Weak blind quantum signature protocol based on entanglement swapping

Minghui Zhang* **and Huifang Li**

School of Electronic and Information, Northwestern Polytechnical University, Xi'an 710129, China
**Corresponding author: nikkoch@163.com*

Received June 26, 2015; revised September 11, 2015; accepted September 12, 2015;
posted September 17, 2015 (Doc. ID 243853); published October 19, 2015

In this paper, we put forward a weak blind quantum signature scheme based on quantum entanglement swapping of Bell states. Different from the existing quantum signature schemes, our scheme can offer two-step verification security services to ensure the validity of the verification. In order to guarantee the unconditional security of the scheme, the quantum key distribution protocol and one-time pad encryption algorithm are employed in our scheme. Besides, the entanglement swapping of Bell states mechanism enhances the security of verification criteria. The proposed scheme has the properties of nonforgeability, nonrepudiation, blindness, and traceability. © 2015 Chinese Laser Press

OCIS codes: (270.0270) Quantum optics; (270.5568) Quantum cryptography; (270.5565) Quantum communications.
http://dx.doi.org/10.1364/PRJ.3.000324

1. INTRODUCTION

Quantum cryptography has received enormous attention in recent years for its proven unconditional security. In general, quantum cryptography includes quantum key distribution (QKD), quantum secret sharing, quantum secure direct communication, and quantum authentication. The purpose of a quantum signature, as part of quantum authentication, is to avoid the signature, and the initial message is forged from the internal dishonest participants or the external attackers; further, the signer cannot deny the signature.

Diffie and Hellman [1] first introduced the digital signature in 1976, which came to play a critical role in authentication, data integrity protection, and other cryptography fields. However, traditional signature schemes can easily be broken with the emergence of quantum computers because the security of these protocols depends on some unproven computational complexity, such as discrete logarithm or factoring problems. Therefore, in order to guarantee the security even against attackers with unlimited computational power, it is necessary to study quantum analogs of digital signature schemes. Gottesman and Chuang [2] proposed the first quantum signature protocol based on the one-way function. Zeng and Keitel [3] presented a pioneering arbitrated quantum signature scheme. Since then, many quantum signature strategies have been proposed [4–10].

However, the ordinary quantum signature mechanism is not a very suitable encryption approach for the E-payment system and E-voting system in which the message owner's privacy should be protected. For instance, in an E-voting system, a ballot needs to be signed by the manager, but the content of the ballot could never be revealed to the manager. In blind signature schemes, the signer generates the signature yet knows nothing about the content that he/she has signed. The blind signature scheme can be divided into the weak blind signature and the strong blind signature on the basis of whether the message owner can be traced by the signatory. Wen *et al.* [11] proposed the first quantum weak blind signature scheme in 2008. However, Naseri [12] had shown that the protocol in its original form cannot fairly complete the task of a blind signature. Afterward, Su *et al.* [13] proposed a blind signature scheme based on two-state vector formalism with 100% efficiency. But Yang *et al.* [14] studied some possible attacks against Su *et al.*'s scheme and proposed an enhanced signature scheme. However, Zhang *et al.* [15] found the dishonest signer can reveal 25% of the message in Yang *et al.*'s enhanced scheme. Almost simultaneously, Su and Li [16] pointed out that Yang *et al.*'s enhanced protocol also has a loophole of participant attack. Soon after that, Wang and Wen [17] presented a fair blind signature scheme based on quantum mechanics. He *et al.* [18] pointed out this protocol cannot, unfortunately, satisfy the property of nonforgeability. After that, Zou and Qiu [19] further analyzed the security of this protocol and put forward a more subtle attack strategy. Recently, Yin *et al.* [20] proposed a blind signature scheme with χ-type entangled states, and Wang *et al.* [21] presented a weak blind quantum signature scheme based on GHZ states. Khodambashi and Zakerolhosseini [22] proposed a sessional blind signature based on quantum cryptography. But Su and Li [23] found that the signature protocol will cause the key information leakage. Wang *et al.* [24] also pointed out there are two security leaks in this protocol.

