

# A Quantum Multi-Proxy Blind Signature Scheme Based on Entangled Four-Qubit Cluster State\*

Xu-Feng Niu (牛旭峰),<sup>1</sup> Jian-Zhong Zhang (张建中),<sup>1,†</sup> and Shu-Cui Xie (谢淑翠)<sup>2</sup>

<sup>1</sup>College of Mathematics and Information Science, Shaanxi Normal University, Xi'an 710119, China

<sup>2</sup>School of Science, Xi'an University of Posts and Telecommunications, Xi'an 710121, China

(Received December 15, 2017; revised manuscript received April 19, 2018)

**Abstract** In this paper, a multi-proxy blind signature scheme based on controlled quantum teleportation is proposed. Entangled four-qubit Cluster state functions as quantum channel, which needs less resource to complete the quantum multi-proxy blind signature. The scheme uses the physical characteristics of quantum mechanics to guarantee its blindness, unforgeability, and undeniability. The eavesdropping check is used to ensure the security. Our scheme has a foreseeable application to the E-business, E-governments, and etc.

**DOI:** 10.1088/0253-6102/70/1/43

**Key words:** multi-proxy blind signature, controlled quantum teleportation, cluster state, von Neumann measurement

## 1 Introduction

Digital signature is one of the most important parts in cryptography. It is an important technique to authenticate the identity and ensure the integrity of legal messages. It has been widely used in E-voting protocols, E-commerce systems and so on. However, the security of classical signature schemes depends on some computational problems that may be solved using quantum algorithms.<sup>[1–2]</sup> The security of quantum cryptography relies on the principles of quantum mechanics, thus quantum signature has attracted much attention. In 2001, Gottesman and Chuang proposed the first quantum signature scheme in Ref. [3]. Then Buhrman *et al.*<sup>[4]</sup> and Barnum *et al.*<sup>[5]</sup> made some significant attempts about quantum signature respectively. More recently, some other kinds of quantum signature schemes were presented, such as quantum multiple signature and quantum group signature.<sup>[6–7]</sup>

As an important cryptographic primitive, proxy signature was first introduced by Mambo, Usada, and Okamoto in 1996.<sup>[8]</sup> It allows a proxy signatory on behalf of an original signatory to sign a message. A quantum proxy signature scheme with public verifiability was presented by Zhou *et al.*<sup>[9]</sup> More recently, some quantum proxy signature schemes were presented. For example, Xu proposed a novel quantum proxy signature without entanglement.<sup>[10]</sup> In 2017, Yang *et al.* implemented a quantum proxy blind signature schemes with Genuine Seven-Qubit Entangled State.<sup>[11]</sup> In addition, Zeng *et al.* proposed a quantum proxy blind signature scheme.<sup>[12]</sup>

In 1982, a blind signature was introduced by David

Chaum.<sup>[13]</sup> It is called blind signature if the signatory generates a signature without revealing any information of the message.<sup>[13]</sup> Subsequently, blind quantum signature has attracted much attention. For example, in 2010, Wang *et al.* proposed a fair quantum blind signature scheme.<sup>[14]</sup> In 2016, Shao *et al.* proposed a quantum multi-proxy multi-blind-signature scheme combining the requirement for the proxy and blind signature scheme.<sup>[15]</sup> In addition, Guo *et al.* proposed a feasible blind quantum signature scheme.<sup>[16]</sup>

Our multi-proxy blind signature scheme has a wide application in practical life. For example, a company's president needs to sign an important and private document when he is temporal absence, he will delegate a group of department managers not a single one to blindly sign the document in order to prevent abuse of the signing authority and avoid exposure of the sensitive information.

The paper is outlined as follows: In the next section, we introduce the controlled quantum teleportation. In Sec. 3, we describe the quantum multi-proxy blind signature scheme in detail. The security analysis and discussion are presented in Sec. 4. Finally, conclusions are drawn in Sec. 5.

