

Quantum Communication Scheme for Blind Signature With Two-Particle Entangled Quantum-Trits

Jinjing Shi^{1,2}, Danping Xu², Guoxiang Xu¹ and Moon Ho Lee²

¹ School of Information Science & Engineering, Central South University, Changsha 410083, China.

² Institute of Information and Communication, Chonbuk National University, Chonju 561-756, Korea.

Email: sjjgz2009@gmail.com, moonho@chonbuk.ac.kr

Abstract—Quantum communication scheme for blind signature is proposed based on two-particle entangled quantum-trits 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 a high efficiency.

Keywords— Quantum communication, Blind signature, Proxy signature, Quantum signature, Quantum cryptography.

I. INTRODUCTION

Digital signatures [1] 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 and Shi *et al.* introduced a multiparty quantum proxy group signature scheme for the entangled-state message [10]–[12].

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-trits. A third fully trusted participant Trent (the arbitrator and proxy) is involved into this scheme. The responsibility of Trent 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-trits are used to create the strings of qutrits for messages and to make distribution of keys.

II. QUANTUM COMMUNICATION SCHEME FOR BLIND SIGNATURE

The classical blind signature is described like this: Bob is a notary, Alice expects Bob can sign the message from her and she does not want to Bob to understand the content of

the message. Bob does not care what the message is, and he only testifies he has notated it at some time [3]. The quantum communication scheme for blind signature utilizes the two-particle entangled quantum-trits [13] which are expressed as follows,

$$|\varphi_2^3\rangle = a_{00}|00\rangle + a_{01}|01\rangle + a_{02}|02\rangle + a_{10}|10\rangle + a_{11}|11\rangle + a_{12}|12\rangle + a_{20}|20\rangle + a_{21}|21\rangle + a_{22}|22\rangle, \quad (1)$$

where $\sum_{i=0, j=0}^2 \|a_{ij}\|^2 = 1$.

Suppose that Alice and Bob share an entangled pair in this state:

$$|\varphi_{AB}\rangle = \frac{1}{3}(|0_A 0_B\rangle + |0_A 1_B\rangle + |0_A 2_B\rangle + |1_A 0_B\rangle + |1_A 1_B\rangle + |1_A 2_B\rangle + |2_A 0_B\rangle + |2_A 1_B\rangle + |2_A 2_B\rangle), \quad (2)$$

Suppose that Alice and Trent share an entangled pair in this state:

$$|\varphi_{AC}\rangle = \frac{1}{3}(|0_A 0_C\rangle + |0_A 1_C\rangle + |0_A 2_C\rangle + |1_A 0_C\rangle + |1_A 1_C\rangle + |1_A 2_C\rangle + |2_A 0_C\rangle + |2_A 1_C\rangle + |2_A 2_C\rangle), \quad (3)$$

Suppose that Bob and Trent share an entangled pair in this state:

$$|\varphi_{BC}\rangle = \frac{1}{3}(|0_B 0_C\rangle + |0_B 1_C\rangle + |0_B 2_C\rangle + |1_B 0_C\rangle + |1_B 1_C\rangle + |1_B 2_C\rangle + |2_B 0_C\rangle + |2_B 1_C\rangle + |2_B 2_C\rangle), \quad (4)$$

The quantum communication scheme for blind signature can be briefly defined as follows and each step is corresponding to Fig. 1.

(1) Alice firstly sends a trying message which is encrypted by her private key to Bob. (2) Bob adds his personal information to this secret message and encrypts it by the sharing key with Alice. (3) Bob sends the secret message with his personal information to Alice which is called the trying blind signature. (4) Alice gets this trying blind signature and decrypts it by

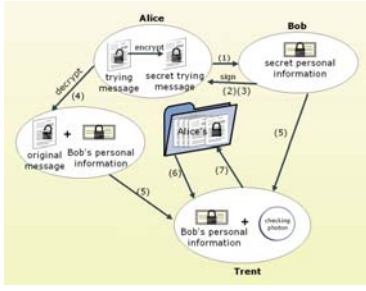


Fig. 1. The process of quantum communication scheme for blind signature.

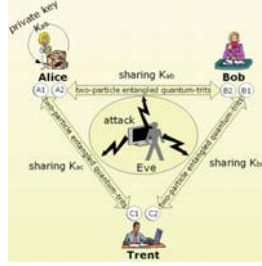


Fig. 2. Figure for distribution of keys in the quantum communication scheme for blind signature.

the sharing key with Bob and judge whether the secret trying message has not been falsify. (5) Alice and Bob separately informs Trent the result of the signature and Trent verifies legalization and authenticity of the trying signature. (6) If the verification is successful, Alice sends quantities of messages to Trent. (7) Trent signs quantities of messages using the the combination of Bob's personal information and Trent's random checking photons.

