle_{34}$	$\|0\rangle_2$
$\|1\rangle_1$	$\|11\rangle_{34}$	$\|1\rangle_2$

Step2: Alice encrypts $M1$, M'' with the secret key K_{AT} to get the message $S_{AT} = E_{K_{AT}}\{M1, M''\}$. We adopt one-time pad [20] as the encryption algorithm to guarantee the unconditional security. Alice sends the message S_{AT} to Trent through QSDC protocols [21–23].

3.4 Trading Purchase Phase

Step1: After Trent received the message S_{AT}, he decrypts it with the secret key K_{AT} to get the message $M1$, M''. Trent encrypts T_i and $M1$ with the secret key K_{B_1T} to get the message $S_{B_1T} = E_{K_{B_1T}}\{T_i, M1\}$. Trent sends S_{B_1T} to Bob1.

Step2: After Bob1 received Trent's signature requirement, he decrypts it with the secret key K_{B_1T} to get the message T_i and $M1$. If he agrees Alice to trade in the third-party platform, he will help Trent finish the controlled teleportation. Bob1 performs the Bell-state measurement on particles (T_i,1) and records the results as $\beta_A = \{\beta(i)_{T_i1}, i = 1, 2, \cdots, n\}(\beta(i)_{T_i1} \in \{|\phi^{\pm}\rangle, |\psi^{\pm}\rangle\})$. Then Bob1 sends $S_A = E_{K_{B_1T}}\{\beta_A\}$ to Trent.

Step3: After Trent received the message S_A, he decrypts it with the secret key K_{B_1T} to get the message β_A. Trent performs a Bell-state measurement on particles (3,4) and records the results as $\beta_B = \{\beta(i)_{34}, i = 1, 2, \cdots, n\}(\beta(i)_{34} \in \{|\phi^{\pm}\rangle, |\psi^{\pm}\rangle\})$. Then Trent announces the signature (M'', β_A, β_B).

3.5 Trading Payment Phase

Step1: According to β_A, β_B from Trent, Charlie performs a corresponding unitary operation on particle 2 to successfully replicate the original unknown quantum state information.

Step2: Then, Charlie measures particle 2 on appropriate base according to the rule by the step 1 in § 3.3. The measuring results could be encoded into two classical bits according to (9), the encoded result is wrote as d.

Step3: If $d = M''$, Charlie accepts the message and the signatures. Then Charlie unblinds M'', namely, the odd number of blind message M'' is the original message $M2$, Charlie confirms the signature $(M2, \beta_A, \beta_B)$.

Step4: If there is no dispute, Charlie should send the corresponding goods to Alice. After Alice receives goods from Charlie, he will inform Trent to pay for Bob2.

Step5: Trent encrypts $M1$ with the secret key K_{B_2T} to get the message $S_{B_2T} = E_{K_{B_2T}}\{M1\}$. Trent sends the message S_{B_2T} to Bob2, meanwhile Bob2 could receive the proper amount from Trent.

4 Scheme Properties and Security Analysis

4.1 Group Property

If a person wants to join a group, he needs to send an application to the group manager Trent. Trent will examine the identify of him, so every member in the group must be eligible. In the scheme, the member of group has to register at group manager Trent, so that others can not send the message instead of Alice. Alice can not communicate with others except Trent, so anyone else can not know which member sent the message. Charlie could verify whether

the message comes from the group without knowing which individual in the group sent the message. In a word, the customer's anonymous is protected.

4.2 Blind Property

The message $M2$ has been blinded into M' by the owner Alice, where every $M'(i) \in \{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$. If Bob1 attempts to gain the states M', the only way is to perform measurement. However, the n states M' are nonorthogonal, so Bob1 can not distinguish the message M'. If Bob1 chooses basis $\{|0\rangle, |1\rangle\}$ or $\{|+\rangle, |-\rangle\}$ randomly to measure M', he can obtain it with the probability of $\frac{1}{2^n}$ which is negligible if n is large enough. So Bob1 can not get the message $M2$. Meanwhile, Bob2 also can get nothing about $M2$. As a result, in the whole transaction, the banks Bob1 and Bob2 are kept blind for the content of message $M2$. In addition, Charlie could verify and accept the message.

4.3 Impossibility of Denial

Firstly, we show that the banks Bob1 and Bob2 can not disavow their message. In our scheme, the group manager Trent is trusty. According to step 3 in § 3.4, Trent decrypts message S_A with key K_{B_1T} can get Bob1's signature β_A, while according to step 5 in § 3.5, group manager Trent sends the message S_{B_2T} to Bob1. All keys are distributed via QKD protocols, which have been proved unconditionally secure and all message are sent through the secure quantum channel. Hence, Bob1 can not deny that he indeed have signed the signature and Bob2 can not deny he has received the message and money.