In this paper, we put forward a weak blind quantum signature protocol based on the entanglement swapping [25] of Bell states. We subject two photons, each of them, respectively, belongs to their own Bell states, to a Bell measurement by which the other two photons also become entangled. Thus, we can utilize the correlation of quantum entanglement swapping to act as the judge foundation in the verification phase. Moreover, the employment of QKD protocol [26] and one-time pad encryption algorithm [27] ensures the unconditional security of the scheme.

The rest of this paper is outlined as follows. In Section 2, we will briefly introduce the local unitary operation and quantum entanglement swapping mechanism. Then, we give a weak blind quantum signature scheme based on the entanglement swapping of Bell states in Section 3. In the next section, we demonstrate the security of our protocol. A conclusion is given in Section 5.

2. PRELIMINARIES

Generally, a practicable weak blind quantum signature protocol should meet the following requirements:

(a) *Nonforgery*. Any counterfeits of the true signature will be discovered in the verification phase. That is, nobody can create the true signature except for the signer.
(b) *Nonrepudiation*. The signature cannot be denied by the signer, and the original message cannot be denied by the message owner.
(c) *Blindness*. The signer cannot learn the content of the message that he/she has signed.
(d) *Traceability*. The message owner can be traced by the signer when a dispute investigation happens.

Before giving our scheme, we will briefly introduce the local unitary operation and the entanglement swapping of Bell states. The four Bell states can be denoted as

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

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

$$|\phi^+\rangle = \frac{1}{\sqrt{2}}(|0\rangle|0\rangle + |1\rangle|1\rangle) = \frac{1}{\sqrt{2}}(|+\rangle|+\rangle + |-\rangle|-\rangle), \quad (3)$$

$$|\phi^-\rangle = \frac{1}{\sqrt{2}}(|0\rangle|0\rangle - |1\rangle|1\rangle) = \frac{1}{\sqrt{2}}(|+\rangle|-\rangle + |-\rangle|+\rangle), \quad (4)$$

where $|\pm\rangle = 1/\sqrt{2}(|0\rangle \pm |1\rangle)$. Let $\sigma_1 = |0\rangle\langle 0| + |1\rangle\langle 1|$, $\sigma_2 = |0\rangle\langle 0| - |1\rangle\langle 1|$, $\sigma_3 = -|1\rangle\langle 0| - |0\rangle\langle 1|$, and $\sigma_4 = |1\rangle\langle 0| - |0\rangle\langle 1|$ as four local unitary operators, which can be used to perform unitary operation on one photon in a Bell state to form the secret information. One can see that $\sigma_1|\psi^-\rangle = |\psi^-\rangle$, $\sigma_2|\psi^-\rangle = |\psi^+\rangle$, $\sigma_3|\psi^-\rangle = |\phi^-\rangle$, and $\sigma_4|\psi^-\rangle = |\phi^+\rangle$. Suppose that Alice and Bob share Bell states $|\psi^-_{AB}\rangle$ and $|\psi^-_{CD}\rangle$. Alice possesses the particles A and C, and Bob keeps the particles B and D. Thus, the following equations hold:

$$\sigma_1|\psi^-_{AB}\rangle \otimes |\psi^-_{CD}\rangle = |\psi^-_{AB}\rangle \otimes |\psi^-_{CD}\rangle = \frac{1}{2}(|\psi^-_{AC}\rangle|\psi^-_{BD}\rangle + |\phi^+_{AC}\rangle|\phi^+_{BD}\rangle - |\psi^+_{AC}\rangle|\psi^+_{BD}\rangle - |\phi^-_{AC}\rangle|\phi^-_{BD}\rangle), \quad (5)$$

$$\sigma_2|\psi^-_{AB}\rangle \otimes |\psi^-_{CD}\rangle = |\psi^+_{AB}\rangle \otimes |\psi^-_{CD}\rangle = \frac{1}{2}(|\psi^+_{AC}\rangle|\psi^-_{BD}\rangle - |\psi^-_{AC}\rangle|\psi^+_{BD}\rangle - |\phi^+_{AC}\rangle|\phi^-_{BD}\rangle + |\phi^-_{AC}\rangle|\phi^+_{BD}\rangle), \quad (6)$$

