J. Cent. South Univ. (2015) 22: 2604−2611
DOI: 10.1007/s11771-015-2790-5

Springer

A chaos-based quantum group signature scheme in quantum cryptosystem

LOU Xiao-ping(娄小平)[1, 2], CHEN Zhi-gang(陈志刚)[2], Moon Ho Lee[3]

1. School of Computer Science and Technology, Hunan University of Arts and Science, Changde 415000, China;
2. School of Information Science and Engineering, Central South University, Changsha 410083, China;
3. Institute of Information and Communication, Chonbuk National University, Chonju 561756, Korea

Abstract: A quantum group signature (QGS) scheme is proposed on the basis of an improved quantum chaotic encryption algorithm using the quantum one-time pad with a chaotic operation string. It involves a small-scale quantum computation network in three phases, i.e. initializing phase, signing phase and verifying phase. In the scheme, a member of the group signs the message on behalf of the group while the receiver verifies the signature's validity with the aid of the trusty group manager who plays a crucial role when a possible dispute arises. Analysis result shows that the signature can neither be forged nor disavowed by any malicious attackers.

Key words: group signature; chaotic encryption; quantum entanglement; quantum cryptography

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. Group signature, introduced by CHAUM and HEYST [1], is a method for allowing a member of a group to sign a message on behalf of the group. It is a specific type where the identity of the signer is anonymous to the receiver for privacy protection. However, it would be broken via Shor's algorithm when a quantum computer becomes available someday [2−3]. Consequently, the quantum signature has been suggested to provide authenticity and nonrepudiation of the message with unconditional security based on quantum mechanics [4−5]. With the development of quantum cryptography, some quantum group signature (QGS) schemes have recently been introduced to ensure security. A pioneering QGS protocol was proposed by WEN et al [6]. In their scheme, the group manager is simply considered the arbitrator and the technique of teleportation is implemented to verify the validity of the signature. XU et al [7] proposed a novel quantum group blind signature protocol without entanglement, which is easier to be realized in practice. However, these two protocols were pointed out that there still are some potential security loopholes [8]. For example, Alice (Bob) could achieve the disavowal in the protocol. Furthermore, the arbitrator can not verify when the disputation happens. ZHANG et al [9] designed a secure QGS scheme for classical messages. In their scheme, the integrity verification was accomplished by a Hash function which is insecure in the quantum encryption system. Recently, SU and LI [10] found that almost all typical QGSs are vulnerable to the inside attack, by which all other legal members of the group can forge the signature utilizing the anti-commutative relationship among the Pauli operation and the encryption operation, and the public board.

In order to conquer these shortcomings, a QGS is proposed using an improved quantum chaotic encryption algorithm with classical communications that are assumed to be susceptible to eavesdropping but not to injection or alteration of the message [11−12]. The proposed quantum chaotic crypotosystem has several interesting characteristics, such as the sensitive dependence on initial conditions and system parameters, pseudo-random property, non-periodicity and topological transitivity. These characteristics meet well secure requirements, such as diffusion and mixing in quantum cryptosystem. Furthermore, our scheme cannot only make up some secure loopholes in the previous protocol, but also preserve several merits in the classical group signature.

Foundation item: Project(61379057) supported by the National Natural Science Foundation of China; Project supported by the Construct Program of the Key Discipline in Hunan University of Arts and Science, China; Project(2012BS01) supported by Science Technology Research and Development Projects of Changde, China; Project supported by Science and the MEST2012-002521, NRF, Korea
Received date: 2014−01−13; **Accepted date:** 2014−09−13
Corresponding author: CHEN Zhi-gang, PhD, Professor; Tel: +86−13508490353; E-mail: czg@csu.edu.cn

2 Quantum chaotic cryptosystem

Without loss of generality, Pauli matrices $\boldsymbol{\sigma}_x$, $\boldsymbol{\sigma}_z$ and $\boldsymbol{\sigma}_y$ denote Pauli-x, Pauli-z and Pauli-y gates. respectively. Let $|P\rangle$ be a quantum message described as $|P\rangle = |P_1\rangle \otimes \cdots \otimes |P_n\rangle$ with $|P_i\rangle = \alpha_i|0\rangle + \beta_i|1\rangle$, where $|\alpha|_i^2 + |\beta|_i^2 = 1$, $\forall \in \{1,2,\cdots,n\}$. Subsequently, E_κ denotes the conventional quantum one-time pad for a given string $\kappa=(\kappa_1, \kappa_2, \cdots, \kappa_{2n})$ of length $2n$, i.e.,

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

where $\sigma_u, \sigma_v \in \{I, \boldsymbol{\sigma}_x, \boldsymbol{\sigma}_z, \boldsymbol{\sigma}_y\}$ and I denotes an identity operation [2].

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

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

where $k_r=k$ denotes the cryptogram string of length $2n$ that is used for the quantum encrypting algorithm in Eq.(1), and C_T is a chaotic key-dependent transformation. In detail, $(k_{i,0}, k_{i,1}, \cdots, k_{i,2n-1})$ denotes each a string k_i of length $2n$ in the i-th round, $\forall i \in \{0,1,\cdots,r\}$. The string κ consists of r rounds of identical transformations applied in a sequence to the initial key k_0. The chaotic transformation C_T is defined as

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

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, $i \in \{1,2,\cdots,2n\}$, $f_0=t_{i,0}$ and $k_{i,2n+2}=k_{i,0}$. The decrypting structure undoes the transformations of the encrypting structure where r decrypting rounds are applied to the received vector κ to recover k_0. In each decrypting round, the inverse transformation can be described as

$$k_{i-1,k} = k_{i,k+1} \oplus f_{k-1}[k_{i-1,1}, \cdots, k_{i-1,k-1}, t_{i-1,k-1}] \tag{4}$$

For example, the chaotic map f can be generated in a quadratic (logistic) chaotic map [13]

