# An arbitrated quantum signature scheme based on entanglement swapping with signer anonymity*

Li Wei(李 伟)[a)b)†], Fan Ming-Yu(范明钰)[b)], and Wang Guang-Wei(王光卫)[b)]

[a)] *School of Information Science and Engineering, Xinjiang University, Urumqi* 830046, *China*
[b)] *School of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu* 610054, *China*

(Received 10 April 2012; revised manuscript received 11 June 2012)

In this paper an arbitrated quantum signature scheme based on entanglement swapping is proposed. In this scheme a message to be signed is coded with unitary operators. Combining quantum measurement with quantum encryption, the signer can generate the signature for a given message. Combining the entangled states generated by the TTP's Bell measurement with the signature information, the verifier can verify the authentication of a signature through a single quantum state measurement. Compared with previous schemes, our scheme is more efficient and less complex, furthermore, our scheme can ensure the anonymity of the signer.

**Keywords:** quantum cryptography, quantum signature, Bell states, entanglement swapping

**PACS:** 03.67.Dd, 03.67.Hk **DOI:** 10.1088/1674-1056/21/12/120305

## 1. Introduction

Quantum cryptography is an important research topic in quantum information, based on the basic principle of quantum mechanism, and it is unconditionally secure compared with the classical cryptosystems. Due to this advantage, the study of quantum cryptography has made much progress since Bennett C H proposed the first quantum key distribution (QKD) protocol BB84 and its revised version B92.[1] At present, the main research topics in this area include quantum key distribution (QKD),[2−5] quantum encryption,[6,7] quantum secrecy sharing (QSS),[8−12] quantum secure directed communication (QSDC), and quantum teleportation.[13−17] Furthermore, there are also some schemes of quantum authentication and quantum signature. Although QKD schemes have been proved to be unconditionally secure, how to ensure the authentication and integrity of messages transmitted in quantum networks remains to be further investigated.

In order to address this problem, people turn to investigate the quantum signature, which is a counterpart of the common digital signature in a quantum computing environment. In Ref. [18] Zeng *et al.* proposed the first quantum signature scheme, in which the unconditional security was ensured by using the correlation of GHZ triplet states with quantum one-time pad. Shortly after that, Gottesman and Chuang[19] proposed a scheme to elucidate the basic principle of quantum signature. In light of the initial scheme in Ref. [18], Zeng and Christoph[20] further proposed a revised scheme, in which both the known and unknown quantum states could be signed. In Ref. [21] Li *et al.* proposed a more efficient scheme by using entangled Bell states, and in Ref. [22] Lee *et al.* proposed two quantum signature schemes with message recovery. Inspired by the trap-door one-way function in classical cryptography, Lu and Feng[23] proposed an efficient scheme based on quantum hash function. Recently, there have been many investigations on quantum signature with additional characteristics, such as quantum blind signature[24,25] and quantum group signature.[26] In order to improve the efficiency, some quantum signature schemes based on single photons were also proposed.[27,28] Furthermore, there are some public key schemes based on the quantum correction code and quantum public key encryption schemes.

In most of the previous investigations, the verifier can know the identity of the true signer, however sometimes perhaps the signer does not want to be identified by the verifier. Inspired by the notion of ring signature schemes in classical cryptography, we propose an anonymous quantum signature scheme in this paper to address the problem. In our scheme, a message to be signed is coded with unitary operators.

*Project supported by the National High Technology Research and Development Program (863 Program) of China (Grant Nos. 2009AA01Z403 and 2009AA01Z435).

†Corresponding author. E-mail: mei7i@yahoo.cn

© 2012 Chinese Physical Society and IOP Publishing Ltd

Combining quantum measurement with quantum encryption, the signer can generate the signature for a given message. Combining the entangled states generated by TTP's Bell measurement with the signature information, the verifier can verify the authentication of a signature through a single quantum state measurement. Compared with the previous schemes, our scheme is efficient and not complex, furthermore, our scheme can ensure the anonymity of the signer.

# 2. Bell states and entanglement Swapping

## 2.1. Bell states

In quantum information, a two-state entanglement system can be denoted with the following four Bell states:

$$\begin{aligned}\left|\Phi^+\right\rangle_{AB} &= \frac{1}{\sqrt{2}}(|00\rangle_{AB}+|11\rangle_{AB})\ \left|\Phi^-\right\rangle_{AB}\\ &= \frac{1}{\sqrt{2}}(|00\rangle_{AB}-|11\rangle_{AB}),\\ \left|\Psi^+\right\rangle_{AB} &= \frac{1}{\sqrt{2}}(|01\rangle_{AB}+|10\rangle_{AB})\ \left|\Psi^-\right\rangle_{AB}\\ &= \frac{1}{\sqrt{2}}(|01\rangle_{AB}-|10\rangle_{AB}).\end{aligned} \tag{1}$$

