A Journal of Software Engineering and Applications, **2013, 6, 16-20**
doi:10.4236/jsea.2013.65B004 Published Online May 2013 (http://www.scirp.org/journal/jsea)

Quantum Group Signature Scheme Based on Chinese Remainder Theorem

Xin Sun[1], Ying Guo[1], Jinjing Shi[1], Wei Zhang[1], Qin Xiao[1], Moon Ho Lee[2]

[1]School of Information Science & Engineering, Central South University, Changsha, China; [2]Institute of Information and Communication, Chonbuk National University, Chonju, Korea.
Email: sunxinshifeng@163.com, moonho@chonbuk.ac.kr

Received 2013

ABSTRACT

A novel quantum group signature scheme is proposed based on Chinese Remainder Theorem (CRT), in order to improve the security of quantum signature. The generation and verification of the signature can be successfully conducted only if all the participants cooperate with each other and with the message owner's and the arbitrator's help. The quantum parallel algorithm is applied to efficiently compare the restored quantum message to the original quantum message. All the operations in signing and verifying phase can be executed in quantum circuits. It has a wide application to E-payment system, Online contract, Online notarization and etc.

Keywords: Quantum Signature; Group Signature; Chinese Remainder Theorem

1. Introduction

Digital signature is one of the most important part of modern cryptography, which serves as a basic module to design cryptography protocols [1]. Digital signature is usually employed to guarantee the authenticity, integrity, and non-disavowal of transmitting messages. Group signature scheme was introduced in 1991 by Chaum and Heyst [2] firstly. In 1997, Camenisch and Stadler [3] improved Chaums scheme and developed the more efficient scheme CS97 for larger groups. CS97 was further enhanced by Bresson and Sterm [4] to be revocable for group numbers. Moreover, Ateniese and Camenisch [5] proposed a safe and efficient group signature scheme in 2000. Those are mostly based on the complexity of the system employed and they become increasingly vulnerable with more powerful computation. This difficulty can be overcome by quantum cryptography [6]. The biggest difference between quantum cryptography and classical cryptography is that quantum cryptography is the combination of quantum mechanics and cryptography, where the security is ensured by physical principles such as the Heisenberg uncertainty principle and the quantum no-cloning theorem. Now quantum cryptography has attracted a great deal of attention because it can stand against quantum attack, and has put forward many advances in quantum cryptography, including quantum secret sharing, quantum key distribution (QKD) [7-10] and quantum secure direct communication (QSDC) [10-14].

Taking advantage of the quantum properties of physical, many quantum signature schemes have been introduced. Zeng *et al.* introduced a quantum signature scheme based on the classical signature theory and quantum cryptography [15-18], whose algorithm is a symmetrical quantum key cryptosystem with Greenberger-Horne-Zeilinger (GHZ) triplet states. Li et al. proposed an arbitrated quantum signature scheme using Bell states [19]. Gottesman and Chuang proposed a quantum digital signature scheme based on quantum one-way function [20], and Lee also presented two quantum signature schemes with message recovery [21]. Unconditional security of the above quantum signature schemes have been proved, but they are not designed for 'group'. Therefore, a group signature can be devised based on quantum cryptography.

In this paper, we propose a group signature scheme based on Chinese Remainder Theorem (CRT). In our scheme, secret key is unforgeable, generated by the owner, and can be shared with the arbitrator based on QSCD protocol. The signing group contains two participants, and they collaborate to sign on the message by applying CRT with arbitrator and restore the message by performing the inverse CRT with arbitrator's assistance for the verification of signature. However, any t-1 or fewer participants can neither sign on the message nor restore the signed message. The message owner cooperate to verify the message by applying a quantum comparison circuit for comparing the restored quantum message to the original quantum message and arbitrator could inform message owner and group participants of

the verified result. Furthermore, all the quantum circuits and operation gates are packaged in black boxes [22] to enhance the security.

The rest of this paper is organized as follows. Sect. 2 introduces the basic knowledge about our scheme. Sect. 3 proposes a quantum group signature scheme which includes an initial phase, a signing phase, and a verification phase. Security analysis is made in Sect. 4, and a brief conclusions are drawn in Sect. 5.

2. Preliminaries

The original Chinese Remainder Theorem was proposed by SunZi and later republished in 1247 by Qin[23]. The CRT is ofen applied in computer science, such as RSA algorithm calculation, classical secret sharing and ect, and several versions of the Chinese Remainder Theorem have been proposed. The general CRT can be described as follows.

