Quantum Communication Scheme for Blind Signature with Arbitrary Two-Particle Entangled System

Jinjing Shi[1], Ronghua Shi[1], Xiaoqi Peng[2] and Moon Ho Lee[3], *Senior Member, IEEE*
[1]School of Information Science & Engineering, Central South University, Changsha 410083, China.
[2]Department of Information Science & Engineering, Hunan First Normal University, Changsha 410205, China.
[3]Institute of Information and Communication, Chonbuk National University, Chonju 561-756, Korea.

***Abstract*—A quantum communication scheme for blind signature is proposed based on two-particle entangled quantum system to create a novel systemetrical quantum cryptosystem. All the messages are encrypted by the private key of the sender Alice during the communication and the authenticity verification of signatures and an arbitrator's batch efficient proxy signature is applied. It demonstrates that a large number of blind signatures can be derived with the characteristics: impossibility of forgery, impossibility of disavowal by the signatory and impossibility of denial by the receiver. The security of our scheme depends on the two-particle entangled system which cannot be deterministically intercepted.**

***Index Terms*—Quantum communication, Blind signature, Proxy signature, Quantum signature, Quantum cryptography.**

I. Introduction

A classical digital signature is an electronic signature that can be used to authenticate the identity of the sender of a message or the signer of a document. It ensures that the original content of the message or document is unchanged [1]. Digital signatures are easily transportable, cannot be imitated by someone else, and can be automatically time-stamped. A blind signature introduced by David Chaum [2] is typically employed in privacy-related protocols and realized by using a number of common public key signing schemes [3]. Fan and Lei [4] proposed a scheme based on the quadratic residues problem in 1996. Zeng [5]–[7] has introduced a quantum signature scheme based on the correlation of quantum entanglement states in 2001. Gottesman and Chuang [8] have also proposed a quantum digital signature scheme based on quantum one-way function. In 2008, Wen [9] proposed a weak blind signature scheme based on quantum cryptography, Shi *et al.* introduced a multiparty quantum proxy group signature scheme for the entangled-state message [10]–[12] and Lee also presented two quantum signature schemes with message recovery [13]. In 2008, Yang and Wen suggested a multi-proxy quantum group signature scheme with threshold shared verification [14], in which only the cooperation of all the signers in the proxy group can generate the proxy signature on behalf of the original signer.

In this paper, a quantum communication scheme for blind signature is proposed to create a new systemetrical quantum key cryptosystem with two-particle entangled quantum system. A third fully trusted participant Charlie (the arbitrator and proxy) is involved. The responsibility of Charlie is to help Alice and Bob trust each other before communication, verify the legalization and authenticity of the trying blind signature and provide batch efficient proxy blind signatures to Alice. During all the communications, two-particle entangled quantum system are applied to create the quantum message strings and to make distribution of keys. The rest of this paper is organized as follows. Sect. II proposes the quantum communication scheme for blind signature. The security analysis and discussions are made in Sect. III. Finally, the conclusions are drawn in Sect. IV.

II. Quantum Communication Scheme for Blind Signature

The classical blind signature is described like this: Bob is a notary, Alice expects that Bob can sign the message from her and she does not let Bob understand the content of the message. Bob does not care the content of the message and only testifies he has notated it at some time [3]. The quantum communication scheme for blind signature utilizes the arbitrary two-particle entangled quantum system [15] which can be expressed as follows,

$$|\varphi\rangle = a_{00}|00\rangle + a_{01}|01\rangle + a_{10}|10\rangle + a_{11}|11\rangle, \tag{1}$$

where $|a_{00}|^2 + |a_{01}|^2 + |a_{10}|^2 + |a_{11}|^2 = 1$.

Suppose that Alice and Bob share a maximally entangled state:

$$|\varphi_{AB}\rangle = \frac{1}{2}(|00\rangle_{AB} + |01\rangle_{AB} + |10\rangle_{AB} + |11\rangle_{AB}), \tag{2}$$

Alice and Charlie share a maximally entangled state:

$$|\varphi_{AC}\rangle = \frac{1}{2}(|00\rangle_{AC} + |01\rangle_{AC} + |10\rangle_{AC} + |11\rangle_{AC}), \tag{3}$$

and Bob and Charlie share a maximally entangled state:

$$|\varphi_{BC}\rangle = \frac{1}{2}(|00\rangle_{BC} + |01\rangle_{BC} + |10\rangle_{BC} + |11\rangle_{BC}) \tag{4}$$

according to Eq. (1).