These four states are convertible under the following operators, which are constructed based on the Pauli matrix:

$$\sigma_{00}=I=\begin{bmatrix}1&0\\0&1\end{bmatrix}\ \sigma_{10}=\mathrm{i}\sigma_y=\begin{bmatrix}0&1\\-1&0\end{bmatrix},$$

$$\sigma_{01}=\sigma_x=\begin{bmatrix}0&1\\1&0\end{bmatrix}\ \sigma_{11}=\sigma_z=\begin{bmatrix}1&0\\0&-1\end{bmatrix}. \tag{2}$$

## 2.2. Entanglement swapping

Entanglement swapping plays an important role in quantum information, especially in quantum cryptography.

Suppose that there are two pairs of photons: one pair (photon 1 and photon 2) are in the entangled state $|\Phi^+\rangle_{12}$, and the other pair (photon 3 and photon 4) are in the entangled state $|\Phi^+\rangle_{34}$, and also suppose that there are two participants: Alice with photons 1, 3, and Bob with photons 2, 4, then the initial state of the system will be

$$\begin{aligned}|\Phi\rangle_{1234} &= |\Phi^+\rangle_{12}\otimes|\Phi^+\rangle_{34}=\frac{1}{\sqrt{2}}(|00\rangle_{34}+|11\rangle_{34})\\ &\otimes\frac{1}{\sqrt{2}}(|00\rangle_{12}+|11\rangle_{12}).\end{aligned} \tag{3}$$

If Alice makes a Bell measurement on her photons, her action will lead to the collapse of the initial entanglement states, which can be expressed as follows:

$$\begin{aligned}|\Phi\rangle_{1234} &= |\Phi^+\rangle_{12}\otimes|\Phi^+\rangle_{34}\\ &= \frac{1}{2}(|\Phi^+\rangle_{13}|\Phi^+\rangle_{24}+|\Phi^-\rangle_{13}|\Phi^-\rangle_{24}\\ &\quad+|\Psi^+\rangle_{13}|\Psi^+\rangle_{24}+|\Psi^-\rangle_{13}|\Psi^-\rangle_{24}).\end{aligned} \tag{4}$$

