

Enhanced quantum multi-signature protocol based on controlled teleportation

Minghui Zhang, Huifang Li, Zhaoqiang Xia

School of Electronic and Information, Northwestern Polytechnical University, Xi'an 710129, China

nikkoch@163.com, luhifang@nwpu.edu.cn, zxia@nwpu.edu.cn

Abstract—The multi-user quantum signature protocol makes the message can be signed by more than one signatory. In this paper, we put forward an enhanced quantum multi-signature scheme based on Bell states and the controlled quantum teleportation. Compared to the previous multi-signature schemes, our protocol can offer higher security guaranteed by the fundamental laws of physics. While ensuring the nice security of the protocol we also pay attention to keeping its efficiency. Moreover, the scheme is more feasible with the present-day technique.

Keywords— quantum cryptography, quantum communications, quantum signature, multi-signature, controlled teleportation.

I. INTRODUCTION

Digital signature had been introduced by Diffie and Hellman [1] for the first time in 1976, which plays a pivotal role in authentication, data integrity protection and non-repudiation and other cryptography fields. However, the traditional digital signature schemes can easily be broken with the emergence of quantum computers since the security of these protocols depends on some unproven computational complexity. Therefore, in order to guarantee the security even against attackers with unlimited computational power, it is necessary to study quantum analogs of digital signature.

Quantum signatures offer a means of sending a message, which cannot be forged or repudiated, with security verified by information-theoretical limits and quantum mechanics. Quantum signature as a significant branch of quantum cryptography combines quantum theory with classical digital signature. In general, quantum signature scheme should satisfy two security requirements, unforgeability and undeniability. For unforgeability, neither the internal dishonest participants nor an external attacker can counterfeit a signature. For undeniability, the signatory who issues a signature cannot later deny having provided her/his signature.

Quantum signature was first investigated by Gottesman and Chuang [2] in 2001, they proposed a signature scheme based on quantum one-way function. Zeng and Keitel [3] put forward a pioneering arbitrated quantum signature scheme based on Greenberger-Horne-Zeilinger (GHZ) states with unconditional security. Subsequently, Curty et al. [4] analyzed

Zeng et al.'s scheme and argued that the security statements of the scheme are incorrect. Soon after, Zeng's response for this comment was put forward for further discussion [5]. After that, Li et al. [6] presented another arbitrated quantum signature scheme based on Bell states, which simplifies Zeng et al.'s scheme by replacing GHZ states with Bell states as the carrier. Dunjko et al. [7] proposed a quantum digital signature that does not need quantum memory, and Collins et al. [8] gave the realization of this scheme. Wallden et al. [9] proposed two schemes for quantum digital signatures which have the same experimental requirements as quantum key distribution. By far, there is a lot of attention focused on this topic [10-17].

However, in some special cases, the message needs to be signed by more than one signer, namely, multi-user signature. Wen et al. [15] proposed a quantum multi-signature scheme with many merits (denoted as WLS protocol hereafter). The WLS protocol is based on the controlled quantum teleportation [16] and the GHZ states. However, we observe that although the WLS protocol takes advantage of the GHZ states, the particles in the GHZ states hold by Alice have not been used in subsequent signature and verification phases. Therefore, the GHZ states used in the WLS protocol can be replaced by Bell states which can be prepared and distributed more simply with the present-day technologies [6]. Besides, the parameters of the initial information in the WLS protocol subject to certain restriction, i.e., two eigenstate parameters can only be 0 or 1. That is to say, the WLS scheme can only be used to sign on the specific message. Furthermore, the WLS protocol can only prevent some simple forged signature attacks and it is vulnerable to some complicated attacks due to its security flaws. Therefore, in this paper, we put forward an enhanced quantum multi-signature scheme which not only resolves all these problems mentioned above, but also retains the efficiency of WLS protocol.

The rest of this paper is organized as follows. In Sec. II, we will review the WLS protocol briefly. Then we give an enhanced quantum multi-signature scheme in Sec. III. In fact, our proposed scheme is the improvement of the WLS protocol. The next section we compare the security of the WLS protocol and our protocol and prove that our protocol has better safety. At last, a conclusion is given in Sec. V.

Please direct correspondence to Zhaoqiang Xia (zxia@nwpu.edu.cn)

II. REVIEW OF WLS PROTOCOL

The message that Alice sends to Bob is expressed as M , Alice's signature and Charlie's signature are denoted as S_A and S_C , respectively.