$$\sigma_3|\psi^-_{AB}\rangle \otimes |\psi^-_{CD}\rangle = |\phi^-_{AB}\rangle \otimes |\psi^-_{CD}\rangle = \frac{1}{2}(|\phi^+_{AC}\rangle|\psi^+_{BD}\rangle + |\phi^-_{AC}\rangle|\psi^-_{BD}\rangle - |\psi^+_{AC}\rangle|\phi^+_{BD}\rangle - |\psi^-_{AC}\rangle|\phi^-_{BD}\rangle), \quad (7)$$

$$\sigma_4|\psi^-_{AB}\rangle \otimes |\psi^-_{CD}\rangle = |\phi^+_{AB}\rangle \otimes |\psi^-_{CD}\rangle = \frac{1}{2}(|\phi^-_{AC}\rangle|\psi^+_{BD}\rangle - |\psi^+_{AC}\rangle|\phi^-_{BD}\rangle - |\psi^-_{AC}\rangle|\phi^+_{BD}\rangle + |\phi^+_{AC}\rangle|\psi^-_{BD}\rangle). \quad (8)$$

Thus, when the local unitary operator acted on the Bell state $|\psi^-_{AB}\rangle$ is σ_1, Alice subjects particles A and C to a measurement in a Bell basis. If she finds them in the state $|\psi^-_{AC}\rangle$, then qubits B and D measured by Bob will be in the Bell state $|\psi^-_{BD}\rangle$. If Alice observes any other Bell states for particles A and C, particles B and D will also be entangled correspondingly.

3. DESCRIPTION OF THE PROPOSED SCHEME

In fact, quantum signature schemes containing a trusted arbitrator are shown to be applicable and useful, especially with reduced requirements on the trustworthiness of the arbitrator [28]. Our scheme involves four parties: Alice, Bob, Charlie, and an arbitrator. The message owner, Alice, transforms the initial message into the blind message; Bob is considered the signatory who signs on the blind message without knowing the content of the message; Charlie is regarded as the verifier who investigates the authenticity of the signature and the original message with the assistance of the arbitrator. The arbitrator controls the flow of the scheme and provides a useful message to help determine whether the signature is true. Now we will explain our blind quantum signature scheme from the following four stages.

A. Initial Phase

Step 1: Charlie shares the secret key k_{AC} with Alice and k_{BC} with Bob. The arbitrator shares the secret key k_A with Alice, k_B with Bob, and k_C with Charlie. All these secret keys will be obtained via the proved unconditional security QKD protocol.

Step 2: The arbitrator prepares two Bell state sequences with length of $n + l$, both in the state $|\psi^-\rangle$, that is, the total state is $|\psi^-_{AB}\rangle \otimes |\psi^-_{CD}\rangle$, where the subscripts A, B, C, and D express the four different photons. In order to further illustrate the scheme, we denote the single photon sequence as

$$W_j = \{w_j^1, w_j^2, \ldots, w_j^n, \ldots, w_j^{n+l}\} \quad (j \in A, B, C, D). \quad (9)$$

Then, the arbitrator delivers the sequence W_A to Alice and W_C to Bob; he retains the sequences W_B and W_D.

Step 3: In order to prevent possible attack strategies, participants need to check the security of the communication channel. The arbitrator randomly selects l sampling particles from W_B and W_D and measures them in the Bell basis. Then, the arbitrator publishes the positions of these particles and the measurement basis to Alice and Bob. If the arbitrator's result is $|\psi^-_{BD}\rangle$ or $|\phi^+_{BD}\rangle$, Alice and Bob will use the basis X (otherwise use the basis Z). After that, Alice and Bob declare their measurement results to the arbitrator. Finally, the arbitrator calculates the error rate by the outcomes of three parties according to Eq. (5); if the error rate exceeds a certain threshold, then this communication process is revoked. Otherwise, we proceed to the next step.

B. Blinding Phase

Step 1: Alice prepares an n bit classical initial message sequence, $m = \{m(1), m(2), \ldots, m(n)\}(m(i) \in \{0, 1\})$.

Step 2: Alice selects the corresponding unitary operators to act on the photons A according to m. As shown in Table 1, for each $i \in \{1, 2, \ldots\ldots, n\}$, if $m(i-1)m(i) = 00$, Alice will choose the operator σ_1 and encode it into 2-bit message 11. One can see the other correspondences as well in Table 1.