**Table 1.** Entanglement swapping state combination.

| Initial states | Quantum states after entanglement swapping |
|---|---|
| $\|\Phi^+\rangle_{12}\otimes\|\Phi^+\rangle_{34}$ | $\frac{1}{2}(\|\Phi^+\rangle_{13}\|\Phi^+\rangle_{24}+\|\Phi^-\rangle_{13}\|\Phi^-\rangle_{24}+\|\Psi^+\rangle_{13}\|\Psi^+\rangle_{24}+\|\Psi^-\rangle_{13}\|\Psi^-\rangle_{24})$ |
| $\|\Phi^+\rangle_{12}\otimes\|\Phi^-\rangle_{34}$ | $\frac{1}{2}(\|\Phi^+\rangle_{13}\|\Phi^-\rangle_{24}+\|\Phi^-\rangle_{13}\|\Phi^+\rangle_{24}-\|\Psi^+\rangle_{13}\|\Psi^-\rangle_{24}-\|\Psi^-\rangle_{13}\|\Psi^+\rangle_{24})$ |
| $\|\Phi^+\rangle_{12}\otimes\|\Psi^+\rangle_{34}$ | $\frac{1}{2}(\|\Phi^+\rangle_{13}\|\Psi^+\rangle_{24}+\|\Phi^-\rangle_{13}\|\Psi^-\rangle_{24}+\|\Psi^+\rangle_{13}\|\Phi^+\rangle_{24}+\|\Psi^-\rangle_{13}\|\Phi^-\rangle_{24})$ |
| $\|\Phi^+\rangle_{12}\otimes\|\Psi^-\rangle_{34}$ | $\frac{1}{2}(\|\Phi^+\rangle_{13}\|\Psi^-\rangle_{24}+\|\Phi^-\rangle_{13}\|\Psi^+\rangle_{24}-\|\Psi^+\rangle_{13}\|\Phi^-\rangle_{24}-\|\Psi^-\rangle_{13}\|\Phi^-\rangle_{24})$ |
| $\|\Phi^-\rangle_{12}\otimes\|\Phi^+\rangle_{34}$ | $\frac{1}{2}(\|\Phi^+\rangle_{13}\|\Phi^-\rangle_{24}+\|\Phi^-\rangle_{13}\|\Phi^+\rangle_{24}+\|\Psi^+\rangle_{13}\|\Psi^-\rangle_{24}+\|\Psi^-\rangle_{13}\|\Psi^+\rangle_{24})$ |
| $\|\Phi^-\rangle_{12}\otimes\|\Phi^-\rangle_{34}$ | $\frac{1}{2}(\|\Phi^+\rangle_{13}\|\Phi^+\rangle_{24}+\|\Phi^-\rangle_{13}\|\Phi^-\rangle_{24}-\|\Psi^+\rangle_{13}\|\Psi^+\rangle_{24}-\|\Psi^-\rangle_{13}\|\Psi^-\rangle_{24})$ |
| $\|\Phi^-\rangle_{12}\otimes\|\Psi^+\rangle_{34}$ | $\frac{1}{2}(\|\Phi^+\rangle_{13}\|\Psi^-\rangle_{24}+\|\Phi^-\rangle_{13}\|\Psi^+\rangle_{24}+\|\Psi^+\rangle_{13}\|\Phi^-\rangle_{24}+\|\Psi^-\rangle_{13}\|\Phi^+\rangle_{24})$ |
| $\|\Phi^-\rangle_{12}\otimes\|\Psi^-\rangle_{34}$ | $\frac{1}{2}(\|\Phi^+\rangle_{13}\|\Psi^+\rangle_{24}+\|\Phi^-\rangle_{13}\|\Psi^-\rangle_{24}-\|\Psi^+\rangle_{13}\|\Phi^+\rangle_{24}-\|\Psi^-\rangle_{13}\|\Phi^-\rangle_{24})$ |
| $\|\Psi^+\rangle_{12}\otimes\|\Phi^+\rangle_{34}$ | $\frac{1}{2}(\|\Phi^+\rangle_{13}\|\Psi^+\rangle_{24}-\|\Phi^-\rangle_{13}\|\Psi^-\rangle_{24}+\|\Psi^+\rangle_{13}\|\Phi^-\rangle_{24}-\|\Psi^-\rangle_{13}\|\Phi^-\rangle_{24})$ |
| $\|\Psi^+\rangle_{12}\otimes\|\Phi^-\rangle_{34}$ | $\frac{1}{2}(-\|\Phi^+\rangle_{13}\|\Psi^-\rangle_{24}+\|\Phi^-\rangle_{13}\|\Psi^+\rangle_{24}+\|\Psi^+\rangle_{13}\|\Phi^-\rangle_{24}-\|\Psi^-\rangle_{13}\|\Psi^-\rangle_{24})$ |
| $\|\Psi^+\rangle_{12}\otimes\|\Psi^+\rangle_{34}$ | $\frac{1}{2}(\|\Phi^+\rangle_{13}\|\Phi^+\rangle_{24}-\|\Phi^-\rangle_{13}\|\Phi^-\rangle_{24}+\|\Psi^+\rangle_{13}\|\Psi^+\rangle_{24}-\|\Psi^-\rangle_{13}\|\Psi^-\rangle_{24})$ |
| $\|\Psi^+\rangle_{12}\otimes\|\Psi^-\rangle_{34}$ | $\frac{1}{2}(-\|\Phi^+\rangle_{13}\|\Phi^-\rangle_{24}+\|\Phi^-\rangle_{13}\|\Phi^+\rangle_{24}+\|\Psi^+\rangle_{13}\|\Psi^-\rangle_{24}-\|\Psi^-\rangle_{13}\|\Psi^+\rangle_{24})$ |
| $\|\Psi^-\rangle_{12}\otimes\|\Phi^+\rangle_{34}$ | $\frac{1}{2}(-\|\Phi^+\rangle_{13}\|\Psi^-\rangle_{24}+\|\Phi^-\rangle_{13}\|\Psi^+\rangle_{24}-\|\Psi^+\rangle_{13}\|\Phi^-\rangle_{24}+\|\Psi^-\rangle_{13}\|\Phi^+\rangle_{24})$ |
| $\|\Psi^-\rangle_{12}\otimes\|\Phi^-\rangle_{34}$ | $\frac{1}{2}(\|\Phi^+\rangle_{13}\|\Psi^+\rangle_{24}-\|\Phi^-\rangle_{13}\|\Psi^-\rangle_{24}-\|\Psi^+\rangle_{13}\|\Phi^+\rangle_{24}+\|\Psi^-\rangle_{13}\|\Phi^-\rangle_{24})$ |
| $\|\Psi^-\rangle_{12}\otimes\|\Psi^+\rangle_{34}$ | $\frac{1}{2}(-\|\Phi^+\rangle_{13}\|\Phi^-\rangle_{24}+\|\Phi^-\rangle_{13}\|\Phi^+\rangle_{24}-\|\Psi^+\rangle_{13}\|\Psi^+\rangle_{24}+\|\Psi^-\rangle_{13}\|\Psi^+\rangle_{24})$ |
| $\|\Psi^-\rangle_{12}\otimes\|\Psi^-\rangle_{34}$ | $\frac{1}{2}(\|\Phi^+\rangle_{13}\|\Phi^+\rangle_{24}-\|\Phi^-\rangle_{13}\|\Phi^-\rangle_{24}-\|\Psi^+\rangle_{13}\|\Psi^+\rangle_{24}+\|\Psi^-\rangle_{13}\|\Psi^-\rangle_{24})$ |