A. Initial phase

1) Step I1: Alice prepares n triplets of particles system in GHZ states $|\Psi\rangle_{123} = \{|\Psi(1)\rangle_{123}, |\Psi(2)\rangle_{123}, \dots, |\Psi(n)\rangle_{123}\}$.

2) Step I2: Alice prepares n qubits in the eigenstates $(|0\rangle, |1\rangle)$, which correspond to the initial message M . These n particles' states are expressed as:

$$|\Psi\rangle_M = \{|\Psi(1)\rangle_M, |\Psi(2)\rangle_M, \dots, |\Psi(n)\rangle_M\} \\ = \{k_1|0\rangle + l_1|1\rangle, k_2|0\rangle + l_2|1\rangle, \dots, k_n|0\rangle + l_n|1\rangle\}, \quad (1)$$

where $(|k_i|=0, |l_i|=1)$ or $(|k_i|=1, |l_i|=0)$.

3) Step I3: Alice shares a secret key K_a with Bob as well as Charlie shares a secret key K_c with Bob.

B. Signing phase

1) Step S1: Alice performs transform 1 or transform 2 on each triplet according to K_a . If $K_a^i=0$, she performs transform 1 on $|\Psi(i)\rangle_{123}$. If $K_a^i=1$, she performs transform 2 on $|\Psi(i)\rangle_{123}$. Alice records the transformation as $T_A = \{T(1), T(2), \dots, T(n)\}$ with $T(i) \in \{\text{transform 1}, \text{transform 2}\}$. Then Alice obtains her signature $S_A = E_{K_a}\{T_A, (k_1, l_1), (k_2, l_2), \dots, (k_n, l_n)\}$ by encrypting T_A and (k_i, l_i) with K_a .

2) Step S2: To each triplet, Alice holds particles 1, and sends particles $\{M(i)\}$ and particles 2 to Charlie. Meanwhile, she sends S_A with particles 3 to Bob.

3) Step S3: After received particles $\{M(i)\}$ and particles 2, Charlie performs a Bell measurement on them and records the measurement outcomes set as $\beta_C = \{\beta(1), \beta(2), \dots, \beta(n)\}$ with $\beta(i) \in \{|\phi^+\rangle, |\phi^-\rangle, |\psi^+\rangle, |\psi^-\rangle\}$. He encrypts β_C with K_c to get the signature $S_C = E_{K_c}(\beta_C)$, Charlie then sends S_C to Bob.

C. Verification phase

1) Step V1: After received S_A with particles 3 from Alice and S_C from Charlie, Bob decrypts S_A to obtain T_A and (k_i, l_i) by K_a as well as decrypts S_C to obtain β_C by K_c .

2) Step V2: Bob performs the corresponding operation on particle 3 in each triplet in terms of $T(i)$ and $\beta(i)$. The transformation methods refer to Table 1 in Ref [15].

3) Step V3: After the transformation, the particle in the sequence 3 has been recovered to $|\Psi(i)\rangle_3 = (k'_i|0\rangle + l'_i|1\rangle)_3$. Bob measures it with the basis $(|0\rangle, |1\rangle)$, and reads out the values of k'_i and l'_i .

4) Step V4: Bob compares (k'_i, l'_i) with (k_i, l_i) . If $k'_i = k_i$ and $l'_i = l_i$, then he accepts S_A and S_C as the truthful signatures, otherwise, he rejects them.

III. DESCRIPTION OF THE PROPOSED SCHEME

The proposed scheme also includes three phases, the initial phase, the signing phase and the verifying phase, and involves three partners, two signers Alice and Charlie, and a trusted receiver Bob. The desired protocol needs to be secure against cheating, provided that at most one of the two signers is dishonest.

A. Initial phase

1) Step i1: Alice and Charlie obtain their respective secret keys k_A and k_C shared with Bob via BB84 protocol [17] which was proved to be unconditionally secure [18,19].

2) Step i2: Bob prepares n Bell states $|\psi^+\rangle_{AB} = \{|\psi_1^+\rangle_{AB}, |\psi_2^+\rangle_{AB}, \dots, |\psi_n^+\rangle_{AB}\}$ with $|\psi_i^+\rangle_{AB} = 1/\sqrt{2}(|00\rangle + |11\rangle)_{AB}$, where the subscripts A and B correspond to the particles A and B , respectively. Then Bob possesses particles B , while distributes particles A to Alice via a secure and authenticated algorithm [20].