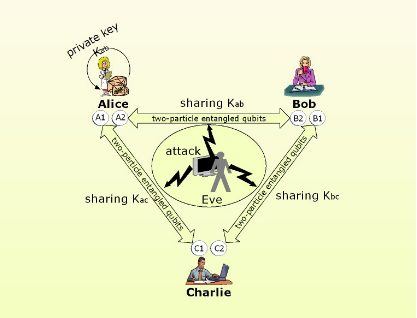
private key
Kab
Alice
Bob
sharing Kab
two-particle entangled qubits
A1
A2
B2
B1
attack
Eve
sharing Kac
sharing Kbc
two-particle entangled qubits
two-particle entangled qubits
C1
C2
Charlie

Fig. 1. The relationship among Alice, Bob and Charlie for the distribution of quantum keys in the quantum communication scheme of blind signature.

The quantum communication scheme for blind signature can be presented as following aspects: preparation of quantum keys and messages, trying quantum blind signature, verification and batch quantum blind signature.

A. *Preparation of Quantum Keys and Messages*

Step 1. Alice owns a private key K_a which is used to encrypt her messages that are excepted to be signed by Bob. Secret keys K_{ab}, K_{ac} and K_{bc} are distributed to Alice, Bob and Charlie, where K_{ab} is employed in the communication between Alice and Bob and it only can be used twice for Bob's encrypting and Alice's decrypting in the first communication, then it will be discarded. K_{ac} and K_{bc} are employed in the communications between Alice and the arbitrator Charlie and between Bob and Charlie respectively. The relationship among Alice, Bob and Charlie for the distribution of quantum keys is given in Fig. 1.

Step 2. Alice prepares quantities of messages which are expected to be signed by Bob which can be described as a matrix

$$M = \begin{array}{c} M_1 \\ M_2 \\ \vdots \\ M_i \\ \vdots \\ M_m \end{array} \begin{bmatrix} m_{11} & m_{12} & \cdots & m_{1j} & \cdots & m_{1n} \\ m_{21} & m_{22} & \cdots & m_{2j} & \cdots & m_{2n} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ m_{i1} & m_{i2} & \cdots & m_{ij} & \cdots & m_{in} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ m_{m1} & m_{m2} & \cdots & m_{mj} & \cdots & m_{mn} \end{bmatrix}, \quad (5)$$

there are m messages $\{M_1, M_2, \ldots M_m\}$ and each message has n bits, for example:

$$M_i = \begin{bmatrix} m_{i1} & m_{i2} & \cdots & m_{ij} & \cdots & m_{in} \end{bmatrix}, \quad (6)$$

and M_1 is chosen to be considered as the trying message for the first trying quantum blind signature.

The quantum communication scheme for blind signature can be briefly defined as following seven steps corresponding to Fig. 2. (1) Alice firstly sends a trying message M_1 encrypted by her private key K_a to Bob. (2) Bob adds his personal information to this secret message and encrypts it by the shared key K_{ab} with Alice. (3) Bob sends the secret message with his personal information to Alice which is called the trying blind signature. (4) Alice receives this trying blind signature and decrypts it by the shared key K_{ab} with Bob and judge whether the secret trying message has been falsified, and if falsified the signature process stops. (5) Alice and Bob separately inform Charlie the result of the signature and Charlie verifies legalization and authenticity of the trying signature. (6) If the verification is successful, Alice sends quantities of messages to Charlie. (7) Charlie signs quantities of messages from Alice with the the combination of Bob's personal information and Charlie's random checking photons.

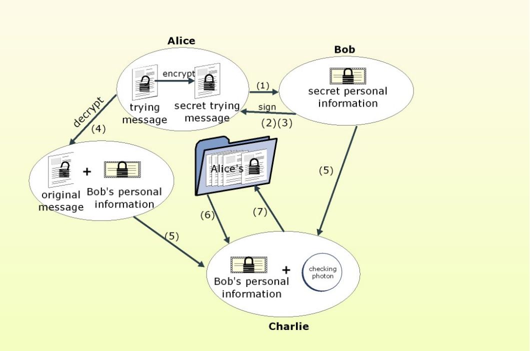

Fig. 2. The process of quantum communication scheme for blind signature. (1) $\sim$ (7) denote that seven steps of quantum communication scheme for blind signature.