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

where $\tilde{y}_j = \text{floor}[y_i(2^{2n} - y_j)/2^{2n-2}]$ with $y_i = k_{j,1} \oplus \cdots \oplus k_{j,k-1} \oplus k_{j,k-1}$. It can be implemented in two steps [14]. In the first step, the logistic map is scaled so that input and output values are in the interval $[0,2^{2n}]$. The second step is discretization of the newly derived map. In addition, this map can also be generated in an exponential chaotic map:

$$f(y_i) = \begin{cases} a^{y_i} \bmod 2^{2n} + 1, \tilde{y}_j < 2^{2n} \\ 0, \tilde{y}_j = 2^{2n} \end{cases} \tag{6}$$

where $\tilde{y}_j = a^{y_i} \bmod 2^{2n} + 1$ and 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, the structure of chaos-based quantum encryption algorithm is considered in terms of quantum one-time pad. Assume that the Hadamard gate can be defined as $\boldsymbol{\sigma}_h = \frac{1}{\sqrt{2}}(\boldsymbol{\sigma}_x + \boldsymbol{\sigma}_z)$. According to the algorithm in Eq. (1) for a given chaotic string κ of length $2n$, an improved quantum chaotic encryption algorithm is described as

$$E_k(|P\rangle) = \bigotimes_{i=1}^{n} \boldsymbol{\sigma}_x^{k_{2i-1}} \boldsymbol{\sigma}_x^{k_{2i}} |P_i\rangle \tag{7}$$

It is obvious that one cannot obtain the exact relationship $\boldsymbol{\sigma}_x\boldsymbol{\sigma}_h = \pm\boldsymbol{\sigma}_h\boldsymbol{\sigma}_x$ due to the intrinsic characteristics of Pauli operations given by [2]

$$\boldsymbol{\sigma}_x\boldsymbol{\sigma}_z = -\boldsymbol{\sigma}_z\boldsymbol{\sigma}_x,\ \boldsymbol{\sigma}_z\boldsymbol{\sigma}_y = -\boldsymbol{\sigma}_y\boldsymbol{\sigma}_z,\ \boldsymbol{\sigma}_y\boldsymbol{\sigma}_x = -\boldsymbol{\sigma}_x\boldsymbol{\sigma}_y \tag{8}$$

This elegant feature can be well suitable for a particular generation of the quantum signature that cannot be forged or disavowed by attackers.

In what follows, the security of the afore-mentioned encryption process described in Eq. (7) is considered. Usually, since the global phase has no physical effect on quantum mechanics, any change conducted by Pauli operations is commutative in quantum encryption process consisting of quantum random rotation. However, in this encryption algorithm, it is impossible for an attacker to find out a commutative quantum operation to change the phase of the transformed state $E_k(|P\rangle)$ without being detected.

Theorem 1: A Pauli operation $\boldsymbol{\sigma}_x$ cannot commute with a unitary operation $\boldsymbol{\sigma}_h$ up to a constant, that is $\boldsymbol{\sigma}_x\boldsymbol{\sigma}_h \neq \alpha\boldsymbol{\sigma}_h\boldsymbol{\sigma}_x$ for any nonzero complex number α.

Proof: According to the definition of operation $\boldsymbol{\sigma}_h$, due to the relation $\boldsymbol{\sigma}_x\boldsymbol{\sigma}_z = -\boldsymbol{\sigma}_z\boldsymbol{\sigma}_x$ [2], one obtains:

$$\boldsymbol{\sigma}_h\boldsymbol{\sigma}_x = \frac{1}{\sqrt{2}}(\boldsymbol{\sigma}_x + \boldsymbol{\sigma}_z)\boldsymbol{\sigma}_x = \frac{1}{\sqrt{2}}(I + \boldsymbol{\sigma}_z\boldsymbol{\sigma}_x) \tag{9}$$

and

$$\begin{aligned} \boldsymbol{\sigma}_x\boldsymbol{\sigma}_h &= \boldsymbol{\sigma}_x\frac{1}{\sqrt{2}}(\boldsymbol{\sigma}_x + \boldsymbol{\sigma}_z) = \frac{1}{\sqrt{2}}(I + \boldsymbol{\sigma}_x\boldsymbol{\sigma}_z) \\ &= \frac{1}{\sqrt{2}}(I - \boldsymbol{\sigma}_z\boldsymbol{\sigma}_x) \end{aligned} \tag{10}$$

Therefore, it is obvious that one cannot achieve the equation $\boldsymbol{\sigma}_x\boldsymbol{\sigma}_h \neq \alpha\boldsymbol{\sigma}_h\boldsymbol{\sigma}_x$ for any nonzero complex number α. This completes the proof of this theorem.

Actually, the unitary operation $\boldsymbol{\sigma}_h$ applied in the quantum encryption algorithm plays an important role in determining its security in terms of the possible phase-flip changes. It is necessary to note that the unitary operation $\boldsymbol{\sigma}_h$ can be generally reformulated by a linear combination of Pauli operations $\boldsymbol{\sigma}_x, \boldsymbol{\sigma}_z$ and $\boldsymbol{\sigma}_y$, i.e., $\boldsymbol{\sigma}_h = a\mathrm{I} + b\boldsymbol{\sigma}_x + c\boldsymbol{\sigma}_y + d\boldsymbol{\sigma}_z$ for some complex numbers a, b, c and d. It is easy to prove that Pauli operation of $\boldsymbol{\sigma}_x$ commutes with $\boldsymbol{\sigma}_h$ up to a nonzero constant if and only if it can be written in two special structures $\boldsymbol{\sigma}_h = a\mathrm{I} + b\boldsymbol{\sigma}_x$ or $\boldsymbol{\sigma}_h = c\boldsymbol{\sigma}_y + d\boldsymbol{\sigma}_z$. This property is elegantly used for the design of a quantum signature scheme with the assistance of an improved chaotic encryption process expressed in Eq. (2) that solves some security problems in previous signature schemes.

