Journal of Modern Physics, **2013, 4, 83-88**
doi:10.4236/jmp.2013.45B014 Published Online May 2013 (http://www.scirp.org/journal/jmp)

An Arbitrated Quantum Signature Scheme Based on Chaotic Quantum Encryption Algorithm

Ying Guo[1], Jun Xie[1], Jun Li[2], Moon Ho Lee[2]
[1]School of Information Science and Engineering, Central South University, Changsha, China
[2]Department of Electronics and Information Engineering, Chonbuk National University, Jeonju, Korea
Email: yingguo@csu.edu.cn, moonho@jbnu.ac.kr

Received 2013

ABSTRACT

An arbitrated quantum signature (AQS) scheme is demonstrated via the improved quantum chaotic encryption algorithm with the quantum one-time pad based on chaotic operation string. In this scheme, the signatory signs the message and the receiver verifies the signature's validity with the aid of the arbitrator who plays a crucial role when a dispute arises. Analysis shows that the signature can neither be forged nor disavowed by the malicious attacker.

Keywords: Component; Formatting; Style; Styling; Insert

1. Introduction

Digital signature that enables to settle disputes about the authenticity of the message is an essential cryptographic primitive. It has been applied in secure electronic commerce, whose security depends much on the intractability of factoring large numbers or solving discrete logarithms. However, it would be broken via Shor's algorithm when a quantum computer would be available someday [1]. Consequently, quantum signature has been suggested to provide the authenticity and nonrepudiation of quantum states with unconditional security based on quantum mechanics [2,3]. There are usually two essential requirements in quantum signature, i.e., unforgeability and undeniability [4].

An arbitrated quantum signature (AQS) scheme [2] was proposed to sign the quantum message via quantum one-time pad [5] using the Greenberger-Horne-Zeilinger (GHZ) states with availability of the trusted arbitrator. The security depends on the secure keys shared among legal users. However, it could be repudiated by the dishonest receiver [6]. After that an improved AQS scheme was presented using Bell states instead of GHZ states while providing a higher efficiency in transmission and reducing the complexity of its implementation [7]. However, it was pointed out that the yielded signature could still be repudiated by the receiver as the original scheme did [6]. Although two AQS schemes were proposed to solve this problem, the receiver would actively negate the signature since he may get the benefits from the denial-of-service (DoS) attack strategy without being detected [8, 9].

Actually, in an AQS scheme the entrusted arbitrator plays an important role when a dispute arises among participants. Since the arbitrator may not solve a dispute when Bob claims that the verification of the signature is not successful, the previous AQS schemes are not always valid due to the contradiction to the undeniable requirement of signatures [2,3,7]. Recently, it has been pointed out [13,14] that those AQS schemes [2,3,7] provide security only against a total break attack and there is an existential forgery attack that can validly modify the signature. In order to conquer this shortcoming, we designate an AQS scheme using an improved quantum chaotic encryption algorithm with classical communications that are assumed to be susceptible to eavesdropping but not to the injection or alteration of the message [10-12]. The quantum chaotic encryption system has several interesting characteristics, such as the sensitive dependence on initial conditions and system parameters, pseudo- random property, non-periodicity and topological transitivity, etc. These characteristics meet some secure requirements such as diffusion and mixing in quantum cryptosystem. The present scheme can not only avoid being disavowed by the receiver, but also can preserve all merits in the previous schemes.

As far as we know, the chaos-based AQS scheme with diffusion quantum operations has not been reported. In this paper, we propose an AQS scheme via the improved quantum chaotic encryption algorithm. This paper is organized as follows. In section II, we designate a quantum chaotic encryption algorithm based on the quantum one-time pad depending on the chaotic operation string performed on quantum states. In section III, we develop

an AQS scheme based on the improved quantum chaotic encryption algorithm. It involves three participants, including the signatory, the receiver and the arbitrator, in three phases, i.e., initializing phase, signing phase and verifying phase. In section IV we analyze the security of the AQS scheme according to the requirements of the quantum signature. It is shown that the present scheme is secure due to the implementation of the quantum chaotic encryption algorithm. Finally, conclusions are drawn in section IV.

