International Journal of Quantum Information
Vol. 5, No. 4 (2007) 553–573

World Scientific
www.worldscientific.com

CONTINUOUS VARIABLE QUANTUM SIGNATURE ALGORITHM

GUIHUA ZENG,*,† MOONHO LEE‡, YING GUO* and GUANGQIANG HE*

*Laboratory of Coding and Communication Security,
Department of Electronic Engineering,
Shanghai Jiaotong University,
Shanghai 200030, China
†ghzeng@sjtu.edu.cn

‡Institute of Information & Communication,
Department of Information & Communication Engineering,
Chonbuk National University,
Chonju 561-756, Korea

Received 9 December 2006

A true quantum signature algorithm based on continuous-variable entanglement state is proposed. In the suggested algorithm, a key-pair, i.e. private signature key and public verification key, is generated based on a one-way function. By employing the signature key, a message state is encoded into a $2k$-particle entangled state and a two-particle entangled state is prepared. The resulting states are exploited as a signature of the message state. The signature can be decoded under the verification key when it needs to be verified. Subsequently, a decoded message state and a two-particle entangled state are obtained. To compare the decoded states and the original states, a quantum circuit for comparing these states is exploited. Making use of measurement results of the quantum circuit one can judge the authenticity of the received signature. According to the security requirement of the signature scheme, the suggested algorithm has been proven to be theoretically secure by using the Shannon information theory.

Keywords: Cryptography; signature algorithm; entanglement; quantum information.

PACS Number(s): 03.67.Dd, 03.65.Ud.

1. Introduction

An important issue in classic cryptography[1] as well as quantum cryptography is the reliable assignment[2–14] of a message to its originator and the integrality verification of a message, which is called its signature scheme. The signature scheme is developed classically so far for this purpose as an addition to a message such that the message can neither be disavowed by the signatory nor can it be forged or changed by the receiver or a possible attacker. Up to now, conventional (handwritten) and digital approaches have been employed in practical applications. While

conventional signatures cannot be transmitted in the electronic network and are vulnerable with respect to forgery, digital signatures have been used widely and with considerable success in e-commerce. However, classical cryptography and thus also classical signature (digital signature) schemes are in general not theoretically secure and are in addition difficult to assign to messages in qubit format. Especially, the rapid development of quantum computers[15–17] increasingly jeopardizes the security of the digital signature scheme which depends on classically computational complexity.

There are two categories of signature algorithms, i.e. arbitrated and true signature scheme, in the digital signature as well as the quantum signature.[18,19] Recently, the arbitrated quantum signature algorithm has been investigated by several groups.[19,20] Their algorithms take advantage of the correlation of GHZ state, various qubit operations and a symmetrical quantum key cryptosystem. Since a trustable arbitrator is always necessary in the arbitrated quantum signature scheme, there is a few limitations for this kind of signature scheme in practical applications. A more popular signature scheme is the so-called true signature scheme. In this category, the signature algorithm and verification algorithm can be executed independently by the signatory and receiver, respectively. The signature key is secret but the verification key is public. An arbitrator may be called only to settle possible disagreements or disputes between the signatory and receiver. In practices, the true signature algorithm is in general favorable.

In this paper, we put forward a true quantum signature algorithm. The proposed algorithm takes advantage of pure quantum effects. It is shown to be theoretically secure, i.e. may not be forged or modified in any way by the receiver and the attacker, and the disavowal is impossible. Physically, the proposal is implemented by exploiting properties of the continuous-variable qubits and quantum encoding procedure. To verify the authenticity of the received signature, a quantum circuit for comparing different quantum states is exploited.

The article is arranged as follows. In Sec. 2, we describe at first the general principles we demand for a quantum signature scheme which is then proposed and presented in detail in Sec. 3. The proposed scheme includes an initial phase, a signing phase and a verifying phase. According to the security requirement of signature scheme, the unconditional security of the proposed algorithm is derived. That is, the quantum signature is shown neither to be disavowable by the signatory nor to be forged by the attacker. To compose a practical quantum signature scheme, a discussion is presented in Sec. 4. Finally, conclusions are drawn in Sec. 5.

2. Architecture of Quantum Signature Algorithms

In analogy to digital signature algorithms, quantum signature algorithms should consist also of three phases: the initial phase, the signature phase and the verification phase. In the initial phase, the communicators generate and distribute a private

and public key which will be employed in the signature phase and verification phase, respectively. In the signature phase, the signatory signs the message and obtains a signature of the message via a signature algorithm. The signature is employed to verify the authenticity and integrality of the message. In the verification phase, the receiver verifies independently signatory's signature via a verification algorithm. Quantum signature as well as digital signature scheme can be divided into two categories, i.e. the true and arbitrated signature schemes. The true signature scheme involves two partners, i.e. the signatory and the receiver. The arbitrator is only needed for settling possible disagreements or disputes. However, the arbitrated signature scheme involves directly three partners, i.e. the signatory, the receiver and the arbitrator. The arbitrator takes part in the signature and/or verification procedure.[19]

As usual the signatory, receiver and possible attacker are referred to as Alice, Bob and Oscar, respectively, where appropriate. We assume the message to be signed to be carried by a quantum state $|P\rangle$. The signing algorithm is denoted QS_{K_s} with key K_s to be used in the signature phase. In the verification phase, the resulting signature $|S\rangle$ with $|S\rangle = QS_{K_s}(|P\rangle)$ can subsequently be verified using a verification algorithm QV_{K_v} with key K_v. Note the keys K_s and K_v may be the same (symmetrical key cryptosystem) or be different (public key cryptosystem)[1] as assumed here. Given a pair $(|P\rangle, |S\rangle)$, the verification algorithm when applied is required to result "true" or "false" depending on whether the signature is authentic or forged.

A quantum signature scheme may thus be defined as a five-tuple $(\mathcal{P}, \mathcal{S}, \mathcal{K}, \mathcal{Q}_s, \mathcal{Q}_v)$ with following abbreviations: $\mathcal{P}$ is a set of possible messages carried by qubits. $\mathcal{S}$ is a set of possible signatures, which may consist of qubits or classical bits. $\mathcal{K}$ is a set of possible keys. It may be a quantum key or a classical key. $\mathcal{Q}_s$ is a set of possible quantum signature algorithms. And $\mathcal{Q}_v$ is a set of possible quantum verification algorithms.

For each key $K \in \mathcal{K}$, there needs be a signature algorithm $QS_{K_s} \in \mathcal{Q}_s$ and a corresponding verification algorithm $QV_{K_v} \in \mathcal{Q}_v$. $QS_{K_s} : \mathcal{P} \to \mathcal{S}$ and $QV_{K_v} : \mathcal{P} \times \mathcal{S} \to \{true, false\}$ are functions such that the following equation is satisfied for every message $|P\rangle \in \mathcal{P}$ and for every signature $|S\rangle \in \mathcal{S}$:

$$QV_{K_v}(|P\rangle, |S\rangle) = \begin{cases} true & if\ |S\rangle = QS_{K_s}(|P\rangle) \\ false & if\ |S\rangle \neq QS_{K_s}(|P\rangle). \end{cases} \tag{1}$$

We emphasize that the signature $|S\rangle$ and the keys may be composed of quantum or classic bits, but we require the signature and verification algorithms QS_{K_s} and QV_{K_v} to be of quantum nature. In addition, Eq. (1) is associated with the comparison of different qubits. In classic information theory the comparison between two bits is very easy. However, it is complex between two qubits since the qubits may be non-orthogonal states.

3. Quantum Signature Algorithms Based on Public Key Cryptosystem

3.1. *Key generation*

This phase generates the keys for signature and verification phases, i.e. signature key and verification key. To construct these keys, we start with a linear transformation which expands a k-dimension vector to a $2k$-dimension vector in real space. Then an arbitrary non-singular $k \times k$ matrix from a set with C_{2k-1}^{k} elements is chosen to compose a unitary matrix. Finally, a pair of keys are generated by employing the k-dimension vector and the composed unitary matrix. The signature key is private but the verification key is public. Although the linear transformation has been exploited at the start, we stress here, however, the relationship between two keys are nonlinear which guarantees the unconditional security of the private key. This property will be proven mathematically later. In the following we show firstly the details of the construction of the key-pair.