B. *Trying Quantum Blind Signature*

Step 1. Alice creates a qubit string $|\psi_{M_1}\rangle$ for the trying message. She transforms the trying message M_1 into a qubit string $|\psi_{M_1}\rangle$, and there are n qubits in this string such as $|\psi_{M_1}\rangle$, i.e.,

$$|\psi_{M_1}\rangle = \{|\psi_{11}\rangle, |\psi_{12}\rangle, \ldots, |\psi_{1j}\rangle, \ldots, |\psi_{1n}\rangle\}, \quad (7)$$

where $|\psi_{1j}\rangle$ is a single qubit in the string $|\psi_{M_1}\rangle$. Any qubit $|\psi_{1j}\rangle (j = 1, 2, \ldots, n)$ in $|\psi_{M_1}\rangle$ can be expressed as a superposition of the two eigenstates $\{|0\rangle, |1\rangle\}$, ,i.e.,

$$|\psi_{1j}\rangle = \alpha_{1j}|0\rangle + \beta_{1j}|1\rangle, \quad (8)$$

where α_{1j} and β_{1j} are complex number satisfying $|\alpha_{1j}|^2 + |\beta_{1j}|^2 = 1$. The general quantum message states $|\psi_{M_i}\rangle$ can be expressed as the tensor product of the qubits in that message string, i.e.,

$$\begin{aligned} |\psi_{M_i}\rangle &= |\psi_{i1}\rangle \otimes |\psi_{i2}\rangle \cdots \otimes |\psi_{ij}\rangle \cdots \otimes |\psi_{in}\rangle \\ &= sum_{\gamma=1}^{2^n} \lambda_{i\gamma} |\mu_{i\gamma}^1 \mu_{i\gamma}^2 \cdots \mu_{i\gamma}^j \cdots \mu_{i\gamma}^n\rangle, \end{aligned} \quad (9)$$

where $\sum_{\gamma=1}^{2^n} |\lambda_{i\gamma}|^2 = 1$ and $\mu_{i\gamma}^j \in \{0, 1\}$.

Step 2. Alice transforms her private key $K_a = \{|K_a^1\rangle, |K_a^2\rangle, \ldots, |K_a^j\rangle, \ldots, |K_a^n\rangle\}$ to a sequence of measurement operators M_{k_a},i.e.,

$$M_{k_a} = \{M_{k_a^1}^1, M_{k_a^2}^2, \ldots, M_{k_a^j}^j, \ldots, M_{k_a^n}^n\}, \quad (10)$$

where the operator $M_{k_a^j}^j$ is defined to arise from the key $|K_a^j\rangle$ for $j \in \{1, 2, \ldots, n\}$. A more detailed method is described in Ref. [5]. After the transformation, Alice measures the information string of qubits $|\psi_{M_1}\rangle$ with M_{k_a} to derive a secret string

$$|T\rangle = M_{k_a}|\psi_{M1}\rangle = \{|t_1\rangle, |t_2\rangle, \ldots, |t_j\rangle, \ldots, |t_n\rangle\}, \quad (11)$$

where $|t_j\rangle = M_{k_a^j}^j |\psi_{1j}\rangle$ and it denotes the j-th qubit in the

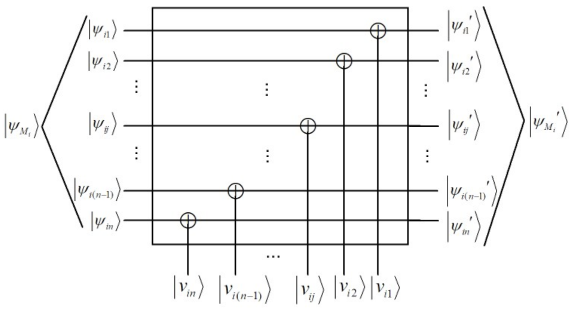

Fig. 3. The comparison quantum circuit for verifying whether $|\psi'_{M_i}\rangle$ matches to $|\psi_{M_i}\rangle$.

string of $|T\rangle$. Thus $|T\rangle$ is the secret state of the trying message and she directly sends it to Bob and expects Bob to sign it.