Secondly, we show that it is impossible for Trent and Charlie to disavow their message. Trent announces the signatures by step 3 in § 3.4. Moreover, the process of the verifying indicates Charlie has received the signatures and message. Therefore Trent can not deny that he has signed the message and Charlie can not deny he has received the signatures.

4.4 Impossibility of Forgery

Firstly, we show that it is impossible for the dishonest insider to forge Bob1's or Trent's signature. Suppose that the merchant Charlie is dishonest and attempts to forge Bob1's and Trent's signature. If this happens, he can not pass the verification by step 3 in § 3.5. The only way to forge signature is to get the information about K_{B_1T} or K_{B_2T}, however it is impossible. Otherwise, he can not forge the message which is encrypted by secret key K_{AT}. Similarity, everyone in the scheme can not forge other's signature. In a word, the dishonest insider can not forge the signatures.

Secondly, we discuss the forgery made by the outside attacker Eve. Assume that the outsider Eve intend to forge Bob1's signature β_A, as Eve has not the secret key K_{B_1T}, she can not send secret message S_A to Trent. Even if Eve gets K_{B_1T}, he only can get the valid β_A with the probability of $\frac{1}{2^n}$ which is negligible if n is large enough. If Eve attempts to eavesdrop the quantum channel, he will be detected by step 3 in § 3.2. In a word, Bob1's signature can not be forged. Similarity, the Trent's signature can not be forged either.

4.5 Traceability Property

Only the group manager Trent knows that who sent the message, meanwhile, he records all the signatures and message. If there exists a dispute, Trent can reveal the identify of the sender and indicate who tells a lie.

4.6 Unconditional Security

Our scheme ensures security by the following three aspects. Firstly, the protocol BB84 is adopted for quantum key distribution; Secondly, we employ one-time pad to encrypt the message and signatures; Finally, 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 security.

5 Conclusion

Combined with the actual demand for third-party E-payment, in this paper, we propose a third-party quantum E-payment protocol based on quantum group blind signature. Compared with previous works in [7–10, 24], our protocol can blind the customer's payment message into the blinded message, which can protect the payment messages. Furthermore, our protocol can protect customer's anonymity. Meanwhile, our scheme is based on four-qubit state which achieves a higher security. As the key techniques of our protocol only rely on the Bell-measurement, which can make the protocol reliable and practical.

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. 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-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. Wen, X.J., Nie, Z.: An E-payment system based on quantum blind and group signature. Phys. Scr. **82**(6), 5468–5478 (2010)
8. 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)
9. 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)
10. Chou, Y.H., Lin, F.J., Zeng, G.H.: An efficient novel online shopping mechanism based on quantum communication. Electron. Commer. Res. **14**, 349–367 (2014)
11. Huang, W., Yang, Y.H., Jia, H.Y.: Cryptanlysis and improvement of a quantum communication-based online shopping mechanism. Quantum. Inf. Process. **14**, 2211–2225 (2015)
12. Zhou, R.G., Wei, L., et al.: An online banking system based on quntum cryptography communication. Int. J. Thero. Phys. **53**, 2177–2190 (2014)
13. Xu, R., Huang, L., et al.: Quantum group blind signature scheme without entangled. Opt. Commun. **284**, 3654–3658 (2011)
14. Shao, A.X., Zhang, J.Z., Xie, S.C.: A quantum multi-proxy multi-blind-signture scheme based on genuine six-qubit entangled state. Int. J. Theor. Phys. **55**, 5216–5224 (2016)

15. 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**, 809–816 (2015)
16. Li, R.: Controlled dense coding with four-qubit entangled state. Int. J. Theor. Phys. **51**, 3208–3212 (2012)
17. Shor, P.W., Preskill, J.: Simple proof of security of the BB84 quantum key distribution protocol. Phys. Rev. Lett. **85**(2), 441–444 (2000)
18. Mayers, D.: Unconditional security in quantum cryptography. J. Assoc.: Comput. Math. **48**(1), 351–406 (2001)
19. Inamon, H., Lutkenhaus, N., Mayers, D.: Unconditional security of practical quantum key distribution. Eur. Phys. J. D. **41**(3), 599–627 (2007)
20. Guo, W., Zhang, J.Z., Li, Y.P., et al.: Multi-proxy strong blind quantum signature scheme. Int. J. Thero. Phys. **55**(8), 3524–3536 (2016)
21. Deng, F.G., Long, G.L., et al.: Two-step quantum direct communication using the Einstein-podolsky-Rosen pair block. Phys. Rev. A **68**, 042317 (2003)
22. Deng, F.G., Long, G.L.: Secure direct communication with a quantum one-time pad. Phys. Rev. A **69**, 052319 (2004)
23. Cai, Q.Y., Li, B.W.: Deterministic secure communication without using entanglement. Chin. Lett **21**, 601–603 (2004)
24. Shao, A.X., Zhang, J.Z., Xie, S.C.: An E-payment protocol based on quantum multi-proxy blind signature. Int. J. Thero. Phys. **56**, 1241–1248 (2017)