Lemma 1. Let n > 2, $b_1, b_2, \cdots, b_n$ be relatively prime in pairs, and $a_1, a_2, \cdots, a_n \in \mathbb{Z}$. The system of equations

$$\begin{cases} Y \equiv a_1 \bmod b_1 \\ \quad \vdots \\ Y \equiv a_n \bmod b_n \end{cases} \tag{1}$$

has solutions in Z if $\gcd(b_i, b_j) \equiv 1$, for all $1 \le i \le n$, $1 \le j \le n$. The solution can be obtained as

$$Y = \sum_{i=1}^{n} T_i B_i a_i \bmod B \tag{2}$$

where $B = b_1 \times b_2 \times \cdots b_n$, $B_i = B/b_i$, $T_i \times B_i \bmod b_i = 1$, for all $1 \le i \le n$, and Y < B.

According to this theorem, Alice can obtain the group signature. Suppose Alice sends the message number x to the Bob(group participants), Bob encrypts x by the secret key b_i based on Equation (1), and the result a_i is the element of the sequence of the signature. In this way, Alice can obtain his group signature.

3. Scheme Descriptions

The text above shows the basic signing algorithm of this scheme. Next the details of the scheme can be illustrated as follows, which contains three participants Alice (the message owner), G (the signing group), and Trent (the arbitrator). The three phases of our quantum signature scheme is introduced as follows.

3.1. Initial Phase

Step 1. Set up a signing group G, whose participants are $Bob_\xi (\xi = 1, 2, \cdots, n)$. According to QSDC protocol, G can share the secret key $K_\xi (\xi = 1, 2, \cdots, n)$ with Trent, in which K_ξ denotes the own private key of Bob_ξ and K_ξ is relatively prime.

Step 2. In this paper, we discuss the binary 3-qubit system, which can be defined as

$$|\psi\rangle_{xyz} = \frac{1}{\sqrt{2}}\left[|0xy\rangle + (-1)^z |1\bar{x}\bar{y}\rangle\right], \tag{3}$$

where $x, y, z \in \{0,1\}$.

3.2. Quantum Group Signing Phase

In this quantum group signature scheme, Alice prepares a quantum message. The group G generates a signature with assistance of Trent who doesn't understand the details about the signing algorithm. The participants of group G don't communicate with other.

Step 1. Alice's quantum message sequence $|P\rangle$ contains m qubits, i.e.

$$|P\rangle = \{|p_0\rangle, |p_1\rangle, \cdots, |p_\lambda\rangle, \cdots, |p_{m-1}\rangle\}, \tag{4}$$

where $|p_\lambda\rangle$ forms as Eq. (3).

Step 2. Alice sends the sequence $|P\rangle$ to Trent with superdense coding. Alice encodes $|p_\lambda\rangle$ as $|p_\lambda^*\rangle$ with the unitary operations U_{xyz}. The transformations can be summarized as

$$|p_{uvw}^*\rangle = U_{(xyz \oplus uvw)} |p_{xyz}\rangle, \tag{5}$$

where $x, y, z, u, v, w \in \{0,1\}$, binary strings *xyz* and *uvw* correspond to the decimal numbers, and $U_{000} = I \otimes I \otimes I$, $U_{001} = I \otimes I \otimes X$, $U_{010} = I \otimes X \otimes I$, $U_{011} = I \otimes X \otimes X$, $U_{100} = X \otimes I \otimes I$, $U_{101} = X \otimes I \otimes X$, $U_{110} = X \otimes X \otimes I$, $U_{111} = X \otimes X \otimes X$.

Step 3. Trent receives the

$$|P^*\rangle = \{|p_0^*\rangle, |p_1^*\rangle, \cdots, |p_\lambda^*\rangle, \cdots |p_{m-1}^*\rangle\}.$$

According to Eq.(3), the quantum message $|P^*\rangle$ can be rewritten as

$$|\psi\rangle_{P^*} = \prod_{\lambda=0}^{m-1} \frac{1}{\sqrt{2}}\left[|0x_\lambda y_\lambda\rangle + (-1)^{z_\lambda} |1\bar{x}_\lambda \bar{y}_\lambda\rangle\right], \tag{6}$$

where $x_\lambda, y_\lambda, z_\lambda \in \{0,1\}$. The states of $|P^*\rangle$ refer to a binary sequence $R = \{x_0 y_0 z_0 x_1 y_1 z_1, \cdots, x_{m-1}, y_{m-1} z_{m-1}\}$, so the corresponding classical message X can be acquired by Trent.