2. Quantum Chaotic Encryption Algorithm

We let Pauli matrices σ_x, σ_z and σ_y denote Pauli-X, Pauli-Z and Pauli-Y gates respectively. Let $|P\rangle$ be a quantum message described as $|P\rangle = |P_1\rangle \otimes \cdots |P_n\rangle$ with $|P_i\rangle = \alpha_i |0\rangle + \beta_i |1\rangle, \forall i \in \{1, \cdots, n\}$. Subsequently, E_κ denotes the conventional quantum one-time pad for a given string $\kappa = (\kappa_1, \cdots, \kappa_{2n})$ of length 2*n*, i.e.,

$$E_\kappa(|P\rangle) = \bigotimes_{i=1}^{n} \sigma_u^{\kappa_{2i-1}} \sigma_v^{\kappa_{2i}} |P_i\rangle, \quad (1)$$

with $\sigma_u, \sigma_v \in \{I, \sigma_x, \sigma_z, \sigma_y\}$, where *I* denotes an identity operation.

Recall that for a given key $k_0 = (k_{0,1}, \cdots, k_{0,2n})$ of length 2*n* there is a chaotic encryption algorithm expressed in a recursive fashion

$$k_i = C_T[k_{i-1}],\ i \in \{1, \cdots, r\}, \quad (2)$$

where $k_r = \kappa$ denotes the cryptogram string of length 2*n* that is used for the quantum encrypting algorithm in Equation(1), and C_T is a chaotic key-dependent transformation. In detail, we write $k_{i,0}, \cdots, k_{i,2n-1}$ for each a string k_i of length 2*n* in the i^{th} round, $\forall i = \{0, \cdots, r\}$.

The string κ consists of *r* rounds of identical transformations applied in a sequence to the initial key k_0. The chaotic transformation CT is defined as

$$k_{i,k+1} = k_{i-1,k} \oplus f_{k-1}[k_{i-1,1}, \cdots, k_{i-1,k-1}, t_{i-1,k-1}], \quad (3)$$

where $t_i = (t_{i,0}, \cdots, t_{i,2n-1})$ denotes a subkey that controls the i^{th} round, each function f_i is obtained via discretization of a conventional nonlinear map with mixing property and robust chaos, $f_0 = t_{i,0}, k_{i,2n} = k_{i,0}$, $i \in \{1, \cdots, l\}$ and $k \in \{1, \cdots, 2n\}$. The decrypting structure undoes the transformations of the encrypting structure where *r* decrypting rounds are applied to the received vector k_r to recover k_0. In each decrypting round, the inverse transformation can be described as

$$k_{i-1,k} = k_{i-1,k+1} \oplus f_{k-1}[k_{i-1,1}, \cdots, k_{i-1,k-1}, t_{i-1,k-1}]. \quad (4)$$

We note that the afore-mentioned chaotic map *f* can be generated in a quadratic (logistic) chaotic map [20] given by

$$f(y_j) = \begin{cases} \text{floor}\left[y_j\left(2^{2n} - y_j\right)/2^{2n-2}\right], & \text{if } \tilde{y}_j < 2^{2n} \\ 2^{2n} - 1, & \text{if } \tilde{y}_j = 2^{2n} \end{cases} \quad (5)$$

with $\tilde{y}_j = \text{floor}\left[y_j\left(2^{2n} - y_j\right)/2^{2n-2}\right]$ for $\tilde{y}_j = k_{j,1} \oplus \cdots \oplus k_{j,k-1} \oplus t_{j,k-1}$. It can be implemented in two steps [21]. In the first step, the logistic map is scaled so that input and output values are in the interval [0, 22*n*]. The second step is discretization of the newly derived map.

In addition, this map can also be generated in an exponential chaotic map

$$f(y_j) = \begin{cases} a^{y_j} \bmod 2^{2n} + 1, & \text{if } \tilde{y}_j < 2^{2n} \\ 0, & \text{if } \tilde{y}_j = 2^{2n} \end{cases} \quad (6)$$

with $\tilde{y}_j = a^{y_j} \bmod 2^{2n} + 1$, where the number *a* is a generator of the multiplicative group of nonzero elements of the Galois field of order $2^{2n} + 1$.