Choose a linear mapping in real space, $\mathcal{L} : \mathbb{R}^k \to \mathbb{R}^{2k}$. For an arbitrary vector $\mathbf{x} = (x_0, x_1, \ldots, x_{k-1}) \in \mathbb{R}^k$, a $2k \times 1$ matrix may be created by the linear mapping $\mathcal{L}$,

$$\mathcal{L} : \mathbf{x} \to y(\mathbf{x}) = [y_0(x), y_1(x), y_2(x), \ldots, y_{2k-1}(x)]^T . \tag{2}$$

Without loss of the generality, one may let $y_0(x) = x_0$ which can be implemented by choosing an appropriate linear transformation $\mathcal{L}$. To satisfy the requirement of the proposed signature scheme, the linear mapping $\mathcal{L}$ is constrained by the requirement that the components of any k-element subset of $\{x_0, y_1, \ldots, y_{2k-1}\}$ are linearly independent. This requirement can always be satisfied which has been exploited in quantum error correction code (QECC) and quantum secret sharing scheme.[21,22] Let $(r_1, r_2, \ldots, r_{2k})$ be an arbitrary permutation of indices $(0, 1, \ldots, 2k-1)$. As any k-element subset in $\{x_0, y_1, \ldots, y_{2k-1}\}$ is linearly independent, one can easily understand that subsets $\{y_{r_1}, y_{r_2}, \ldots, y_{r_k}\}$ and $\{x_0, y_{r_{k+1}}, \ldots, y_{2k-1}\}$ are linearly independent, respectively. Accordingly, there exists a non-singular $k \times k$ matrix T such that,

$$T \begin{pmatrix} y_{r_1} \\ y_{r_2} \\ \vdots \\ y_{r_k} \end{pmatrix} = \begin{pmatrix} x_0 \\ y_{r_{k+1}} \\ \vdots \\ y_{r_{2k-1}} \end{pmatrix} . \tag{3}$$

Actually, T denotes the space transformation from space V spanned by $\{y_{r_1}, y_{r_2}, \ldots, y_{r_k}\}$ to space W spanned by $\{x_0, y_{r_{k+1}}, \ldots, y_{2k-1}\}$. Apparently, there exist C_{2k-1}^{k} transformations like the matrix T. Denote all these matrixes by a set $\mathcal{T}$, then one has $T \in \mathcal{T}$.

Generate two states $|\Psi_1\rangle = |y_{r_1}\rangle_{r_1} \ldots |y_{r_k}\rangle_{r_k}$ and $|\Psi_2\rangle = |x_0\rangle_{r_1} |y_{r_k+1}\rangle_{r_2} \ldots |y_{r_{2k-1}}\rangle_{r_k}$ by exploiting k-element subsets $\{y_{r_1}, y_{r_2}, \ldots, y_{r_k}\}$ and $\{x_0, y_{r_{k+1}}$

$, \ldots, y_{r_{2k-1}}\}$, respectively. According to Eq. (3), $|\Psi_1\rangle$ and $|\Psi_2\rangle$ satisfy the following equation,

$$U|\Psi_1\rangle = \|T\|^{\frac{1}{2}}|\Psi_2\rangle, \tag{4}$$

where $\|T\| = \|\det T\|$. Actually, given T, there exists a unitary operator $U(T)$ such that above equation exists. The matrix elements of U in the continuous basis $|\mathbf{x}\rangle = \{|x_0\rangle_{r_1}, \ldots, |x_k\rangle_{r_k}\}$ are,

$$\langle \mathbf{x}'|U|\mathbf{x}''\rangle = \|T\|^{\frac{1}{2}} \prod_{i=0}^{k-1} \delta\left(\sum_{j=0}^{k-1} T_{ij}x''_j - x'_i\right), \tag{5}$$

where $\langle x_i|x_j\rangle = \delta(x_i - x_j)$, and T_{ij} is an element of the matrix T. Equation (5) shows that the matrix U depends simultaneously on the non-singular $k \times k$ matrix T and the k-dimension vector $\mathbf{x}$.

From Eqs. (2–5), one may construct a new transformation G which is expressed as follows,

$$G : \{\mathcal{L}, \mathbf{x}, T_{ij}\} \to \{U, \|T\|^{\frac{1}{2}}\}. \tag{6}$$

Obviously, there is a special relationship between $\{\mathcal{L}, \mathbf{x}, T_{ij}\}$ and $\{U, \|T\|^{\frac{1}{2}}\}$. That is, making use of the vector $\mathbf{x} \in \mathbb{R}^k$, the linear transformation $\mathcal{L}$ and the matrix $T \in \mathcal{T}$, one can obtain easily the unitary operator $U(T)$, however, the inverse procedure is impossible. This property can be concluded by the following theorem.

Theorem 1. *The transformation G expressed in Eq.* (6) *is a nonlinear transformation, and the mapping described by G is a one-way function. Here the linear mapping $\mathcal{L}$ is constrained by the requirement of any subset of k-element in $\{x_0, y_1, \ldots, y_{2k-1}\}$ is independent, $\mathbf{x} \in \mathbb{R}^k$, $T \in \mathcal{T}$ and U is determined by Eq.* (5).

Proof. Since U depends on the multiplication of T and $\mathbf{x}$, the characteristic of G being a nonlinear transformation is straightforward. An example, Eq. (3) shows that T depends on x_0, combining Eq. (5) one gains U is a function of x_0^2, which means G is a nonlinear transformation on x_0.

In the following, we consider the one-way property of the transformation G. From Eq. (5), element $U_{x'x''}$ of the matrix U is determined completely by parameters x_i, T_{ij} and $\|T\|^{\frac{1}{2}}$. If $\mathbf{x}$ and $\mathcal{L}$ are given, the $2k$-dimension vector $y(\mathbf{x})$ can be calculated. Subsequently, the non-singular $k \times k$ matrix set $\mathcal{T}$ can be constructed. Choosing a proper matrix T from the set $\mathcal{T}$, then T_{ij} and $\|T\|^{\frac{1}{2}}$ can be obtained. Thus, construction of the matrix U is straightforward.

Now we investigate the inverse transformation, i.e. G^{-1}. In this situation, the matrix U and thus its elements $U_{x'x''}$ are given, but the parameters $\mathbf{x}$ and T need to be solved. From Eq. (5), any element of the matrix U depends simultaneously

on the vector $\mathbf{x}$ and the matrix T. Although $\|T\|^{\frac{1}{2}}$ is given, $U_{x'x''}$ is still a function with two kinds of variables, i.e. $T_{i,j}$ and x_i, which can be denoted as,

$$U_{x'x''} = g(T_{i,j}, x_i), \tag{7}$$

where $i, j = 0, 1, \ldots, k-1$. Obviously, T_{ij} and x_i cannot be solved by the above equation. Especially, T is one element of the set $\mathcal{T}$ which is not given. This characteristic improves the difficulty of finding a proper T, and subsequently T_{ij}. Therefore the inverse transformation from $\{U, \|T\|^{\frac{1}{2}}\}$ to $\{\mathcal{L}, \mathbf{x}, T_{ij}\}$ is impossible, which means G is a strict one-way function. □

Theorem 1 shows that the nonlinear transformation G is a strict one-way mapping, which means that from $\{\mathcal{L}, \mathbf{x}, T_{i,j}\}$ to $\{U, \|T\|^{\frac{1}{2}}\}$ is easy but the inverse procedure is impossible. Making using of this characteristic, the signature key and verification key are generated and distributed by the following steps.

Step 1. The signatory chooses secretly a random k-dimension vector $\mathbf{x} = (x_0, x_1, \ldots, x_{k-1})$ in real space as well as an appropriate mapping $\mathcal{L}$ as the private key, which will be exploited as a signature key. Denoting the private key by K_s, which may be expressed mathematically as,

$$K_s = \{\mathcal{L}, x_i | i = 1, 2, \ldots, k\}. \tag{8}$$

Then the signatory keeps secretly the generated private key K_s.