## 2 Controlled Quantum Teleportation

Our multi-proxy blind signature scheme is based on the controlled quantum teleportation, which takes the entangled four-qubit Cluster state as its quantum channel. It is given by

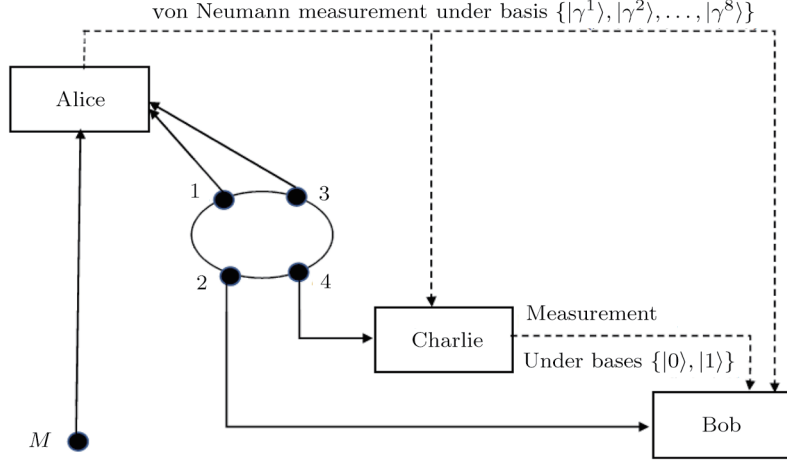
$$|\xi\rangle_{1234} = \frac{1}{2}(|0000\rangle + |0011\rangle + |1100\rangle - |1111\rangle)_{1234}. \quad (1)$$

\*Supported by the National Natural Science Foundation of China under Grant Nos. 61402275, 61402015, 61273311, the Natural Science Foundation of Shaanxi Province under Grant Nos. 2015JM6263, 2016JM6069, and the Fundamental Research Funds for the Central Universities under Grant No. GK201402004

<sup>†</sup>E-mail: 1416655910@qq.com

As shown in Fig. 1, this controlled quantum teleportation involves the following three partners: a sender Alice, a controller Charlie, and a receiver Bob. Alice holds par-

ticles (1, 3), Charlie, and Bob own particle 4 and particle 2, respectively.



**Fig. 1** The model of quantum teleportation.

Suppose that the quantum state of particle carrying message in Alice is

$$|\psi\rangle_M = (\alpha|0\rangle + \beta|1\rangle)_M, \quad (2)$$

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

The system quantum state composed of particle  $M$  and (1, 2, 3, 4) is given by

$$|\Psi\rangle_{M1234} = |\psi\rangle_M \otimes |\xi\rangle_{1234} = (\alpha|0\rangle + \beta|1\rangle)_M \otimes |\xi\rangle_{1234}. \quad (3)$$

(i) Alice performs a von Neumann measurement on particle  $M$  and particles (1, 3) with the basis  $\{|\gamma^1\rangle, |\gamma^2\rangle, |\gamma^3\rangle, |\gamma^4\rangle, |\gamma^5\rangle, |\gamma^6\rangle, |\gamma^7\rangle, |\gamma^8\rangle\}$ , where the quantum state of  $|\gamma^i\rangle$ , ( $i = 1, 2, 3, 4, 5, 6, 7, 8$ ) satisfies

$$\begin{aligned} |\gamma^1\rangle &= \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle), & |\gamma^2\rangle &= \frac{1}{\sqrt{2}}(|000\rangle - |111\rangle), \\ |\gamma^3\rangle &= \frac{1}{\sqrt{2}}(|001\rangle + |110\rangle), & |\gamma^4\rangle &= \frac{1}{\sqrt{2}}(|001\rangle - |110\rangle), \\ |\gamma^5\rangle &= \frac{1}{\sqrt{2}}(|010\rangle + |101\rangle), & |\gamma^6\rangle &= \frac{1}{\sqrt{2}}(|010\rangle - |101\rangle), \\ |\gamma^7\rangle &= \frac{1}{\sqrt{2}}(|100\rangle + |011\rangle), & |\gamma^8\rangle &= \frac{1}{\sqrt{2}}(|100\rangle - |011\rangle). \end{aligned} \quad (4)$$