A. Initial phase

Step 1. Alice and Bob are distributed the secret keys K_{ab} , K_{ac} , K_{bc} , 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 Trent and between Bob and the arbitrator Trent. Besides K_{ab} , K_{ac} , K_{bc} , Alice owns a private key K_a which is used for her to encrypt the messages excepted to be signed by Bob. The relationship among Alice, Bob and Trent and the distribution of keys is given in Fig. 2.

Step 2. Alice has quantities of messages which are expected to be signed by Bob, and they can be described as a matrix like this:

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

there are m messages $\{M_1, M_2, \dots, M_m\}$ and each message

has n trits, for example:

$$M_i = [m_{i1} \ m_{i2} \ \cdots \ m_{ij} \ \cdots \ m_{in}], \quad (6)$$

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

B. Trying Quantum Blind Signature Phase

Step 1. Alice creates a qutrit string $|\psi_{M_1}\rangle$ for the trying message. Alice transforms the trying message M_1 into a qutrit string $|\psi_{M_1}\rangle$, there are n qutrits in this string, such as $|\psi_{M_1}\rangle$ reads:

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

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

$$|\psi_{1j}\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle + \alpha_2|2\rangle, \quad (8)$$

where $\alpha_0, \alpha_1, \alpha_2$ are complex number with $|\alpha_0|^2 + |\alpha_1|^2 + |\alpha_2|^2 = 1$.

Step 2. Alice creates a secret string of qutrits $|T\rangle$ and relates her private key $K_a = \{|K_a^1\rangle, |K_a^2\rangle, \dots, |K_a^j\rangle, \dots, |K_a^n\rangle\}$ to a sequence of measurement operators M_{k_a} , i.e.,

$$M_{k_a} = \{M_{k_a^1}^1, M_{k_a^2}^2, \dots, M_{k_a^j}^j, \dots, M_{k_a^n}^n\}, \quad (9)$$

the operators $M_{k_a^j}^j$ are defined to arise from the key $|K_a^j\rangle$ for $j \in \{1, 2, \dots, n\}$. A more detailed method is described in Ref. [5]. After the transformation, Alice is required to measure the information string of qutrits $|\psi_{M_1}\rangle$ with M_{k_a} and obtains:

$$|T\rangle = M_{k_a}|\psi_{M_1}\rangle = \{|t_1\rangle, |t_2\rangle, \dots, |t_j\rangle, \dots, |t_n\rangle\}, \quad (10)$$

where $|t_j\rangle = M_{k_a^j}^j|\psi_{1j}\rangle$ and it denotes the j th qutrit in the string of $|T\rangle$ which is the secret state of the trying message. Alice directly sends it to Bob and expects Bob to sign it.

Step 3. Bob can add his personal information to sign the secret message though he doesn't need to understand the content of the secret message.

(1) Bob creates a qutrit string of his own personal information $|\psi_p\rangle$, there are n qutrits in the string, such as $|\psi_p\rangle$ reads:

$$|\psi_p\rangle = \{|\psi_{p1}\rangle, |\psi_{p2}\rangle, \dots, |\psi_{pj}\rangle, \dots, |\psi_{pn}\rangle\}, \quad (11)$$

where $|\psi_{pj}\rangle$ is a single qutrit in the string $|\psi_p\rangle$. Any qutrit $|\psi_{pj}\rangle$ ($j = 1, 2, \dots, n$) in $|\psi_p\rangle$ can be expressed as a superposition of the three eigenstates $|0\rangle, |1\rangle, |2\rangle$ like $|\psi_{1j}\rangle$ in the Step 1.

(2) Bob also doesn't expect Alice know the content of his personal information and he encrypts $|\psi_p\rangle$ by K_{bc} . He relates the key $K_{bc} = \{|K_{bc}^1\rangle, |K_{bc}^2\rangle, \dots, |K_{bc}^j\rangle, \dots, |K_{bc}^n\rangle\}$ to a sequence of measurement operators $M_{k_{bc}}$, often referred to as a measurement basis, the modulus is like Eq.(10). After this transformation, Bob is required to measure the personal information string of qutrits $|\psi_p\rangle$ with $M_{k_{bc}}$ and obtains

$$|P\rangle = M_{k_{bc}}|\psi_p\rangle = \{|P_1\rangle, |P_2\rangle, \dots, |P_j\rangle, \dots, |P_n\rangle\}, \quad (12)$$

where $|p_j\rangle = M_{k_{bc}}^j |\psi_{p_j}\rangle$ and denotes the j th qutrit in the string of $|p\rangle$.

