SCIENCE CHINA
Physics, Mechanics & Astronomy

• Article •

September 2013 Vol. 56 No. 9: 1636–1641
doi: 10.1007/s11433-013-5170-x

A blind quantum signature protocol using the GHZ states

WANG MingMing[1], CHEN XiuBo[1,2*] & YANG YiXian[1]

[1] *Information Security Center, State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing 100876, China;*
[2] *State Key Laboratory of Information Security (Institute of Information Engineering, Chinese Academy of Sciences), Beijing 100093, China*

Received May 16, 2012; accepted June 28, 2012; published online July 22, 2013

Recently, some blind quantum signature (BQS) protocols have been proposed. But the previous schemes have security and efficiency problems. Based on the entangled Greenberger-Horne-Zeilinger (GHZ) states, a new weak BQS protocol is proposed. Compared with some existing schemes, our protocol has 100% efficiency. Besides, the protocol is simple and easy to implement. The security of the protocol is guaranteed by the correlation of the GHZ particles held by each participant. In our protocol, the signatory is kept blind from the content of the message. According to the security analysis, the signatory cannot disavowal his/her signature while the signature cannot be forged by others.

blind quantum signature, GHZ state, efficiency, security

PACS number(s): 03.67.Dd, 03.65.Ud, 03.67.Hk

Citation: Wang M M, Chen X B, Yang Y X. A blind quantum signature protocol using the GHZ states. Sci China-Phys Mech Astron, 2013, 56: 1636–1641, doi: 10.1007/s11433-013-5170-x

1 Introduction

Digital signature, which was independently introduced by Diffie and Hellman [1] and Merkle [2], provides a means for an entity to bind its identity to a piece of information. As a primitive of cryptograph, digital signature plays a fundamental role in authentication, authorization and non-repudiation. However, the security of conventional signature is based on some unproven assumptions of computational complexity, like hardness of factoring large integers or solving discrete logarithms. With the development of quantum computation, especially Shor's algorithm for factoring large integers [3], conventional signature schemes face serious security challenges.

In the past decades, quantum cryptography has attracted much attention and applications like quantum key distribution (QKD) [4–6], quantum secure direct communication (QSDC) [7–10] and quantum secret sharing (QSS) [11–13] have been developed. The striking properties of quantum mechanics can also be applied to provide unconditionally secure digital signature. Gottesman and Chuang [14] proposed the first quantum signature scheme based on quantum one-way functions in 2001. After that, many applications have been studied. Zeng et al. [15–17] proposed an arbitrated quantum signature (AQS) scheme by using GHZ states and quantum one-time pad. Li et al. [18] simplified the scheme by using Bell states and Zou and Qiu [19] further improved the protocol without utilizing entangled states. However, Gao et al. [20] analyzed the security of the AQS protocols and pointed out that those AQS protocols are insecure. In 2004, Lee et al. [21] presented two quantum signature schemes with message recovery. Furthermore, Yang et al. [22] proposed an arbitrated quantum signature protocol with an untrusted arbitrator.

*Corresponding author (email: flyover100@163.com)

The blind signature is a specific type of digital signature where the content of a message is disguised to the signatory for privacy protection before it is signed [23]. Applications of blind signature include E-cash system [23] and E-voting system [24], etc. Usually, there are two types of blind signature: weak blind and strong blind. A weak blind signature scheme has the ability to trace some illegal behaviors of participants. For example, in the E-cash system, a weak blind signature can enable the bank to trace the misuse of the E-cash. While a strong blind signature scheme has the feature of untraceability, which is suitable for anonymous voting where a voter does not want to be traced by anyone. Recently, some quantum protocols of blind signature have been proposed. In 2009, Wen et al. [25] presented the first weak BQS scheme based on EPR pairs and one-time pad. However, Naseri [26] has shown that the scheme in its original form does not complete the task of a blind signature fairly. Soon after that, Su et al. [27] also proposed a BQS scheme based on Two-State Vector Formalism (TSVF) and their scheme has 100% efficiency, which is different from the scheme of Wen et al. [25]. But Yang et al. [28] pointed out some possible attacks against Su et al. [27] BQS scheme. In 2011, Xu et al. [29] proposed a quantum group blind signature scheme using single-qubits. In their scheme, anonymous communication technology is used to provide anonymity for voters, and a hash function is used to blind the message. Very recently, Yin et al. [30] proposed a BQS scheme with χ-type entangled states.