The measurement will collapse the state of  $|\Psi\rangle_{M1234}$  into one of the following states

$$\begin{aligned} \langle\gamma^1_{M13}|\Psi\rangle_{M1234} &= \frac{1}{2\sqrt{2}}(\alpha|00\rangle - \beta|11\rangle)_{24}, \\ \langle\gamma^2_{M13}|\Psi\rangle_{M1234} &= \frac{1}{2\sqrt{2}}(\alpha|00\rangle + \beta|11\rangle)_{24}, \\ \langle\gamma^3_{M13}|\Psi\rangle_{M1234} &= \frac{1}{2\sqrt{2}}(\alpha|01\rangle + \beta|10\rangle)_{24}, \end{aligned}$$

$$\langle\gamma^4_{M13}|\Psi\rangle_{M1234} = \frac{1}{2\sqrt{2}}(\alpha|01\rangle - \beta|10\rangle)_{24},$$

$$\langle\gamma^5_{M13}|\Psi\rangle_{M1234} = \frac{1}{2\sqrt{2}}(\alpha|10\rangle + \beta|01\rangle)_{24},$$

$$\langle\gamma^6_{M13}|\Psi\rangle_{M1234} = \frac{1}{2\sqrt{2}}(\alpha|10\rangle - \beta|01\rangle)_{24},$$

$$\langle\gamma^7_{M13}|\Psi\rangle_{M1234} = \frac{1}{2\sqrt{2}}(-\alpha|11\rangle + \beta|00\rangle)_{24},$$

$$\langle\gamma^8_{M13}|\Psi\rangle_{M1234} = \frac{1}{2\sqrt{2}}(\alpha|11\rangle + \beta|00\rangle)_{24}. \quad (5)$$

Then Alice sends her measurement result to Charlie and Bob.

(ii) Charlie sends particle 4 through a Hadamard gate, the corresponding states in Eq. (5) can be changed into

$$\langle\gamma^1_{M13}|\Psi\rangle_{M1234}^* = \frac{1}{4}(\alpha|00\rangle + \alpha|01\rangle - \beta|10\rangle + \beta|11\rangle)_{24},$$

$$\langle\gamma^2_{M13}|\Psi\rangle_{M1234}^* = \frac{1}{4}(\alpha|00\rangle + \alpha|01\rangle + \beta|10\rangle - \beta|11\rangle)_{24},$$

$$\langle\gamma^3_{M13}|\Psi\rangle_{M1234}^* = \frac{1}{4}(\alpha|00\rangle - \alpha|01\rangle + \beta|10\rangle + \beta|11\rangle)_{24},$$

$$\langle\gamma^4_{M13}|\Psi\rangle_{M1234}^* = \frac{1}{4}(\alpha|00\rangle - \alpha|01\rangle - \beta|10\rangle - \beta|11\rangle)_{24},$$

$$\langle\gamma^5_{M13}|\Psi\rangle_{M1234}^* = \frac{1}{4}(\alpha|10\rangle + \alpha|11\rangle + \beta|00\rangle - \beta|01\rangle)_{24},$$

$$\langle\gamma^6_{M13}|\Psi\rangle_{M1234}^* = \frac{1}{4}(\alpha|10\rangle + \alpha|11\rangle + \beta|01\rangle - \beta|00\rangle)_{24},$$

$$\langle\gamma^7_{M13}|\Psi\rangle_{M1234}^* = \frac{1}{4}(\alpha|11\rangle - \alpha|10\rangle + \beta|00\rangle + \beta|01\rangle)_{24},$$

$$\langle \gamma_{M13}^8 | \Psi \rangle_{M1234}^* = \frac{1}{4}(\alpha|10\rangle - \alpha|11\rangle + \beta|00\rangle + \beta|01\rangle)_{24}. \quad (6)$$