For example, if Trent receives a quantum sequence like $|P^*\rangle = \{|000\rangle, |001\rangle, |110\rangle\}$, it can be represented as

$$|\psi\rangle_{P^*} = \frac{1}{2\sqrt{2}}\left[|000\rangle + |111\rangle\right]\left[|001\rangle - |110\rangle\right]\left[|010\rangle - |101\rangle\right],$$

corresponding a binary sequence $R = \{000111101\}$, and Trent can derive the decimal classical message X = 28 + 26 + 25 + 24 = 368. Then Trent sends X to the group G.

Step 4. The participants of group G receives X collectively. As discussed in CRT's function in the paper, Bob

$(Bob_1, Bob_2, \cdots, Bob_t)$ sign on the quantum message $|P\rangle$ by transforming X as following algorithm

$$S = X \bmod K_\xi \tag{7}$$

where $K = \{K_\xi \,|\, 1 \le K_\xi \le 64, \xi = 1,2,\cdots,t\}$ is the Bob_ξ's private key, and $S = \{S_\xi \,|\, 0 \le S_\xi \le 63, \xi = 1,2,\cdots,t\}$ is the generated classical remainder. K_ξ and S_ξ can be represented by 6-bit binary sequence and according to Equation (3) the state can be shown as

$$\begin{aligned} |\psi\rangle_S &= \prod_{\xi=0}^{2(t-1)} \frac{1}{2}\left[|0 x_\xi y_\xi\rangle + (-1)^{z_\xi} |1\overline{x_\xi}\,\overline{y_\xi}\rangle\right] \\ |\psi\rangle_K &= \prod_{\xi=0}^{2(t-1)} \frac{1}{2}\left[|0 x_\xi y_\xi\rangle + (-1)^{z_\xi} |1\overline{x_\xi}\,\overline{y_\xi}\rangle\right] \end{aligned} \tag{8}$$

Signature $|S\rangle$ can be donated as follows

$$|S\rangle = \left\{ \underbrace{S_1, S_2, \cdots, S_\xi}_{t}, |\psi\rangle_S \right\} \tag{9}$$

where S_ξ is the classical remainder, $|\psi\rangle_S$ is the corresponding state of S_ξ.

Step 5. Bob can send the signature $|S\rangle$ to Trent.

3.3. Verification Phase

A verification algorithm is developed here based on the CRT such that Alice is able to verify Bob's signature $|S\rangle$. The verification process requires the assistance of Trent.

Step 1.When Trent receives Bob's signatures $|S\rangle$, he restores message as Equation (2) to X^*. The algorithm can be showed as follows,

$$X^* = \sum_{\xi=1}^{t} T_\xi D_\xi S_\xi \bmod D \tag{10}$$

where $D = K_1 \times K_2 \times \cdots K_t$, $D_\xi = D/K_\xi$, $T_\xi \times D_\xi \bmod K_\xi = 1$, for all $\xi \in \{1,2,\cdots,t\}$. If $X^* \ne X$, the signature has obviously been forged and Trent may reject this signature immediately. If $X^* = X$, Trent goes on for further verification.

Step 2. Trent transforms X^* to the binary sequence $\tilde{X}^*$. The process can be described as follows,

$$\begin{cases} \tilde{X}^* = \left(\dfrac{X^* - \sum_{z=0}^{m-1} \tilde{X}^*_{z-1} d^{\zeta-1}}{d^\zeta} \right) \bmod d, \zeta > 0 \\ \tilde{X}^* = 0, \zeta \le 0 \end{cases} \tag{11}$$

where d = 2. The binary sequence can be represented as $\tilde{X}^* = \{\tilde{X}^*_0, \tilde{X}^*_1, \cdots, \tilde{X}^*_{m-1}\}$, which corresponds to the states of $|\tilde{P}^*\rangle$. In this way, Trent gets the quantum message $|\tilde{P}^*\rangle$.