3) Step i3: Alice gets a qubit string $|P\rangle = \{|P_1\rangle, |P_2\rangle, \dots, |P_n\rangle\}$ related to the initial message with $|P_i\rangle = (a_i|0\rangle + b_i|1\rangle)_P$, where a_i and b_i are the parameters of eigenstates $(|0\rangle, |1\rangle)$, and meet $|a_i|^2 + |b_i|^2 = 1$.

Here note that if the message to be signed is known for all the participants, Alice don't need to prepare any copy of $|P\rangle$ and if unknown quantum states are to be signed, a copy $|P\rangle_1$ of the initial message is necessary.

B. Signing phase

1) Step s1: Alice transforms the qubit $|\psi_i^+\rangle_{AB}$ into one of the four Bell states $\{|\psi_i^+\rangle_{AB}, |\phi_i^+\rangle_{AB}, |\psi_i^-\rangle_{AB}, |\phi_i^-\rangle_{AB}\}$ according to k_A . Here k_A is related to the unitary operators, which can be expressed as:

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \sigma_z = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \sigma_x = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \sigma_y = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}. \quad (2)$$

Take the i -th particle for example, when $k_A^i k_A^{i+1} = 01$, $k_A^i \in \{0, 1\}$, Alice performs the operation $\sigma_z \otimes I$ on the particle A_i in each Bell state $|\psi_i^+\rangle_{AB}$ and thus the new Bell state is $|\phi_i^+\rangle_{AB}$. One can see the other similar transformations in Table 1. We denote the unitary operators set as $M_A = \{M_A^1, M_A^2, \dots, M_A^n\}$ and $M_A^i \in \{I \otimes I, \sigma_z \otimes I, \sigma_x \otimes I, \sigma_y \otimes I\}$. Then Alice encodes these operators as qubits, such as $I \otimes I \rightarrow |00\rangle$, $\sigma_z \otimes I \rightarrow |01\rangle$, $\sigma_x \otimes I \rightarrow |10\rangle$ and $\sigma_y \otimes I \rightarrow |11\rangle$. Alice generates her signature $|S_A\rangle = E_{k_A}(M_A)$ for the initial message $|P\rangle$ with k_A by using quantum one-time pad encryption algorithm [21].

TABLE 1. THE CRITERIA OF BELL STATE'S TRANSFORMATION

$k_A^{i,j}k_A^{i+1}$	Alice's operations	New states
00	$(I \otimes I) \psi_i^+\rangle_{AB}$	$ \psi_i^+\rangle_{AB} = 1/\sqrt{2}(00\rangle + 11\rangle)$
01	$(\sigma_z \otimes I) \psi_i^+\rangle_{AB}$	$ \phi_i^+\rangle_{AB} = 1/\sqrt{2}(10\rangle + 01\rangle)$
10	$(\sigma_x \otimes I) \psi_i^+\rangle_{AB}$	$ \psi_i^-\rangle_{AB} = 1/\sqrt{2}(00\rangle - 11\rangle)$
11	$(\sigma_y \otimes I) \psi_i^+\rangle_{AB}$	$ \phi_i^-\rangle_{AB} = 1/\sqrt{2}(01\rangle - 10\rangle)$

2) Step s2: Alice entangles each qubit of information string $|P\rangle$ with one particle of the Bell state particles string to form a particle pair. This may be implemented by applying a joint measurement on both particles, such as in a quantum logic gate operation [22]. Each combination generates a three-particle entangled state:

$$|\Phi_1\rangle = (a_i|0\rangle + b_i|1\rangle)_p \otimes \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{AB}$$

$$= \frac{1}{2} \{ |\phi_i^+\rangle_{PA}(a_i|0\rangle + b_i|1\rangle)_B + |\psi_i^+\rangle_{PA}(a_i|1\rangle + b_i|0\rangle)_B + |\phi_i^-\rangle_{PA}(a_i|0\rangle - b_i|1\rangle)_B + |\psi_i^-\rangle_{PA}(a_i|1\rangle - b_i|0\rangle)_B \} \quad (3)$$

$$|\Phi_2\rangle = (a_i|0\rangle + b_i|1\rangle)_p \otimes \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)_{AB}$$