In order to describe the chaotic behavior of entanglement of the transformed quantum states $E_k(|P|)$, the initial parameter t_i=0 is designated in the chaos-based quantum system. The characteristics of the quantum chaotic system that depends on the chaotic strings κ achieved from the nonlinear dynamic system described in Eq. (6) are described with two different initial parameters k_0=124 and k_0=125, respectively. As shown in Fig. 1, the entanglement of the yielded state depends much on the given initial value k_0. In addition, the autocorrelation of the string κ is specially shown in Fig. 2, which implies that the autocorrelation of the string κ is closely related to the delta function. It implies that the chaotic entanglement based on the nonlinear system has a good pseudorandom performance that is suitable for quantum encryption.

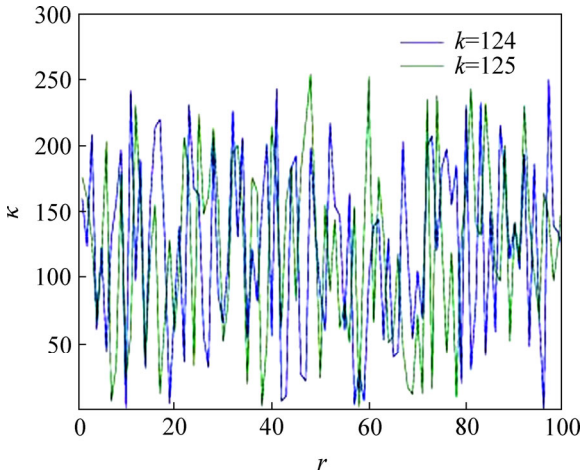

Fig. 1 Chaotic behaviors of quantum entanglement based on generated chaotic string κ with different initial parameters

Different from the traditional quantum encryption algorithm, the chaos-based encryption algorithm makes the qubits of the initial state $|P\rangle$ become increasingly anarchic, which results in the chaotic entanglement in essence. It gets rid of a flaw of short periodicity due to the relationship of the initial state and its transformation that corresponds to the chaotically entangled states $|P'\rangle$. This chaotic feature of the yielded entanglement can be well suitable for the security requirements of the signature that is processed in an imperfect quantum system.

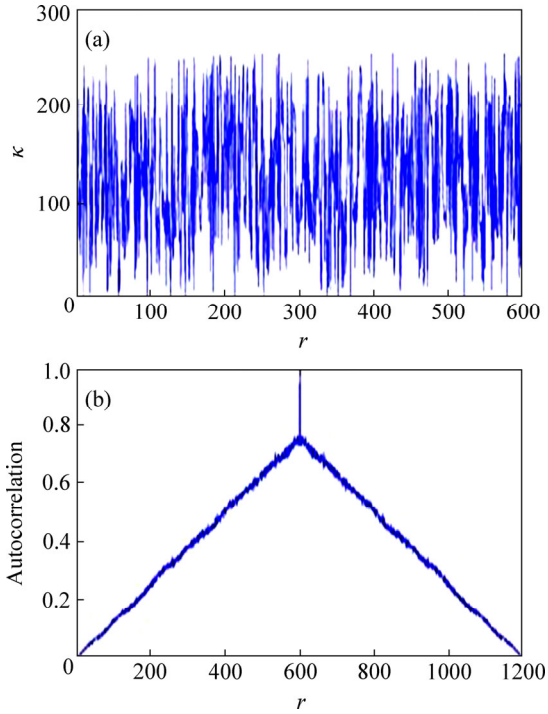

Fig. 2 Chaotic behavior of quantum entanglement based on generated string κ (a) with initial parameters t_0=0 and k_0=123 and autocorrelation of generated string κ (b) with initial parameters t_0=0 and k_0=123

3 QGS scheme based on chaotic quantum encryption

As a secure QGS scheme, it should satisfy at least three constraints. Firstly, only the member of a group can sign the message while the anonymity is protected. Secondly, the receiver of the signature can verify whether it is a valid signature from the group, but it can not distinguish who is the signer. Finally, the group manager can identify the signer in the case of dispute.

In order to clarify our QGS scheme, three characters are defined as follows:

1) Alice-i: A member of the group who wants to sign the message M.

2) Bob: The receiver of the signature who can verify the validity of a signature.

3) Charlie: The group manager that is considered a trusted arbitrator. He can open the signature to identify the signer when a dispute rises.

The QGS scheme is ready to be designed as shown in Fig. 3, which consists of three phases, i.e., initializing

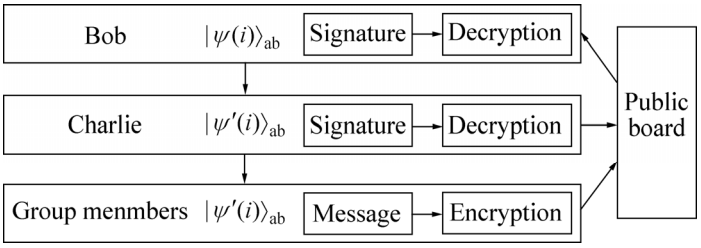

Fig. 3 QGS scheme based on chaotic sequences in cryptosystem

phase, signing phase and verifying phase.

3.1 Initial phase

Step I1: Group setup. Alice-i sends an application to Charlie for permission to join the group and then Charlie transforms her ID number A_i to the initial secret key k_0^{a} of length $2n$ shared by Alice using hash function $H(A_i)^{2n}$. Then, Alice selects another private subkey $t_{\mathrm{a}}=\{t_1, t_2,\cdots, t_r\}$ of length $2n$ shared by Charlie. After implementing the chaotic encrypting algorithm in Eq. (2), she obtains a string κ of length $2n$. Similarly, Bob generates his $2n$−bits secret key k_0^{b} shared before handing with Charlie.

Step I2: Message transformation. Alice-i encodes the message $M=(m(1), m(2), \cdots, m(i), \cdots, m(n))$ into three copies of quantum states $|P\rangle=\otimes_{i=1}^{n}|P(i)\rangle$ denoted as $|P(i)\rangle=\frac{1}{\sqrt{2}}(|0\rangle+m_i|1\rangle)$, where $m_i=1$ or $m_i=-1$ corresponds to $m(i)=1$ or $m(i)=0$, respectively. In order to obtain a low error probability in verifying phase, n should be large enough; otherwise, $|P\rangle\otimes m$ instead of $|P\rangle$ can be used, where m is a large enough integer.