Step 3. Trent performs the corresponding reverse transformations U_{xyz}^{-1} $(x, y, z \in \{0,1\})$ on each state of $|\tilde{P}^*\rangle$. He can obtain the the states of $|\tilde{P}\rangle$. According to Equation (3), $|\tilde{P}\rangle$ can be described as

$$|\psi\rangle_{\tilde{P}} = \prod_{\tilde{\lambda}=0}^{m-1} \frac{1}{\sqrt{2}}\left[|0 x_{\tilde{\lambda}} y_{\tilde{\lambda}}\rangle + (-1)^{z_{\tilde{\lambda}}} |1\overline{x_{\tilde{\lambda}}}\,\overline{y_{\tilde{\lambda}}}\rangle\right] \tag{12}$$

where $x_{\tilde{\lambda}}, y_{\tilde{\lambda}}, z_{\tilde{\lambda}} \in \{0,1\}$. At last the restored message is acquered. Then Trent input it into the quantum verification circuit which is shown in **Figure 1** [24] directly, and sends the signature $|S\rangle$ to Alice at the same time.

Step 4. The message owner Alice also input the originnal message $|\psi\rangle_P$ into the quantum verification circuit at the same time. Then Alice starts to wait for the verifycation from Trent.

Step 5. We generalize the qubit string comparator introduced by Ref. [25] with quantum parallel algorithm [22] which makes the quantum computation on quantum message more effectively to compare $|\psi\rangle_{\tilde{P}}$ with $|\psi\rangle_P$. The quantum circuit which is presented in **Figure 1**. In a measurement of the outputs (O_1 and O_2), if $O_1 = 1$ and $O_2 = 0$ then $|\psi\rangle_P > |\psi\rangle_{\tilde{P}}$; if $O_1 = 0$ and $O_2 = 1$ then $|\psi\rangle_P < |\psi\rangle_{\tilde{P}}$; at last, if $O_1 = 0$ and $O_2 = 0$ then $|\psi\rangle_P = |\psi\rangle_{\tilde{P}}$. When $O_1 = 0$ and $O_2 = 0$, the arbitrator Trent informs Alice and Bob the signature is legal and credible, otherwise he informs them that signature is invalid.

4. Conclusions

So far we have proposed a group signature scheme based on CRT. Now let us discuss the security of the group signature scheme. A secure quantum signature scheme should satisfy two requirements: one is that the message should not be forged by the attacker and the other is the impossibility of disavowal by the message originator and the signatory.

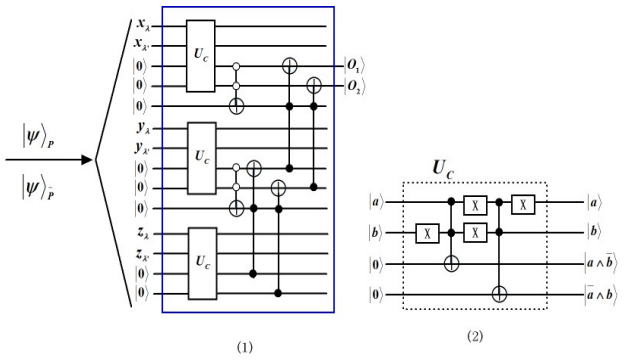

Figure 1. The quantum circuit for comparing $|\psi\rangle_{\tilde{P}}$ to $|\psi\rangle_P$ in the black box. Each particle of $|\psi\rangle_P$ and $|\psi\rangle_{\tilde{P}}$ is inputted into this quantum circuit from left, and (2) is a processing unit of (1).

4.1. Impossibility of Forgery

In this scheme, the arbitrator Trent is trusted, K» cannot be forged. Anyone attempts to forge Bob's signature would definitely be detected.

Specifically, assuming that Eve wants to imitate Bob's signature $|S\rangle$ sign on X which corresponding the message $|P\rangle$. As shown by Equation (7), Eve must know the se- cret keys K_ξ, but K_ξ cannot be forged.

The signature is unforgeable even by the message owner Alice who knows the messages and the corresponding signatures because of the unforgeable secret keys.

4.2. Impossibility of Disavowal by the Signatory and the Message Originator

According to Equation (7), Bob(signatory) would send $|S\rangle$ to Trent. Since $|S\rangle$ includes the keys K_ξ, which is only known by Bob and Trent, Bob cannot disavow his signa- ture $|S\rangle$.