The system will be in any one of the four new states with a probability of 0.25. For example, if Alice's measurement result is $|\Psi^-\rangle_{13}$, when she informs Bob of this result, Bob will know that photon 2 and photon 4 have formed a new Bell state, and the state is $|\Psi^-\rangle_{24}$.

In this example, photon 2 and photon 4 have become a new entangled state because Alice's Bell measurement is on photon 1 and photon 3. This is an entanglement swapping operation, and all the Bell state entanglement operations are listed in Table 1.

# 3. Outline of our scheme

In our scheme there are three participants, which is different from the usual quantum signature schemes, and $N$ possible signers $U_1, U_2, \ldots, U_N$, and furthermore there is a verifier Bob, a trusted third party TTP. Randomly generate two secure hash functions $h_1 : \{0,1\}^* \to \{0,1\}^{2n}$ and $h_2 : \{0,1\}^* \to \{0,1\}^n$, let each signer generate a $2n$-bit private key shared with the TTP, and suppose that all the private keys are $\mathrm{Pr}_1, \mathrm{Pr}_2, \ldots, \mathrm{Pr}_N$, then the corresponding public key will be $Pu_i = h_1(\mathrm{Pr}_i)$, $(i = 1, 2, \ldots, N)$ and the verifier Bob's private key will be $\mathrm{Pr}_B$, which is also shared with the TTP.

## 3.1. Initialization

Supposing that the true signer is $U_S$ $(1 \leq S \leq N)$ with the private key $\mathrm{Pr}_S$, where $\mathrm{Pr}_S = (x_1, y_1, \ldots, x_n, y_n)$, the TTP should first generate the following two Bell states:

$$|\Phi\rangle_{ST1} = (|\Phi^+\rangle_{\mathrm{st}1}, |\Phi^+\rangle_{\mathrm{st}2}, \ldots, |\Phi^+\rangle_{\mathrm{st}n}), \quad (5)$$

$$|\Phi\rangle_{\mathrm{BT}2} = (|\Phi^+\rangle_{\mathrm{bt}1}, |\Phi^+\rangle_{\mathrm{bt}2}, \ldots, |\Phi^+\rangle_{\mathrm{bt}n}). \quad (6)$$

Here

$$|\Phi^+\rangle_{\mathrm{sti}} = \frac{1}{\sqrt{2}}(|00\rangle_{\mathrm{st}} + |11\rangle_{\mathrm{st}}),$$
$$|\Phi^+\rangle_{\mathrm{bti}} = \frac{1}{\sqrt{2}}(|00\rangle_{\mathrm{bt}} + |11\rangle_{\mathrm{bt}}). \quad (7)$$

In Eqs. (5) and (6), the quantum states sequence with subscripts $S$ and $B$ will be sent to $U_S$ and Bob, respectively. Denote the sequences of $U_S$ as $|A\rangle = (|A_1\rangle, |A_2\rangle, \ldots, |A_n\rangle)$ and Bob's sequence as $|B\rangle = (|B_1\rangle, |B_2\rangle, \ldots, |B_n\rangle)$, then at present there will be two quantum state sequences on the TTP's side, which are $T_1$ (entangled with sequence $|A\rangle$) and $T_2$ (entangled with sequence $|B\rangle$).

Then the TTP generates a Bell state sequence $|\Phi\rangle_{A'B'} = (|\Phi^+\rangle_{\mathrm{sb}1}, |\Phi^+\rangle_{\mathrm{sb}2}, \ldots, |\Phi^+\rangle_{\mathrm{sb}n})$, and sends $|A'\rangle$ and $|B'\rangle$ to $U_S$ and Bob, respectively. During the distribution of the quantum states, the TTP may calibrate the corresponding particles according to the pre-shared private keys. For example, we can use gate $I$ to denote bit 0, and gate $H$ to denote bit 1. So, if the private key is 10011, then the calibrated operators are ($H$, $I$, $I$, $H$, $H$). Because $H^2 = I^2 = I$, the receiver can recover the quantum state sequence through implementing the same operators according to its private key.

## 3.2. Signing phase

The signing phase includes the following steps.