Step I3: Quantum channel setup. Bob prepares n pairs of Bell states $|\Phi^+\rangle=\frac{1}{\sqrt{2}}(|00\rangle+|11\rangle)$ denoted by $|\psi(i)\rangle_{ab}, i\in\{1,2,\cdots,n\}$.

3.2 Signature phase

Step S1: Alice-i asks Charlie permission for signatory and Charlie informs Bob.

Step S2: After receiving Charlie's notification, Bob first creates a unique serial number SN_{B} to distinguish each signature task. Since SN_{B} is a n-bit classical string, Bob transfers it to a quantum states sequence $|S_{\mathrm{B}}\rangle$ with the base $B_z=\{|0\rangle,|1\rangle\}$. He keeps photons denoted as $|\psi(i)\rangle_{\mathrm{b}}, i\in\{1,2,\cdots,n\}$, whose states subscript b are from $|\psi(i)\rangle_{ab}$. Then, Bob uses the secret key k_0^{b} to encrypt $|\psi(i)\rangle_{\mathrm{a}}$ and $|S_{\mathrm{B}}\rangle$ which is denoted as

$$|S_{\mathrm{BT}}\rangle=E_{k_0^b}(|\psi(i)\rangle_{\mathrm{a}}\otimes|S_{\mathrm{B}}\rangle) \tag{11}$$

where the encryption is that Bob applies Hadamard gate to the i-th qubit under the control of the i-th bit of the secret key k_0^{b}. After that, Bob generates some decoy states, which are randomly in one of the four states $(|0\rangle,|1\rangle,|+\rangle,|-\rangle)$, and randomly inserts them into the encrypted states. At last, Bob records the positions of the decoy states and sends these encrypted quantum states to Charlie.

Step S3: After Charlie receives the quantum states, Charlie asks Bob for the help of eavesdropping check. Bob first tells Charlie the positions of the decoy states and the measurement bases, then Charlie measures these qubits and informs Bob the results and Bob compares the results and the states that he generates. If there is an error, he aborts; otherwise, the scheme continues.

Step S4: Charlie decrypts these remaining particles with secret key k_0^{b} and gets $|\psi(i)\rangle_{\mathrm{a}}$ and S_{B}. Then, he chooses a random number r_{c} and obtains classical $2n$-bits string $T=H(r_{\mathrm{c}}\,||\,S_{\mathrm{B}}\,||\,k_0^{\mathrm{b}})^{2n}=\{t_1,t_2,\cdots,t_i,\cdots t_{2n}\}$, where "||" denotes "concatenate". He transforms $|\psi(i)\rangle_{ab}$ to $|\psi(i)'\rangle_{ab}$ by performing a unitary operation $\varepsilon_i\in\{\varepsilon_{t_{2i-1}},t_{2i}\}, i\in\{1,2,\cdots n\}$ on his photons, i.e.,

$$\boldsymbol{\varepsilon}_{00}=1,\boldsymbol{\varepsilon}_{01}=\boldsymbol{\sigma}_x,\boldsymbol{\varepsilon}_{10}=\boldsymbol{\sigma}_z,\boldsymbol{\varepsilon}_{11}=i\boldsymbol{\sigma}_y \tag{12}$$

After that, Charlie encrypts $|\psi(i)'\rangle_{\mathrm{a}}$ and $|S_{\mathrm{B}}\rangle$ again with the secret key k_0^{a} using the same quantum states encryption algorithm. Then, Charlie also generates some decoy states, which are randomly in one of the four states $(|0\rangle,|1\rangle,|+\rangle,|-\rangle)$, and randomly inserts them into the encrypted states $|S_{\mathrm{AT}}\rangle=E_{k_0^b}(|\psi(i)'\rangle_{\mathrm{a}}\otimes|S_{\mathrm{B}}\rangle)$. Finally, he records the positions of the decoy states and sends these encrypted quantum states to Alice-i.

Step S5: Alice-i asks Charlie for the help of eavesdropping check. The process is similar to **Step S3**.

Step S6: Alice-i decrypts these encrypted states with her subkey k_0^{a} and transforms the message $|P\rangle$ into the private qubit string $|P'\rangle=E_{r_{\mathrm{a}}}(|P\rangle)$ using quantum one-time pad algorithm as Eq. (1) with a $2n$-bit random number.

Step S7: Alice-i performs a chaotic encryption algorithm as Eq. (7) on the second copy of $|P'\rangle$ with κ, which generates the chaotic qubit string $|S_{\mathrm{a}}\rangle=E_{\kappa}(|P'\rangle)$. Alice-i combines each qubit of the third copy of $|P(i)'\rangle$ with the received photons $|\psi(i)'\rangle_{\mathrm{a}}$. Without loss of generality, assuming

$|\psi(i)'\rangle_{ab}=\frac{1}{\sqrt{2}}(|00\rangle_{ab}+|11\rangle_{ab})$, the combined systems $|\phi(i)\rangle=|P(i)'\rangle\otimes|\psi(i)'\rangle_{ab}$ can be rewritten as

$$|\phi(i)\rangle=\frac{1}{2\sqrt{2}}\{|\Phi^+\rangle(|0\rangle+m_i|1\rangle)+|\Phi^-\rangle(|0\rangle-m_i|1\rangle)+|\Psi^+\rangle(|1\rangle+m_i|0\rangle)|\Psi^-\rangle(|1\rangle-m_i|0\rangle)\} \quad (13)$$

where $|\Phi^{\pm}\rangle=\frac{1}{\sqrt{2}}(|00\rangle\pm|11\rangle)$ and $|\Psi^{\pm}\rangle=\frac{1}{\sqrt{2}}(|01\rangle\pm|10\rangle)$.

After implementing Bell state measurements (BSMs) on her photon pairs, she obtains the signature $|M_a\rangle=\{|M_a^{(i)}\rangle\}$ where $|M_a^{(i)}\rangle$ denotes a possible BSM performed on the *i*th photon pair.