In what follows, we consider an improved quantum chaotic encryption algorithm with a quantum one-time pad based on the chaotic string throughout this paper. Assume that the Hadamard gate can be defined as $\sigma_h = 1/\sqrt{2}(\sigma_x + \sigma_z)$. According to the algorithm in Equation(1) for a given chaotic string κ of length 2*n*, we obtain the similar quantum chaotic encryption algorithm given by

$$E_\kappa(|P\rangle) = \bigotimes_{i=1}^{n} \sigma_x^{\kappa_{2i-1}} \sigma_h^{\kappa_{2i}} |P_i\rangle. \quad (7)$$

It is obvious that one can not obtain the exact relationship $\sigma_x \sigma_h = \pm \sigma_x \sigma_h$ due to the properties of Paulioperations [1]. This feature can be well suitable for a particular purpose of the generation of the quantum signature that can not be forged or disavowed by the attacker.

3. Prepare Arbitrated Quantum Signature Scheme with Chaotic Encryption

As an AQS scheme, it should satisfy at least two constraints, i.e., one is that the signature should not be forged by the attacker and another is the impossibility of disavowal of the signatory and receiver. It usually involves three participants, including the signatory Alice, the receiver Bob and the trusted arbitrator Charlie, in three signing phases, i.e., initializing phase, signing phase and verifying phase. In the previous AQS scheme [2,3], it has been stated that Bob can not disavow that he has obtained the signature. However, he can repudiate the integrality of the signature since he can reject the signature in verifying phase [6,8,9]. It means that Bob can admit receipt of the signature but deny its correctness. In order to conquer this shortcoming, we design an improved AQS scheme based on the quantum chaotic encryption algorithm with the prepared chaotic string using

the shared key and subkey.

Suppose that Alice wants to sign the quantum message $|P\rangle = |P_1\rangle \otimes \cdots \otimes |P_n\rangle$ and has at least three copies of $|P\rangle$. In order to obtain a low error probability in verifying phase, we can assume that n is large enough; otherwise we can use $|P\rangle^{\otimes m}$ instead of $|P\rangle$, where m is a large enough integer. Then the proposed AQS scheme goes as follows.

3.1. Initializing Phase

Step I1. Alice shares an initial secret key k_0^a of length $2n$ with Charlie through quantum key distribution (QKD) protocol [10,11]. Then she selects another private subkey $t_a = \{t_1, \cdots, t_r\}$ of length $2n$ kept by herself. Implementing the chaotic encrypting algorithm in Equation (2), she achieves a string κ_a of length $2n$. Similarly, Bob generates another sequence κ_b using his initially secret key κ_0^b and subkey t_b shared beforehand with Charlie.

Step I2. Charlie generates n Bell states $|\psi\rangle = (|\psi_1\rangle, \cdots, |\psi_n\rangle)$ with $|\psi_i\rangle = \frac{1}{\sqrt{2}}(|00\rangle_{ab} + |11\rangle_{ab}), i \in \{1, \cdots, n\}$, where the subscripts a and b denote the photons that are transmitted to Alice and Bob via the authenticated quantum channel [15,16].

3.2. Signing Phase

Step S1. Alice transforms the message $|P\rangle$ into the random qubit string $|P'\rangle = E_{t_a}(|P\rangle)$ using the quantum one-time pad algorithm expressed in Equation (7) with her subkey t_a. For each resulting qubit, one obtains

$$|P_i'\rangle = \alpha_i'|0\rangle + \beta_i'|1\rangle.$$

Step S2. Alice performs a quantum chaotic encryption algorithm with the encrypted string κ_a and generates the chaotic qubit string $|S_a\rangle = E_{\kappa_a}(|P'\rangle)$.

Step S3. Alice combines each qubit $|P_i'\rangle$ with Bell state $|\psi_i\rangle$. The combined system $|\phi_i\rangle = |P_i'\rangle \otimes |\psi_i\rangle$ can be rewritten as

$$\begin{aligned}|\phi_i\rangle = \frac{1}{2}[&|\psi^+\rangle(\alpha_i'|0\rangle + \beta_i'|1\rangle) + |\psi^-\rangle(\alpha_i'|0\rangle - \beta_i'|1\rangle) \\ &+ |\Phi^+\rangle(\alpha_i'|1\rangle + \beta_i'|0\rangle) + |\Phi^-\rangle(\alpha_i'|1\rangle - \beta_i'|0\rangle)],\end{aligned} \quad (8)$$

After implementing Bell state measurements on her photon pairs, she obtains $|M_a\rangle = \{|M_a^{(i)}\rangle : i \in \{1, \cdots, n\}\}$ where $|M_a^{(i)}\rangle$ denotes one of Bell states performed on the i[th] photon pair.