$$= \frac{1}{2} \{ |\phi_i^+\rangle_{PA}(a_i|1\rangle + b_i|0\rangle)_B + |\psi_i^+\rangle_{PA}(a_i|0\rangle + b_i|1\rangle)_B + |\phi_i^-\rangle_{PA}(a_i|1\rangle - b_i|0\rangle)_B + |\psi_i^-\rangle_{PA}(a_i|0\rangle - b_i|1\rangle)_B \} \quad (4)$$

$$|\Phi_3\rangle = (a_i|0\rangle + b_i|1\rangle)_p \otimes \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)_{AB}$$

$$= \frac{1}{2} \{ |\phi_i^+\rangle_{PA}(-a_i|1\rangle + b_i|0\rangle)_B + |\psi_i^+\rangle_{PA}(a_i|0\rangle - b_i|1\rangle)_B + |\phi_i^-\rangle_{PA}(-a_i|1\rangle - b_i|0\rangle)_B + |\psi_i^-\rangle_{PA}(a_i|0\rangle + b_i|1\rangle)_B \} \quad (5)$$

$$|\Phi_4\rangle = (a_i|0\rangle + b_i|1\rangle)_p \otimes \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)_{AB}$$

$$= \frac{1}{2} \{ |\phi_i^+\rangle_{PA}(-a_i|0\rangle + b_i|1\rangle)_B + |\psi_i^+\rangle_{PA}(a_i|1\rangle - b_i|0\rangle)_B + |\phi_i^-\rangle_{PA}(-a_i|0\rangle - b_i|1\rangle)_B + |\psi_i^-\rangle_{PA}(a_i|1\rangle + b_i|0\rangle)_B \} \quad (6)$$

In order to prevent eavesdropping attack, participants need to check the security of the communication channel. Alice randomly inserts m decoy photons into $|P\rangle_1$ to generate $|P^*\rangle_1$, and then she delivers $|P^*\rangle_1$ followed by $|S_A\rangle$ to Bob. Then Alice announces the positions of these decoy photons and the measurement basis to Bob. According to the measurement results replied from Bob, Alice can check the existence of attackers. After that, Bob owns the particles sequence $|P\rangle_1$ by eliminating decoy photons. Alice transmits the particles A and particles P to Charlie via a secure algorithm.

3) Step s3: After having received the particles A and particles P sent from Alice, Charlie performs the corresponding operation $\{\sigma_x, \sigma_z\}$ on particle P_i in each Bell state in terms of k_C . If $k_C = 0$, he performs the operator σ_x on P_i , if $k_C = 1$, he performs σ_z on P_i . After that, Charlie implements n Bell measurement on the particles A and particles P , and records the measurement outcomes set as

$\hat{M}_C = \{\hat{M}_C^1, \hat{M}_C^2, \dots, \hat{M}_C^n\}$ with $\hat{M}_C^i \in \{|\phi^+\rangle_{PA}, |\phi^-\rangle_{PA}, |\psi^+\rangle_{PA}, |\psi^-\rangle_{PA}\}$. Then he creates his signature $|S_C\rangle = E_{k_C}(\hat{M}_C)$ by quantum one-time pad algorithm as well. Charlie sends his signature $|S_C\rangle$ to Bob.

C. Verification phase

1) Step v1: Upon receiving $|S_A\rangle$, $|S_C\rangle$ and $|P\rangle_1$. Bob deciphers $|S_A\rangle$ with k_A to get M_A and deciphers $|S_C\rangle$ with k_C to get $\hat{M}_C$. Then he converts $\hat{M}_C$ into the original state M_C by performing the reverse operation of Step s3.

2) Step v2: Bob creates a verification parameter λ_A to judge the authenticity of Alice's signature. When M_A corresponds to k_A as described in Table 1, he considers that Alice's signature is true and sets $\lambda_A = 1$; otherwise she sets $\lambda_A = 0$.

3) Step v3: The equality $\lambda_A = 1$ just means that Alice's signature $|S_A\rangle$ hasn't been forged, but cannot confirm that Charlie's signature $|S_C\rangle$ is true. Therefore, an additional validation step is necessary. Bob recovers $|P^*\rangle$ by quantum teleportation. That is, Bob performs the corresponding operations on the particles B in his site according to M_A and M_C (See Table 2) to get the qubits $|P^*\rangle$. Then he compares $|P^*\rangle$ with $|P\rangle_1$ publicly by adopting the approach in Ref [23], if $|P^*\rangle = |P\rangle_1$, Bob accepts the signatures $|S_A\rangle$ and $|S_C\rangle$; otherwise he rejects them.