Step 3: Alice creates the secret messages $M = E_{k_{AC}}(m')$ and $M^* = E_{k_A}(m')$ by encrypting m' in terms of the secret keys k_{AC} and k_A with a classical one-time pad algorithm.

Step 4: Alice sends the secret blind message M to Charlie and M^* to the arbitrator.

C. Signing Phase

Step 1: Charlie decrypts M with k_{AC} and obtains the blind message m'. Then, he decrypts m' to acquire the corresponding unitary operators; thus, he can deduce the original message m. Similarly, the arbitrator can learn the unitary operators by decrypting M^* with k_A. For instance, if $m' = \{10000111\}$, then the operators Alice utilized is $\sigma = \{\sigma_2, \sigma_4, \sigma_3, \sigma_1\}$, and Charlie can learn that $m = \{0|1100\}$.

Step 2: The arbitrator performs the Bell measurement on the rest n particles in W_B and W_D and records the result as $|C\rangle = \{|C(1)\rangle, |C(2)\rangle, \ldots, |C(n)\rangle\}$ with $|C(i)\rangle \in \{|\psi^+_{BD}\rangle, |\psi^-_{BD}\rangle, |\phi^+_{BD}\rangle, |\phi^-_{BD}\rangle\}$. At this point, the photons A and C have collapsed a certain Bell state due to the property of quantum entanglement swapping. The measurement basis Alice and Bob should use depends on $|C\rangle$ and the operator as shown in Table 2. Let the basis correspond to a classical bit, respectively, i.e., X to "0," Z to "1," then the arbitrator encrypts the classical bits with k_A and k_B via classical one-time pad algorithm, respectively, and sends the encrypted message to Alice and Bob.

Step 3: Alice and Bob decrypt the secret message with k_A and k_B to get the measurement basis. Then Alice and Bob measure their respective photons sequence and record their results as $|A\rangle = \{|A(1)\rangle, |A(2)\rangle, \ldots, |A(n)\rangle\}$ and $|B\rangle = \{|B(1)\rangle, |B(2)\rangle, \ldots, |B(n)\rangle\}$ with $\{|A(i)\rangle, |B(i)\rangle\} \in \{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$.

Step 4: Alice encrypts $|A\rangle$ in terms of k_A with quantum one-time pad encryption algorithm and gets the secret message $M_A = E_{k_A}(|A\rangle)$. Bob encrypts $|B\rangle$ with k_B by the same encryption algorithm and obtains the signature $S = E_{k_B}(|B\rangle)$. Then, Alice and Bob transmit M_A and S to Charlie, respectively.

Table 1. Initial Message is Converted into Blind Message

$m(i)$	$m(i-1)m(i)$	Operator	Blind Message m'
0			
1	01	σ_2	10
1	11	σ_4	00
0	10	σ_3	01
0	00	σ_1	11

Table 2. Criteria of Measurement Base Selection

Operator	$\|C\rangle$	Basis
σ_1 or σ_4	$\|\psi^-_{BD}\rangle$ or $\|\phi^+_{BD}\rangle$	X
	$\|\psi^+_{BD}\rangle$ or $\|\phi^-_{BD}\rangle$	Z
σ_2 or σ_3	$\|\psi^-_{BD}\rangle$ or $\|\phi^+_{BD}\rangle$	Z
	$\|\psi^+_{BD}\rangle$ or $\|\phi^-_{BD}\rangle$	X

