Quantum dual signature scheme based on coherent states with entanglement swapping*

Jia-Li Liu(刘佳丽), Rong-Hua Shi(施荣华), Jin-Jing Shi(石金晶)†, Ge-Li Lv(吕格莉), and Ying Guo(郭迎)

School of Information Science and Engineering, Central South University, Changsha 410083, China

(Received 18 March 2016; revised manuscript received 12 April 2016; published online 25 June 2016)

A novel quantum dual signature scheme, which combines two signed messages expected to be sent to two diverse receivers Bob and Charlie, is designed by applying entanglement swapping with coherent states. The signatory Alice signs two different messages with unitary operations (corresponding to the secret keys) and applies entanglement swapping to generate a quantum dual signature. The dual signature is firstly sent to the verifier Bob who extracts and verifies the signature of one message and transmits the rest of the dual signature to the verifier Charlie who verifies the signature of the other message. The transmission of the dual signature is realized with quantum teleportation of coherent states. The analysis shows that the security of secret keys and the security criteria of the signature protocol can be greatly guaranteed. An extensional multi-party quantum dual signature scheme which considers the case with more than three participants is also proposed in this paper and this scheme can remain secure. The proposed schemes are completely suited for the quantum communication network including multiple participants and can be applied to the e-commerce system which requires a secure payment among the customer, business and bank.

Keywords: quantum dual signature, coherent states, entanglement swapping, quantum communication network

PACS: 03.67.–a, 03.67.Ac, 03.67.Dd, 03.67.Hk **DOI:** 10.1088/1674-1056/25/8/080306

1. Introduction

Quantum cryptography is a new cryptosystem which combines quantum theory with classical cryptography.[1] Because it is based on the Heisenberg uncertainty principle and quantum no-cloning theorem,[2] it has provable security. Quantum cryptography includes a lot of branches, such as quantum key distribution (QKD), quantum secret sharing (QSS), quantum identification (QI), quantum secure direct communication (QSDC), quantum signature (QS), quantum encryption algorithm (QEA), etc.

A QS is considered as the additional information to the message for the purpose of preventing the message from being forged or tampered with.[3] It is based on the physical properties which provide unconditional security and is one of the most important ways to realize identity and message authentication. QSs are classified into two categories, i.e., arbitrated quantum signatures (AQSs) and true quantum signatures (TQSs). An AQS always needs the participation of a trusted arbitrator. However, only in the case of dispute, a TQS requires a trusted arbitrator. Moreover, a QS algorithm must follow three principles, namely, non-forgery, non-repudiation, and quantum properties.

So far, scholars and researchers have proposed a lot of quantum signature schemes. In accordance with quantum one-way functions and quantum swap-test, Gottesman and Chuang first presented a quantum digital signature protocol in 2001.[4] In 2002, Zeng and Keitel put forward a signature scheme based on the Greenberger–Horne–Zeilinger (GHZ) triplet states, whose realization depends upon a trusty arbitrator.[1,5,6] In 2007, Wen and Liu presented a quantum signature protocol without the participation of the arbitrator.[7] Then Zeng *et al.*[3] presented a true quantum signature protocol based on a continuous variable entangled state in the same year. Shi *et al.* proposed a multiparty quantum proxy group signature scheme[8] in 2011 and a (t,n)-threshold quantum group signature scheme[9] in 2012 which are both based on quantum Fourier transform. In 2013, Shi *et al.*[10] presented a batch proxy quantum blind signature scheme with three-dimensional two-particle-entangled quantum-trits. In 2014, Dunjko *et al.*[11] introduced a quantum digital signature scheme, which applies coherent states without quantum memory. In 2014, Chao *et al.* investigated the cryptanalysis and the corresponding improvements of the previous proposed AQS schemes, and constructed a novel enhanced AQS scheme.[12] Recently, Shang *et al.*[13] first proposed a quantum homomorphic signature protocol by using entanglement swapping, which is used to authenticate data packets of multiple streams for quantum networks.

However, the signature protocols mentioned above either utilize discrete variables, or consider the situation for

*Project supported by the National Natural Science Foundation of China (Grant Nos. 61272495, 61379153, and 61401519) and the Research Fund for the Doctoral Program of Higher Education of China (Grant No. 20130162110012).