Step 2. The signatory chooses randomly a non-singular $k \times k$ matrix from the set $\mathcal{T}$. The elements T_{ij} $(i, j = 0, 1, \ldots, k-1)$ of the matrix T are secret, but the $\|T\|^{\frac{1}{2}}$ is public as a part of the public key which will be composed in the next step.

Step 3. Calculate the operator U by exploiting Eq. (5) according to the obtained private key and the chosen matrix T. Then, the signatory publicly announces the unitary operator $U(T)$ and $\|T\|^{\frac{1}{2}}$ as the verification key K_v,

$$K_v = \{U(T), \|T\|^{\frac{1}{2}}\}. \tag{9}$$

The verification key will be exploited in the verification phase. We stress here that verification key is a public key which may be announced as a telephone number so that any communicators can obtain it.

The public key, i.e. the verification key K_v depends on the private key K_s. However, except the signatory, i.e. Alice, anyone cannot get the private key by the public key, since the mapping from the signature key K_s to the verification key K_v is a one-way function which is described in Theorem 1. The security of the key pairs will be analyzed in detail in subsection 3.4 of this section.

3.2. *Signature of message*

This phase corresponds to the actual signature algorithm QS_{K_s}, i.e. to sign the message $|P\rangle$ with a suitable signature $|S\rangle$. The signature algorithm is implemented

by encoding the message state and preparing a proper two-particle entangled state according to the private signature key. Since the linear mapping $\mathcal{L}$ in Eq. (2) can always be satisfied, there are no limitations for the message format in the proposed scheme, i.e. the message may be denoted by continuous variables or discrete variables quantum state. Recently, the continuous-variables quantum cryptography has become a favorite since the discrete variable is not easy in generation as well as detection in experiment.[23] In addition, quantum communication based on continuous-variables may provide a high channel capability.[24] These advantages lead the continuous-variable quantum state to be employed in the proposed scheme. The signature algorithm QS_{K_s} executes the following steps.

Step 1. The signatory prepares $2k-1$ ancilla states according to the private key K_s. To encode the original message state $|P\rangle$ with wave function $\langle x_0|P\rangle$, Alice firstly creates a $2k \times 1$ matrix $y(\mathbf{x})$ by exploiting the private key K_s. Then she composes a product state $|\omega(\mathbf{x})\rangle$ by exploiting $\{y_1(\mathbf{x}), \ldots, y_{2k-1}(\mathbf{x})\}$. The product state can be denoted as,

$$|\omega(\mathbf{x})\rangle = |y_1(\mathbf{x})\rangle_1 \ldots |y_{2k-1}(\mathbf{x})\rangle_{2k-1}. \tag{10}$$

Step 2. The signatory encodes the message state $|P\rangle$. In the case of the message state $|P\rangle$ being continuous variable qubit, the encoding procedure can be denoted the following way,

$$K_s|P\rangle \mapsto |\widetilde{S}\rangle = \int |P\rangle|\omega\rangle d\mathbf{x}. \tag{11}$$

The encoding procedure can be described by a quantum circuit plotted in Fig. 1. The input states are the message state $|P\rangle$ and the ancilla state $|\omega\rangle$, while the output state is a $2k$-particle entanglement state. The procedure in Fig. 1 is actually an encoding process of continuous-variable QECC. Since the inner product of the

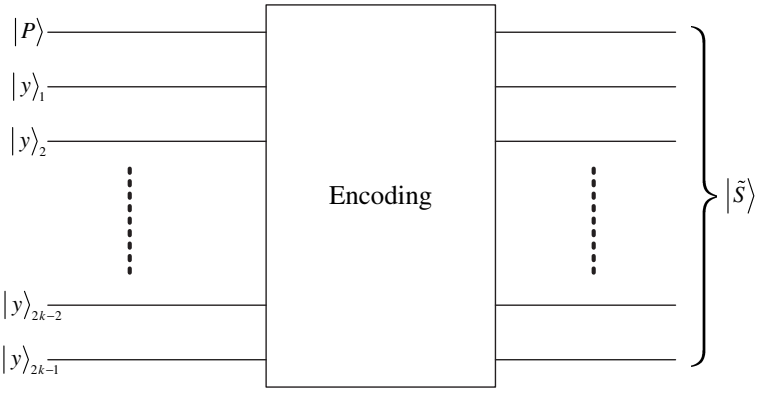

Fig. 1. Encoding procedure of message state $|P\rangle$ through the quantum signature algorithm.

encoded state and the message state satisfies,

$$\begin{aligned}\langle P|\widetilde{S}\rangle &= \int \langle P(x_0')|P(x_0)\rangle|\omega(\mathbf{x})\rangle d\mathbf{x}\\ &= \int \delta(x_0'-x_0)|\omega(\mathbf{x})\rangle d\mathbf{x}\\ &= |\omega(x_0')\rangle\\ &\neq |\omega(\mathbf{x})\rangle, \end{aligned} \tag{12}$$

the state $|\omega(\mathbf{x})\rangle$ associated with the private key K_s cannot be disclosed by the decoded state and the original message states.

Step 3. The signatory prepares a two-particle entangled state according to the private key. Making use of the states $|y_{r_k+1}\rangle_{r_2}$ and $|y_{r_k+1}\rangle_{r_k+1}$ which are associated with the private key K_s, Alice prepares a two-particle entanglement state,

$$|\widetilde{\Omega}\rangle = \int_{\mathbb{R}} |y_{r_k+1}\rangle_{r_2}|y_{r_k+1}\rangle_{r_k+1}dx. \tag{13}$$

Obviously, the prepared state $|\widetilde{\Omega}\rangle$ is associated with the private signature key. In addition, $|\widetilde{\Omega}\rangle$ may be an unknown state to the receiver and attacker since $|y_{r_k+1}\rangle_{r_2}$ and $|y_{r_k+1}\rangle_{r_k+1}$ are associated with the private key.

Step 4. The signatory creates signature of the message, and sends the message following the signature to the receiver. Combining the resulting states $|\widetilde{S}\rangle$ and $|\widetilde{\Omega}\rangle$ yields a signature state,

$$|S\rangle = |\widetilde{S}\rangle \otimes |\widetilde{\Omega}\rangle. \tag{14}$$

After the signature state has been created, Alice sends the message state $|P\rangle$ followed by the signature state $|S\rangle$ to Bob. It is stressed here that the message state $|P\rangle$ may be known or unknown to the communicators, i.e. Alice and Bob, and thus to Oscar, while the signature state $|S\rangle$ must be unknown to Bob and Oscar in any situation since the receiver and attacker do not posses the signature key.

The signature is associated with $|P\rangle$ because $|S\rangle$ was generated via the message state. We note also at this state already that Alice's secret key was crucial in preparing the signature such that it appears impossible for Alice to disavow it in the face of the arbitrator or for Bob and attacker to forge it. In addition we realize that the separation of message and signature by Oscar would not benefit him because the message is valid only with the correct signature and new messages will be assigned new signatures.

3.3. *Verification of signature*

A verification algorithm QV_{K_v} is developed here such that the receiver, Bob, is enabled to verify Alice's signature $|S\rangle$ and consequently judge the authenticity of the message state $|P\rangle$. In previous schemes, the verification procedure require the

arbitrator's participation because Bob does not possess Alice's key which is necessary for the verification of the signature. However, in this scheme the verification procedure does not need any third party. The verification phase is executed by the following procedures.