Following some ideas of refs. [25,27,29,30], we propose a new and efficient weak BQS scheme utilizing the GHZ states as message carriers. Compared with previous BQS protocols, the proposed protocol is more efficient, simpler and easier to implement. The security of the protocol is guaranteed by the correlation of the entanglements and we will show that the protocol is secure in details.

The rest of this paper is organized as follows. In sect. 2, we give some preliminaries related to the protocol. In sect. 3, we present the blind signature scheme. The security of the protocol is analyzed in sect. 4. And we conclude the paper in sect. 5.

2 Preliminaries

The entanglement used in the blind signature protocol is the three-partite GHZ state which has the following form

$$|\phi\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)_{123}. \tag{1}$$

And two well-known measurement bases X and Y are given for security check where their eigenstates are

$$|x_{\pm}\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle), \quad |y_{\pm}\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm \mathrm{i}|1\rangle). \tag{2}$$

Suppose a GHZ triplet is shared among three parties Alice, Bob and Charlie. Each of them has one particle of the GHZ state and chooses to measure their particle in the X basis or the Y basis randomly. As is pointed out by Hillery et al. in ref. [11], if two parties use the same basis, then the GHZ qubit held by the third party becomes an eigenstate of the Pauli X operator; otherwise, it is an eigenstate of the Y operator, which can also be seen in the following equation

$$\begin{aligned}
|\phi\rangle &= \frac{1}{2}\,(\,|x_+\rangle|x_+\rangle|x_+\rangle + |x_+\rangle|x_-\rangle|x_-\rangle \\
&\quad + |x_-\rangle|x_+\rangle|x_-\rangle + |x_-\rangle|x_-\rangle|x_+\rangle\,)_{123} \\
&= \frac{1}{2}\,(\,|x_+\rangle|y_+\rangle|y_-\rangle + |x_+\rangle|y_-\rangle|y_+\rangle \\
&\quad + |x_-\rangle|y_+\rangle|y_+\rangle + |x_-\rangle|y_-\rangle|y_-\rangle\,)_{123} \\
&= \frac{1}{2}\,(\,|y_+\rangle|x_+\rangle|y_-\rangle + |y_+\rangle|x_-\rangle|y_+\rangle \\
&\quad + |y_-\rangle|x_+\rangle|y_+\rangle + |y_-\rangle|x_-\rangle|y_-\rangle\,)_{123} \\
&= \frac{1}{2}\,(\,|y_+\rangle|y_+\rangle|x_-\rangle + |y_+\rangle|y_-\rangle|x_+\rangle \\
&\quad + |y_-\rangle|y_+\rangle|x_+\rangle + |y_-\rangle|y_-\rangle|x_-\rangle\,)_{123}\,.
\end{aligned} \tag{3}$$

3 Quantum blind signature protocol

3.1 Security requirements

Three participants are involved in the weak blind signature scheme, the message owner, the signatory and the verifier. In general, there are some basic security requirements for a weak blind signature protocol.

(i) No forgery. Nobody can counterfeit the valid signature except for the signatory.

(Ii) No disavowal of original. The signatory who has signed a message cannot deny having signed it at a later time.

(iii) Blindness. The signatory cannot know the content of the message he/she has signed.

(iv) Traceability. Once a disagreement happens, the signatory is able to trace the message owner.

3.2 Our BQS protocol

In our protocol, three characters are defined as follows.

Alice: Alice is the message owner who wants her message m to be signed while keeping the content secret.

Bob: Bob is the signatory who should sign the blind message without knowing it.

Charlie: Charlie is the verifier who can test whether the signature is legal. Similar to refs. [27,29], Charlie is trusted.

The signed message is $m = \{m_1, m_2, \ldots, m_i, \ldots, m_n\}$ where $m_i \in \{0, 1\}$ with $i \in \{1, 2, \ldots, n\}$. Our scheme can be described as follows.

Step 1. Initial phase

(a) Alice and Charlie share a secret key K_{AC} which can be generated by performing the QKD protocol [4].

(b) Similarly, Bob and Charlie share a secret key K_{BC}.

Step 2. Signing phase

(a) Charlie prepares a tri-qubit sequence where each tri-qubit is in the state $|\phi\rangle$. The $(n+l)$-length sequence is denoted as

$$S = \{P_1(1,2,3), P_2(1,2,3), \ldots, P_{n+l}(1,2,3)\}, \quad (4)$$

where the subscript labels the order of entangled state in the sequence. Charlie divides the sequence into three subgroups

$$S_i = \{P_1(i), P_2(i), \ldots, P_{n+l}(i)\}, \quad (5)$$

with $i = 1, 2, 3$. Then Charlie sends S_1 and S_2 to Alice and Bob, while he keeps S_3.