Step 3. Bob adds his personal information to the secret message $|T\rangle$ though he doesn't understand the content of it.

(1) Bob creates a qubit string $|\psi_p\rangle$ of his own personal information which contains n qubits, i.e.,

$$|\psi_p\rangle = \{|\psi_{p_1}\rangle, |\psi_{p_2}\rangle, \ldots, |\psi_{p_j}\rangle, \ldots, |\psi_{p_n}\rangle\}, \qquad (12)$$

where $|\psi_{p_j}\rangle$ is a single qubit in $|\psi_p\rangle$. Any qubit $|\psi_{p_j}\rangle(j = 1, 2, \ldots, n)$ in $|\psi_p\rangle$ can be expressed as a superposition of the two eigenstates $\{|0\rangle, |1\rangle\}$ like $|\psi_{1j}\rangle$ in the Step 1.

(2) Bob doesn't expect Alice know the content of his personal information either and he encrypts $|\psi_p\rangle$ with K_{bc}. He relates the key $K_{bc} = \{|K_{bc}^1\rangle, |K_{bc}^2\rangle, \ldots, |K_{bc}^j\rangle, \ldots, |K_{bc}^n\rangle\}$ to a sequence of measurement operators $M_{k_{bc}}$ and the modus is like Eq.(10). Then Bob measures the personal information string $|\psi_p\rangle$ with $M_{k_{bc}}$ and obtains

$$|P\rangle = M_{k_{bc}}|\psi_p\rangle = \{|P_1\rangle, |P_2\rangle, \ldots, |P_j\rangle, \ldots, |P_n\rangle\}, \quad (13)$$

where $|p_j\rangle$ denotes the j-th qubit in the string of $|p\rangle$ and $|p_j\rangle = M^j_{k^j_{bc}}|\psi_{p_j}\rangle$.

(3)Bob utilizes k_{ab}, $|T\rangle$, $|P\rangle$ to provide a quantum blind signature to the secret trying message, which can be implemented as this way: he encrypts $|T\rangle$, $|P\rangle$ with k_{ab} to drive

$$S_b = k_{ab}(|T\rangle, |P\rangle), \qquad (14)$$

where S_b is a blind signature on Alice's secret trying message.

Step 4. Bob sends S_b back to Alice and waits for the verification of the signature.

C. *Verification*

Step 1. Alice receives S_b and uses k_{ab} to decrypt S_b to derive $|T'\rangle$ and $|P'\rangle$. Then she uses her private key k_a to decrypt $|T'\rangle$ to obtain a quantum string $|\psi'_{M_1}\rangle$.

Step 2. Alice verifies whether the signature is blindness. She compares $|\psi'_{M_1}\rangle$ to her $|\psi_{M_1}\rangle$ which she has reserved in the Step 1 of trying quantum blind signature phase. The comparison quantum circuit is presented in Fig. 3. It implies that $|v_{ij}\rangle = |\psi'_{ij}\rangle \oplus |\psi_{ij}\rangle$ and we can justify whether $|\psi'_{M_i}\rangle$ matches to $|\psi_{M_i}\rangle$ according to the output qubit string $|V_i\rangle = \{|v_{i1}\rangle, |v_{i2}\rangle, \ldots, |v_{ij}\rangle, \ldots, |v_{i(n-1)}\rangle, |v_{in}\rangle\}$. Because $|0\rangle \oplus |0\rangle = |0\rangle$, $|1\rangle \oplus |1\rangle = |0\rangle$, $|0\rangle \oplus |1\rangle = |1\rangle$, $|\psi'_{M_i}\rangle$ may match to $|\psi_{M_i}\rangle$ when $|V_i\rangle = \{|0\rangle, |0\rangle, \ldots, |0\rangle, \ldots, |0\rangle\}$ is derived. If $|\psi'_{M_1}\rangle \neq |\psi_{M_1}\rangle$, it means the secret message has been misrepresented. Maybe there is somebody has measured the trying message or intercepted the whole or parts of the content, because any measurement may change the state of quantum photons. Then the protocol should be terminated. If $|\psi'_{M_1}\rangle = |\psi_{M_1}\rangle$, we can suggest that there is nobody knows the content of the trying message except Alice, thus the blind signature can be established.