Step 1. The receiver performs syndrome measurement on the state $|\widetilde{S}\rangle$. Since the $2k$-particle entanglement state $|\widetilde{S}\rangle$ is actually a QECC, Bob applies σ_x (x component of the Pauli matrix) on the $(2k)^{\text{th}}$ particle in the state $|\widetilde{S}\rangle$, which is equivalent to introducing a bit flip error on the final particle in the code. This operation leads $|\widetilde{S}\rangle$ changes to be $\sigma_x^{2k}|\widetilde{S}\rangle$, where the subscript $2k$ denotes that σ_x is applied on the $(2k)^{\text{th}}$ particles in the state $|\widetilde{S}\rangle$. By performing a syndrome measurement on the state $\sigma_x^{2k}|\widetilde{S}\rangle$, Bob obtains a value of the error syndrome denoted by s_e. If $s_e = 2k$, the state $|\widetilde{S}\rangle$ is a $2k$-particle QECC. In this case Bob applies σ_x^{-1} on the $(2k)^{\text{th}}$ particle in the state $|\widetilde{S}\rangle$ and proceeds with the following steps. Otherwise, Bob rejects the signature $|S\rangle$ and stops his further operations since in this situation the state $|\widetilde{S}\rangle$ is forged.

Step 2. The receiver decodes the state $|\widetilde{S}\rangle$ exploiting the verification key K_v. In terms of Eqs. (4) and (11), the signature can be decoded as follows,

$$\begin{aligned} K_v|S\rangle &\mapsto U|\widetilde{S}\rangle \\ &= J\|T\|^{\frac{1}{2}} \int \{|P\rangle|x_0\rangle_{r_1}|y_{r_k+1}\rangle_{r_2}|y_{r_k+1}\rangle_{r_k+1}\cdots \\ &\quad \times |y_{r_{2k-1}}\rangle_{r_k}|y_{r_{2k-1}}\rangle_{r_{2k-1}}\}\, d\mathbf{x} \\ &= J\|T\|^{\frac{1}{2}}|P\rangle_{r_1}|\Omega\rangle_{r_2,r_{k+1}}|\Omega\rangle_{r_3,r_{k+2}}\cdots|\Omega\rangle_{r_k,r_{2k-1}}, \end{aligned} \tag{15}$$

where J is the Jacobian for the transformation from $\mathbf{x}$ to $y(\mathbf{x})$, and $|\Omega\rangle_{i,j} = \int_{\mathbb{R}} |y_l\rangle_i|y_l\rangle_j dx$ $(i = r_2, r_3, \ldots, r_k, j, l = r_k+1, \ldots, r_{2k-1})$, which is an entanglement state of particles i and j.

Step 3. The receiver verifies the entanglement of the particles i and j after the state $|\widetilde{S}\rangle$ has been decoded. The aim of this operation is to ensure that the received state $|\widetilde{S}\rangle$ is an entanglement state of $2k$ particles so that Bob can judge the authenticity of the signature $|S\rangle$ in the following operations. Equation (15) shows the decoded state is a product state of the decoded message state and $k-1$ two-particle entanglement states. Accordingly, Bob only needs to verify the entanglement properties of $k-1$ particle-pairs denoted by $\{r_2, r_{k+1}\}, \{r_3, r_{k+2}\}, \ldots, \{r_{r_k}, 2k-1\}$, which correspond to the states $|\Omega\rangle_{r_2,r_{k+1}}, |\Omega\rangle_{r_3,r_{k+2}}, \ldots, |\Omega\rangle_{r_k,r_{2k-1}}$, respectively. The verification of the first state $|\Omega\rangle_{r_2,r_k+1}$ will be presented later, while the remainder $k-2$ two-particle states are verified via correction between two particles by employing the Bell theory[3] or the approach presented in Ref. 25. Since the physical mechanism of measuring the correlation of entanglement state is beyond this paper, thus we employ directly the approach presented in Ref. 25. If the measurement results show that each particle-pair holds the correlation of a two-particle entangled state, Bob

continues the remaining steps in the verification phase. Otherwise the signature state is forged and Bob stops his operations.

Step 4. The receiver compares the decoded message state and the received (original) message state, and compares the decoded two-particle entangled state $|\Omega\rangle_{r_2,r_k+1}$ and the received two-particle entangled state $|\widetilde{\Omega}\rangle$. To compare in detail these states, we borrow the technique of controlled-swap operation proposed in Ref. 26. For the sake of description, the decoded message state is denoted as $|P'\rangle$. Since $|P\rangle$ and $|P'\rangle$ as well as $|\Omega\rangle_{r_2,r_k+1}$ and $|\widetilde{\Omega}\rangle$ can be compared by employing the same approach, we only consider the comparison of the decoded message state and the received message state in the following.

Equation (15) shows that the message state $|P\rangle$ can be decoded from the signature $|S\rangle$. If the message state is known to Bob, the verification is very easy since Bob only needs to compare directly the received (original) message state with the decoded message state obtained from Eq. (15). However, due to the message qubit $|P\rangle$ may be a unknown state, Bob cannot judge directly whether or not the decoded state is the same as the received message state. To verify the authenticity of the signature, the original state $|P\rangle$ and the decoded state $|P'\rangle$ needs to be compared. Now we compose a machine for comparison of two arbitrary quantum states by using the controlled-swap operation. The machine completes the following operations on the states $|P\rangle$, $|P'\rangle$ and $|0\rangle$ and generates a complex qubit,

$$\begin{aligned}
&(H\otimes I)(U_{\text{swap}})(H\otimes I)|0\rangle|P\rangle|P'\rangle \\
&\quad=\frac{1}{\sqrt{2}}(H\otimes I)(U_{\text{swap}})\left(|0\rangle|P\rangle|P'\rangle+|1\rangle|P\rangle|P'\rangle\right) \\
&\quad=\frac{1}{\sqrt{2}}(H\otimes I)\left(|0\rangle|P\rangle|P'\rangle+|1\rangle|P'\rangle|P\rangle\right) \\
&\quad=\frac{1}{2}|0\rangle(|P\rangle|P'\rangle+|P'\rangle|P\rangle)+\frac{1}{2}|1\rangle(|P\rangle|P'\rangle-|P'\rangle|P\rangle), \qquad (16)
\end{aligned}$$

where H is the Hadamard transform, which is defined by,

$$H|0\rangle=\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle),$$

and

$$H|1\rangle=\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle).$$

U_{swap} is the controlled-SWAP (controlled by the first qubit) defined by the following operations,

$$U_{\text{swap}}|0\rangle|P\rangle|P'\rangle\rightarrow|0\rangle|P\rangle|P'\rangle) \qquad (17)$$

$$U_{\text{swap}}|1\rangle|P\rangle|P'\rangle\rightarrow|1\rangle|P'\rangle|P\rangle). \qquad (18)$$

Obviously, U_{swap} is associated with SWAP operation which is defined as the operation $|P\rangle|P'\rangle\rightarrow|P'\rangle|P\rangle$.

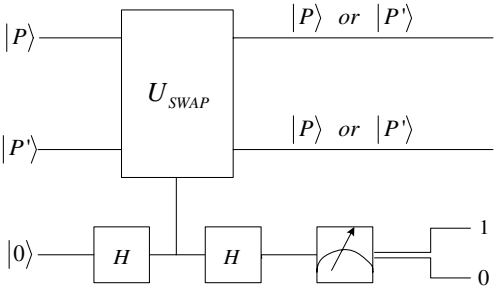

Fig. 2. Quantum circuit for comparison of two arbitrated qubits.

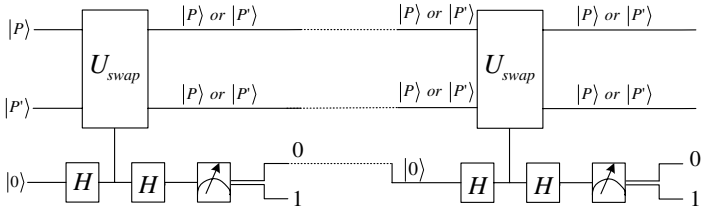

Fig. 3. A quantum machine for verification of quantum signature.