(b) After receiving the sequence, Alice and Bob return the number of received particles to Charlie. If the number is $n+l$, Charlie goes to the next step; or else, Charlie terminates the protocol.

(c) Charlie randomly chooses a subset with length l in S_3 for eavesdropping check. Firstly, Charlie publishes the positions of these chosen sampling particles. Then Alice and Bob measure the corresponding particles in S_1 and S_2 in the X basis or the Y basis randomly. After that, Alice and Bob declare their measurement outcomes to Charlie (The measurement bases are included in the outcomes). Here, Alice's and Bob's declaring order should also be random for each position. For example, Alice declares firstly in one position and then she declares secondly in another position. According to Alice's and Bob's measurement bases, Charlie chooses the right bases to measure the remaining sample particles in S_3. That is, if Alice and Bob have chosen the same basis in one position, Charlie then chooses the X basis; otherwise, he chooses the Y basis. Here Charlie can determine whether the error rate is normal. When the error exceeds a certain threshold, the protocol should be aborted. Otherwise, continue to next step.

(d) After getting rid of the sampling particles, Alice measures the remaining n particles in S_1 according to the message m. If $m_i = 0$, she measures $P_i(1)$ in the X basis. Otherwise, she measures in the Y basis. The measurement results will be in $\{|x_+\rangle, |x_-\rangle, |y_+\rangle, |y_-\rangle\}$, which are denoted as 2 cbits 00, 01, 10 and 11, respectively. Alice records her measurement outcomes as m'_i where $m'_i \in \{00, 01, 10, 11\}$ with $i \in \{1, 2, \ldots, n\}$. Then she encrypts m' with one-time pad and K_{AC} and gets the cipertext $M = E_{K_{AC}}(m')$.

(e) Bob measures the remaining particles $P_i(2)$ in S_2 and each measuring basis is randomly selected from the X basis and the Y basis. Similarly, the measurement results are recorded as b where $b_i \in \{00, 01, 10, 11\}$ with $i \in \{1, 2, \ldots, n\}$. Then he encrypts b with one-time pad and K_{BC} and gets the signature $Sig = E_{K_{BC}}(b)$.

Step 3. Verification phase

(a) Alice sends M to Charlie, then Charlie decrypts M and gets m'. Here, Charlie also gets the message m since m is contained in m'. For instance, if $m' = 00011100$, then $m = 0010$.

(b) Bob sends the signature Sig to Charlie and Charlie can decrypt Sig to get Bob's measurement results b.

(c) Charlie selects the right measurement bases to measure the remaining particles $P_i(3)$ in S_3, i.e. he will choose the X basis if Alice and Bob have chosen the same basis in the corresponding position, while he will choose the Y basis if Alice's and Bob's choices are different. Similarly, Charlie's measurement results are recorded as c where $c_i \in \{00, 01, 10, 11\}$ with $i \in \{1, 2, \ldots, n\}$.

(d) Charlie accepts Sig as the valid blind signature for message m if three parties' measurement outcomes (m', b, c) satisfy the validation rules in Table 1 for all of the n bits. Otherwise, he rejects it. For instance, if $m'_i = 00$ ($|x_+\rangle$), $b_i = 00$ ($|x_+\rangle$), then the valid c_i must be 00 ($|x_+\rangle$).

4 Security analysis

In the following, we will show that our blind signature protocol is secure against both the outside attacker and dishonest participants. First of all, the security of the two shared keys K_{AC} and K_{BC} is guaranteed by the unconditionally secure QKD protocol. It means that the outside attacker Eve and the dishonest participant Alice cannot get K_{BC}, while Eve and Bob cannot get K_{AC}.