Table 3. Validation Rules of the Scheme

Operator	$\|C\rangle$	AC's state	$\{\|A\rangle, \|B\rangle\}$
σ_1	$\|\psi^-_{BD}\rangle$	$\|\psi^-_{AC}\rangle$	$\{\|+\rangle, \|-\rangle\}$ or $\{\|-\rangle, \|+\rangle\}$
	$\|\phi^+_{BD}\rangle$	$\|\phi^+_{AC}\rangle$	$\{\|+\rangle, \|+\rangle\}$ or $\{\|-\rangle, \|-\rangle\}$
	$\|\psi^+_{BD}\rangle$	$\|\psi^+_{AC}\rangle$	$\{\|0\rangle, \|1\rangle\}$ or $\{\|1\rangle, \|0\rangle\}$
	$\|\phi^-_{BD}\rangle$	$\|\phi^-_{AC}\rangle$	$\{\|0\rangle, \|0\rangle\}$ or $\{\|1\rangle, \|1\rangle\}$
σ_2	$\|\psi^-_{BD}\rangle$	$\|\psi^+_{AC}\rangle$	$\{\|0\rangle, \|1\rangle\}$ or $\{\|1\rangle, \|0\rangle\}$
	$\|\phi^+_{BD}\rangle$	$\|\phi^-_{AC}\rangle$	$\{\|0\rangle, \|0\rangle\}$ or $\{\|1\rangle, \|1\rangle\}$
	$\|\psi^+_{BD}\rangle$	$\|\psi^-_{AC}\rangle$	$\{\|+\rangle, \|-\rangle\}$ or $\{\|-\rangle, \|+\rangle\}$
	$\|\phi^-_{BD}\rangle$	$\|\phi^+_{AC}\rangle$	$\{\|+\rangle, \|+\rangle\}$ or $\{\|-\rangle, \|-\rangle\}$
σ_3	$\|\psi^-_{BD}\rangle$	$\|\phi^-_{AC}\rangle$	$\{\|0\rangle, \|0\rangle\}$ or $\{\|1\rangle, \|1\rangle\}$
	$\|\phi^+_{BD}\rangle$	$\|\psi^+_{AC}\rangle$	$\{\|0\rangle, \|1\rangle\}$ or $\{\|1\rangle, \|0\rangle\}$
	$\|\psi^+_{BD}\rangle$	$\|\phi^+_{AC}\rangle$	$\{\|+\rangle, \|+\rangle\}$ or $\{\|-\rangle, \|-\rangle\}$
	$\|\phi^-_{BD}\rangle$	$\|\psi^-_{AC}\rangle$	$\{\|+\rangle, \|-\rangle\}$ or $\{\|-\rangle, \|+\rangle\}$
σ_4	$\|\psi^-_{BD}\rangle$	$\|\phi^+_{AC}\rangle$	$\{\|+\rangle, \|+\rangle\}$ or $\{\|-\rangle, \|-\rangle\}$
	$\|\phi^+_{BD}\rangle$	$\|\psi^-_{AC}\rangle$	$\{\|+\rangle, \|-\rangle\}$ or $\{\|-\rangle, \|+\rangle\}$
	$\|\psi^+_{BD}\rangle$	$\|\phi^-_{AC}\rangle$	$\{\|0\rangle, \|0\rangle\}$ or $\{\|1\rangle, \|1\rangle\}$
	$\|\phi^-_{BD}\rangle$	$\|\psi^+_{AC}\rangle$	$\{\|0\rangle, \|1\rangle\}$ or $\{\|1\rangle, \|0\rangle\}$

D. Verification Phase

Step 1: After having received S and M_A, Charlie creates the ciphertext $V = E_{k_C}(S, M_A)$ by encrypting S and M_A with k_C and then sends V to the arbitrator directly.

Step 2: The arbitrator decrypts V with k_C to get S and M_A. Then, the arbitrator decrypts M_A with k_A to obtain $|A\rangle$ and decrypts S with k_B to get $|B\rangle$.

Step 3: The arbitrator generates a verification parameter λ, which will be helpful in making a decision about the authenticity of Bob's signature. When the measurement results of the three parties $(|A\rangle, |B\rangle, |C\rangle)$ meet the rules in Table 3, the arbitrator considers that the signature is true and sets $\lambda = 1$; otherwise, he sets $\lambda = 0$. After that, the arbitrator obtains the cryptograph $V' = E_{k_C}(S, \sigma, \lambda)$ by encrypting S, σ, and λ with k_C; then, he sends it back to Charlie.

Step 4: Charlie decrypts V' with k_C to get S, σ, and λ. Only when $\lambda = 1$ can Charlie accept Bob's signature and go on to further the verification process. Now Charlie possesses two group unitary operators: one is deduced from the secret message M, and the other comes from V'. Charlie compares two objects for reference equality and, if they are equal, accepts the signatures S and the initial message m; otherwise, he rejects them.

4. SECURITY ANALYSIS AND DISCUSSION

In the following, we will prove that our scheme has the properties of noncounterfeit, nondisavowal, blindness, and traceability.