Figure 2 is a quantum circuit which illustrates the comparison procedure between two arbitrary quantum states. This quantum circuit illustrates the operation presented in Eq. (16). Tracing through the execution of this circuit, one can judge the authenticity of the signature by the measurement results. From Eq. (16), if the measurement result is $|1\rangle$, one can obtain a determined result, i.e. $|P\rangle \neq |P'\rangle$. In this case, Bob can judge that the signature $|S\rangle$ is forged. However, if the measurement result is $|0\rangle$, one can judge $|P\rangle = |P'\rangle$ but with an error probability $(1+\varepsilon^2)/2$, where $\varepsilon = \langle P|P'\rangle$ and $0 \leq \varepsilon < 1$. The reason is as follows: if the signature is true, i.e. $|P\rangle = |P'\rangle$, the measurement result must be $|0\rangle$. However, when $|P\rangle \neq |P'\rangle$, the measurement result may also be $|0\rangle$ with a probability of $(1+\varepsilon^2)/2$ and be $|1\rangle$ with a probability of $(1-\varepsilon^2)/2$.

To give a more accurate comparison result between the received message state $|P\rangle$ and the decoded message state $|P'\rangle$, we exploit a quantum circuit plotted in Fig. 3 which exploits the quantum circuit in Fig. 2 as a basic unit. In Fig. 3, once the measurement result is $|1\rangle$, the procedure is stopped, and the inputs state $|P\rangle$ and $|P'\rangle$ are judged to be different. Otherwise, the outputs of the first unit are as inputs for the following unit. After the process of k units the error probability is $[(1+\varepsilon^2)/2]^k$ which is very small so that it can be neglected.

Using Eq. (16), one can verify the states $|P\rangle$ and $|P'\rangle$, which satisfies $|P\rangle|P'\rangle = |P'\rangle|P\rangle$, and can pass the verification in Fig. 3. Fortunately, this situation still follows the verification algorithm since one can easily obtain $|P'\rangle = c|P\rangle$, where c is a constant which can be eliminated by the normalization treatment. Accordingly,

$|P\rangle$ and $|P'\rangle$ represent the same message state, thus there exists no forgery in this case. Another case is that the message state is an entangled symmetric state. For simplicity we consider an entangled symmetric state with two particles, e.g. p_1 and p_2. Then the message state can be written as $|\psi(p_1, p_2)\rangle$,

$$|\psi(p_1, p_2)\rangle = \frac{1}{\sqrt{2}} \left(|p_1\rangle|p_2\rangle + |p_2\rangle|p_1\rangle\right). \tag{19}$$

Suppose an entangled symmetrical state $|\psi'\rangle = |\psi(p_2, p_1)\rangle$ has been exploited to forge the original message by the signatory or the Oscar. Making use of the quantum nature of the symmetrical state, i.e. $|\psi(p_2, p_1)\rangle = |\psi(p_1, p_2)\rangle$, one can easily obtain, $|\psi'\rangle = |\psi(p_1, p_2)\rangle$. Accordingly, $|\psi'\rangle$ and $|\psi\rangle$ denote the same message, which means not any forgery can be succeeded via such kind of symmetrical state.

A more interesting trick exploiting the entangled symmetric state may be described as follows: the message is encoded in the state $|\psi(p_1, p_2)\rangle$. However, the signature state is generated employing only one particle (e.g. p_1) and another particle p_2 is sent to Bob as if it was the message. Fortunately, this trick is unavailable, which can be demonstrated by using at least three ways. Firstly, this trick cannot pass the verification in the first step. When one employs the above trick to generate the signature, the generated signature should be a $(2k+1)$-particle QECC. At Step 1, the obtained value of error syndrome is $s_e = 2k+1$ when Bob induces one bit-flip error on the final particle in the code. Accordingly this trick cannot pass the verification since $s_e \neq 2k$. In addition, this kind of trick does not follow the nature of the quantum signature scheme since only one particle (e.g. p_2) in a two-particle entanglement state cannot denote a determined message. Subsequently, this trick may be detected by the arbitrator when Alice and Bob have disputes. Furthermore, this trick can also be prevented directly by employing a simple QECC. Before the comparison of $|P\rangle$ and $|P'\rangle$ in Step 3, Bob encodes the particle p_2 with two ancilla $|0\rangle$ states, then a three qubits bit-flip code is generated.[27,28] If p_1 and p_2 are not entangled, the encoding procedure is,

$$|P\rangle|P'\rangle \rightarrow |C_1\rangle = (a|000\rangle + b|111\rangle) \otimes (a'|0\rangle + b'|1\rangle), \tag{20}$$

where $|P\rangle = a|0\rangle + b|1\rangle$ and $|P'\rangle = a'|0\rangle + b'|1\rangle$ are exploited with $|a|^2 + |b|^2 = 1$ and $|a'|^2 + |b'|^2 = 1$. If p_1 and p_2 consist of an entangled symmetrical state $|\psi(P, P')\rangle$, the encoding procedure can be denoted as,

$$\begin{aligned} |P\rangle|P'\rangle + |P'\rangle|P\rangle \rightarrow |C_2\rangle = {} & (a|000\rangle + b|111\rangle) \\ & \otimes (a'|0\rangle + b'|1\rangle) + (a'|000\rangle + b'|111\rangle) \\ & \otimes (a|0\rangle + b|1\rangle). \end{aligned} \tag{21}$$

Apply the operator σ_x on the fourth particle which is equivalent to introducing a bit-flip error on the codes $|C_1\rangle$ and $|C_2\rangle$. Simple calculation shows that syndromes of codes $|C_1\rangle$ and $|C_2\rangle$ are 0 and 4, respectively. Then, what Bob needs to do is to measure the error syndromes of the codes. If the syndrome $s = 4$ which corresponds to the code $|C_2\rangle$, Bob judges p_1 and p_2 are entangled and rejects the

signature. Otherwise Bob recovers the states of particles p_1 and p_2 by applying σ_x^{-1} on the fourth particle in code $|C_1\rangle$ and then decoding the code $|C_1\rangle$ according to the theory of QECC. After these operations, Bob moves on the remaining steps.

3.4. *Security analysis*

The security analysis of the quantum signature scheme is different from what we are used to for quantum key distributions. Similar to the classical digital signatures we demand a quantum signature scheme that satisfies three aspects. First, neither the receiver nor a possible attacker are able to change the signature and create a legal signature of the message. Also they cannot change the attached message after completion. Second, the signatory may not successfully disavow the signature and the signed message. Third, it needs to be possible for the receiver to identify the signatory. In short, in a quantum signature scheme, complete security requires that the signatory cannot disavow the signature, and that the receiver and the attackers have no possibility to obtain the signature or the signature keys so that they may forge the signature.

According to the above security requirement of quantum signature, the proposed scheme provides unconditional security since the attackers (including dishonest Bob) obtains no useful information on the private key from the public parameters, i.e. the original message state and the public key, and the signatory cannot disavow the signature. In following we analyze in detail the security of the proposed algorithm.

Theorem 2. *Given a message state* $|P\rangle$ *and its signature* $|S\rangle$ *generated by Eq.* (14). *Let* $|S'\rangle = |\widetilde{S}'\rangle \otimes |\widetilde{\Omega}'\rangle$, *where* $|\widetilde{S}'\rangle$ *and* $|\widetilde{\Omega}'\rangle$ *are entanglement states of* $2k$ *particles and two-particle entangled state, respectively. Then* $|S'\rangle$ *is the signature of the message state* $|P\rangle$ *if and only if* $|S'\rangle = |S\rangle$, *and two states, i.e.* $|S\rangle$ *and* $|S'\rangle$, *are constructed under the same private key* K_s.