(3) Bob uses k_{ab} , $|T\rangle$, $|P\rangle$ to provide a quantum blind signature to the secret trying message. Bob may operate as this way: he encrypts $|T\rangle$, $|P\rangle$ by k_{ab} get

$$S_b = k_{ab}(|T\rangle, |P\rangle), \quad (13)$$

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 Phase

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

Step 2. Alice verifies whether the signature is blindness. Alice compares $|\psi'_{M_1}\rangle$ to her $|\psi_{M_1}\rangle$ which she has reserved in First quantum blind signing(trying quantum blind signature) phase Step 1. 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 a part of content. Then they drop it and don't go on the following steps. Because any measurement may change the state of quantum photons. If $|\psi'_{M_1}\rangle = |\psi_{M_1}\rangle$, we can suggest that there is nobody understands the content of the trying message except Alice, so the blind signature is established.

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

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

Step 5. The arbitrator Trent obtains $|P'\rangle$ and $|P\rangle$, and he will certify 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. Trent gets $|\psi'_p\rangle$ and $|\psi_p\rangle$, following he compares if $|\psi'_p\rangle = |\psi_p\rangle$. If $|P'\rangle = |P\rangle$ and $|\psi'_p\rangle = |\psi_p\rangle$, we can consider this trying blind signature is successful, then Trent will inform Alice and Bob this trying blind signature is authentic and blindness. Next step, Trent can sign a large number of messages from Alice as a proxy of Bob. But when any condition above is not established, it is necessary to drop this communication.

D. Batch Proxy Quantum Blind Signing Phase

In this phase, Trent as a proxy of Bob will sign quantities of messages $\{M_2, M_2, \dots, M_m\}$ from Alice with the combination of Bob's personal information $|P\rangle$ and his random checking photons $|P_{check}^k\rangle$.

Step 1. Like the Step 1 ~ 3 of the trying quantum blind signature phase, Alice transforms her remaining $m-1$ messages $\{M_2, M_2, \dots, M_m\}$ into $m-1$ strings of qutrits $\{|\psi_{M_2}\rangle, |\psi_{M_3}\rangle, \dots, |\psi_{M_m}\rangle\}$. Then she encrypts them by her private key k_a , the remaining secret messages are expressed as follows:

$$|M_k\rangle = M_{k_a} |\psi_{M_k}\rangle = \{|M_1\rangle, |M_2\rangle, \dots, |M_j\rangle, \dots, |M_n\rangle\}, \quad (14)$$

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

Step 2. Alice sends the remaining $m-1$ strings of qutrits for the $m-1$ secret messages $\{|M_2\rangle, |M_3\rangle, \dots, |M_m\rangle\}$ to Trent successively and waits for the signature from Bob's proxy Trent.

Step 3. Trent add one qutrit random checking photon $|P_{check}^k\rangle$ into $|P\rangle$ which Trent has obtained in Verification phase Step 3 for each message of $\{|M_2\rangle, |M_3\rangle, \dots, |M_m\rangle\}$.

$$|P_{check}^k\rangle = M_{k_{bc}}^r |\psi_{check}^k\rangle, \quad (15)$$

where the form of $|\psi_{check}^k\rangle$ ($k = 2, 3, \dots, m$) is as Eq.(9), and r is a random number in $\{1, 2, \dots, j, \dots, n\}$. It means randomly choosing a $M_{k_{bc}}^j$ from $M_{k_{bc}}$ to measure $|P_{check}^k\rangle$. Then the combining strings of qutrits are presented:

$$\begin{aligned} |P_{BT}^k\rangle &= \{|P\rangle, |P_{check}^k\rangle\} \\ &= \{|P_1\rangle, |P_2\rangle, \dots, |P_j\rangle, \dots, |P_n\rangle, |P_{check}^k\rangle\} \end{aligned} \quad (16)$$

where $k = 2, 3, \dots, m$, each message $|M_k\rangle$ is corresponding to $|P_{BT}^k\rangle$, then Trent will randomly use different $|P_{BT}^k\rangle$ to sign messages from Alice.

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

$$S_{T_k} = k_{ac}(|M_k\rangle, |P_{BT}^k\rangle), \quad (17)$$

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

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

Step 6. Alice receives the blind signature S_{T_k} ($k = 2, 3, \dots, m$) and decrypts them by k_{ac} to get $|M_k\rangle$ ($k = 2, 3, \dots, m$) and $|P_{BT}^k\rangle$ ($k = 2, 3, \dots, m$). Then she decrypts $|M_k\rangle$ ($k = 2, 3, \dots, m$) with k_a to get $|\psi_k\rangle$ ($k = 2, 3, \dots, m$). Because Trent is the third fully trusted arbitrator and the proxy signatures have contained his checking photons and Bob's correct personal information, it is not necessary to suspect the accuracy of the signature. However, perhaps Alice can randomly measure the accuracy of the signature through whether $|\psi_k\rangle = |\psi_{M_k}\rangle$ ($k = 2, 3, \dots, m$) and first n qutrits of $|P_{BT}^k\rangle = |P'\rangle$ ($k = 2, 3, \dots, m$), where $|\psi_{M_k}\rangle$ ($k = 2, 3, \dots, m$) and $|P'\rangle$ have been mentioned in Eq.(15).