Step S8: Alice-i makes the resulting records $|S\rangle=(|S_B\rangle,|P'\rangle,|S_a\rangle,|M_a\rangle)$ into classical bits, and sends it on a public board.

3.3 Verification phase

Step V1: Bob gets $|S\rangle$ from the public board and informs Charlie to verify the signature together. They record the classical messages (S_B, M_a) and recover the quantum states $(|P'\rangle,|S_a\rangle)$.

Step V2: After performing the encryption algorithm on $|P'\rangle$ using Alice-i's chaotic string κ, Charlie obtains $|S_c\rangle=E_\kappa|P'\rangle$, which should be consistent with $|S_a\rangle$. After comparing two states $|S_c\rangle$ and $|S_a\rangle$ [15], he announces the verification parameter V=1 and the r_c in the case of $|S_c\rangle=|S_a\rangle$; otherwise, he announces V=0.

Step V3: If V=0, Bob considers that the signature has been obviously forged and rejects it; otherwise, Bob goes on to the further verification.

Step V4: According to r_c and k_0^b, Bob gets Q which corresponds to the unitary operations ε_i performed by Charlie. With the help of ε_i and M_a, he performs one of the corresponding reverse Pauli transformations on each photon of $|\psi(i)'\rangle_b$ in his hand and gets $|P'\rangle_b$. Then, he makes comparisons between $|P'\rangle_b$ and $|P'\rangle$ [15]. If $|P'\rangle_b\neq|P'\rangle$, Bob rejects the signature; otherwise, he informs Alice-*i* by the public board to publish r_a.

Step V5: Alice-i broadcasts r_a by the public board [16].

Step v6: Bob accepts the signature pair $(|S_B\rangle,|P'\rangle,|S_a\rangle,|M_a\rangle,r_a)$ as a group signature for the message $|P\rangle(M)$.

It is necessary to note that the above-mentioned scheme can achieve a function of the group signature. Actually, in verifying phase Charlie can obtain κ that depends on the two initially shared parameters k_0^a and t_a, and hence he can judge whether the relationship $|S_c\rangle=|S_a\rangle$ holds or not. When it holds, the signature pair on the public board is really published by Alice since others do not generate the chaotic string κ without being provided with both k_0^a and t_a [13−14].

4 Security analysis

So far, a QGS scheme based on chaotic sequences in quantum cryptosystem has been proposed. Furthermore, this scheme can be similarly extended on the basis of the quantum chaotic cryptosystem with the GHZ states or the single-qubit states. In this section, the security of this QGS scheme is concerned. In practice, cryptanalysis plays an important role in a rapid development of quantum cryptography. It estimates a scheme's security level, finds potential loopholes, and tries to overcome security issues. Currently, there are several effective attack strategies in quantum cryptosystem, such as intercept resend attacks [17], dense coding attacks [18−19], teleportation attacks [20], denial of service attacks [21], correlation extractability attacks [22−24], Trojan horse attacks [25−26]. In what follows, the security of the proposed scheme is considered according to the feasible attack strategies.

4.1 Impossibility of forgery attack

It should be noted that all the qualified group members in the group actually have the authority to publish the classical information $|S\rangle=(|S_B\rangle,|P'\rangle,|S_a\rangle,|M_a\rangle)$ on the public board. Therefore, if one of the group members, denoted as Eve, wants to forge Alice-i's signature, she might publish another information.

Furthermore, if the transmitted signature is captured by an eavesdropper Eve, it may be distorted viciously. However, according to the essential characteristics of quantum chaotic encryption process, Eve cannot restore the secret initial key k_0^a that is jointly shared by Alice and Charlie before hand even if she obtains the strings κ_a and t_a [13−14].

Eve might implement an intercept resend attack on the quantum sequence $|S_{AT}\rangle=E_{k_0^b}(|\psi(i)'\rangle_a\otimes|S_B\rangle)$ that randomly chooses some qubit positions P_{S_B} of $E_{k_0^{a1}}(|\psi(i)'\rangle_a\otimes|S_B\rangle)$, where k_0^{a1} represents the last n bits of the key k_0^a. Then, he performs an operation $Y=i\sigma_y$ on the qubits in the position P_{S_B}, which changes S_B to SN_f that cannot be indexed by Bob for verification although Eve does not know the exact S_B. The Eve also chooses other positions of $E_{k_0^{a2}}(|\psi(i)'\rangle_a\otimes|S_B\rangle)$ as $P_{|\psi(i)'\rangle_a}$, where $k_0^{a_2}$ represents the front n bits of the key k_0^a.

Then, she publishes either $(S_B,|P'\rangle_f,|S_a\rangle_f,|M_a\rangle)$ or $(S_B,|P'\rangle,|S_a\rangle,|M_a\rangle_f)$ on the public board.

4.1.1 Impossibility of $(S_B, |P'\rangle_f, |S_a\rangle_f, |M_a\rangle)$

If an attacker Eve tries to forge $(|P'\rangle_f, |S_a\rangle_f)$, she should know the parameters t_a and k_0^a which are shared between the legal participators in advance. However, it is impossible due to the unconditional security of QKD [27−28]. In addition, the usage of the chaotic encryption algorithm also strengthens the security of the present scheme [13−14]. Actually, Charlie would completely find the forgery in verifying phase since the condition $|S_c\rangle = |S_a\rangle$ could not hold in this attack.