**Step 1** In order to generate a signature for message $M$, $U_S$ first computes $h_1(M)$ and obtains a message string $m_1$ with the length $2n$-bit, then transforms $m_1$ into the following unitary operator sequence: $\Omega = (\sigma_1, \sigma_2, \ldots, \sigma_n)$, where $\sigma_i \in \{\sigma_{00}, \sigma_{01}, \sigma_{10}, \sigma_{11}\}$ and the transform rule is $00 \to \sigma_{00}$, $01 \to \sigma_{01}$, $10 \to \sigma_{10}$, and $11 \to \sigma_{11}$. Applying $\Omega$ to $|A\rangle$, the signer can obtain

$$|A_\Omega\rangle = \Omega|A\rangle = (\sigma_1|A_1\rangle, \sigma_2|A_2\rangle, \ldots, \sigma_n|A_n\rangle). \quad (8)$$

**Step 2** Compute $m_2 = h_2(m_1)$ and denote $m_2 = (c_1, c_2, \ldots, c_n)$, $c_i \in \{0,1\}$, then $U_S$ will generate the following quantum state in terms of its private key:

$$|\phi\rangle = |\Psi_{x1\oplus c1, y1}\rangle \otimes |\Psi_{x2\oplus c2, y2}\rangle \otimes \cdots \otimes |\Psi_{xn\oplus cn, yn}\rangle. \quad (9)$$

Here,

$$|\Psi_{0,0}\rangle = |0\rangle, \quad |\Psi_{0,1}\rangle = |+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}},$$
$$|\Psi_{1,0}\rangle = |1\rangle, \quad |\Psi_{1,1}\rangle = |-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}. \quad (10)$$

The signer $U_S$ then sends quantum state $|\phi\rangle$ and $m_1$ to the TTP.

**Step 3** The TTP computes $m_2 = h_2(m_1)$, then carries out quantum measurement operation on states $|\phi\rangle$ using the base $\mathrm{Pr}_S = (x_1, y_1, \ldots, x_n, y_n)$ and obtains the measurement result $m_2'$. If $m_2' \neq m_2$ the TTP aborts the protocol, otherwise it computes $Pu = Pu_1 \oplus Pu_2 \oplus \cdots \oplus Pu_N$ and generates a quantum state $|\phi'\rangle$ based on $Pu$ and $m_2'$ according to the procedure in Step 2. The TTP then chooses a random number $r$, generates $|R\rangle = E_{\mathrm{Pr}\,B}(|\phi'\rangle, r)$ by using the secure quantum encryption algorithm and sends $r$ and $|R\rangle$ to $U_S$.

**Step 4** $U_S$ generates unitary operators $M_{KA} = (M_{KA1}, M_{KA2}, \ldots, M_{KAn})$ by using its private key $\mathrm{Pr}_S$ according to the following relationships:

$$(x_i, y_i) = (0,0) \Rightarrow M_{KAi} = \sigma_{00},$$
$$(x_i, y_i) = (0,1) \Rightarrow M_{KAi} = \sigma_{01},$$

$$(x_i, y_i) = (1, 0) \Rightarrow M_{KAi} = \sigma_{10},$$
$$(x_i, y_i) = (1, 1) \Rightarrow M_{KAi} = \sigma_{11}. \quad (11)$$

The $U_S$ then computes $|R_A\rangle = M_{KA}|A_\Omega\rangle$.

**Step 5** $U_S$ applies operators $\Omega = (\sigma_1, \sigma_2, \ldots, \sigma_n)$ to quantum states $|A'\rangle$, which is entangled with Bob's sequence $|B'\rangle$, so the sequence of $U_S$ turns into $|A'_\Omega\rangle = \Omega|A'\rangle = (|A'_{\Omega 1}\rangle, |A'_{\Omega 2}\rangle, \ldots, |A'_{\Omega n}\rangle)$, where $|A'_{\Omega i}\rangle = \sigma_i|A'_i\rangle$, at present $|A'_\Omega\rangle$ and $|B'\rangle$ become new entangled states.

**Step 6** Finally the signature is $|S\rangle = (|R\rangle, |R_A\rangle, |A_\Omega\rangle, |A'_\Omega\rangle, r)$.

### 3.3. Verifying Phase

After receiving the signature, Bob's verification steps are as follows.