Alice also cannot disavow his recieving. Because the verifier Bob who really has verified the signature cannot later deny his involvement in that his verification of the message needs the help of Trent. If he denies his involvement, Trent can confirm that he tells a lie.

5. Conclusions

In this paper, we present a group signature scheme based on Chinese Remainder Theorem in which participants share their own key with arbitrator while they don't communicate with other. Only when all the t participants cooperate with each other and with the message owner's and the arbitrator's assistance, the signature can be generated and verified successfully. The analysis of this scheme and show that secure signature can be derived. Moreover, by allowing the arbitrator to keep a record of all intermediate transmissions and computations, it is able to arbitrate the dispute between two users.

6. Acknowledgements

This work was supported by the National Natural Science Foundation of China (Grant Nos. 61272495), the Program for New Century Excellent Talents in University of Ministry of Education of China (NCET-11-0510), the Hunan Provincial Innovation Foundation For Postgraduate (Grant Nos. CX2011B087), the Excellent Doctoral Dissertation Fund of Central South University (Grant Nos. 2011ybjz030) and WCU 32-2010-000-20014-0 NRF (Korea).

REFERENCES

[1] S. William, "Cryptography and Network Security, Principles and Practice," 2nd Edition,Prentice Hall, New Jersey, 2003.

[2] D. Chaum and E. V. Heyst, "Group Signatures," *Lecture Notes in Computer Science*, Vol. 547, 1991, pp. 257-265. doi:10.1007/3-540-46416-6_22

[3] J. Camenisch and M. Stadler, "Efficient Group Signature Schemes for Large Groups," Berlin, Springer 1296, 1997, pp. 410-424.

[4] E. Bresson and J. Stem, "Efficient Revocation in Group Signature," *Proceeding of PKC01 LNCS* 1992, Berlin, Springer, 2001, pp. 190-206.

[5] G. Ateniese, J. Camenisch and M. Joye, "A Practical and Provably Secure Coalition-resistant Group Signature Scheme,"*Advances in Cryptology-Crypto2000 LNCS1880*, 2000, pp. 255-270.

[6] N. Gisin, G. Ribordy, W. Tittel and H. Zbinden, "Quantum Cryptography," *Reviews of Modern Physics*, Vol. 74, No. 145, 2002. doi:10.1103/RevM5odPhys.74.14

[7] C. H. Bennett and G. Brassard, "Quantum Cryptography: Public Key Distribution and Coin Tossing," *Proceeding of IEEE International Conference on Computers Systems*, 1984, pp. 175-179.

[8] A. K. Ekert, "Quantum Cryptography Based on Bells Theorem," *Physical Review Letters*, Vol. 67, 1991, pp. 661-663. doi:10.1103/PhysRevLett.67.661

[9] N. R Zhou, L. J Wang, L. H Gong, X. W. Zuo and Y. Liu, "Quantum Deterministic Key Distribution Protocols Based on Teleportation and Entanglement Swapping," *Optics Communication*, Vol. 284, 2011, pp. 4836-4842.

[10] C. H. Bennett, "Quantum Cryptography Using any Two Nonorthogonal States," *Physical Review*.

[11] R. Cleve, D.Gottesman and H. K. Lo, "How to Share a Quantum Secret," *Physical Review Letters*, Vol. 83, 1999, pp. 648-651. doi:10.1103/PhysRevLett.83.648

[12] M. Hillery, V. Buzek and A. Berthiaume, "Quantum Secret Sharing," *Physics Review A*, Vol. 59, 1999, pp. 1829-1834. doi:10.1103/PhysRevA.59.1829

[13] A. Karlsson, M. Koashi and N. Imoto, "Quantum Entanglement for Secret Sharing and Secret Splitting," *Physical Review A*, Vol. 59, 1999, pp. 162-168. doi:10.1103/PhysRevA.59.162

[14] G. L. Long and X. S. Liu, "Theoretically Efficient High-capacity Quantum-key-distribution Scheme," *Physical Review A*, Vol. 65, 2002, pp 1-3.

[15] G. H. Zeng and C. H. Keitel, "Arbitrated Quantum Signature Scheme," *Physical Review A*, Vol. 65, 2002, pp. 1-6.

[16] M. Curty and N. Lutkenhaus, Comment on "Arbitrated Quantum-signature Scheme," *Physical Review A*, 2008, pp. 1-4.