In the previous signature schemes [4−7], there are some security flaws due to the usage of two Pauli operations $\boldsymbol{\sigma}_x$ and $\boldsymbol{\sigma}_z$ that have a relation $\boldsymbol{\sigma}_x\boldsymbol{\sigma}_z = \pm\boldsymbol{\sigma}_z\boldsymbol{\sigma}_x$ in a quantum one-time pad algorithm. Namely, there is a possible forgery attack that Eve can change one message-signature pair $(|P'\rangle, |S_a\rangle)$ to another $(|P'\rangle_f, |S_a\rangle_f)$ by performing operation $Q = \otimes_{i=1}^{2n} u_i$ without any knowledge of k_0^a and t_a, where u_i denotes a single-qubit unitary operation, i.e. $(Q|P_t'\rangle, (Q|S_{at}\rangle) = (|P'\rangle_f, (|S_a\rangle_f)$. In this attack, Eve does not care about the content of the message but how to use the relation of the message-signature pair. However, in the present scheme, the signing process is based on the chaotic operation string which includes $(\boldsymbol{\sigma}_x + \boldsymbol{\sigma}_z)$, instead of $\boldsymbol{\sigma}_x$ and $\boldsymbol{\sigma}_z$. It is easy to prove that there is no nontrivial quantum operation Q commuting with $\boldsymbol{\sigma}_x(\boldsymbol{\sigma}_x + \boldsymbol{\sigma}_z)$. Therefore, Eve cannot implement such an attack successfully, and his dishonest behaviors will be detected with high probability due to the composite chaotic character of the quantum encryption derived from a nonlinear system that makes the resulting qubit string in possession of a fantastic random [13−14].

Next, this attack is described in details. In order to create the forgery $(|P'\rangle_f, |S_a\rangle_f)$, Eve performs an operation Q on $(|P'\rangle, |S_a\rangle)$, which produces

$$|P'\rangle_f = \overset{n}{\underset{i=1}{\otimes}} u_i |P(i)'\rangle \tag{14}$$

and

$$\begin{aligned} |S_a\rangle_f &= \overset{n}{\underset{i=1}{\otimes}} u_i E_\kappa |P'\rangle_f \\ &= \overset{n}{\underset{i=1}{\otimes}} u_i \boldsymbol{\sigma}_x^{\kappa_{2i-1}} \left(\frac{1}{\sqrt{2}} (\boldsymbol{\sigma}_x + \boldsymbol{\sigma}_z)^{\kappa_{2i}} |P'\rangle_f \right) \end{aligned} \tag{15}$$

However, for any operation Q, it is difficult for Eve to achieve the relation given by

$$u_{2i-1}\boldsymbol{\sigma}_x^{\kappa_{2i-1}} (\boldsymbol{\sigma}_x + \boldsymbol{\sigma}_z)^{\kappa_{2i}} = \boldsymbol{\sigma}_x^{\kappa_{2i-1}} (\boldsymbol{\sigma}_x + \boldsymbol{\sigma}_z)^{\kappa_{2i}} u_{2i-1} \tag{16}$$

due to the fact $\boldsymbol{\sigma}_x(\boldsymbol{\sigma}_x + \boldsymbol{\sigma}_z) \neq \pm(\boldsymbol{\sigma}_x + \boldsymbol{\sigma}_z)\boldsymbol{\sigma}_x$ and $\boldsymbol{\sigma}_z(\boldsymbol{\sigma}_x + \boldsymbol{\sigma}_z) \neq \pm(\boldsymbol{\sigma}_x + \boldsymbol{\sigma}_z)\boldsymbol{\sigma}_z$.

Therefore, Eve cannot achieve the forgery signature,

$$\begin{aligned} |S_a\rangle_f &= \overset{n}{\underset{i=1}{\otimes}} \boldsymbol{\sigma}_x^{\kappa_{2i-1}} (\boldsymbol{\sigma}_x + \boldsymbol{\sigma}_z)^{\kappa_{2i}} u_i |P(i)'\rangle \\ &= \overset{n}{\underset{i=1}{\otimes}} \boldsymbol{\sigma}_x^{\kappa_{2i-1}} (\boldsymbol{\sigma}_x + \boldsymbol{\sigma}_z)^{\kappa_{2i}} |P'\rangle_f \end{aligned} \tag{17}$$

which can pass in verifying phase. It means that Eve cannot select the most preferred operation Q and forge the signature $|S_a\rangle_f$ of Alice-i for the transformed string $|P'\rangle_f$.

4.1.2 Impossibility of $(S_B, |P'\rangle, |S_a\rangle, |M_a\rangle_f)$

If an attacker EVE tries to forge $|M_a\rangle_f$, she performs an intercept resend attack on positions $P_{|\psi(i)'\rangle_a}$ of the quantum sequence $|S_{AT}\rangle = E_{k_0^a}(|\psi(i)'\rangle_a \otimes |S_B\rangle)$.

For simplicity, $P_{|\psi(i)'\rangle_a}$ contains only the position of the first qubit of $E_{k_0^{a2}}(|\psi(i)'\rangle_a)$. Eve performs operation $Y = i\boldsymbol{\sigma}_y$ on the first qubit, because of the anti-commutativity and commutativity between the operations, then the quantum sequence transforms into

$$E_f \begin{cases} E_{k_0^{a_n}}(Y \otimes I^{\otimes(n-1)} \{|\psi(i)'\rangle_a\}), k_0^{a_n} = 1 \\ E_{k_0^{a_n}}(-Y \otimes I^{\otimes(n-1)} \{|\psi(i)'\rangle_a\}), k_0^{a_n} = 0 \end{cases} \tag{18}$$

where $k_0^{a_2}$ represents the last n bits of the key k_0^a.

Eve sends E_f to Alice. As soon as Alice-i received E_f, she decrypts these encrypted states with her key $k_0^{a_2}$. Next, she combines each qubit of $Y \otimes I^{\otimes(n-1)} \{|\psi(i)'\rangle_a\}$ (up to global phase) with the corresponding $|P'\rangle$ and performs the Bell basis measurements. After that, Alice-i publishes the signature pair $(S_f, |P'\rangle, |S_a\rangle, |M_a\rangle)$ which cannot be indexed by Bob for verification due to S_B having been changed to S_f. Subsequently, Eve finds the position where she has replaced the qubits, and flips the corresponding bits of S_f to recover S_B. Then, she publishes $(S_B, |P'\rangle, |S_a\rangle, |M_a\rangle_f)$ in the public board, where $|M_a^{(1)}\rangle_f = \overline{|M_a^{(1)}\rangle}$. Bob will hold $|\psi(1)'\rangle_b = |P(1)'\rangle$ after applying reverse operation on each photon $|\psi'(i)'\rangle_b$ according to Table 1.