**Step 1** Bob sends $|R_A\rangle, |A_\Omega\rangle, |A'_\Omega\rangle$ to TTP and TTP generates $|R'_A\rangle$ by using $|A_\Omega\rangle$ through the procedures in Step 4 of the signing phase, and then sets $\gamma = 1$ if $|R'_A\rangle = |R_A\rangle$ holds, otherwise sets $\gamma = 0$. Note that this step includes quantum state comparison. There are many approaches to making the comparison at present, for instance the schemes in Ref. [7]

**Step 2** The TTP implements a Bell measurement on sequences $T_1$ and $T_2$. This operation turns $|T_1\rangle$ and $|T_2\rangle$ into a pair of Bell entanglement states, while $|A_\Omega\rangle$ and $|B\rangle$ becomes another pair of entangled states. This is an entanglement swapping process and can be denoted as follows:

$$|\Phi_1\rangle_{ST1} \otimes |\Phi_2\rangle_{BT2} = |\Phi_3\rangle_{SB} \otimes |\Phi_4\rangle_{(T1)(T2)}, \quad (12)$$

where $|\Phi_i\rangle$ $(i = 1, 2, 3, 4)$ are all Bell states, $|\Phi_1\rangle_{ST1}$ is the entangled Bell state between $U_S$ and the TTP after signing phase, which is related to $m_1$. $|\Phi_2\rangle_{BT2} = |\Phi\rangle_{BT2}$, and $|\Phi_4\rangle_{(T1)(T2)}$ is the measurement result of the TTP, and $|\Phi_3\rangle_{SB}$ is the new entangled state as the result of TTP's Bell measurement on $|T_1\rangle$ and $|T_2\rangle$. Formula (12) should satisfy the relationships in Table 1.

**Step 3** The TTP generates

$$|Y_{TB}\rangle = E_{\mathrm{Pr}\,B}(|S\rangle, |A_\Omega\rangle, |A'_\Omega\rangle, |\Phi_4\rangle_{(T1)(T2)}, \gamma)$$

and sends $|Y_{TB}\rangle$ to Bob.

**Step 4** Bob decrypts $|Y_{TB}\rangle$ and obtains $|S\rangle$, $|A_\Omega\rangle$, $|A'_\Omega\rangle$, $|\Phi_4\rangle_{(T1)(T2)}$, $\gamma$. Bob aborts the protocol if $\gamma = 0$, otherwise continues the following steps.

**Step 5** Bob collects the public keys of $U_1, U_2, \ldots, U_N$ and computes $Pu = Pu_1 \oplus Pu_2 \oplus \cdots \oplus Pu_N$ which is denoted as $Pu = (k_1^a, k_1^b, \ldots, k_n^a, k_n^b)$.

Bob decrypts $|R\rangle$ and obtains $|\phi'\rangle, r'$, and if $r' = r$ he will implement the following operation

$$W : |\phi'\rangle \to |\phi^*\rangle, \quad (13)$$

where the operator $W$ is defined as

$$W = U_1V_1 \otimes U_2V_2 \otimes \cdots \otimes U_nV_n, \quad (14)$$

with

$$U_i = U(k_i^a), \quad V_i = V(k_i^b), \quad (15)$$
$$U(0) = |0\rangle\langle 0| + |1\rangle\langle 1|,$$
$$U(1) = \mathrm{i}\sigma_y = |0\rangle\langle 1| - |1\rangle\langle 0|,$$
$$V(0) = |0\rangle\langle 0| + |1\rangle\langle 1|,$$
$$V(1) = H = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\langle 0| + \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\langle 1|. \quad (16)$$

Bob implements quantum measurement on state $|\phi^*\rangle$ by using the base $(0, 0, \ldots, 0)$ and obtains the result $m'_2$, then makes a Bell measurement on entangled states $|A'_\Omega\rangle$ and $|B'\rangle$ to obtain $m'_1$.

**Step 6** Bob implements the following two sub-steps:

**Step 6.1** Verify that $m'_2 = h_2(m'_1)$ holds if $m'_1 = h_1(M)$;

**Step 6.2** Compute $|\Phi_1\rangle_{ST1}$ according to $m'_1$, by combining $|\Phi_2\rangle_{BT2}$, $|\Phi_4\rangle_{(T1)(T2)}$, and $|\Phi\rangle_{BT2}$, then verifying whether formula (12) satisfies the relationship in Table 1.

Bob accepts the signature only if the preceding two sub-steps are implemented successfully.

## 4. Security analysis

In our scheme, the legitimate signature cannot be forged by the attackers, including the malicious receiver, furthermore the signer identity is anonymous to the outside.

### 4.1. Anonymity

According to the signing phase, the final signature is $|S\rangle = (|R\rangle, |R_A\rangle, |A_\Omega\rangle, |A'_\Omega\rangle, r)$, where $|A_\Omega\rangle$ and $|A'_\Omega\rangle$ are determined by the message to be signed and their computational process has nothing to do with the signer's private key, and $r$ is a random number generated by the TTP. So, an outsider cannot infer any useful information about the signer from them. The computation of $|R\rangle$ and $|R_A\rangle$ will need the signer's private key, but according to the basic requirement of the quantum encryption algorithm, one cannot infer any useful information about the encrypted key according to the cipher, so $|R\rangle$ betrays nothing about the signer's identity. An attacker can eavesdrop $M$ and $|R_A\rangle$ through quantum measurement, which can be easily detected in quantum communication just as

the detection approaches can do in the BB84 protocol. Step 3 of the signing phase and Step 5 of verifying phase will need a public key for all the signers, including the true signer's, but these two steps will not divulge the public key of the true signer.