†Corresponding author. E-mail: shijinjing@csu.edu.cn

© 2016 Chinese Physical Society and IOP Publishing Ltd

only one message. It is known that the transmission efficiency of discrete-variable protocols is much lower than that of continuous-variable protocols, and a single photon for the discrete variable is detected with difficulty. Thus the efficiency of signature protocols is expected to be improved with continuous variables. The coherent state is one of the continuous-variable states and it is the quantum state which is closest to the classical state. The entangled coherent state (ECS) which is made up of coherent states is wildly exploited in quantum information processing.[14–16] There are two advantages of the ECS. On one hand, the ECS is robust to decoherence caused by the absorption of photons.[17] On the other hand, quantum information processing based on the ECS can be achieved with existing experimental techniques, such as linear optics. What is more, the multi-signature requirement in the quantum communication network which involves multiple participants should be taken into consideration as well. In the e-commerce system, a classical dual signature can be utilized for realizing the connection of two different messages.[18,19] In detail, the dual signature, which combines the customer's order information and payment information that are encrypted with separate secret keys, can be used to solve the problem that the customer's order information (payment information) should be hidden to the bank (business) while the payment information should be blindly forwarded to the bank by the business.

Inspired by the dual signature schemes and the advantages of continuous variables, a new quantum dual signature scheme based on coherent states with entanglement swapping[20–22] is proposed in this paper. Compared with these discrete-variable schemes, the message and signature states in our scheme are convenient to generate and operate. Specifically, the quantum dual signature is generated by combining two signed messages with entanglement swapping. The information transmission in our scheme takes advantage of quantum teleportation of coherent states.[23,24] Our proposed scheme is absolutely satisfied with the security criteria of the signature protocol.

The main contributions of this paper are presented below.

(i) Our scheme makes use of coherent states so that the generation of the information carriers is much easier and the detection efficiency is much higher than that of discrete-variable schemes.

(ii) The quantum dual signature scheme which involves multiple participants in the communication network is first presented in our scheme. It is a new way to connect two quantum messages expected to be sent to different receivers.

(iii) Our scheme has a wide application to the e-commerce system and solves the secure communication problem for the consumer, business, and bank in electronic transaction. What is more, our protocol can be extended to the case with more than three participants and still remain safe.

The rest of this paper is organized as follows. In Section 2, we introduce the beam splitter with coherent states. Section 3 describes the quantum dual signature algorithm including the initial phase, the signing phase, and the verification phase. The security of the proposed scheme is analyzed in Section 4. The quantum dual signature scheme which involves more than three participants is discussed in Section 5. Finally, conclusions are drawn in Section 6.

2. Beam splitter with coherent states

Beam splitters (BSs) are the most commonly applied optical components.[24,25] They are passive components which do not need external energy and can actually operate in the laboratory. The BS couples incident lights or generates two light beams with the same frequency. A loss-less 50:50 BS is denoted with

$$B_{12} = \exp\left[\mathrm{i}\frac{\pi}{4}(\hat{a}_1^\dagger \hat{a}_2 + \hat{a}_2^\dagger \hat{a}_1)\right],$$

and it transforms the coherent state $|\alpha\rangle_1|\beta\rangle_2$ to be

$$B_{12}|\alpha\rangle_1|\beta\rangle_2 = \left|(\alpha+\mathrm{i}\beta)/\sqrt{2}\right\rangle_1 \left|(\beta+\mathrm{i}\alpha)/\sqrt{2}\right\rangle_2, \quad (1)$$

where $\hat{a}_j^\dagger$ and $\hat{a}_j$ respectively represent the bosonic creation and annihilation operators of system $j \in \{1,2\}$. It is well known that a $-\pi/2$ phase shifter can be described with the unitary operator $P_2 = \mathrm{e}^{-\mathrm{i}\pi\hat{a}_2^\dagger\hat{a}_2/2}$. Equipping the BS with a pair of $-\pi/2$ phase shifters, then we can obtain the operator[26] $T_{12} = P_2 B_{12} P_2$ which transforms the state $|\alpha\rangle_1|\beta\rangle_2$ to be

$$T_{12}|\alpha\rangle_1|\beta\rangle_2 = \left|(\alpha+\beta)/\sqrt{2}\right\rangle_1 \left|(\alpha-\beta)/\sqrt{2}\right\rangle_2. \quad (2)$$