However, after S4 in signing phase, if Eve still performs the attack strategy, for each qubit that she wants to temple, she cannot distinguish whether it is the normal information qubit or the checking qubit, thus, it is inevitable for her to disturb the decoy states. If Eve performs operation Y on checking qubit, it will flip the state, and in the eavesdropping check process, it will be detected ultimately. Hence, the above attack strategy cannot influence our scheme.

4.2 Impossibility of disavowal attack

The proposed scheme provides a potential approach for Charlie to settle the dispute that is provoked by Alice or Bob. Otherwise, it is just a message authentication scheme. For example, Bob says that Alice-i signed for

the message $|P\rangle$, but Alice announces that she did not sign such a message (maybe she indeed signed another message $|P\rangle = |P\rangle$) for her own benefits.

In this case, Charlie is required to make a judgment. Actually, Charlie can confirm that Alice-i has signed the message since Alice-i's parameters t_a and k_0^a are both involved the chaotic string κ and hence in the state $|S_a\rangle$. If the comparison result of $|S_c\rangle = |S_a\rangle$ is positive, it implies that Alice is disavowing her signature. Otherwise, the signature is distorted by Bob since all transmissions are processed in the authenticated two-hop channels with the eavesdropping check process, and the signature $|S\rangle$ was announced in the public board. Thus, Alice-i cannot deny signing the message M.

In addition, Alice-i may not publish her correct random number r_a in the public board after Bob completes his comparison operations for the verification. This gives Alice-i an opportunity to send other random number r_a' that may not equal r_a. However, Bob and Charlie can only accept Alice-i's signature $(|S_a'\rangle, r_a')$ for $E_{r_a'}^{-1}(E_{r_a}(|P\rangle))$ but not for $|P\rangle$.

In order to avoid disavowal of Bob, Bob is not allowed to achieve the whole signature in verifying phase. Actually, Alice-i only signed the transformed message $|P'\rangle$ via the quantum encryption algorithm based on the chaotic operation string. To restore the initial message $|P\rangle$, Bob has to require Alice-i to publish her random number r_a and then obtains real message $|P\rangle$. It implies that Bob has no chance to repudiate the received signature without r_a.

A possible case is that Bob claims $|P_b'\rangle \neq |P'\rangle$ even if $|P_b'\rangle = |P'\rangle$ since Charlie would not check whether $|M_a\rangle$ is correct or not. However, this attack cannot work in the present scheme due to the fact that he has to recover the initial message $|P\rangle$ with r_a. Namely, if Bob claims $|P_b'\rangle \neq |P'\rangle$, it means that Alice-i would not announce r_a. Actually, in order to avoid being disavowed by Bob, this scheme utilizes the secure public channel for the transmission of the r_a that is assumed not be susceptible to be altered by any attackers.

4.3 Verifiability

The verifier Bob can check the validity of a signature with the help of trusted Charlie. After the announcement of a 4-tuple $|S\rangle = (S_B, |P'\rangle, |S_a\rangle, |M_a\rangle)$ by the Alice-i, Charlie is informed to verify the integrity of the message hidden in $|S_a\rangle$. He computes $|S_c\rangle = E_k |P'\rangle$ to check whether $|S_c\rangle = |S_a\rangle$. If the result is positive, it means that the message, which is signed by Alice-i, has not been changed by anyone else. Then, he broadcasts the random number r_c. Bob will get T and SN_B and k_0^b. Based on the value of $T(\varepsilon_i)$ as shown in Eq. (12) and M_a, Bob will perform one of the corresponding Pauli transformations on each photon of $|\psi(i)'\rangle_b$ in his hand to extract the message $|P'\rangle_c$. Here, the reverse Pauli transformation can be seen in Table 1. After getting the result of $|P'\rangle_c = |P'\rangle$ by comparison [15], Bob informs Alice-i to publish r_a to get back $|P\rangle(M)$ [16].

Table 1 Bob's corresponding reverse Pauli transformation to $|\psi(i)'\rangle_b$

$\|M_a\rangle$	ε_i			
	I	$\boldsymbol{\sigma}_z$	$\boldsymbol{\sigma}_x$	$i\boldsymbol{\sigma}_y$
$\|\Phi^+\rangle$	I	$\boldsymbol{\sigma}_z$	$\boldsymbol{\sigma}_x$	$i\boldsymbol{\sigma}_y$
$\|\Psi^+\rangle$	$\boldsymbol{\sigma}_x$	$i\boldsymbol{\sigma}_y$	I	$\boldsymbol{\sigma}_z$
$\|\Phi^-\rangle$	$\boldsymbol{\sigma}_z$	I	$i\boldsymbol{\sigma}_y$	$\boldsymbol{\sigma}_x$
$\|\Psi^-\rangle$	$i\boldsymbol{\sigma}_y$	$\boldsymbol{\sigma}_x$	$\boldsymbol{\sigma}_z$	I

4.4 Anonymity

In order to sign a message on behalf of the group, a group member Alice-i should register and share the ID number as the initial secret key with the manager of the group, Charlie, so that others cannot sign the message M. Owing to the principle of teleportation, a quantum state has been transmitted between signer and verifier in the entanglement of photons as shown in Eq. (13), even though they never interacted with each other in the past. With the help of trusted Charlie, Bob can decide whether a signature was generated by a group member, but he cannot identify which individual of the group has signed the message since Alice-i's information about signing is broadcasting in a public board which hides the identities of the signer. So, the anonymity of the signer is protected in the proposed scheme.

4.5 Traceability

In a group signature scheme, signatory Bob should trace the illegal signer with the help of trusted entity Charlie when some disagreements arise. The most interesting property of our QGS protocol is that the identity of the message owner Alice could be traced. The quantum communication during the protocol is solely dependent on the composite chaotic character of the chaotic entanglement derived from a nonlinear system that makes the entanglement in possession of a fantastic random. The pseudo-random property is applied in the chaotic position string, which cannot be altered due to the parameters k. Alice-i leaves records of her activities in the form of Eq. (7).