TABLE 2. THE VALIDATION RULES OF THE SCHEME

M_A	The states	M_C	Operation
$I \otimes I$	$ \psi_i^+\rangle_{AB}$	$ \phi_i^+\rangle_{PA}$	I
		$ \psi_i^+\rangle_{PA}$	σ_z
		$ \phi_i^-\rangle_{PA}$	σ_x
		$ \psi_i^-\rangle_{PA}$	σ_y
$\sigma_z \otimes I$	$ \phi_i^+\rangle_{AB}$	$ \phi_i^+\rangle_{PA}$	σ_z
		$ \psi_i^+\rangle_{PA}$	I
		$ \phi_i^-\rangle_{PA}$	σ_y
		$ \psi_i^-\rangle_{PA}$	σ_x
$\sigma_x \otimes I$	$ \psi_i^-\rangle_{AB}$	$ \phi_i^+\rangle_{PA}$	$-\sigma_y$
		$ \psi_i^+\rangle_{PA}$	σ_x
		$ \phi_i^-\rangle_{PA}$	$-\sigma_z$
		$ \psi_i^-\rangle_{PA}$	I
$\sigma_y \otimes I$	$ \phi_i^-\rangle_{AB}$	$ \phi_i^+\rangle_{PA}$	$-\sigma_x$
		$ \psi_i^+\rangle_{PA}$	σ_y
		$ \phi_i^-\rangle_{PA}$	$-I$
		$ \psi_i^-\rangle_{PA}$	σ_z

For example, if Alice performs $\sigma_z \otimes I$ on the particle A_i , i.e., M_A^i is $\sigma_z \otimes I$, subsequently, the state of the particles A_i and B_i has been converted into $|\phi_i^+\rangle_{AB}$, as shown in the second column of Table 2. And if Charlie's measurement result M_C^i is $|\phi_i^+\rangle_{PA}$, then the state of the particle B_i is $(a_i|1\rangle + b_i|0\rangle)_B$, thus Bob needs to take a bit flip operation σ_z on the particle B_i to recover $|P_i\rangle$.

IV. SECURITY ANALYSIS AND DISCUSSION

As we know, a practical quantum signature mechanism should meet two security requirements: unforgeability and undeniability. Security against forging means that the recipient will with high probability reject any message which was not originally sent by the signers. Security against repudiation guarantees that signatories cannot deny that they have signed on the initial message. In the following, we will demonstrate that our scheme can provide more highly security than the WLS protocol.

A. Impossibility of forgery

1) Attacker's forgery strategy: Like the WLS protocol, the proposed scheme can detect the attacker's forgery strategy as well. In our protocol, Alice's signature associates with k_A , which is distributed via BB84 protocol and secretly hold by Alice and Bob. If an attacker, say Eve, tries to forge Alice's signature. Eve has to utilize a randomly generated k_A to create Alice's signature, random guesses would have only succeeded about a half of the time for each bit. Thus his forgery will be found by Bob with the probability larger than $1 - 1/2^{|k_A|}$, where $|k_A|$ denotes as the length of k_A . The probability $1 - 1/2^{|k_A|}$ is approximates to 1 if $|k_A| \gg 0$. Likewise, Charlie's signature can't be counterfeited by Eve since k_C is secret for Eve. If Eve can obtain k_C by certain way, however, the forgery strategy is also unlikely to succeed since Eve can't learn Charlie's measurement result. The correlations of quantum teleportation will be destroyed if Eve utilizes the wrong measurement result $\hat{M}_C$ to replace the right one.

However, the WLS scheme is insecure by presenting two attack strategies, one is that Alice can deduce Charlie's secret key and the other is that Charlie can forge Alice's valid signature at will.

2) Alice's forgery strategy: For symmetrical cryptosystem, one can derive encryption keys if there is an express integrity plaintext and the corresponding ciphertext. In the WLS protocol, Charlie's secret key K_C will be leaked to Alice by the following steps: In Step S2, Alice measures the particles M and particles 2 with Bell basis and obtains the measurement result β_C , i.e., the plaintext. Subsequently, in Step S3, Alice intercepts the signature $S_C = E_{K_C}(\beta_C)$ and measures it with Bell basis, i.e., she can get the corresponding ciphertext S_C . Therefore, Alice can get enough information about K_C . However, in our scheme, although Alice can

intercept Charlie's signature $|S_C\rangle = E_{K_C}(\hat{M}_C)$ and gets the signature message by measuring it with Bell basis, she can't obtain $\hat{M}_C$ which associates with k_C . That is to say, Alice can obtain the ciphertext $|S_C\rangle$ but not the plaintext $\hat{M}_C$, thereby she cannot get k_C .