### 4.2. Impossibility of forgery

If the attacker Eve wants to forge a valid signature $|S\rangle = (|R\rangle, |R_A\rangle, |A_\Omega\rangle, |A'_\Omega\rangle, r)$ for her own benefit, according to the signing phase the computation of $|R\rangle$ will need the signer's private key, but the private key is distributed through secure QKD protocol, so Eve cannot obtain it. Furthermore, the construction of $|R_A\rangle$ will need the Bell states between the signer and TTP, if all the Bell states have been distributed, then Eve cannot acquire any useful information about these states, her counterfeit quantum states will not be entangled with the TTP's states and can be easily detected in Step 2 of the verifying phase, furthermore the counterfeit states will not generate entanglement swapping through the TTP's measurement. So, formula (12) will not satisfy the relationships in Table 1 and this case can be easily detected in Step 6 of the verifying phase. The only means for Eve is to eavesdrop the quantum channel in the initializing phase, but we have made calibrated operation before quantum states are distributed, and the quantum states transmitted are no-orthodox states, so they are indiscernible to Eve and she cannot infer any useful information about the quantum states, furthermore, this action can be easily detected through detecting the quantum channel integrity.

As to the receiver Bob, he can know $|A'\rangle$ through a Bell measurement of $|B'\rangle$, but as to $|A'_\Omega\rangle$, he will face the same situation as Eve, so a malicious receiver cannot forge a valid signature.

## 5. Efficiency and complexity

In Ref. [27] Wang *et al.* proposed the following formula to measure the efficiency of a quantum signature scheme:

$$\eta = \frac{B_s}{Q_t + B_t}. \tag{17}$$

Here $B_s$ is the length of the message to be signed, $Q_t$ and $B_t$ are the quantum bit number and the classical bit number transmitted in the protocol respectively. So, $Q_t + B_t$ is the total bit number transmitted in order to transmit $B_s$ bit signature message.

Using formula (17), the efficiencies of the signature schemes in Refs. [18], [22], and [23] are 9%, 11%, and 11% respectively. In Ref. [26] Wang *et al.* made some improvement on the existing schemes based on single photons, and the efficiency of their scheme is 16%, the efficiency of the scheme in Ref. [19] is given as $N/(N + MN)$, where $M$ is the public keys involved in the signature protocol. It is easy to see that the maximum efficiency of their scheme will not exceed 50%. One of the main advantages of our scheme is that the private key is a constant variable and is irrelevant to the message to be signed, which is beneficial to the improvement of efficiency.

In order to sign a message of $|M|$ bits, all the information needed to be transmitted is as follows.

Signing phase: including $|\phi\rangle$ (1 bit), $m_1$ ($2n$ bits), $r$ ($|r|$bit), $|R\rangle$ ($|r| + 1$bit), and $|S\rangle$ ($2|r| + 6n + 1$bit);

Verifying phase: including the message that Bob sends to the TTP in Step 1 (the length is $6n$-bit), $|Y_{TB}\rangle$ ($2|r| + 12n + 2$bit);

Furthermore, the original message $M$ needs to be transmitted during the protocol, so according to formula (17) the efficiency of our scheme is

$$\eta = \frac{|M|}{|M| + 6|r| + 26n + 5}. \tag{18}$$

Here, $r$ is a random number, and $|r| \approx n$ in reality, so formula (18) can be approximately written as

$$\eta \approx \frac{|M|}{|M| + 32n + 5}. \tag{19}$$

Here, $n$ is related to the hash function used in the system, its output length is $2n$ bits. If we choose SHA-1, then $n = 80$. Using formula (19), it is easy to know that the signature efficiency for 512-bit message is 16.6%, as to messages with lengths of $1-k$ and $2-k$ bits, the efficiencies will be 28.5% and 44.4% respectively. In general, the scheme is more efficient for a longer message.