Proof. Firstly, we consider the case of fixing the private key, i.e. any signature depending on the same private key. Supposing there is another signature $|S'\rangle$ of the given message state $|P\rangle$, i.e. both $|S'\rangle$ and $|S\rangle$ are simultaneously different signatures of the same message state $|P\rangle$, and,

$$|S'\rangle \neq |S\rangle. \tag{22}$$

Then, in terms of Eq. (14) and definition of $|S'\rangle$ one acquires,

$$|\widetilde{S}'\rangle \otimes |\widetilde{\Omega}'\rangle \neq |\widetilde{S}\rangle \otimes |\widetilde{\Omega}\rangle. \tag{23}$$

Applying $U(T)$ on Eq. (23) gives,

$$|P'\rangle \otimes |\Gamma'\rangle \otimes |\widetilde{\Omega}'\rangle \neq |P\rangle \otimes |\Gamma\rangle \otimes |\widetilde{\Omega}\rangle. \tag{24}$$

where $|\Gamma\rangle = J\|T\|^{\frac{1}{2}} \prod_{i=2}^{k} |\Omega\rangle_{r_i, r_{i+k-1}}$ and $|\Gamma'\rangle = J'\|T'\|^{\frac{1}{2}} \prod_{i=2}^{k} |\Omega'\rangle_{r_i, r_{i+k-1}}$. For a fixedly private key K_s, the above equation gives,

$$|P'\rangle \neq |P\rangle, \tag{25}$$

which is inconsistent with the assumption. Therefore, we get the result,

$$|S'\rangle = |S\rangle. \tag{26}$$

Secondly, suppose there are two keys K_s^1, K_s^2 with $K_s^1 \neq K_s^2$, and these keys create the same signature for a given message state $|P\rangle$, i.e. $|S'\rangle_{K_s^1} = |S\rangle_{K_s^2}$. Since $|\omega(\mathbf{x})\rangle$ is generated from the private key, one gets two different states, $|\omega^1(\mathbf{x})\rangle$ and $|\omega^2(\mathbf{x})\rangle$, which corresponds to K_s^1 and K_s^2, respectively. From Eq. (11), one obtains,

$$|\widetilde{S}'\rangle_{K_s^1} = \int |P\rangle|\omega^1(\mathbf{x})\rangle d\mathbf{x}, \tag{27}$$

and

$$|\widetilde{S}\rangle_{K_s^1} = \int |P\rangle|\omega^2(\mathbf{x})\rangle d\mathbf{x}. \tag{28}$$

Then

$$\int |P\rangle(|\omega^1(\mathbf{x})\rangle - |\omega^2(\mathbf{x})\rangle) d\mathbf{x} = 0. \tag{29}$$

Since $|P\rangle \neq 0$, the above equation gives $|\omega^1(\mathbf{x})\rangle = |\omega^2(\mathbf{x})\rangle$, subsequently, $K_s^1 = K_s^2$, which contradicts the assumption. □

Theorem 2 implicates that the signature state is unique for a given message state under control of the private key K_s, i.e. a given message state generating a unique signature state and vice versa. Since the attacker does not know the private key K_s, a forged signature $|S'\rangle$ which is not consistent with Eq. (14) leads $|S'\rangle \neq |S\rangle$, and subsequently Eq. (25) exists. According to Fig. 3, different inputs $|P\rangle$ and $|P'\rangle$ will be detected easily with a measurement result "1". While the signature states created under different signature keys are different, subsequently the attacker may be detected by employing Step 3 in the verification phase. Thus the attackers' forgery shall not be successful, which means this kind of attack strategy cannot be succeed.

Besides the above situation, the attacker cannot forge the signature for a given message by employing the public parameters K_v, $|P\rangle$ and $|\widetilde{\Omega}\rangle$. This conclusion is given in the following theorem.

Theorem 3. *Let $|P\rangle$ be a known message state, and $|S\rangle$ be an unknown signature state. Then the signature state $|S\rangle$ may not be derived from the public key K_v and the transmitted states $|P\rangle$ and $|\widetilde{\Omega}\rangle$.*

Proof. Theorem 1 and definitions of K_s and K_v show that the transformation from the public key to private key is impossible, i.e.

$$K_v \nrightarrow K_s. \tag{30}$$

Therefore,

$$K_v|P\rangle \nrightarrow K_s|P\rangle. \tag{31}$$

From the signature phase, one may find the following transformation,

$$K_s|P\rangle \longrightarrow |\widetilde{S}\rangle. \tag{32}$$

For a fixedly private key, Eqs. (31) and (32) give,

$$K_v|P\rangle \nrightarrow |\widetilde{S}\rangle. \tag{33}$$

In addition, clone of the state $|\widetilde{\Omega}\rangle$ is impossible according to the no-clone Theorem 24 since it is an unknown state. Thus the signature may not be created by the public parameters K_v, $|P\rangle$ and $|\widetilde{\Omega}\rangle$. □

In Theorems 2 and 3, the message state is given, i.e. there is no forgery on the message state. However, this situation may occurred in practice. Suppose the attacker has forged a message state $|\widehat{P}\rangle$ and created a forged signature $|\widehat{S}\rangle$. Since the attacker does not possesses the private key K_s, the signature $|\widehat{S}\rangle$ must be created by another key $\widehat{K}_s$. However, the forged message and signature cannot pass successfully through the verification phase according to the following theorem.

Theorem 4. *Let $|P\rangle$ and $|\widehat{P}\rangle$ be the original message state and a forged message state, respectively. If these states are different, i.e. $|\widehat{P}\rangle \neq |P\rangle$, any operation $\mathcal{E}$ cannot give a legitimate signature state so that the verification phase can be passed.*

Proof. To forge a message state $|\widehat{P}\rangle$ which is different from the original message state $|P\rangle$, and then generate a legitimate signature state based on the forged message state $|\widehat{P}\rangle$, the state $|\widehat{P}\rangle$ needs to be encoded by employing Eq. (11) and a two-particle state $|\widetilde{\Omega}\rangle$ needs to be prepared. However, the legitimate signature key is absent to the attacker, then a forged key $\widehat{K}_s$ would be used. Let $|\widehat{\omega}\rangle$ correspond to the key $\widehat{K}_s$, and one gets,

$$|\widehat{S}\rangle = \int |\widehat{P}\rangle|\widehat{\omega}\rangle d\mathbf{x}. \tag{34}$$

Since the key-pair K_s and K_v is a strict one-way mapping, any forgery on the private key leads the destruction of the transformation relationship between the private key K_s and the public key K_v. Due to the fact that state $|\widehat{\omega}\rangle$ does not match up to the verification key K_v, applying the unitary operator U on the state $|\widehat{S}\rangle$ will not accord with Eq. (15). Accordingly, any operation $\mathcal{E}$ cannot give a legitimate signature state so that the verification phase can be passed. □

Due to the unitary property of the operator U in the verification key, there is a special case in Theorem 4. We demonstrate this situation in the following theorem.

Theorem 5. *Let $|P\rangle$ and $|\widehat{P}\rangle$ be the original message state and a forged message state, respectively. Making use of the unitary transformation U and the forged message state $|\widehat{P}\rangle$ may generate a new signature state $|X\rangle$. However, the generated state $|X\rangle$ cannot pass the verification phase.*

Proof. To forge the signature by employing the inverse of U, the attacker prepares a forged state $|F\rangle$. Applying the inverse of the unitary operation U and the forged message state $|\widehat{P}\rangle$, the attacker creates the state $|X\rangle$,

$$|X\rangle = U^{-1}|F\rangle, \tag{35}$$

where U^{-1} denotes the inverse of the unitary operation U, and $|F\rangle$ is the state involved in the forged message state $|\widehat{P}\rangle$. The generated state $|X\rangle$ is regarded as a signature state by the attacker. Then the attacker sends the state $|\widehat{P}\rangle$ together with $|X\rangle$ and a two-particle state $|\widehat{\Omega}\rangle$ which plays the same role as the state $|\widetilde{\Omega}\rangle$ to Bob. In what follows we prove the impossibilities of forging successfully the signature by using U^{-1} through three situations. Firstly, suppose $|F\rangle$ is a product-state of the state $|\widehat{P}\rangle$ and $k-1$ two-particle entangled states, i.e. $|F\rangle = |\widehat{P}\rangle \otimes |F_\omega\rangle$, where $|F_\omega\rangle$ denotes the product-state of $k-1$ two-particle entangled states. Apparently, without Step 1 in the verification phase, the attacker's strategy can pass the verification stage. However, since the forged signature state $|X\rangle$ is not a QECC, Bob cannot obtain a corrected value of the error syndrome in Step 1. Thus the state $|X\rangle$ cannot pass the verification. Secondly, suppose $|F\rangle$ is a $2k$ particles entanglement state and $|X\rangle$ is a QECC which is different from the state $|S\rangle$. In this case, the first step in the verification phase can be passed. However, attacker's strategy cannot pass the Steps 2–4. Even if Step 2 has been passed, Steps 3 and 4 cannot be bypassed since the attacker does not possess the private key. Thirdly if $|F\rangle$ is an arbitrary mixed state of $2k$ particles, Theorem 4 has shown the impossibility of passing the verification. □