Step S4. Alice transforms $|M_a\rangle$ into another random qubit string $|M_a'\rangle = E_{t_a}|M_a\rangle$ using the quantum one-time pad algorithm with her subkey t_a.

Step S5. Alice transmits $|S\rangle = (|P'\rangle, |M_a'\rangle, |S_a\rangle)$ to Bob via the authenticated quantum channels.

3.3. Verifying Phase

Step V1. Bob performs the quantum chaotic encryption algorithm on $|P'\rangle$ and $|S_a\rangle$ using his chaotic string κ_b. Then he obtains $|T_b\rangle = E_{\kappa_b}(|P'\rangle, |S_a\rangle)$, which is sent to Charlie.

Step V2. Charlie decrypts $|T_b\rangle$ using the calculated string κ_b with parameters k_b^0 and t_b, and obtains $|P'\rangle$ and $|S_a\rangle$. Similarly, he performs a quantum chaotic encryption algorithm on $|P'\rangle$ using another string κ_a with parameters k_a^0 and t_a, and obtains $|S_c\rangle = E_{\kappa_a}(|P'\rangle)$, which should be consistent with $|S_a\rangle$. After comparing two unknown states $|S_a\rangle$ and $|S_c\rangle$ [17-19], he sets the verification parameter $V = 1$ if $|S_a\rangle = |S_c\rangle$; otherwise he sets $V = 0$.

Step V3. Charlie performs another quantum chaotic encryption algorithm on $|P'\rangle, |S_a\rangle$ and V using the chaotic string κ_b, and achieves $|T_c\rangle = E_{\kappa_b}(|P'\rangle, |S_a\rangle, V)$. Then he sends $|T_c\rangle$ back to Bob.

Step V4. Bob decrypts $|T_c\rangle$ using κ_b and obtains $|P'\rangle$, $|S_a\rangle$ and V. If $V = 0$, then it shows that the signature has been obviously forged; otherwise Bob informs Alice to publish her subkey t_a and goes on to the next verification.

Step V6. Alice publishes the subkey t_a by the secure public channel.

Step V7. After Bob receives t_a, he recovers Alice's encrypted qubit string $|M_a\rangle$ from $|M_a'\rangle$. After that he obtains $|P_b'\rangle$ on his photons after implementing some suitable unitary operation based on the yielded states $|M_a\rangle$ [1]. Then he makes a comparison between $|P_b'\rangle$ and $|P'\rangle$. If $|P_b'\rangle \neq |P'\rangle$, he gives it up; otherwise he restores the initial message $|P\rangle$ from $|P'\rangle$ with t_a. He holds $|S_a\rangle$ as Alice's signature for the message $|P\rangle$.

We note that in this AQS scheme it can achieve a function of the signature. Actually, in verifying phase Charlie can obtain κ_a that depends on parameters K_0^a and t_a, and hence he can judge whether the equation $|R_a\rangle = |R_c\rangle$ holds or not. When it holds, the signed message has really come from Alice since others do not know k_0^a and t_a and hence generate the chaotic string κ_a [20,21]. After Charlie's verification, the message is transmitted to Bob, and hence he does not know the content

of the message excepts for his judgment *V* that shows its authenticity. Actually, it provides a potential approach for Charlie to resolve a dispute between Alice and Bob. Otherwise it is an exact message authentication instead of a signature. For example, Bob says that Alice signed for the message $|P\rangle$, but Alice announces that she did not sign such a message (maybe she indeed signed another message $|\mathcal{P}\rangle \neq |P\rangle$). In this condition, Charlie requires Bob to provide $|P'\rangle$ and $|S_a\rangle$, encrypts $|P'\rangle$ to obtain $|S_c\rangle$ with the chaotic string κ_a, and then verifies whether $|S_a\rangle$ equals to $|S_c\rangle$ or not. If the comparison result is positive, it implies that Alice is disavowing her signature. Otherwise, the signature is forged by Bob.

In addition, this AQS scheme can be similarly extended on the basis of the quantum chaotic encryption algorithm in terms of the GHZ triplet states or the single-qubit states without being entangled. As the aforementioned statements, it can also strengthen the security of the corresponding signature in a small-scale quantum computation network.