[17] G. H. Zeng, Reply to "Comment on 'Arbitrated Quantum-signature Scheme,"*Physical Review A*, Vol. 78, 2008, pp. 1-5.

[18] G. H. Zeng, M. H. Lee, Y. Guo and G. Q. He, "Continuous Variable Quantum Signature Algorithm," *International Journal of Quantum Infermation*, Vol. 5, No. 4, 2007, pp. 553-573. doi:10.1142/S0219749907003031

[19] Q. Li, W. H. Chan and D. Y. Long, "Arbitrated Quantum Signature Scheme Using Bell States," *Physics Review A. 79*, 2009, pp. 1-4.

[20] D. Gottesman and I. Chuang, "Quantum Digital Signatures," 2001, pp. 1-8.

[21] H. Lee, C. H. Hong and H. Kim, "Arbitrated Quantum Signature Scheme with Message Recovery," *Physical Letters A*, Vol. 32, 2004, pp. 295-300. doi:10.1016/j.physleta.2003.12.036

[22] M. Nielsen and I. Chuang, "Quantum Computation and Quantum Information," Cambridge University Press, Cambridge, 2000, pp. 171-180.

[23] C. Ding, D. Pei and A. Salomaa, "Chinese Remainder Theorem: Applications in Computing, Coding, Cryptography," *World Scientific Publishing Co., Inc.*, 1996, pp. 1-8. doi:10.1142/9789812779380_0001

[24] 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, 2011, pp. 653-670. doi:10.1007/s11128-010-0225-7

[25] D. S. Oliveira and R. V. Ramos, "Quantum Bit String Comparator: Circuits and Applications," *Quatum Computers and computing*, Vol. 7, No. 1, 2007, pp.17-26.

[26] X. J. Wen, "A Group Signature Scheme Based on Quantum Teleportation," *Physica Scripta*, Vol. 81, No. 5, 2001.

[27] X. J. Wen, X. M. Niu, L. P. Ji and Y. Tian, "A Weak Blind Signature Scheme Based on Quantum Cryptography," *Optics Communication*, Vol. 282, No. 4, 2009, pp. 666-669.

[28] Y. G. Yang and Q. Y. Wen, "Arbitrated Quantum Signature of Classical Messages against Collective Amplitude Damping Noise," *Opticcs Communication*, Vol. 283, No. 16, 2010, pp. 3198-3201. doi:10.1016/j.optcom.2010.04.020

[29] T. Hwang, S. K. Chong, Y. P. Luo and T. X. Wei, "New Arbitrated Quantum Signature of Classical Messages Against Collective Amplitude Damping Noise," *Optics Communication*, Vol. 284, 2011, No. 12. pp. 3144-3148. doi:10.1016/j.optcom.2011.01.025

[30] R. Xu, L. S. Huang, W. Yang and L. B. He, "Quantum Group Blind Signature Scheme without Entanglement," *Optics Communication*, Vol. 284, 2011, No. 14, pp. 3144-3148. doi:10.1016/j.optcom.2011.03.083

[31] M. M. Wang, X. B. Chen, X. X. Niu and Y. X. Yang, "Re-examining the Security of Blind Quantum Signature Protocols," *Physica Scripta*, Vol. 86, No. 5, 2012. doi:10.1088/0031-8949/86/05/055006

[32] T. Y. Wang and Q. Y. Wen, "Fair Quantum Blind Signatures," *Chinese Physics B*, Vol. 19, No. 6, 2010. doi:10.1088/1674-1056/19/6/060307

[33] F. Gao, S. J. Qin, F. Z. Guo and Q. Y. Wen, "Cryptanalysis of the Arbitrated Quantum Signature Protocols," *Physical Review A*, Vol. 84, No. 2, 2011. doi:10.1103/PhysRevA.84.022344

[34] Q. Li, W. H. Chan and D. Y. Long, "Arbitrated Quantum Signature Scheme Using Bell States," *Physics Review A*, Vol. 79, No.5, 2009. doi:10.1103/PhysRevA.79.054307

[35] T. Hwang, Y. P. Luo and S. K. Chong, "Comment on 'Security Analysis and Improvements of Arbitrated Quantum Signature Schemes'," *Physics Review A*, Vol. 85, No. 5, 2012. doi:10.1103/PhysRevA.85.056301