A. Impossibility of Forgery

First, the application of both QKD protocol and a quantum one-time pad encryption algorithm guarantees the nonforgeability of the scheme. We assume that Alice is a dishonest participant and attempts to forge Bob's signature; however, it is impossible because Bob's signature associates with k_B, which is generated via an unconditionally secure QKD protocol, which is secretly held by Bob and the arbitrator. Random guesses would have only succeeded about half of the time for each bit. Therefore, the total success rate is almost zero when the information bit sequence is quite long. Even if Alice can obtain k_B by some certain methods, the attacking strategy is still unlikely to succeed. The application of quantum entanglement swapping causes Alice and Bob's measurement results to depend on the arbitrator's measurement result, which is only known for himself. Because Alice cannot know the arbitrator's result, she cannot learn Bob's outcome as well. The correlations of the entanglement swapping of two EPR pairs will be destroyed if Alice uses the wrong one to replace Bob's outcome.

Second, our scheme can resist the intercept-resend attack. In Step 2 (in Section 3.1), the arbitrator delivers the photon sequence W_A to Alice and W_C to Bob, respectively. If dishonest Alice attempts to intercept W_C and resends the sequence W'_C to Bob, however, it is still inevitable that the attacking tactic will be discovered by the arbitrator in Step 3 (in Section 3.1). Thus, Alice can neither copy the qubits W_C nor learn the right measurement basis Bob used. That is, the sequence W'_C is not equal to W_C. Further, the use of W'_C will make the error rate exceed the threshold.

Furthermore, our scheme adds an extra verification step to determine the validity of the initial message. If the attacker tries to forge Alice's initial message, it is no doubt that the attack can be found by Charlie by the comparison of two group operators. The fact remains that nobody can counterfeit Bob's signature and Alice's initial message for their own interests without being detected.

B. Impossibility of Disavowal

Bob cannot deny his signature because his signature message S contains the secret key k_B, which is secretly kept by Bob and the arbitrator. If Bob tries to deny his own signature, the arbitrator just needs to decrypt the signature and investigate whether the signature message associates with Bob's secret key k_B. If so, the arbitrator considers that the signature has been signed by Bob. Similarly, Alice also cannot disavow her initial message because her initial message M contains k_A, which is secretly kept by Alice and the arbitrator. The arbitrator can confirm whether the initial information belongs to Alice by k_A.

C. Blindness

It is obvious that the signer Bob cannot learn the content of the original message in our signature scheme. Bob just needs to measure the particles sequence W_C in the basis X or Z and then generate the signature with a quantum one-time pad encryption algorithm.

D. Traceability

When Bob starts to suspect the message owner Alice's motives, he can trace the identity of Alice with the assistance of the arbitrator. Because the secret key k_A is shared between Alice and the arbitrator, Bob can trace the message owner Alice according to k_A and the parameters set $(M_A, |A\rangle, |B\rangle, |C\rangle, \sigma)$.

5. CONCLUSION

In this paper, we present a weak blind quantum signature protocol based on quantum entanglement swapping of Bell states. The proposed scheme adopts a two-step verification process to guarantee the security, i.e., the tasks of verifying the authenticity of the original message and the signature are carried out simultaneously. Through the security analysis discussed above, we confirm that it is impossible for anyone to counterfeit the signature in our scheme. Meanwhile, the signer cannot deny the signature, and the message owner cannot deny the initial message. The proposed scheme can also maintain the inherent characteristics of the weak blind quantum signature scheme, i.e., blindness and traceability.

ACKNOWLEDGMENT

This work is supported by the National Natural Science Foundation of China (grant no. 61273250).