Step 3. Bob transmits $|P\rangle$ to the arbitrator Charlie. $|P\rangle$ is the encrypted result of $|\psi_p\rangle$ with $M_{k_{bc}}$, and it is secret to anyone except Bob and the arbitrator Charlie. So Bob can send it directly to Charlie through the quantum channel.

Step 4. Alice sends $|P'\rangle$ to Charlie.

Step 5. The arbitrator Charlie receives $|P'\rangle$ and $|P\rangle$, and he certifies whether the signature is authentic. He firstly compares if $|P'\rangle = |P\rangle$, and then he uses k_{bc} to decrypt $|P'\rangle$ and $|P\rangle$ separately. Charlie obtains $|\psi'_p\rangle$ and $|\psi_p\rangle$, and then he compares whether $|\psi'_p\rangle = |\psi_p\rangle$. If $|P'\rangle = |P\rangle$ and $|\psi'_p\rangle = |\psi_p\rangle$, we can consider this trying blind signature is successful, then Charlie will inform Alice and Bob this trying blind signature is authentic and blindness. Charlie can also apply the comparison quantum circuit in Fig. 3 to implement the verification procedure. Next step, Charlie can sign a large number of messages from Alice as a proxy of Bob. However, when any previous condition is not satisfied, the communication should be terminated.

D. *Batch Proxy Quantum Blind Signature*

Charlie may become a proxy of Bob and sign quantities of messages $\{M_2, M_3, \ldots M_m\}$ of Alice with the combination of Bob's personal information $|P\rangle$ and his random checking photons $|P^k_{check}\rangle$.

Step 1. Alice transforms her remaining messages $\{M_2, M_3, \ldots M_m\}$ into $m-1$ strings of qubits $\{|\psi_{M_2}\rangle, |\psi_{M_3}\rangle \ldots, |\psi_{M_m}\rangle\}$ like the Step 1 $\sim$ 3 of the trying quantum blind signature phase. Then she encrypts them by her private key k_a, thus the remaining secret messages can be expressed as follows,

$$|M_k\rangle = M_{k_a}|\psi_{M_k}\rangle = \{|m_{k1}\rangle, |m_{k2}\rangle, \ldots, |m_{kj}\rangle, \ldots, |m_{kn}\rangle\}, \qquad (15)$$

where $k = 2, 3, ..., m$.

Step 2. Alice sends $\{|M_2\rangle, |M_3\rangle, ...|M_m\rangle\}$ to Charlie successively and waits for the signature from Bob's proxy Charlie.

Step 3. Charlie adds one qubit random checking photon $|P^k_{check}\rangle$ into $|P\rangle$ which Charlie has obtained in the step 3 of verification phase, where

$$|P^k_{check}\rangle = M^r_{k^r_{bc}}|\psi^k_{check}\rangle \qquad (16)$$

and $|\psi^k_{check}\rangle(k = 2, 3, \ldots, m)$ is formed as Eq.(9). r is a random number in $\{1, 2, \ldots j \ldots, n\}$. It means Charlie may randomly choose a $M^j_{k^j_{bc}}$ from $M_{k_{bc}}$ to measure $|P^k_{check}\rangle$. Thus the general expression of the combining qubit strings is

$$\begin{aligned} |P^k_{BT}\rangle &= \{|P\rangle, |P^k_{check}\rangle\} \\ &= \{|P_1\rangle, |P_2\rangle, \ldots, |P_j\rangle, \ldots, |P_n\rangle, |P^k_{check}\rangle\} (17) \end{aligned}$$

where $k = 2, 3, \ldots m$. Each message state $|M_k\rangle$ is corresponding to a $|P_{BT}^k\rangle$, and Charlie can randomly use a different $|P_{BT}^k\rangle$ to sign a message from Alice.

Step 4. Charlie separately signs $m-1$ secret messages with the string $|P_{BT}^k\rangle (k = 2, 3, \ldots, m)$ which is the combination of Bob's personal information and Charlie's checking photons, and he encrypts them by k_{ac}. Thus the proxy blind signatures are obtained:

$$S_{T_k} = k_{ac}(|M_k\rangle, |P_{BT}^k\rangle), \tag{18}$$

where $k = 2, 3, \ldots, m$.