(iii) If Charlie agrees the two parties of communication to complete their teleportation, he performs a single particle measurement on particle 4 with the basis  $\{|0\rangle, |1\rangle\}$ . Suppose that Alice's measurement outcome is  $|\gamma^1\rangle_{M13}$ , Charlie's measurement will collapse particle 2 into one of the following states

$$\langle 0_4 | \langle \gamma_{M13}^1 | \Psi \rangle_{M1234}^* = \frac{1}{4}(\alpha|0\rangle - \beta|1\rangle)_2,$$

$$\langle 1_4 | \langle \gamma_{M13}^1 | \Psi \rangle_{M1234}^* = \frac{1}{4}(\alpha|0\rangle + \beta|1\rangle)_2. \quad (7)$$

Then Charlie sends his measurement result to Bob.

(iv) Because of the entanglement property,<sup>[17–24]</sup> Bob can perform an appropriate unitary operator on particle 2 to rebuild the original state  $|\psi\rangle_M$  according to Alice's, Charlie's measurement results. The corresponding relationship between the measurement results and Bob's unitary transformations is in Table 1.

**Table 1** The relationship between Alice's, Charlie's measurement outcomes, and Bob's operation.

Alice's measurement outcome	Charlie's measurement outcome	Bob's operation
$ \gamma^1\rangle_{M13}$	$ 0\rangle_4$	$(\sigma_z)_2$
	$ 1\rangle_4$	$I_2$
$ \gamma^2\rangle_{M13}$	$ 0\rangle_4$	$I_2$
	$ 1\rangle_4$	$(\sigma_z)_2$
$ \gamma^3\rangle_{M13}$	$ 0\rangle_4$	$I_2$
	$ 1\rangle_4$	$(-\sigma_z)_2$
$ \gamma^4\rangle_{M13}$	$ 0\rangle_4$	$(\sigma_z)_2$
	$ 1\rangle_4$	$-I_2$
$ \gamma^5\rangle_{M13}$	$ 0\rangle_4$	$(\sigma_X)_2$
	$ 1\rangle_4$	$(i\sigma_Y)_2$
$ \gamma^6\rangle_{M13}$	$ 0\rangle_4$	$(i\sigma_Y)_2$
	$ 1\rangle_4$	$(\sigma_X)_2$
$ \gamma^7\rangle_{M13}$	$ 0\rangle_4$	$(-i\sigma_Y)_2$
	$ 1\rangle_4$	$(\sigma_X)_2$
$ \gamma^8\rangle_{M13}$	$ 0\rangle_4$	$(\sigma_X)_2$
	$ 1\rangle_4$	$(-i\sigma_Y)_2$

### 3 Quantum Multi-Proxy Blind Signature Scheme

In our scheme, four participants are defined as follows.

(i) Alice: the message owner; (ii)  $U_j$ : one member of proxy signers ( $j = 1, 2, \dots, t$ ); (iii) Charlie: the original signer; (iv) Bob: the verifier.

The detailed procedure of our scheme can be described as follows.

#### 3.1 Initial Phase

(i) Alice shares secret key  $K_{AB}$  with Bob,  $K_{AU_j}$  ( $j = 1, 2, \dots, t$ ) with signer  $U_j$ , respectively. In addition, Bob establishes secret key  $K_{BC}$  with Charlie,  $K_{BU_j}$  with  $U_j$  ( $j = 1, 2, \dots, t$ ). These distribution tasks can be fulfilled via QKD protocols, which have been proved unconditionally security.<sup>[25–28]</sup>