3) Charlie's forgery strategy: In the WLS protocol, Charlie can forge Alice's signature for any $\otimes(\sigma_i|P_i\rangle)$ where $\sigma_i \in \{I, \sigma_z, \sigma_x, \sigma_y\}$ by such an attack strategy: In Step S2, Charlie intercepts the particles 3 and performs the operator σ_i on each particle in particles 3, and then resends them to Bob. After that, Charlie sends $\otimes((\sigma_i \otimes I)S_C^i)$ instead of S_C to Bob.

However, our scheme can resist this attack strategy by using decoy photons. The decoy states $\{|+\rangle, |-\rangle, |0\rangle, |1\rangle\}$ are randomly inserted in $|P_i\rangle$. Without knowing the positions of these decoy photons and the corresponding measurement basis, so if Charlie attempts to intercept $|P_i\rangle$ and resends $\otimes(\sigma_i|P_i^*\rangle)$ to Bob, his cheating strategy will be detected in public discussion with a probability of $1 - (1/3)^m$, where m is the number of the decoy photons, and $1/3$ is the probability for Charlie to pass the check in the situation of one decoy photon. The probability $1 - (1/3)^m \approx 1$ if m is large enough. And at the same time, the employment of decoy states can check the existence of eavesdropper with the probability $1 - (3/4)^m$.

Charlie may implement entangle auxiliary particle attack [24], to forge Alice's signature in the WLS protocol. However, our scheme can resist this attack since Charlie can't deduce which operator Alice selected through the two possible measurement result of the auxiliary particle.

B. Impossibility of disavowal

Alice can't disavowal her own signature since the signature corresponds to the secret key k_A . Suppose that Alice with suspected denies her signature. Bob just needs to decrypt the signature and determine whether the signature contains Alice's secret key. Bob confirms that Alice has indeed signed on the initial message if the signature corresponds to k_A . Likewise, Charlie can't disavowal his own signature as well.

V. CONCLUSIONS

In this paper, we put forward an improved quantum multi-signature protocol. Through the security analysis discussed above, we prove that our protocol can offer higher security than the WLS protocol. Besides, we modify the two details of the WLS protocol: one is to replace GHZ states with Bell states since the particles in the GHZ states kept by Alice are useless whether in the signature phase or the verification phase, the other is to lift restrictions on the eigenstate parameters in the initial message.