The complexity of a quantum signature scheme is related to quantum state preparation, quantum state measurement, and quantum state comparison. The schemes in Refs. [18], [20], and [22] need GHZ triple states. Compared with Bell states, the GHZ states are difficult to prepare. Furthermore, there are four quantum states that need to be measured and one quantum state that needs to be compared in Ref. [18], while for the scheme in Ref. [22], the signer needs to implement one-GHZ state measurement in the signing phase, in the verifying phase the verifier and the arbitrator need to implement a one-GHZ state measurement separately, and in addition, there is one quantum state that needs to be compared in the verifying phase, so the their scheme needs three-GHZ state measurements and one quantum state comparison. The

scheme in Ref. [21] is a revision to that in Ref. [18], although there is no GHZ state in this scheme, it still needs to measure three Bell states (one in the signing phase and two in the verifying phase) and compare one quantum state. For our scheme, there is one single quantum state that needs to be measured in Step 3 in the signing phase, in the verifying phase, there is one quantum state that needs to be compared in Step 1, a Bell state that needs to be measured in Step 2 and a single quantum state that needs to be measured in Step 5. So our scheme will need to measure three quantum states (one Bell measurement and two single state measurements) and to compare one quantum state. Compared with the Bell measurement and GHZ measurement, the single state measurement is simple,[29] so the complexity of implementing our scheme is reduced compared with those of implementing previous schemes. Besides, our scheme provides signer anonymity.

## 6. Conclusion

Based on the basic principle of entanglement swapping, we proposed an arbitrated quantum scheme in this paper. Through coding a message with unitary operators and combining quantum measurement with quantum encryption, the signer can generate a signature for a given message. Combining the entangled states generated by the TTP's Bell measurement with the signature information, the verifier can verify the authentication of a signature through single quantum state measurement. Compared with previous schemes, our scheme is efficient and not too complex. Furthermore, our scheme can ensure the anonymity of the signer.

## References


[1] Bennett C H, Brassard G and Mermin N D 1992 *Phys. Rev. Lett.* **68** 557

[2] Lin Q Q , Wang F Q and Mi J R 2007 *Acta Phys. Sin.* **56** 5796 (in Chinese)

[3] Deng F G and Long G L 2003 *Phys. Rev.* A **68** 042315

[4] Zhou N R, Wang L J, Ding J, Gong L H and Zuo X W 2010 *Int. J. Theor. Phys.* **49** 2035

[5] Chen X B, Wen Q Y, Sun Z X, Shangguan L Y and Yang Y X 2010 *Chin. Phys.* B **19** 010303

[6] Waks E, Inoue K and Santori C 2002 *Nature* **420** 762

[7] Zeng G H 2004 *Chin. J. Electronics* **13** 651

[8] Hillery M, Buzek V and Berthiaume A 1999 *Phys. Rev.* A **59** 1829

[9] Lance A M, Symul T and Bowen W P 2003 *New J. Phys.* **5** 4

[10] Yang Y G, Wen Q Y and Zhu F C 2007 *Sci. Chin.* G **50** 331

[11] Liu Y and Zhang B B 2010 *Chin. Phys.* B **19** 010312

[12] Zhu Z C, Zhang Y Q and Fu A M 2011 *Chin. Phys.* B **20** 040306

[13] Lee J, Lee S and Kim J 2004 *Phys. Rev.* A **70** 032305

[14] Dong L, Xiu X M, Gao Y J and Chi F 2009 *Opt. Commun.* **282** 1688

[15] Yen C A, Horng S J, Goan H S, Kao T W and Chou Y H 2009 *Quantum Inf. Comput.* **9** 376

[16] Han L F, Chen Y M and Yuan H 2009 *Commun. Theor. Phys.* **51** 648

[17] Wang T Y and Wen Q Y 2011 *Chin. Phys.* B **20** 040307

[18] Zeng G H, Ma W P and Wang X M 2001 *Acta Electron. Sin.* **29** 1098 (in Chinese)

[19] Gottesman D and Chuang I 2001 http://arxiv.org/abs/ quant-ph/0105032

[20] Zeng G H and Christoph K 2002 *Phys. Rev.* A **65** 042312

[21] Li Q, Chan W H and Long D Y 2009 *Phys. Rev.* A **79** 054307

[22] Lee H, Hong C and Kim H 2004 *Phys. Lett.* A **321** 295

[23] Lu X and Feng D G 2004 http://arxiv.org/abs/ quant-ph/ 0403046

[24] Wang T Y and Wen Q Y 2010 *Chin. Phys.* B **19** 060307

[25] He L B, Huang L S, Yang W and Xu R 2012 *Chin. Phys.* B **21** 030306

[26] Xu R, Huang L S, Yang W and He L B 2011 *Opt. Commun.* **284** 3654

[27] Wang J, Zhang Q and Tang C J 2006 *Optoelectronic Lett.* **2** 0209

[28] Zou X H and Qiu D W 2010 *Phys. Rev.* A **82** 042325

[29] Du L, Hou J M, Ding J Y, Zhang W X, Tian Z and Chen T T 2011 *Chin. Phys.* B **20** 020306