4. Security Analysis

So far we have proposed an AQS scheme based on an improved quantum chaotic encryption algorithm. In this section, what we are concerned is the security of this scheme.

4.1. Impossibility of Forgery Attack

If an attacker Eve tries to forge Alice's signature $|S_a\rangle$ for her own sake, she should know the initially shared secret key k_0^a and subkey t_a. However, it is impossible due to the unconditional security of quantum key distribution (QKD) [10,11]. In addition, the usage of the chaotic encryption algorithm enhances the security of the present scheme [20,21]. In a worse case that k_0^a is exposed to Eve, she can not succeed in forging the signature since she can not create the appropriate Bell state measurement $|M_a\rangle$ related to the transformed message $|P'\rangle$. Actually, Bob would completely find the forgery using the correlation of Bell states since the further verification about the condition $|P_b'\rangle \neq |P'\rangle$ could not be hold without the correct measurement result $|M_a\rangle$. Consequently, the forgery of Eve is impossible.

If the malicious Bob attempts to counterfeit Alice's signature $|S_a\rangle$ in verifying phase, he also has to know Alice's secret key k_0^a to generate $|S_a\rangle$. However, the information that he can achieve betrays nothing about k_0^a from $|S_a\rangle$ due to the properties of the chaotic operation string performed in quantum chaotic encryption algorithm [20,21]. Therefore, Bob can not forge Alice's signature.

Furthermore, in the previous AQS schemes [13,14], the security is mostly ensured against the distillation of the secret key from the transmitted signature. Unfortunately, there are some security flaws due to the usage of quantum one-time pad with Pauli operations σ_x and σ_z that have a relation $\sigma_x\sigma_z = \pm\sigma_z\sigma_x$. Therefore, there is a possible forgery attack that enables a dishonest user to modify the signature even without any knowledge of the secret key. Without loss of generality, we consider a case that the malicious Bob is an attacker. The goal of Bob's forgery attack is to change the message and signature $(|P\rangle, |S_a\rangle)$ to $(|\mathcal{P}\rangle, |S_a\rangle)$ by performing operation $Q = \otimes_{i=1}^{n} U_i$ without any knowledge of k_0^a and t_a and hence κ_b, where U_i denotes a single-qubit unitary operation, i.e., $(Q|P\rangle, Q|S_a\rangle) = (|\mathcal{P}\rangle, |S_a\rangle)$. In this attack, Bob does not care about the content of the message but how to use the relation of the message and signature. It has been shown that the previous schemes may be cracked by this forgery attack because all operations performed for random rotation and encryption are only Pauli operations that commute or anticommute with each other. Namely, taking a message $|P\rangle$, the signature is in form of $ER|P\rangle$, where *R* and *E* denote a quantum random operation and a quantum one-time pad encryption, respectively. If Bob implements a forgery attack by performing an operation *Q*, then the resulting signature becomes $QER|P\rangle$. In the verifying phase, Charlie obtains $R^{\dagger}E^{\dagger}QER|P\rangle$. Therefore, Bob could select a suitable operation *Q* that commutes with *E* and *R* since the encryption is based on the usage of Pauli operations σ_x and σ_z that commute or anticommute with each other [1]. However, in the present scheme, the signing process is based on the quantum chaotic encryption algorithm that depends on the chaotic operation string including operations σ_x and σ_h, instead of σ_x and σ_z. It is easy to prove that there is no nontrivial quantum operation *Q* that commutes with σ_x and σ_h. It implies that Bob can not implement this forgery attack successfully, and his dishonest behaviors will be detected with high probability due to the composite chaotic character of the quantum chaotic encryption algorithm derived from a nonlinear system that makes the yielded qubit sequence in possession of a fantastic random [20, 21].