According to the above theorems, one may find that if Oscar can get the private key, i.e. signature key K_s, the forgery attacking strategy is possible. Fortunately, this strategy may not be successful since the attacker, i.e. Oscar, cannot get useful information on the private key. For convenience, we use a boldface typesetting for a random variable in the followings. Let $\mathbf{K}_s$,$\mathbf{K}_v$, $\mathbf{S}$ and $\mathbf{P}$ be random variables corresponding to the private key K_s, the public key K_v, the signature state $|S\rangle$ and the message state $|P\rangle$, respectively. Suppose the attacker employs an arbitrary attacking strategy $\mathcal{E}$ on the proposed algorithm. The random variable of the attacking strategy is denoted $\mathbf{E}$. Then, at the situation of given the public key, the signature and the message states, there is a bound on information of the attacker obtaining, which can be described by the following theorem.

Theorem 6. *Let* $I(\mathbf{K}_s, \mathbf{E}|\mathbf{K}_p, \mathbf{S}, \mathbf{P})$ *be the Shannon mutual information between* $\mathbf{K}_s$ *and* $\mathbf{E}$ *given* $\mathbf{K}_p, \mathbf{S}, \mathbf{P}$, *i.e. given the public key* K_p, *message state* $|P\rangle$ *and its signature* $|S\rangle$. *For every* $\sigma > 0$, $\xi > 0$ *and* $L^{\max} > 0$, *the mutual information that the attacker obtains about the private key* K_s *is less than* $\sigma/\ln 2 + L^{\max}\xi$.

Proof. In Shannon theory, the condition mutual information is defined as,

$$I(\mathbf{X}, \mathbf{Y}|\mathbf{Z}) = \sum_z p(z) \left(H_z(\mathbf{X}) - H_z(\mathbf{X}|\mathbf{Y})\right), \tag{36}$$

where $H_z(\mathbf{X})$ and $H_z(\mathbf{X}|\mathbf{Y})$ are defined respectively by,

$$H_z(\mathbf{X}) = -\sum_{x,y} p(x, y|z) \log_2 p(x), \tag{37}$$

and

$$H_z(\mathbf{X}|\mathbf{Y}) = -\sum_{x,y} p(x, y|z) \log_2 p(x|y). \tag{38}$$

From Theorems 2 and 3, one obtains $\mathbf{S}(|P\rangle) = |S\rangle$, thus

$$p(\mathbf{K}_v, \mathbf{S}, \mathbf{P}) = p(\mathbf{K}_v, \mathbf{S}). \tag{39}$$

Note the public key K_v and $\mathbf{S}$ are independent, and the determined public key in the proposed algorithm leads $\mathbf{K}_v(\mathcal{E}) = K_v$ so that $p(\mathbf{K}_v) = 1$. Thus one has,

$$p(\mathbf{K}_v, \mathbf{S}) = p(\mathbf{K}_v) p(\mathbf{S}) = p(\mathbf{S}). \tag{40}$$

In addition, secrecy of the signature state depends directly on the private key K_s via a one-to-one mapping according to Eq. (11), then,

$$p(\mathbf{S}) = p(\mathbf{K}_s). \tag{41}$$

Combining Eqs. (39–41) yields,

$$p(\mathbf{K}_v, \mathbf{S}, \mathbf{P}) = p(\mathbf{K}_s). \tag{42}$$

For simplicity, we abbreviate $\{\mathbf{K}_v, \mathbf{S}, \mathbf{P}\}$ to $\{\Theta\}$ in the following. According to Eq. (36), the mutual information between $\mathbf{K}_s$ and $\mathbf{E}$ given $\mathbf{K}_v, \mathbf{S}, \mathbf{P}$ can be expressed as,

$$I(\mathbf{K}_s, \mathbf{E}|\Theta) = \sum_{K_s} p(K_s) \left(H_{K_s}(\mathbf{K}_s) - H_{K_s}(\mathbf{K}_s|\mathbf{E})\right). \tag{43}$$

Since $p(K_s) = \sum_{K_s, \mathcal{E}|\mathbf{K}_s(\mathcal{E})=K_s} P(K_s, \mathcal{E})$, the above equation gives,

$$\begin{aligned} I(\mathbf{K}_s, \mathbf{E}|\Theta) &= \sum_{K_s, \mathcal{E}} p(K_s, \mathcal{E}) \left(H(\mathbf{K}_s) + \log_2 p(K_s|\mathcal{E})\right), \\ &= \sum_{K_s, \mathcal{E}} p(K_s, \mathcal{E}) H(\mathbf{K}_s) + \sum_{K_s, \mathcal{E}} p(K_s, \mathcal{E}) \log_2 p(K_s|\mathcal{E}). \end{aligned} \tag{44}$$

Denote event $\mathcal{P}$ which is true whenever the attacker can obtain information on the private key from the public parameters, i.e. $\mathbf{K}_v, \mathbf{S}$ and $\mathbf{P}$, then we have,

$$\sum_{K_s,\mathcal{E}} p(K_s,\mathcal{E})H(\mathbf{K}_s) = \sum_{K_s,\mathcal{E}|\mathcal{P}} p(K_s,\mathcal{E})H(K_s) + \sum_{K_s,\mathcal{E}|\overline{\mathcal{P}}} p(K_s,\mathcal{E})H(K_s). \tag{45}$$

This property exists also for the second term in Eq. (44). Since $\mathcal{E} \in \overline{\mathcal{P}}$ implies $H(\mathbf{K}_s) = 0$ and $p(K_s|\mathcal{E}) = 1$. Equation (44) can be rewritten as,

$$I(\mathbf{K}_s, \mathbf{E}|\Theta) = \sum_{K_s,\mathcal{E}|\mathcal{P}} p(K_s,\mathcal{E}) \left\{H(K_s) + \log_2 p(K_s|\mathcal{E})\right\}. \tag{46}$$

Define a new event $\mathcal{N}_\sigma$ which is true whenever the attacking strategy $\mathcal{E}$ is σ-information about K_s, where the conception of σ-information about variable ζ is borrowed from Ref. 30. Then one gains the following expression for any $\sigma \geq 0$ in the event $\mathcal{N}_\sigma$,

$$\left| p(K_s|\mathcal{E}) - 2^{-H(K_s)} \right| \leq 2^{-H(K_s)}\sigma. \tag{47}$$

Making use of the event $\mathcal{N}_\sigma$, Eq. (46) can be rewritten as,

$$\begin{aligned} I(\mathbf{K}_s, \mathbf{E}|\Theta) &= \sum_{(K_s,\mathcal{E})|\mathcal{F}} p(K_s,\mathcal{E}) \left\{H(K_s) + \log_2 p(K_s|\mathcal{E})\right\}, \\ &\quad + \sum_{(K_s,\mathcal{E})|\mathcal{P}\cap\bar{\mathcal{F}}} p(K_s,\mathcal{E}) \left\{H(K_s) + \log_2 p(K_s|\mathcal{E})\right\} \\ &\leq \sum_{(K_s,\mathcal{E})|\mathcal{F}} p(K_s,\mathcal{E}) \log_2(1 + \lambda_{K_s,\mathcal{E}}) \\ &\quad + \sum_{(K_s,\mathcal{E})|\mathcal{P}\cap\bar{\mathcal{F}}} p(K_s,\mathcal{E}) H(K_s), \end{aligned} \tag{48}$$

where $\mathcal{F} = \mathcal{N}_\sigma \cap \mathcal{P}$, $\lambda_{K_s,\mathcal{E}} \leq \sigma$.