REFERENCES

1. W. Diffie and M. Hellman, "New directions in cryptography," IEEE Trans. Inf. Theory. **22**, 644–654 (1976).
2. D. Gottesman and I. Chuang, "Quantum digital signatures," arXiv: quant-ph/0105032v2 (2001), pp. 1–8.
3. G. H. Zeng and C. H. Keitel, "Arbitrated quantum-signature scheme," Phys. Rev. A **65**, 042312 (2002).
4. H. Lee, C. Hong, H. Kim, J. Lim, and H. J. Yang, "Arbitrated quantum signature scheme with message recovery," Phys. Lett. A **321**, 295–300 (2004).
5. X. J. Wen, Y. Liu, and Y. Sun, "Quantum multi-signature protocol based on teleportation," Z. Naturforsch. **62**, 147–151 (2007).
6. G. H. Zeng, M. H. Lee, Y. Guo, and G. Q. He, "Continuous variable quantum signature algorithm," Int. J. Quantum Inform. **5**, 553–573 (2007).
7. M. Curty and N. Lütkenhaus, "Comment on 'arbitrated quantum-signature scheme," Phys. Rev. A **77**, 046301 (2008).
8. G. H. Zeng, "Reply to 'comment on arbitrated quantum-signature scheme," Phys. Rev. A **78**, 016301 (2008).
9. Q. Li, W. H. Chan, and D. Y. Long, "Arbitrated quantum signature scheme using Bell states," Phys. Rev. A **79**, 054307 (2009).
10. X. F. Zou and D. W. Qiu, "Security analysis and improvements of arbitrated quantum signature schemes," Phys. Rev. A **82**, 042325 (2010).
11. X. J. Wen, X. M. Niu, L. P. Ji, and Y. Tian, "A weak blind signature scheme based on quantum cryptography," Opt. Commun. **282**, 666–669 (2009).
12. M. Naseri, "Comment on a weak blind signature based on quantum cryptography," Int. J. Phys. Sci. **6**, 5051–5053 (2011).
13. Q. Su, Z. Huang, Q. Y. Wen, and W. Li, "Quantum blind signature based on two-state vector formalism," Opt. Commun. **283**, 4408–4410 (2010).
14. C. W. Yang, T. Hwang, and Y. P. Luo, "Enhancement on 'quantum blind signature based on two-state vector formalism," Quantum Inf. Process. **12**, 109–117 (2013).
15. M. Zhang, G. A. Xu, X. B. Chen, S. Yang, and Y. X. Yang, "Attack on the improved quantum blind signature protocol," Int. J. Theor. Phys. **52**, 331–335 (2013).
16. Q. Su and W. M. Li, "Cryptanalysis of enhancement on 'quantum blind signature based on two-state vector formalism," Quantum Inf. Process. **13**, 1245–1254 (2014).
17. T. Y. Wang and Q. Y. Wen, "Fair quantum blind signatures," Chin. Phys. B **19**, 060307 (2010).
18. L. B. He, L. S. Huang, W. Yang, and R. Xu, "Cryptanalysis of fair quantum blind signatures," Chin. Phys. B **21**, 030306 (2012).
19. X. F. Zou and D. W. Qiu, "Attack and improvements of fair quantum blind signature schemes," Quantum Inf. Process. **12**, 2071–2085 (2013).
20. X. R. Yin, W. P. Ma, and W. Y. Liu, "A blind quantum signature scheme with χ-type entangled states," Int. J. Theor. Phys. **51**, 455–461 (2012).
21. M. M. Wang, X. B. Chen, and Y. X. Yang, "A blind quantum signature protocol using the GHZ states," Sci. China **56**, 1636–1643 (2013).

22. S. Khodambashi and A. Zakerolhosseini, "A sessional blind signature based on quantum cryptography," Quantum Inf. Process. **13**, 121–130 (2014).
23. Q. Su and W. M. Li, "Cryptanalysis of a sessional blind signature based on quantum cryptography," Quantum Inf. Process. **13**, 1917–1929 (2014).
24. T. Y. Wang, X. Q. Cai, and R. L. Zhang, "Reexamining the security of fair quantum blind signature schemes," Quantum Inf. Process. **13**, 1677–1685 (2014).
25. M. Zukowski, A. Zeilinger, M. A. Horne, and A. K. Ekert, "Event-ready-detectors bell experiment via entanglement swapping," Phys. Rev. Lett. **71**, 4287–4290 (1993).
26. C. H. Bennett, "Quantum cryptography using any two nonorthogonal states," Phys. Rev. Lett. **68**, 3121–3124 (1992).
27. P. O. Boykin and V. Roychowdhury, "Optimal encryption of quantum bits," Phys. Rev. A **67**, 042317 (2003).
28. H. Meijer and S. Akl, "Advance in cryptography," in *Proceedings of Crypto '81* (Springer-Verlag, 1981), p. 65.