Once some disputes happen, the traceability will be seen in step I1. With the assumption of Charlie, the A_i is only known to Charlie and Alice. In order to check the identity of the message sender, Charlie computes $K_0^a = H(\cdot)^{2n}$ using the sender's ID number. The identity of the message sender will be obtained in the case of $K_0^a = k_0^a$. Thus, the traceability condition is satisfied.

5 Conclusions

A QGS of classical messages has been investigated based on the quantum chaotic cryptosystem with the aid of a trusted arbitrator, who can solve the disputes fairly. The security is ensured by the employment of the quantum chaotic cryptosystem with the initial secret key and subkey being embedded in. It not only provides us an elegant approach for a member of the group to sign a message anonymously, but also increases the security of signature with the employment of the quantum chaotic encryption algorithm since it is more difficult for an attacker to take effective strategies to forgery or disavowal than that of the previous scheme with only quantum one-time pad encryption. Security analysis shows that all the characteristics of group signature are achieved, and some possible loopholes have been prevented. In addition, neither the external attacker nor the qualified group member can successfully forge the signature.

References

[1] CHAUM D, van HEYST E. Group signatures [C]// Advances in Cryptology EUROCRYPT'91. Berlin, Heidelberg: Springer, 1991: 257−265.

[2] NIELSEN M A, CHUANG I L. Quantum computation and quantum information [M]. Cambridge: Cambridge University Press, 2000: 2−12.

[3] SHOR P W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer [J]. SIAM Journal on Computing, 1997, 26(5): 1484−1509.

[4] LI Q, CHAN W H, LONG D Y. Arbitrated quantum signature scheme using Bell states [J]. Physical Review A, 2009, 79(5): 054307.

[5] ZOU X, QIU D. Security analysis and improvements of arbitrated quantum signature schemes [J]. Physical Review A, 2010, 82(4): 042325.

[6] WEN X, TIAN Y, JI L, NIU X. A group signature scheme based on quantum teleportation [J]. Physica Scripta, 2010, 81(5): 055001.

[7] XU R, HUANG L, YANG W, HE L. Quantum group blind signature scheme without entanglement [J]. Optics Communications, 2011, 284(14): 3654−3658.

[8] ZHANG K J, SUN Y, SONG T T, ZUO H J. Cryptanalysis of the quantum group signature protocols [J]. International Journal of Theoretical Physics, 2013, 52(11): 4163−4173.

[9] ZHANG K, SONG T, ZUO H, ZHANG W. A secure quantum group signature scheme based on Bell states [J]. Physica Scripta, 2013, 87(4): 045012.

[10] SU Q, LI W M. Improved group signature scheme based on quantum teleportation [J]. International Journal of Theoretical Physics, 2013, 53(4): 1208−1216.

[11] EKERT A K. Quantum cryptography based on Bell's theorem [J]. Physical Review Letters, 1991, 67(6): 661−663.

[12] BENNETT C H. Quantum cryptography using any two non-orthogonal states [J]. Physical Review Letters, 1992, 68(21): 3121.

[13] BAPTISTA M S. Cryptography with chaos [J]. Physics Letters A, 1998, 240(1): 50−54.

[14] JAKIMOSKI G, KOCAREV L. Chaos and cryptography: Block encryption ciphers based on chaotic maps [J]. IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications, 2001, 48(2): 163−169.

[15] PANG S, WU S. Comparison of mixed quantum states [J]. Physical Review A, 2011, 84(1): 012336.

[16] CHAUM D. The dining cryptographers problem: Unconditional sender and recipient untraceability [J]. Journal of Cryptology, 1988, 1(1): 65−75.

[17] GAO F, GUO F Z, WEN Q Y, ZHU F C. Comment on "Experimental demonstration of a quantum protocol for byzantine agreement and liar detection" [J]. Physical Review Letters, 2008, 101(20): 208901.

[18] GAO F, QIN S J, GUO F Z, WEN Q Y. Dense-coding attack on three-party quantum key distribution protocols [J]. IEEE Journal of Quantum Electronics, 2011, 47(5): 630−635.

[19] QIN S J, GAO F, WEN Q Y. Improving the security of multiparty quantum secret sharing against an attack with a fake signal [J]. Physics Letters A, 2006, 357(2): 101−103.

[20] GAO F, WEN Q Y, ZHU F C. Teleportation attack on the QSDC protocol with a random basis and order [J]. Chinese Physics B, 2008, 17(9): 3189−3193.

[21] GAO F, GUO F Z, WEN Q Y, ZHU F C. Consistency of shared reference frames should be reexamined [J]. Physical Review A, 2008, 77(1): 014302.

[22] GAO F, WEN Q Y, ZHU F C. Comment on: "Quantum exam" [J]. Physics Letters A, 2007, 360(6): 748−750.

[23] GAO F, WEN Q Y, ZHU F C. A special eavesdropping on one-sender versus N-receiver QSDC Protocol [J]. Chinese Physics Letters, 2008, 25(5): 1561−1563.

[24] GAO F, QIN S J, WEN Q Y. Cryptanalysis of multiparty controlled quantum secure direct communication using Greenberger–Horne–Zeilinger state [J]. Optics Communications 2010, 283(1): 192−195.

[25] GISIN N, FASEL S, KRAUS B, H. Trojan-horse attacks on quantum-key-distribution systems [J]. Physical Review A, 2006, 73(2): 022320.

[26] DENG F G, LI X H, ZHOU H Y, ZHANG Z J. Improving the security of multiparty quantum secret sharing against Trojan horse attack [J]. Physical Review A, 2005, 72(4): 044302.

[27] BENNETT C H, BRASSARD G. Quantum cryptography without Bell's theorem [J]. Physical Review Letters, 1992, 68(5): 557.

[28] BENNET C H, WIESNER S J. Communication via one-and two-particle operators on Einstein-Podolsky-Rosen states [J]. Physical Review Letters, 1992, 69(20): 2881−2884.

(Edited by YANG Hua)