4.2. Impossibility of Disavowal Attack

Suppose that Alice wants to disavow her signature for her own benefits. In this case, Charlie is required to make a judgment. Actually, Charlie can confirm that Alice has signed the message since Alice's initial secret key k_0^a and subkey t_a are both involved in the chaotic string κ_a and hence in the signature $|S_a\rangle$. Thus Alice can not deny signing the message $|P\rangle$. In addition, Alice may not publish her correct subkey t_a in the public board after Bob completes his comparison operations for the

verification. This gives Alice an opportunity to send any subkey $t_a^{'}$ that may not be equal to t_a. However, Bob and Charlie can only accept Alice's signature $|S_a^{'}\rangle$ that contains $t_a^{'}$ instead of $|S_a\rangle$ that embraces t_a. Moreover, the correct subkey t_a has been shared beforehand with Charlie. If Alice sets $t_a^{'} \neq t_a$, it can be completely detected by Charlie since he has to generate $|S_c\rangle$ using the quantum chaotic encryption algorithm dependent on subkey $t_a^{'}$, which results in $|S_c\rangle \neq |S_a\rangle$ in verifying phase. It means that Alice has to send Bob the correct subkey t_a if she wants to transmit the message with her real signature. Someone may worry about that the attacker may change the published subkey t_a in verifying phase so that Bob can not recover the message $|P\rangle$ without t_a. We note that the deployed classic channel is assumed be securely established, and the alteration of the subkey t_a would not happen.

In order to avoid disavowal of Bob, we would not let Bob achieve the whole signature in verifying phase. Actually, Alice only sign the transformed message via the quantum chaotic encryption algorithm based on the chaotic operation string. To restore the initial message $|P\rangle$, Bob has to require Alice to publish her subkey t_a and then recovers the measurement result $|M_a\rangle$ from the received string $|M_a^{'}\rangle$. It implies that Bob has no chance to repudiate the received signature. Moreover, Bob can not disavow the receipt of $(|P^{'}\rangle, |S_a\rangle)$ since he has transmitted $|T_b\rangle$ that contains his initial secret key κ_0^b and subkey t_a to Charlie for the verification of the signature. For the further verification, Charlie needs to decrypt $|T_b\rangle$ to recover $|P^{'}\rangle$ and $|S_a\rangle$ with k_0^b and t_b. Also, he obtains $|S_c\rangle = E_{\kappa_a}(|P^{'}\rangle)$. If $|S_c\rangle \neq |S_a\rangle$, then Bob's disavowal is detected.

In addition, Bob would not repudiate the integrality of the signature. We consider a case that Bob claims $|P_b^{'}\rangle \neq |P^{'}\rangle$ even when $|P_b^{'}\rangle = |P^{'}\rangle$ since Charlie would not check whether $|M_a^{'}\rangle$ is correct or not. However, this attack can not work on the present scheme due to the fact he has to recover the initial message $|P\rangle$ with $|M_a\rangle$ that is obtained from $|M_a^{'}\rangle$ in verifying phase. Namely, if Bob claims $|P_b^{'}\rangle \neq |P^{'}\rangle$, it means that he has not received the correct signature $|S_a\rangle$. It shows that Bob can not repudiate the integrality of the signature. Actually, in order to avoid being disavowed by Bob, this scheme utilizes the secure classic channel for the transmission of the subkey t_a that is assumed not be susceptible to be altered by an attacker [16].

5. Conclusions

We have investigated an AQS scheme based on the quantum chaotic encryption system in three phases, i.e., initialing phase, signing phase and verifying phase. The signatory sign the message via the improved quantum chaotic encryption algorithm based on the chaotic operation string tied to the initial key and subkey shared with the arbitrator. The receiver verifies the signature with the aid of the arbitrator, who plays a crucial role when a possible dispute arises. The security is ensured by the employment of the quantum chaotic encryption system with the secret key and subkey being embedded in. Security analysis shows that the signature can not be forged by the attacker. In addition, neither the signatory nor the receiver can successfully disavow the signed message.

6. Acknowledgements

This work was supported by the National Natural Science Foundation of China (60902044, 61272495), the New Century Excellent Talents in University, China (NCET-11-0510), and partly by the World Class University R32-2010-000-20014-0 NRF, MEST 2012-002521 NRF, and Fundamental Research 2010-0020942 NRF, Korea.

REFERENCES

[1] M. Nielsen and I. Chuang, "Quantum computation and quantum information," Cambridge University Press, Cambridge, 2000.

[2] G. Zeng and C. H. Keitel, "Arbitrated Quantum-Signature Scheme," *Physical Review A*, Vol. 65, No. 4, 2002, 042312. doi:10.1103/PhysRevA.65.042312

[3] G. H. Zeng, "Reply to 'Comment on Arbitrated Quantum-Signature Scheme'," *Physical Review A*, Vol. 78, No. 1, 2008, 016301. doi:10.1103/PhysRevA.78.016301

[4] D. Gottesman and I. Chuang, arXiv:quant-ph/0105031v2.