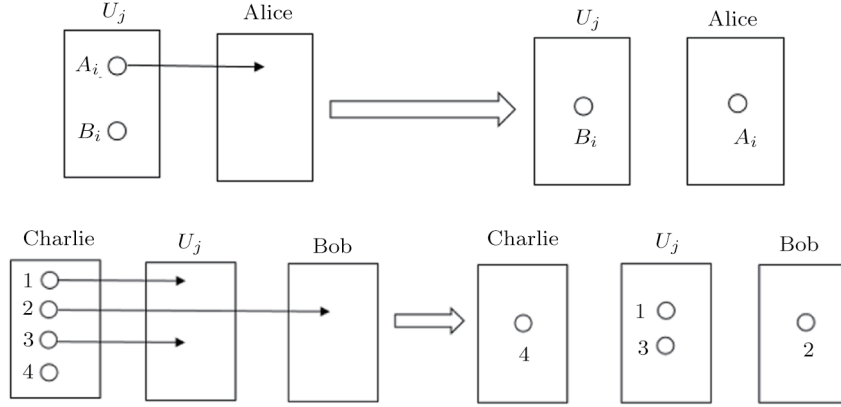
(ii)  $U_j$  prepares  $Q$  ( $Q \gg n$ ) EPR pairs such that

$$|\psi_i\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{A_i B_i}, \quad (8)$$

where the superscripts  $A_i$  and  $B_i$  indicate the  $i$ -th of two entangled particles. And in each EPR pair,  $U_j$  sends particle  $A_i$  to Alice, while he keeps particle  $B_i$ . In addition, Charlie generates  $TN$  ( $TN \gg tn$ ) four-qubit Cluster

states as showed in Eq. (1) to be the quantum channel. He sends particle 2 to Bob, (1, 3) to  $U_j$  while leaving the last one 4 to himself. The schematic of transmission on the  $i$ -th particles is shown in Fig. 2.

(iii) To guarantee the security of the quantum channel, Charlie and  $U_j$  arrange eavesdropping checks. On the one hand, Charlie chooses  $TN$ - $tn$  groups of particle 4 randomly, remembers the positions and performs a measurement with the basis  $\{|0\rangle, |1\rangle\}$ , then Charlie publishes the positions. According to Charlie's published positions,  $U_j$  performs measurement on the particles (1, 3) with the basis  $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$ , Bob performs measurement on the particle 2 with the basis  $\{|0\rangle, |1\rangle\}$ . After that, Charlie,  $U_j$  and Bob all declare their measurement outcomes. Here, the declared order of them should be random. If their measurement outcomes satisfy the relationship in Table 2 or error rate is less than the threshold value, the quantum channel is safe. Otherwise, they give up this process. On the other hand,  $U_j$  also arranges eavesdropping check by randomly choosing  $Q$ - $n$  EPR pairs to ensure the safety of the quantum channel between  $U_j$  and Alice. This process is similar to the above mentioned, we do not repeat the details.



**Fig. 2** Schematic of transmission on the  $i$ -th particles.

**Table 2** The relationship between Charlie's,  $U_j$ 's, and Bob's measurement results.

Charlie's measurement result	$U_j$ 's measurement result	Bob's measurement result
$ 0\rangle$	$ 00\rangle$	$ 0\rangle$
$ 0\rangle$	$ 10\rangle$	$ 1\rangle$
$ 1\rangle$	$ 01\rangle$	$ 0\rangle$
$ 1\rangle$	$ 11\rangle$	$ 1\rangle$

### 3.2 Blind the Message Phase

(i) Alice transforms her message into an  $n$ -bit message string  $m = \{m(1), m(2), \dots, m(n)\} = \{m(i), i = 1, 2, \dots, n\}$ , where  $m(i) \in \{0, 1\}$ .

(ii) Alice measures her particle sequence according to message  $m$ . If  $m(i) = 0$ , she measures particle  $A_i$  with the basis  $\{|0\rangle, |1\rangle\}$ . Otherwise, she measures under the basis  $\{|+\rangle, |-\rangle\}$ . The measurement results can be denoted as  $m' = \{m'(1), m'(2), \dots, m'(n)\} = \{m'(i), i = 1, 2, \dots, n\}$ , where  $m'(i) \in \{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$  and Alice transforms the measurement results into classical binary sequence  $M = \{M(1), M(2), \dots, M(n)\} = \{M(i), i = 1, 2, \dots, n\}$ , where  $M(i) \in \{00, 01, 10, 11\}$ . The measuring and encoding rules for quantum states are shown in Table 3. Now, message  $m$  ( $n$ -bit) could be blinded as  $M$  ( $2n$ -bit).