Step 5. Charlie sends the secret messages with blind signatures $\{S_{T_2}, S_{T_3}, \ldots, S_{T_m}\}$ back to Alice successively.

Step 6. Alice receives the blind signatures $S_{T_k}(k = 2, 3, \ldots, m)$ and decrypts them by k_{ac} to get $|M_k\rangle (k = 2, 3, \ldots, m)$ and $|P_{BT}^{k'}\rangle (k = 2, 3, \ldots, m)$. Then she decrypts $|M_k\rangle (k = 2, 3, \ldots, m)$ with k_a to obtain $|\psi_k\rangle (k = 2, 3, \ldots, m)$. Because Charlie is the fully trusted arbitrator and the proxy signatures contain his checking photons and Bob's correct personal information, it is not necessary to suspect the accuracy of the signature. However, Alice can randomly measure the accuracy of the signatures by justifying whether they satisfy $|\psi_k\rangle = |\psi_{M_k}\rangle (k = 2, 3, \ldots, m)$ and $|P_{BT}^{k'}\rangle = |P'\rangle (k = 2, 3, \ldots, m)$.

III. Security Analysis And Discussions

The security of this scheme can be analyzed as following four aspects: impossibility of forgery, impossibility of disavowal by the signatory, impossibility of denial by the receiver and the security of the entangled quantum system.

A. *Impossibility of Forgery*

If an dishonest participant Eve wants to forge the signature of Bob, she may sign the illegal messages herself by imitating Bob's signature or pretend the legal user Alice to require for Bob's signature. Even if Eve succeeds to sign her messages by forging Bob's personal information. Denote the spurious Bob's personal information is $|P_s$, she may be detected in the verification phase, and the arbitrator Charlie can judge $|P_s\rangle$ does not match to the Bob's correct personal information $|P\rangle$. The communication of the signing phase should be terminated immediately.

If the attacker Eve expects to forge the signature of Bob, she may be recognized in the step 3 of initial phase. Even though she is so lucky to escape identity verification and she can send her trying secret message to Bob, Bob doesn't care what the content of the message is but only signs it. Because the signing message is encrypted by k_{ab} before she sends it back to Eve, Eve can not decrypt it for lack of k_{ab}.

B. *Impossibility of Disavowal by the Signatory*

Suppose Bob has added his personal information to sign the trying message, and the signature is obtained by Alice. Because the arbitrator Charlie can judge whether the signature is authentic or not, once it is proved to be authentic, the Bob's personal information has already denoted for a register from him, then the following signing for the last $m-1$ messages is the responsibility of the arbitrator and proxy Charlie, and he will utilize the combination of his checking photons and Bob's personal information to do this. If Bob disavow it, he will be discovered by Charlie immediately. In this scheme, as long as Bob has signed the trying message and the signature has been proved to be authentic by Charlie, the mechanism of proxy signature make Bob have no chance to disavow the remaining $m-1$ signature. Thus the signatory Bob is impossible to disavow the signature.

C. *Impossibility of Denial by the Receiver*

In the verification phase, Alice derives S_b and use k_{ab} to decrypt S_b to obtain $|T'\rangle$ and $|P'\rangle$. After the arbitrator Charlie's authentication, if $|P'\rangle = |P\rangle$ and $|\psi_p'\rangle = |\psi_p\rangle$, Charlie informs Alice and Bob this trying blind signature is authentic, otherwise, the trying signature will be considered incredible and the process of signature is discontinued at once. It means the two participants Alice and Bob can not deny the signature any way and Charlie is considered to be a judge. If one of them deny or disavow the signature, Charlie can unconditionally suspect the identification of them, and they may be no longer join in this communication.