[5] P. O. Boykin and V. Roychowdhury, "Optimal Encryption of Quantum Bits," *Physical Review A*, Vol. 67, No. 4, 2003, 042317 . doi:10.1103/PhysRevA.67.042317

[6] G. Zou and D. Qiu, "Security Analysis and Improvements of Arbitrated Quantum Signature Schemes," *Physical Review A*, Vol. 82, No. 4, 2010, 042325. doi:10.1103/PhysRevA.82.042325

[7] Q. Li, W. H. Chan and D. Y. Long, "Arbitrated Quantum Signature Scheme Using Bell States," *Physical Review A*, Vol. 79. No. 5, 2009, 054307. doi:10.1103/PhysRevA.79.054307

[8] T. Hwang, Y. Luo and S. Chong, "Comment on 'Security Analysis and Improvements of Arbitrated Quantum Signature Schemes'," *Physical Review A*, Vol. 85, No.5, 2012, 056301. doi:10.1103/PhysRevA.85.056301

[9] Q. Y. Cai, "The 'Ping-Pang' Protocol Can Be Attacked

without Eavesdropping," *Physical Review letters*, Vol. 91, 2003, 109801. doi:10.1103/PhysRevLett.91.109801

[10] A. K. Ekert, "Quantum Cryptography Based on Bell' s Theorem," *Physical Review Letters*, Vol. 67, No. 6, 1991, pp. 661-663. doi:10.1103/PhysRevLett.67.661

[11] C. H. Bennett, "Quantum Cryptography Using Any Two Nonorthogonal," *Physical Review Letters*, Vol. 68, 1992, pp. 3121-3124. doi:10.1103/PhysRevLett.68.3121

[12] S. K. Chong, Y. P. Luo and T. Hwang, "On 'Arbitrated Quantum Signature of Classical Messages Against Collective Amplitude Damping Noise'," *Optics Communications*, Vol. 284, No. 3, 2011, pp. 893-895. doi:10.1016/j.optcom.2010.09.080

[13] J. W. Choi, K. Y. Chang and D. Hong, "Security Problem on Arbitrated Quantum Signature Schemes," *Physical Review A*, Vol. 84. No. 6, 2011, 062330. 84, 062330. doi:10.1103/PhysRevA.84.062330.

[14] F. Gao, S.-J. Qin, F.-Z. Guo and Q.-Y. Wen, "Cryptanalysis of the Arbitrated Quantum Signature Protocols," *Physical Review A*, Vol. 84, 2011, 022344. doi:10.1103/PhysRevA.84.022344

[15] M. Curty, D. J. Santos, E. Pierez, and P. Garcia-Fernandez, "Qubit Authentication," *Physical Review A*. Vol. 66. No. 2, 2002, 022301. doi:10.1103/PhysRevA.66.022301

[16] L.-M. Duan, M. D. Lukin, J. I. Cirac and P. Zoller, "Long-Distance Quantum Communication with Atomic Ensembles and Linear Optics," *Nature*. Vol. 414, 2001, pp. 413-418. doi:10.1038/35106500

[17] H. Buhrman, R. Cleve, J. Watrous and R. de Wolf, "Quantum Fingerprinting,"*Physical Review Letters*. Vol. 87, 2001, 167902. doi:10.1103/PhysRevLett.87.167902

[18] Q. Li, W. H. Chan and D. Y. Long, "Arbitrated Quantum Signatyre Scheme Using Bell States," *Physical Review A*. Vol. 79, 2009, 054307. doi:10.1103/PhysRevA.79.054307

[19] S. Pang and S. Wu, "Comparison of Mixed Quantum States," *Physical Review A*, Vol. 84, 2011, 012336. doi:10.1103/PhysRevA.84.012336

[20] M. S. Baptista, "Cryptography With Chaos,"*Physics Letters A*. Vol. 240. No. 1-2, 1998, pp. 50-54. doi: 10.1016/S0375-9601(98)00086-3

[21] G. Jakimoski and L. Kocarev, "Circuits and Systems Ⅰ: Fundamental Theory and Applications on," *IEEExplore*. Vol. 48. No. 2, 2001, pp. 163-169. doi:10.1109/81.904880