**Table 3** The measuring and encoding rules for quantum states.

$m(i)$	Measuring base	Measuring result	Encoding rule
0	$\{ 0\rangle,  1\rangle\}$	$ 0\rangle$	00
0	$\{ 0\rangle,  1\rangle\}$	$ 1\rangle$	01
1	$\{ +\rangle,  -\rangle\}$	$ +\rangle$	10
1	$\{ +\rangle,  -\rangle\}$	$ -\rangle$	11

(iii) Alice gets the secret message  $M'$  by encrypting  $M$  with one-time pad and key  $K_{AB}$ , we have

$$M' = E_{K_{AB}}\{M(1), M(2), \dots, M(n)\}.$$

Alice sends  $M'$  to Bob.

### 3.3 Authorizing and Signing Phase

We choose a proxy signer  $U_j$  on behalf of all proxy signers to complete this signature.

(i) In order to distinguish every proxy signers, Alice generates a unique serial  $SN$ , and transforms it to a quantum state sequence  $|SN\rangle$  in the basis  $\{|0\rangle, |1\rangle\}$ . Then she encrypts  $|SN_j\rangle$  with key  $K_{AU_j}$ , and sends the secret state to  $U_j$  via a quantum channel.

(ii) After  $U_j$  received  $E_{K_{AU_j}}(|SN_j\rangle)$ , he decrypts it to gain  $|SN_j\rangle$ .  $U_j$  performs a von Neumann measurement on particle  $B_i$  and particles (1, 3), he gains  $\beta_{U_j} = (\{\beta(i)_{B_{i13}}, i = 1, 2, \dots, n\}, |SN_j\rangle)$  by combining the measurement results and  $|SN_j\rangle$ , now  $\beta_{U_j}$  is  $U_j$ 's proxy signature of the blinded message  $M$ . Then  $U_j$  encrypts  $\beta_{U_j}$  with key  $K_{BU_j}$  to get the message  $S_{U_j} = E_{K_{BU_j}}(\beta_{U_j})$ , he sends it to Bob and also sends  $\beta_{U_j}$  to Charlie as his proxy request.

(iii) After receiving  $U_j$ 's proxy request  $\beta_{U_j}$ , Charlie will help  $U_j$  and Bob to complete their teleportation if he agrees  $U_j$  to sign the message. Charlie operates a Hadamard gate on particle 4 and then he measures particle 4 with the basis  $\{|0\rangle, |1\rangle\}$ , and he combines the measurement result  $\beta(i)_4$  with  $|SN_j\rangle$  to get

$$\beta_{C_j} = (\{\beta(i)_4, i = 1, 2, \dots, n\}, |SN_j\rangle),$$

where  $\beta(i)_4 \in \{|0\rangle, |1\rangle\}$ . Then he encrypts  $\beta_{C_j}$  with key  $K_{BC}$  to get the message  $S_{C_j} = E_{K_{BC}}(\beta_{C_j})$ , he sends it to Bob. If Charlie does not agree  $U_j$  to sign the message, he terminates this teleportation.

### 3.4 Verifying Phase

(i) Bob decrypts  $M'$  to acquire the message  $M$ .

(ii) Bob gets  $\beta_{U_j}$  and  $\beta_{C_j}$  by using  $K_{BU_j}$  and  $K_{BC}$  to decrypt  $S_{U_j}$  and  $S_{C_j}$  respectively. Then Bob performs a proper unitary operator on particle 2 to rebuild the unknown state. In Table 1, we show the relationship between  $U_j$ 's Charlie's measurement results and Bob's unitary transformation (we replace Alice's measurement results by  $U_j$ 's).