Secondly, the qubit sequences S_1 and S_2 are transmitted from Charlie to Alice and Bob in Step 2(a). If an attacker can successfully intercept the signatory's particles in S_2 without introducing any error, then he/she has the chance to produce a fake signature. To ensure the security, Charlie needs to check the qubits transmission procedure in Step 2(c). If Eve or a dishonest participant tries to perform some attacks during the qubits transmission, like the attack and the ancilla attack, she will be detected with nonzero probability. Let us take the intercept-measure-resend attack performed by Eve into consideration firstly. Suppose that Eve has intercepted sequences S_1 and S_2 in Step 2(a). Since she has no idea of Alice's and

Table 1 Validation rules of our blind signature protocol

Alice/Bob	$b_i = 00$	$b_i = 01$	$b_i = 10$	$b_i = 11$
$m'_i = 00$	$c_i = 00$	$c_i = 01$	$c_i = 11$	$c_i = 10$
$m'_i = 01$	$c_i = 01$	$c_i = 00$	$c_i = 10$	$c_i = 11$
$m'_i = 10$	$c_i = 11$	$c_i = 10$	$c_i = 01$	$c_i = 00$
$m'_i = 11$	$c_i = 10$	$c_i = 11$	$c_i = 00$	$c_i = 01$

Bob's measurement bases, if Eve uses randomly the X basis or the Y basis to measure the two particles that Charlie sends to Alice and Bob, she will have 3/4 probability to choose the wrong basis. For each of these wrong measuring bases that Eve has chosen, there is 50% probability to make error in public discussion in Step 2(c). So in each of the l checking positions, the error rate introduced by Eve is $p_e = \frac{3}{4} \times \frac{1}{2} = \frac{3}{8}$. On the other hand, if Eve has intercepted only one sequence, e.g. Bob's sequence S_2, and she still chooses the X basis or the Y basis randomly to measure the particles, then Eve has a probability of 1/2 to choose the wrong basis and a probability of 50% to cause an error in the wrong basis. In this case, Eve's attack will be detected with probability $p_e = \frac{1}{2} \times \frac{1}{2} = \frac{1}{4}$ in each of the checking positions.

Another possible attack performed by Eve will be the ancilla attack, where Eve entangles an ancilla with transmitted particles of the GHZ state and then measures the ancilla after getting published information. For one thing, Alice and Bob only perform measurement, no unitary operation is involved. And there is not secret information in Alice's and Bob's published messages. For another thing, as is discussed in ref. [11], if Eve wants to introduce no error into the checking procedure (i.e. $p_e = 0$), then the combined quantum state $|\Psi\rangle$ must be a product state of a GHZ triplet and the ancilla, which means Eve will gain no information about the signature. This can be described as

$$|\Psi\rangle = \sum_{j,k,n=0}^{1} |jkn\rangle_{123} \left|R_{jkn}\right\rangle_E \xrightarrow{p_e=0} |\Psi\rangle = |\phi\rangle_{123} |R\rangle_E, \quad (6)$$

where $|jkn\rangle_{123}$ a three-qubit state and $\left|R_{jkn}\right\rangle_E$ is an ancilla state.

Actually, our security check procedure is an improved version of the security check of QSS protocol in ref. [11] where its related security issues have been discussed extensively in refs. [11,31,32]. Once the security check is passed in Step 2(c), it means that S_1 and S_2 have been securely sent from Charlie to Alice and Bob.

Some special attacks like the Trojan horse attack [33,34] or the photon-number splitting attack [35,36] may be carried out by Eve. In this case, inserting a filter in front of every reception device to wipe off the photon signals with an illegitimate wavelength and setting a photon number splitter to split the redundant photons will defeat such kind of attacks.

Now, we will discuss whether our protocol satisfies the security requirements of weak blind signature in details.

4.1 No forgery

The verifier Charlie is considered to be authentic in our scheme, so we will consider the cases that Eve and Alice try to forge Bob's signature. The validation of the signature is guaranteed by the correlations of participants' measurements. Under different measurement bases, the entanglement relationship of the GHZ state should always be consistent. Because of K_{BC} and one-time pad, Eve and Alice cannot get the measurement outcomes of the signatory Bob, which means they will not get or forge Bob's signature in Step 3(b).

Eve or Alice may try to intercept Bob's sequence S_2 in Step 2(a) to produce a fake signature. As is mentioned above, such attack performed by Eve will be detected since she does not know Bob's measurement bases. But Alice's attack strategy is more complicated than Eve since she has one of the GHZ particles and is fully participated in the discussion procedure. Similar to the participant attack shown in refs. [31,32], a dishonest Alice may try to intercept S_2, interact them with her ancillas and then resend S_2 to Bob. After Bob reveals his information in Step 2(c), Alice then measures her corresponding qubits to get useful information. Besides, Alice also needs to announce outcomes according to Bob's measurement basis to avoid introducing any error. It has been pointed out that the order of declaring the testing bit is crucial to the security of GHZ based protocol [31]. The reason behind the success of this participant attack is that dishonest Alice can always get Bob's measurement bases before she announces her own outcomes. While in our scheme, Alice and Bob's declaring order is random for every position. In half of the time, Alice has to declare her measurement outcomes firstly. This implies that Alice's attack strategy will not work in our scheme.