D. *Security of Entangled Quantum System*

Suppose an attacker Eve can entangle her ancila system with the two-particle entangled quantum system $|\varphi\rangle$ in Eq. (1) by applying the strongest collective attack with probabilities. The combined Eve's and quantum system state can be expressed as

$$\begin{aligned} |E\varphi\rangle &= \lambda_{00}a_{00}|00\rangle|e_{00}\rangle + \lambda_{01}a_{01}|01\rangle|e_{01}\rangle \\ &\quad + \lambda_{10}a_{10}|10\rangle|e_{10}\rangle + \lambda_{11}a_{11}|11\rangle|e_{11}\rangle, \end{aligned} \tag{19}$$

where $|e_{00}\rangle$, $|e_{01}\rangle$, $|e_{10}\rangle$ and $|e_{11}\rangle$ are un-normalized states of Eve and $|\lambda_{00}\rangle$, $|\lambda_{01}\rangle$, $|\lambda_{10}\rangle$ and $|\lambda_{11}\rangle$ are parameters relative to her attack probabilities. If Eve is clever enough to implement single qubit QND measurement on one particle of $|\varphi\rangle$ with the measurement operator $\rho = \frac{1}{2}|0\rangle\langle 0| \pm \frac{1}{2}|1\rangle\langle 1|$, she can derive the ideal entangled states

$$\begin{aligned} |E\rangle &= \frac{1}{2}\{(\lambda_{00}a_{00}|0e_{00}\rangle + \lambda_{01}a_{01}|1e_{01}\rangle) \\ &\quad \pm(\lambda_{10}a_{10}|0e_{10}\rangle + \lambda_{11}a_{11}|1e_{11}\rangle)\} \end{aligned} \tag{20}$$

according to Eq. (19). Thus the entanglement entropy of $|E\rangle$ can be analyzed based on the degree of entanglement [16] to indicate the maximal amount of information which can be intercepted by Eve. The entanglement entropy is

$$\begin{aligned} \mathcal{S}_E &= -\frac{1+\sqrt{1-\varepsilon}}{2}\log_2\frac{1+\sqrt{1-\varepsilon}}{2} \\ &\quad -\frac{1-\sqrt{1-\varepsilon}}{2}\log_2\frac{1-\sqrt{1-\varepsilon}}{2}, \end{aligned} \tag{21}$$

where $\varepsilon = 4|\lambda_{00}\lambda_{11}a_{00}a_{11} - \lambda_{01}\lambda_{10}a_{01}a_{10}|^2$. Even though Eve can adjust the parameters $|\lambda_{00}\rangle$, $|\lambda_{01}\rangle$, $|\lambda_{10}\rangle$ and $|\lambda_{11}\rangle$ to make $\mathcal{S}_E$ approach the maximal value 1 (when $\varepsilon = 1$) while the maximal entropy of the two-particle entangled quantum system $|\varphi\rangle$ is 2. Therefore the entangled quantum system state cannot be deterministically intercepted.

IV. Conclusions

A quantum communication scheme for blind signature with two-particle entangled quantum system is proposed, which is a new quantum key cryptosystem that combines proxy signature and blind signature. The two-particle entangled quantum states are applied to create the strings of qubits for messages and make distribution of keys. No matter the trying message or the remaining $m-1$ messages, they are encrypted by the private key k_a of Alice. Moreover, an authenticity verification of signatures and an arbitrator's efficient proxy signature are both applied. The analysis shows that a large number of blind signatures for quantities of messages can be achieved with the characteristics: impossibility of forgery, impossibility of disavowal by the signatory and impossibility of denial by the receiver. The security of our scheme depends on the two-particle entangled system which cannot be deterministically intercepted.

Acknowledgment

This work was supported by the National Natural Science Foundation of China (Grant Nos. 61272495), WCU R32-2010-000-20014-0 (Fundamental Research2010-0020942NRF, Korea), the Hunan Provincial Innovation Foundation For Postgraduate (Grant Nos. CX2011B087) and the Excellent Doctoral Dissertation Fund of Central South University (Grant Nos. 2011ybjz030).

References

[1] S. William, *Cryptography and Network Security: Principles and Practice*, Prentice Hall, New Jersey, 2^{nd} ed., 2003, p.67.

[2] D. Chaum, *Advance in Cryptography*, Proceedings of Crypto'82 Springer-Verlag, Berlin, 1982, p.267.

[3] B. Schneier, *Applied Cryptography:Protocols, Algorithms, and Source Code in C*, John Wiley and Sons, New York, 2^{nd} ed., 1996, p.79.

[4] C. Fan and C. Lei, Efficient blind signature scheme based on quadratic residues, Electronic Letters., vol. 32, no. 811, 1996.