(iii) Bob encodes particle 2 to get a two bits classical string  $c(j)$  by using the similar strategy as shown in Subsec. 3.2. If  $c(j) = M$ , this signature is valid, otherwise, he rejects it.

(iv) Bob collects  $\{(S_{U_j}, S_{C_j}), j = 1, 2, \dots, t\}$ . Then according to Subsec. 3.2, he gets the message  $\{c(j), j = 1, 2, \dots, t\}$ . If  $c(j) = M$  ( $j = 1, 2, \dots, t$ ), Bob will ensure this signature and get the final signature  $S = \{\beta_{U_1}, \beta_{U_2}, \dots, \beta_{U_t}\}$ , otherwise, he terminates the signature.

## 4 Security Analysis and Discussion

In this section, we will prove that this scheme satisfies the properties of blindness, undeniability, and unforgeability.

### 4.1 Message's Blindness

According to Subsec. 3.2, the message  $m$  has been transformed into  $m' = \{m'(1), m'(2), \dots, m'(n)\}$ , where each  $m'(i) \in \{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ . If  $U_j$  attempts to get the message  $m$ , the only way is to perform measurements. However, he has no idea of Alice's measurement basis of particle  $A_i$ , which means  $U_j$  can not acquire  $m'$  and  $m$ . Therefore, each proxy signers can not know the content of the message  $m$  when he signs it. This means the message is blind for proxy signers.

### 4.2 Impossibility of Denial

In this scheme, we prove that Charlie can not deny his delegation and  $U_j$  can not disavow his signature. According to Step 2 in Subsec. 3.2, Bob decrypts messages  $S_{C_j} = E_{K_{BC}}(\beta_{C_j})$  with keys  $K_{BC}$  can get Charlie's authorization  $\beta_{C_j}$ . Similarly, Bob can get  $U_j$ 's proxy request and his serial number  $|SN_j\rangle$ . All keys are distributed via QKD protocols, which have been proved unconditionally and all messages are sent through the secure quantum channel. Therefore, Charlie can not deny his delegation and  $U_j$  can not disavow his signature.

### 4.3 Impossibility of Forgery

In the following, we will show that our scheme is secure against the forgery of both internal attacker and outsider attacker. First of all, we demonstrate that it is impossible for the dishonest participants to forge message and signature. Suppose Bob is dishonest and he attempts to forge message or signature, according to Subsec. 3.2, Bob can not obtain particle  $A_i$ , he has no idea of Alice's measurement basis. It means that Bob can not get the true signature. If Bob randomly uses basis  $\{|0\rangle, |1\rangle\}$  or  $\{|+\rangle, |-\rangle\}$ , he will obtain the correct results at a probability  $1/2^n$ , and this probability will vanish to zero if  $n$  is large enough. Therefore, the dishonest inner attacker can not forge message and signature. Secondly, we indicate that it is impossible for the outsider attacker Eve to forge signature. Eve can forge signature successfully unless he has the secret key  $K_{BU_j}$ . However, the security of the shared key  $K_{BU_j}$  is guaranteed by unconditionally secure QKD protocols. That is, Eve's forgery can be avoided.

## 5 Conclusion

In this paper, we propose a quantum multi-proxy blind signature scheme, which uses entangled four-qubit Cluster state as quantum channel. The security of our scheme is guaranteed by the quantum one-time pad and quantum key distribution, which is different from the previous signature schemes in classical cryptography. In addition, different from some existing quantum signature schemes, our scheme has some advantages. Firstly, our scheme is based on entangled four-qubit Cluster state, which needs less resource rather than the quantum signature proposed in Refs. [29–30]. Secondly, differing from the quantum blind signature scheme,<sup>[31]</sup> our scheme has arranged eavesdropping checks to ensure the security. Thirdly, our scheme has a stronger security because of the cluster state's maximum connectedness and persistency of entanglement. Fourthly, our scheme adopts von Neumann measurement and single particle measurement, which are easy to implement with current technologies and experimental conditions. However, the received state's fidelity may reduce because of the experimental environment, and this will be a question to be studied further.