III. SECURITY ANALYSIS AND DISCUSSION

A. Impossibility of Forgery

All the strings of qutrits for messages mentioned in the steps above all have three eigenstates, it makes the attackers more difficult to succeed. Eq.(9) has presented the form of one qubit of the trying message and the Shannon binary entropy is calculated like this:

$$\begin{aligned} H(p_{1j}) &= ||\alpha_0||^2 \log_2 \frac{1}{||\alpha_0||^2} + ||\alpha_1||^2 \log_2 \frac{1}{||\alpha_1||^2} \\ &+ ||\alpha_2||^2 \log_2 \frac{1}{||\alpha_2||^2}, \end{aligned} \quad (18)$$

because $||\alpha_0||^2 + ||\alpha_1||^2 + ||\alpha_2||^2 = 1$, only when $||\alpha_0|| = ||\alpha_1|| = ||\alpha_2|| = \frac{1}{\sqrt{3}}$, the maximum Shannon binary entropy is presented. Here $H(p_{1j}) = (\frac{1}{3}\log_2 3) \times 3 = \log_2 3 = 1.58\text{bit}$, it stands for the degree of uncertainty, so even if the attackers obtain one or some parts of qubits, the original state can not be completely determined.

If the dishonest Alice wants to forge the signature of Bob, she may sign the illegal messages herself through imitating Bob's signature or pretend the legal user Alice to ask for Bob's signature. Even if the dishonest Alice is successfully sign her messages by forging Bob's personal information, let the spurious Bob's personal information be $|P_s\rangle$, she will be found out in the Verification phase, the arbitrator Trent can judge $|P_s\rangle$ is not similar to the Bob's real personal information $|P\rangle$ from Bob. The communication of the signing phase will be terminated immediately.

If the attacker Eve expect to forge the signature of Bob, like the dishonest Alice, he will be recognized in the Initial phase Step 3. Identity verification too. Even though he luckily passes the identity verification and he can send his 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 he sends it back to Eve, Eve can not decrypt it for lack of k_{ab} .

B. Impossibility of Disavowal by the Signatory

It is assumed that Bob has added his personal information to sign the trying message, then the signature is obtained by Alice, because of the arbitrator Trent, he can judge whether the signature is authentic or not. Once it is proved to be authentic by the arbitrator Trent, the Bob's personal information has already stood for a register from him, then the following signing for the last $m - 1$ messages is the responsibility of the arbitrator and proxy Trent, and he will use the combination of his checking photons and Bob's personal information to do this. If Bob disavow it, he will be discovered by Trent immediately any way, in this scheme, as long as Bob has signed the trying message and the signature has been proved to be authentic by Trent, the mechanism of proxy signature make Bob have no chance to disavow the last $m - 1$ signature. So we can get the conclusion that the signatory Bob is impossible to disavow the signature.

C. Impossibility of Denial by the Receiver

We should also concern that whether the receiver Alice has chance to deny the signature of Bob. In the Verification phase, Alice get S_b and use k_{ab} to decrypt S_b to get $|T'\rangle$ and $|P'\rangle$. Though $|P'\rangle$ may not be the real personal information of Bob, after the arbitrator Trent's authentication, If $|P'\rangle = |P\rangle$ and $|\psi'_p\rangle = |\psi_p\rangle$, Trent will inform Alice and Bob this trying blind signature is authentic, otherwise, the trying signature will be considered incredible and the process of signature will be discontinued at once. It means the two participants Alice and Bob can not deny the signature any way and Trent is considered to be a judge. If one of them deny or disavow the

signature, Trent can unconditionally suspect the identification of them, then they will no longer hold on this communication.

IV. CONCLUSIONS

A quantum communication scheme for blind signature with two-particle entangled quantum-trits is proposed, which is a new quantum key cryptosystem that combines batch signature, proxy signature and blind signature for the first time. The two-particle entangled quantum-trits 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 expected to be signed, 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 efficiently.

ACKNOWLEDGMENT

This work was supported by WCU R32-2010-000-20014-0 (Fundamental Research2010-0020942NRF, Korea), BK21 (the Second stage, Korea), the Hunan Provincial Innovation Foundation For Postgraduate (Grant Nos. CX2011B087), the State Scholarship Fund organized by the China Scholarship Council, and the Excellent Doctoral Dissertation Fund of Central South University (Grant Nos. 2011yb030).

REFERENCES

- [1] S. William, *Cryptography and Network Security: Principles and Practice*, Prentice Hall, New Jersey, 2nd 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, 2nd 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] M. Nielsen and I. Chuang, *Quantum computation and quantum information*, Cambridge University Press, Cambridge, 2000, p.171.