4.2 Blindness

In our protocol, the signatory Bob cannot know the content of the message m when he signs it. Also, he will not get m in Step 3(a) because m is encrypted with one-time pad and K_{AC}. Bob may also try to perform ancilla attack to get Alice's message m, but this kind of attack will not work. On the one hand, Bob's attack will be detected by Charlie in the public discussion in Step 2(c) since in half of the time he has to publish his measurement outcomes firstly. On the other hand, even if Bob has successfully entangled his ancillas with Alice's sequence S_1 without being detected which rarely happens, he can still get nothing meaningful since Alice only performs measurements in the following step and she will not publish anything about her measurements. This means the message m is blind for the signatory Bob.

4.3 No disavowal of original

As is discussed above, nobody can counterfeit the valid signature except for the signatory. Since Bob does not know Alice and Charlie's measurement bases which is chosen from two non-orthogonal bases X and Y, he cannot conclude all the

consistent measurement results of Alice and Charlie. If a signature has passed the verification process, it is only possible that the signature is created by Bob. This means the signatory Bob cannot deny having signed the message.

4.4 Traceability

If a disagreement happens, the signatory Bob can trace the message owner Alice with the help of the trusted verifier Charlie. Here, by using the signature triple (m', b, c) and the shared keys K_{AC} and K_{BC}, Charlie is able to verify whether the signature is valid and to trace Alice since K_{AC} is only known by Alice and Charlie.

5 Conclusions

In summary, we propose a new and efficient BQS protocol based on the GHZ states. Our protocol has the following features. For one thing, compared with some previous BQS protocols such as Wen et al.'s [25] and Yin et al.'s [30], the proposed protocol has 100% efficiency since Charlie can always select the right measurement bases and every single bit can be used for verification. For another, our protocol is simpler since no anonymous communication technology, hash function [29] or quantum one-way function [30] has been used. Moreover, the protocol is easy to implement in practical situations based on current technologies [37,38].

In our protocol, Charlie can always choose the right bases to measure his qubits, which means each tuple of the measurement results in the protocol is correlated rather than random in refs. [25,30]. Therefore, the security problem shown in ref. [26] can be avoided. The security of the protocol is guaranteed by the entanglement correlations of the GHZ states, the secret keys K_{AC} and K_{BC} and the one-time pad algorithm, all of which have been proven unconditionally secure. According to the security analysis, neither the outside attacker nor the dishonest participants can break the security requirements of the blind signature.

This project was supported by the National Natural Science Foundation of China (Grant Nos. 61003287, 61170272, 61121061 and 61272514), the Specialized Research Fund for the Doctoral Program of Higher Education (Grant No. 20100005120002), the Fok Ying Tong Education Foundation (Grant No. 131067), the Asia Foresight Program under NSFC (Grant No. 61161140320), and the Fundamental Research Funds for the Central Universities (Grant No. BUPT2012RC0221).

1 Diffie W, Hellman M. New directions in cryptography. IEEE Trans Inf Theory, 1976, 22: 644–654

2 Merkle R. Secrecy, Authentication, and Public Key Systems. Dissertation for Doctoral Degree. Stanford: Stanford University, 1979

3 Shor P W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM J Sci Statist Comput, 1997, 26: 1484–1509

4 Bennett C H, Brassard G. Quantum cryptography: Public key distribution and coin tossing. In: Proceedings of IEEE International Conference on Computer Systems and Signal Processing, Bangalore, 1984. 175–179

5 Ekert A K. Quantum cryptography based on Bell's theorem. Phys Rev Lett, 1991, 67: 661–663

6 Bennett C H. Quantum cryptography using any two nonorthogonal states. Phys Rev Lett, 1992, 68: 3121–3124

7 Bostrom K, Felbinger T. Deterministic secure direct communication using entanglement. Phys Rev Lett, 2002, 89: 187902

8 Deng F G, Long G L, Liu X S. Two-step quantum direct communication protocol using the Einstein-Podolsky-Rosen pair block. Phys Rev A, 2003, 68: 042317

9 Chen X B, Wang T Y, Du J Z, et al. Controlled quantum secure direct communication with quantum encryption. Int J Quantum Inf, 2008, 6: 543–551