[5] G. H. Zeng and C. H. Keitel, Arbitrated quantum-signature scheme, Phys. Rev. A., vol. 65, no. 042312, 2002.

[6] M. Curty and N. Lutkenhaus, Comment on ”Arbitrated quantum-signature scheme”, Phys. Rev. A., vol. 77, no. 046301, 2008.

[7] G. H. Zeng, Reply to ”Comment on ’Arbitrated quantum-signature scheme’”, Phys. Rev. A., vol. 78, no. 016301, 2008.

[8] D. Gottesman and I. Chuang, Quantum digital signatures, arXiv:quant-ph/0105032.

[9] X. J. Wen, X. M. Niu, L. P. Ji, and Y. Tian, A weak blind signature scheme based on quantum cryptography, Optics Communications., vol. 282, no. 666, 2009.

[10] J. J. Shi, R. H. Shi, Y. Tang and M. H. Lee, A multiparty quantum proxy group signature scheme for the entangled-state message with quantum Fourier transform. Quantum Information Processing, Vol. 10, No. 5, 653-670, 2011.

[11] J. J. Shi, R. H. Shi, Y. Guo, X. Q. Peng and Y. Tang, Batch proxy quantum blind signature scheme, SCIENCE CHINA Information Sciences, doi: 10.1007/s11432-011-4422-5, 2011.

[12] J. J. Shi, R. H. Shi , Y. Guo, X. Q. Peng, M. H. Lee and D. S. Park, A (t,n)-Threshold Scheme of Multi-party Quantum Group Signature with Irregular Quantum Fourier Transform, International Journal of Theoretical Physics, DOI 10.1007/s10773-011-0978-5, 2011.

[13] H. Lee, C. H. Hong, and H. Kim, Arbitrated quantum signature scheme with message recovery, Phys. Lett. A. **32**, 295-300 (2004).

[14] Y. G. Yang, Multi-proxy quantum group signature scheme with threshold shared verification, Chin. Phys. B. Vol. **17**, No. 2, 415-418 (2008).

[15] M. Nielsen and I. Chuang, *Quantum computation and quantum information*, Cambridge University Press, Cambridge, 2000, p.171.

[16] R. V. Buniy and S. D. H. Hsu, Entanglement entropy, black holes and holography, Phys. Lett. B., 64 (2007), pp. 72-76.

Jinjing Shi is now a joint Ph.D. student of Central South University, China and Chonbuk National University, Korea, and participating in the World Class University (WCU) project sponsored by the National Research Foundation (NRF), Korea. She received her B. E. degree in the School of Information Science and Engineering, Central South University, Changsha, China, in 2008. Her research interests are quantum communications, quantum cryptography and network security.

Ronghua Shi received the B.S., M.S., and Ph.D. degrees in electrical engineering from Central South University (CSU), Changsha, China, in 1986, 1989, and 2007, respectively. He is presently a Professor and the Vice Dean of the School of Information Science and Engineering at Central South University. His research interests include information security, quantum cryptography and network security.

Xiaoqi Peng received the B.S., M.S., and Ph.D. degrees in automation and control from Chongqing University, Harbin Institute of Technology and Central South University respectively. He is presently a Professor of the School of Information Science and Engineering at Central South University, and the dean of Hunan First Normal University. His research interests include intelligent detection of complex industrial processes, optimization of the decision-making and intelligent control.

Moon Ho Lee is a professor in Chonbuk National University, Korea. He received the Ph.D. degree from Chonnam National University, Korea in 1984, and from the University of Tokyo, Japan in 1990, both Electrical Engineering, He was in University of Minnesota, U.S.A, from 1985 to 1986 as a post-doctor. He was conferred an honorary doctorate from the Bulgaria Academy of Sciences in 2010. Dr. Lee has made significant original contributions in the areas of mobile communication code design, channel coding, and multidimensional source and channel coding. He has authored 34 books, 135 SCI papers in international journals, and 240 papers in domestic journals, and delivered 350 papers at international conferences. Dr. Lee is a member of the National Academy of Engineering in Korea and the National Academy of Mathematical Sciences in India, and a Foreign Fellow of the Bulgaria Academy of Sciences. He is the inventor of Jacket Matrix and it in Wikipedia was cited over 49,559 times.