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*, vol. 22, pp. 644–654, Nov. 1976.
- [2] D. Gottesman and I. Chuang, "Quantum digital signatures," <http://www.arXiv:quant-ph/0105032v2>.
- [3] G.H. Zeng and C.H. Keitel, "Arbitrated quantum-signature scheme," *Phys. Rev. A*, vol. 65, 042312, Apr. 2002.
- [4] M. Curty and N. Lütkenhaus, "Comment on 'arbitrated quantum-signature scheme'," *Phys. Rev. A*, vol. 77, 046301, Apr. 2008.
- [5] G.H. Zeng, "Reply to 'Comment on Arbitrated quantum-signature scheme'," *Phys. Rev. A*, vol. 78, 016301, Jul. 2008.
- [6] Q. Li, W.H. Chan, and D.Y. Long, "Arbitrated quantum signature scheme using Bell states," *Phys. Rev. A*, vol. 79, 054307, May. 2009.
- [7] V. Dunjko, P. Wallden, and E. Andersson, "Quantum Digital Signatures without Quantum Memory," *Phys. Rev. Lett.*, vol. 112, 040502, Jan. 2014.
- [8] R.J. Collins, R.J. Donaldson, V. Dunjko, P. Wallden, and et al, "Realization of Quantum Digital Signatures without the Requirement of Quantum Memory," *Phys. Rev. Lett.*, vol. 113, 040502, Jul. 2014.
- [9] P. Wallden, V. Dunjko, A. Kent, and E. Andersson, "Quantum digital signatures with quantum-key-distribution components," *Phys. Rev. A*, vol. 91, 042304, Apr. 2015.
- [10] H. Lee, C. Hong, H. Kim, J. Lim, and H.J. Yang, "Arbitrated quantum signature scheme with message recovery," *Phys. Lett. A*, vol. 321, pp. 295–300, Feb. 2004.
- [11] G.H. Zeng, M.H. Lee, Y. Guo, and G.Q. He, "Continuous variable quantum signature algorithm," *Int. J. Quantum. Inform.*, vol. 5, pp. 553–573, Aug. 2007.
- [12] Y.G. Yang, "Multi-proxy quantum group signature scheme with threshold shared verification," *Chin. Phys. B*, vol. 17, pp. 415–418, Feb. 2008.
- [13] X.J. Wen, X.M. Niu, L.P. Ji, and Y. Tian, "A weak blind signature scheme based on quantum cryptography," *Opt. Commun.*, vol. 282, pp. 666–669, Feb. 2008.
- [14] M.H. Zhang and H.F. Li, "Weak blind quantum signature protocol based on entanglement swapping," *Photon. Res.*, vol. 3, pp. 324–328, Dec. 2015.
- [15] X.J. Wen, Y. Liu, and Y. Sun, "Quantum multi-signature protocol based on teleportation," *Z. Naturforsch.*, vol. 62, pp.147–151, Mar. 2007.
- [16] A. Karlsson and M. Bourennane, "Quantum teleportation using three-particle entanglement," *Phys. Rev. A*, vol. 58, pp. 4394–4400, Dec. 1998.
- [17] C.H. Bennett and G. Brassard, "Quantum cryptography: public key distribution and coin tossing," in *Proc. IEEE ICCSSP*, 1984, p. 175.
- [18] H.K. Lo and H.F. Chau, "Unconditional security of quantum key distribution over arbitrarily long distances," *Science*, vol. 283, pp. 2050–2056, Mar. 1999.
- [19] P. Shor and J. Preskill, "Simple proof of security of the BB84 quantum key distribution protocol," *Phys. Rev. Lett.*, vol. 85, pp. 441–444, Jul. 2000.
- [20] H. Barnum, C. Crepeau, D. Gottesman, A. Smith, and A. Tapp, "Authentication of quantum messages," in *Proc. IEEE SCFCS*, 2002, pp. 449–458.
- [21] P. Boykin and V. Roychowdhury, "Optimal encryption of quantum bits," *Phys. Rev. A*, vol. 67, 042317, Apr. 2003.
- [22] A. Barenco, D. Deutsch, A. Ekertand, and R. Jozsa, "Conditional quantum dynamics and logic gates," *Phys. Rev. Lett.*, vol. 74, pp. 4083–4086, May. 1995.
- [23] H. Buhrman, R. Cleve, J. Watrous and R. de Wolf, "Quantum fingerprinting," *Phys. Rev. Lett.*, vol. 87, 167902, Oct. 2001.
- [24] H.J. Zuo, K.J. Zhang, and T.T. Song, "Security analysis of quantum multi-signature protocol based on teleportation," *Quantum Inf. Process.*, vol. 12, pp. 2343–2353, Jul. 2013.



Minghui Zhang was born in Jilin, China, in 1986. She received the B.S. degree in electronics and information engineering from Northwest Agriculture & Forestry University, Xi'an, China, in 2008, and M.S. degree in control engineering from Beijing Jiaotong University, Beijing, China, in 2012. She is currently working toward the Ph.D. degree in information and communication engineering at the laboratory of quantum information, Northwestern Polytechnical University, Xi'an, China. Her current research is focused on the quantum information process and quantum communication, especially the quantum secure communication and quantum signature.



Huifang Li was born in 1962. He received the B.S. degree in electronic science and technology from Lanzhou University, Lanzhou, China, in 1984 and M.S. and Ph.D. degrees in electronic science and technology from Northwestern Polytechnical University, Xi'an, China, in 1990, and 2004, respectively. Since 1990, he has been a faculty member in Northwestern Polytechnical University, Xi'an, China, where he is currently a professor of school of electronic and information. He was a visiting scholar with the University of North Carolina at Charlotte, Charlotte, NC, USA, from 2010 to 2011. His current research interests include topics related to image detection and recognition, multimedia information process, quantum information processing and etc. His specific interests include the quantum secure communication and quantum signature.



Zhaoqiang Xia is a lecturer at Northwestern Polytechnical University Xi'an, China. He received the B.S. degree and Ph.D. degree at school of electronics and information from Northwestern Polytechnical University in 2008 and 2014, respectively. His current research interests include topics related to multimedia computing and analysis, quantum information processing and etc.