Let $L^{\max}$ be the maximal Shannon entropy of $H(K_s)$, and $Pr(\mathcal{P} \cap \bar{\mathcal{F}}) \leq \xi$, where the probability $Pr(\cdot)$ is defined by $Pr(\mathbf{X}) = Pr(\mathbf{X} = x)$. Making use of the inequality $\log_2(1 + x) \leq |x|/\ln 2$ for any $x > -1$, we obtain finally,

$$I(\mathbf{K}_s, \mathbf{E}|\mathbf{K}_p, \mathbf{S}, \mathbf{P}) \leq \frac{\sigma}{\ln 2} + L^{\max}\xi. \tag{49}$$

By far the theorem is complete. □

Theorem 5 gives a upper bound on the amount of information of what the attacker can obtain. Since σ and ξ are any positive numbers, Eq. (49) shows that the mutual information $I(\mathbf{K}_s, \mathbf{E}|\mathbf{K}_v, \mathbf{S}, \mathbf{P})$ may be arbitrary-small even tending to zero. Thus the attacker cannot obtain useful information on the private key by any

attacking strategy, although there are publicly given parameters, i.e. $K_v, |P\rangle$ and $|S\rangle$. Therefore, the private key is unconditional security.

Finally, we analyze the impossibility of disavowal for the signatory. If Alice disavows her signature, it is very easy to discover it, because Alice's key is contained in the signature $|S\rangle$. Thus, if Alice and Bob are engaged in a dispute because of Alice's disavowal, they just need to send the signature $|S\rangle$ and the message to the arbitrator. If the signature $|S\rangle$ can be decoded by Alice's public key K_v, this signature has been carried out by Alice, otherwise, the signature has been forged by Bob or the attacker. Obviously, the arbitrator is only in the position to judge whether Alice has disavowed her signature when the dispute or disagreement occurs.

4. Discussion

By far the signature $|S\rangle$ in the quantum signature scheme can only be used one. However, the signature is always required to exploit multi-times in practice. This property can be found easily in the digital signature scheme. In this section, we try to extend the proposed quantum signature to be one that can be used multi-times.

In the signature phase, Alice prepares n identical signature states $|S_k\rangle (k = 1, 2, \ldots n)$ of the same message, and sends them to the receiver, e.g. Bob. If the signature states $|S_k\rangle (k = 1, 2, \ldots n)$ are true, one should have $|S_1\rangle = |S_2\rangle = \cdots = |S_n\rangle$. After receiving the original message state $|P\rangle$ and n signatures $|S_l\rangle$, Bob first checks whether or not any two signatures are the same, i.e.

$$|S_l\rangle = |S_m\rangle, \tag{50}$$

where, $l, m = 1, 2, \ldots, n, l \neq m$. The comparison approach of $|S_l\rangle$ and $|S_m\rangle$ is the same as that in Fig. 3. If any two signatures cannot satisfy the above equation, Bob rejects the received signatures since there is a possible forgery in this case. Otherwise, Bob employs every time one signature state $|S_l\rangle$ from the set of received signature states $\{|S_1\rangle, |S_2\rangle, \ldots, |S_n\rangle\}$ and the message state $|P\rangle$ to verify the authenticity of the signature according to the approaches presented in the verification phase, i.e. exploiting the quantum circuit presented in Fig. 3. We note here that the comparison procedure presented in Fig. 3 does not destroy the original message state when the signature is true. Thus multiple uses of the proposed algorithm is possible.

5. Conclusion

We propose a continuous-variable quantum signature scheme in this paper. Similar to the digital signature scheme, our quantum signature scheme includes three phases: the initial phase, the signature phase and the verification phase. In the initial phase, two keys, i.e. the signature key and verification key are created by exploiting an appropriate linear transformation at the start. However, the transformation from the signature key to the verification key is nonlinear and a one-way function. This property guarantees the unconditional security of the private key.

In the signature phase, a quantum signature is generated in association with the message by a quantum encoding procedure and a two-particle entangled state. The receiver verifies the authenticity of the quantum signature in the verification phase by using the techniques of error syndrome of QECC, the entanglement detection of two-particle state and comparison of two arbitrary quantum states. Consider the decoded message state may be an unknown state, we exploit a quantum circuit to compare the original states and the decoded states. In terms of the measurement result in the quantum circuit, one can judge the authenticity of the signature. The security analysis shows that the proposed scheme is theoretically secure and may neither be disavowed by the signatory nor may it be forged by Oscar. If the signatory prepares n signature states and the attached message state, the proposed scheme can be exploited in practices like the digital signature scheme.

Acknowledgments

This work is supported by the Natural Science Foundation of China (Grant number 60472018); and is partly supported by Ministry of Information and Communication (MIC) under the IT Foreign Specialist Inviting Program (ITFSIP), supervised by IIFA; and ITRC is supervised by IITA and International Cooperative Research Program of the Ministry of Science and Technology and KOTEF, 2nd stage BK21, Korea.

References

1. B. Schneier, *Applied Cryptography: Protocols, Algorithms, and Source Code in C* (John Wiley & Sons, Inc., 1994).
2. C. H. Bennett and G. Brassard, *Advances in Cryptology: Proceedings of Crypto'84* (Springer-Verlag, 1984), p. 475.
3. A. K. Ekert, *Phys. Rev. Lett.* **67** (1991) 661.
4. C. H. Bennett, *Phys. Rev. Lett.* **68** (1992) 3121.
5. B. Schumacher, *Phys. Rev. Lett.* **80** (1998) 5695.
6. H.-K. Lo and H. F. Chau, *Science* **283** (1999) 2050
7. P. W. Shor and J. Preskill, *Phys. Rev. Lett.* **85** (2000) 441
8. D. S. Naik *et al.*, *Phys. Rev. Lett.* **84** (2000) 4733.
9. A. Kent, *Phys. Rev. Lett.* **83** (1999) 1447.
10. H. P. Yuen, quant-ph/0109055.
11. H. P. Yuen, quant-ph/0106001
12. H. Buhrman, R. Cleve, J. Watrous and R. D. Wolf, *Phys. Rev. Lett.* **87** (2001) 167902.
13. G. Zeng and W. Zhang, *Phys. Rev. A* **61** (2000) 032303.
14. N. Gisin, G. Ribordy, W. Tittel and H. Zbinden, *Rev. Mod. Phys.* **74** (2002) 145.
15. I. L. Chuang, R. Laflamme, P. W. Shor and W. H. Zurek, *Science* **270** (1995) 1633.
16. P. W. Shor, in *Proceedings of the 35th Annual Symposium on FoCS* (IEEE Press, Los Alamos, CA, 1994), p. 116.
17. J. I. Cirac and P. Zoller, *Phys. Rev. Lett.* **74** (1995) 4091.
18. H. Meijer and S. Akl, *Advance in Cryptography, Proceedings of Crypto'81* (Springer-Verlag, Berlin, 1981), p. 65.
19. G. Zeng and C.H. Keitel, *Phys. Rev. A* **65** (2002) 042135.

20. H. Lee C. H. Hong, H. Kim *et al.*, *Phys. Lett. A* **321** (2004) 295.
21. R. Cleve, D. Gottesman, H.-K. Lo, *Phys. Rev. Lett.* **83** (1999) 648.
22. T. Tyc and B. C. Sander, *Phys. Rev. A* **65** (2002) 042310.
23. S. L. Braunstein and P. v. Loock, *Rev. Mod. Phy.* **77** (2005) 513 and reference therein.
24. F. Grosshans *et al.*, *Nature* **421** (2003) 238.
25. C. H. Bennett, G. Brassard and N. D. Mermin, *Phys. Rev. Lett.* **68** (1992) 557.
26. H. Buhrman, R. Cleve, J. Watrous and R. Wolf, *Phys. Rev. Lett.* **87** (2001) 167902.
27. A. M. Steane, *Phys. Rev. Lett.* **77** (1996) 793.
28. M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, 2000), p. 428.
29. W. K. Wooters and W. H. Zurek, *Nature* **299** (1982) 802.
30. D. Mayers, *J. ACM* **48**(3) (2001) 351.