10 Chen X B, Wen Q Y, Guo F Z, et al. Controlled quantum secure direct communication with W state. Int J Quantum Inf, 2008, 6: 899–906

11 Hillery M, Buzek V, Berthiaume A. Quantum secret sharing. Phys Rev A, 1999, 59: 1829–1834

12 Gottesman D. Theory of quantum secret sharing. Phys Rev A, 2000, 61: 042311

13 Chen X B, Niu X X, Zhou X J, et al. Multi-party quantum secret sharing with the single-particle quantum state to encode the information. Quantum Inf Process, 2013, 12: 365–380

14 Gottesman D, Chuang I. Quantum digital signatures. arXiv: quant-ph/0105032, 2001

15 Zeng G H, Keitel C H. Arbitrated quantum-signature scheme. Phys Rev A, 2002, 65: 042312

16 Curty M, Lutkenhaus N. Comment on "Arbitrated quantum-signature scheme". Phys Rev A, 2008, 77: 046301

17 Zeng G H. Reply to "Comment on 'Arbitrated quantum-signature scheme' ". Phys Rev A, 2008, 78: 016301

18 Li Q, Chan W H, Long D Y. Arbitrated quantum signature scheme using Bell states. Phys Rev A, 2009, 79: 054307

19 Zou X F, Qiu D W. Security analysis and improvements of arbitrated quantum signature schemes. Phys Rev A, 2010, 82: 042325

20 Gao F, Qin S J, Guo F Z, et al. Cryptanalysis of the arbitrated quantum signature protocols. Phys Rev A, 2011, 84: 022344

21 Lee H, Hong C, Kim H, et al. Arbitrated quantum signature scheme with message recovery. Phys Lett A, 2004, 321: 295–300

22 Yang Y G, Zhou Z, Teng Y W, et al. Arbitrated quantum signature with an untrusted arbitrator. Eur Phys J D, 2011, 61: 773–778

23 Chaum D. Blind signatures for untraceable payments. In: Proceedings of CRYPTO'82. New York: Plenum Publishing, 1982. 199–203

24 Benaloh J C, Yung M. Distributing the power of a government to enhance the privacy of voters. In: Proceedings of the 5th Annual ACM Symposium on Principles of Distributed Computing, Calgary, 1986. 52–62

25 Wen X J, Niu X M, Ji L P, et al. A weak blind signature scheme based on quantum cryptography. Opt Commun, 2009, 282: 666–669

26 Naseri M. A weak blind signature based on quantum cryptography. Int J Phys Sci, 2011, 6: 5051–5053

27 Su Q, Huang Z, Wen Q Y, et al. Quantum blind signature based on two-state vector formalism. Opt Commun, 2010, 283: 4408–4410

28 Yang C W, Hwang T, Luo Y P. Enhancement on "quantum blind signature based on two-state vector formalism". Quantum Inf Process, 2013, 12: 109–117

29 Xu R, Huang L S, Yang W, et al. Quantum group blind signature scheme without entanglement. Opt Commun, 2011, 284: 3654–3658

30 Yin X R, Ma W P, Liu W Y. A blind quantum signature scheme with χ-type entangled states. Int J Theor Phys, 2012, 51: 455–461

31 Karlsson A, Koashi M, Imoto N. Quantum entanglement for secret sharing and secret splitting. Phys Rev A, 1999, 59: 162–168

32 Qin S J, Gao F, Wen Q Y, et al. Cryptanalysis of the Hillery-Buzcaronek-Berthiaume quantum secret-sharing protocol. Phys Rev A, 2007, 76: 062324

33 Deng F G, Li X H, Zhou H Y, et al. Improving the security of multiparty quantum secret sharing against Trojan horse attack. Phys Rev A, 2005, 72: 044302

34 Gisin N, Fasel S, Kraus B, et al. Trojan-horse attacks on quantum-key-distribution systems. Phys Rev A, 2006, 73: 022320

35 Huttner B, Imoto N, Gisin N, et al. Quantum cryptography with coherent states. Phys Rev A, 1995, 51: 1863–1869

36 Brassard G, Lutkenhaus N, Mor T, et al. Limitations on practical quantum cryptography. Phys Rev Lett, 2000, 85: 1330–1333

37 Tittel W, Zbinden H, Gisin N. Experimental demonstration of quantum secret sharing. Phys Rev A, 2001, 63: 042301

38 Chen Y A, Zhang A N, Zhao Z, et al. Experimental quantum secret sharing and third-man quantum cryptography. Phys Rev Lett, 2005, 95: 200502