## References

- [1] P. Shor, SIAM J. Comput. **26** (1997) 1484.
- [2] L. K. Grover, arXiv:quant-ph/9605043.
- [3] I. L. Chuang, D. Gottesman, arXiv:quant-ph/0105032.
- [4] H. Buhrman, R. Cleve, J. Watrous, *et al.*, Phys. Rev. Lett. **87** (2001) 167902.
- [5] H. Buhrman, C. Crepeau, D. Gottesman, *et al.*, *Authentication of Quantum Messages*, IEEE Comput. Soc. Press, Canada (2002).
- [6] X. J. Wen, Y. Tian, L. P. Ji, and X. M. Niu, Phys. Scr. **81** (2010) 055001.
- [7] Y. Tian, H. Chen, S. F. Ji, *et al.*, Opt. Quant. Electron. **46** (2014) 769.
- [8] M. Mambo, K. Usada, and E. Okamoto, IEICE Trans. Fuan. Electr. **79** (1996) 1338.
- [9] J. X. Zhou, Y. J. Zhou, X. X. Niu, and Y. X. Yang, Sci. China Ser. G. **54** (2011) 1828.

- 
- [10] G. B. Xu, Int. J. Theor. Phys. **54** (2015) 2605.
- [11] Y. Y. Yang, S. C. Xie, and J. Z. Zhang, Int. J. Theor. Phys. **56** (2017) 2293.
- [12] C. Zeng, J. Z. Zhang, and S. C. Xie, Int. J. Theor. Phys. **56** (2017) 1762.
- [13] D. Chaum, Lect. Notes. Comput. Sc. **15** (1983) 199.
- [14] T. Y. Wang and Q. Y. Wen, Chin. Phys. B **19** (2010) 66.
- [15] A. X. Shao, J. Z. Zhang, and S. C. Xie, Int. J. Theor. Phys. **55** (2016) 5216.
- [16] W. Guo, J. Z. Zhang, Y. P. Li, *et al.*, Int. J. Theor. Phys. **55** (2016) 3524.
- [17] J. S. Bell, Physica **1** (1964) 195.
- [18] N. Gisin, Phys. Lett. A **154** (1991) 201.
- [19] S. Popescu and D. Rohrlich, Phys. Lett. A **166** (2016) 293.
- [20] R. Chaves, Phys. Rev. Lett. **116** (2016) 010402.
- [21] D. Rosset, C. Branciard, T. J. Barnea, *et al.*, Phys. Rev. Lett. **116** (2016) 010403.
- [22] N. Gisin, Q. Mei, A. Tavakoli, *et al.*, Phys. Rev. A **96** (2017) 020304(R).
- [23] M. X. Luo, Phys. Rev. Lett. **120** (2018) 140402.
- [24] M. J. Hu, Z. Y. Zhou, X. M. Hu, *et al.*, arXiv:quant-ph/1609.01863.
- [25] P. Shor and J. Preskill, Phys. Rev. Lett. **85** (2000) 441.
- [26] D. Mayers, J. Assoc.: Comput. Math. **48** (2001) 351.
- [27] H. K. Lo, J. Phys. A: Math. Gen. **34** (2012) 6957.
- [28] H. Inamon, N. Lutkenhaus, and D. Mayers, Eur. Phys. J. D. **41** (2007) 599.
- [29] H. J. Cao, Y. Y. Zhu, and P. F. Li, Int. J. Theor. Phys. **53** (2014) 419.
- [30] H. J. Cao, Y. F. Yu, Q. Song, and L. X. Gao, Int. J. Theor. Phys. **54** (2015) 1325.
- [31] L. Fan, Int. J. Theor. Phys. **55** (2016) 1558.