This is a significant operation which can be used to generate ECSs. Generally, the bipartite ECS[27] with two modes of the electromagnetic field is described as

$$|\varphi\rangle = \mu|\alpha\rangle_1|\beta\rangle_2 + \nu|\gamma\rangle_1|\delta\rangle_2, \quad (3)$$

where μ and ν are complex numbers. $|\alpha\rangle$ and $|\gamma\rangle$ ($|\beta\rangle$ and $|\delta\rangle$) are coherent states of system 1 (2).

Based on Eq. (2), if a coherent superposition state[17]

$$|\psi\rangle_1 = \frac{1}{\sqrt{N_\alpha}}\left(\left|\sqrt{2}\alpha\right\rangle_1 - \left|-\sqrt{2}\alpha\right\rangle_1\right)$$

and a vacuum state $|0\rangle_2$ are input states of the BS which is accompanied by two $-\pi/2$ phase shifters, the outcome will be

$$|\phi\rangle_{12} = \frac{1}{\sqrt{N'_\alpha}}\left(|\alpha\rangle_1|\alpha\rangle_2 - |-\alpha\rangle_1|-\alpha\rangle_2\right), \quad (4)$$

where $|\alpha\rangle$ and $|-\alpha\rangle$ are coherent states with opposite amplitudes, N_α and N'_α are the normalization factors. Thus, we

acquire the ECS $|\phi\rangle_{12}$ which plays an important role in our scheme.

Generally, we consider the following four two-mode ECSs[28] as quasi-Bell states, i.e.,

$$|C_1\rangle^{\pm} = \frac{1}{\sqrt{N_1}}(|\alpha\rangle|\alpha\rangle \pm |-\alpha\rangle|-\alpha\rangle), \tag{5}$$

$$|C_2\rangle^{\pm} = \frac{1}{\sqrt{N_2}}(|\alpha\rangle|-\alpha\rangle \pm |-\alpha\rangle|\alpha\rangle), \tag{6}$$

where N_1 and N_2 are normalization factors. Then we construct a pair of orthonormal bases[28] which are conducted by $|\alpha\rangle$ and $|-\alpha\rangle$, i.e.,

$$|+\rangle = \frac{1}{\sqrt{N_\omega}}(\cos\omega|\alpha\rangle - \sin\omega|-\alpha\rangle), \tag{7}$$

$$|-\rangle = \frac{1}{\sqrt{N_\omega}}(-\sin\omega|\alpha\rangle + \cos\omega|-\alpha\rangle), \tag{8}$$

where $N_\omega = \cos^2 2\omega$ is the normalization factor, and the parameter ω satisfies $\sin 2\omega = \langle\alpha|-\alpha\rangle$. We also define four operators I, σ_x, $\mathrm{i}\sigma_y$, and σ_z and their functions[29] are shown as follows:

$$\begin{aligned} I|+\rangle &= |+\rangle, \\ I|-\rangle &= |-\rangle; \end{aligned} \tag{9}$$

$$\begin{aligned} \sigma_x|+\rangle &= |-\rangle, \\ \sigma_x|-\rangle &= |+\rangle; \end{aligned} \tag{10}$$

$$\mathrm{i}\sigma_y|+\rangle = \frac{1}{\sqrt{N_\omega}}(-\sin\omega|\alpha\rangle - \cos\omega|-\alpha\rangle),$$

$$\mathrm{i}\sigma_y|-\rangle = \frac{1}{\sqrt{N_\omega}}(\cos\omega|\alpha\rangle + \sin\omega|-\alpha\rangle); \tag{11}$$

$$\sigma_z|+\rangle = \frac{1}{\sqrt{N_\omega}}(\cos\omega|\alpha\rangle + \sin\omega|-\alpha\rangle),$$

$$\sigma_z|-\rangle = \frac{1}{\sqrt{N_\omega}}(-\sin\omega|\alpha\rangle - \cos\omega|-\alpha\rangle). \tag{12}$$

The above operations of BSs are important to most of the quantum information processes which involve the coherent states. Additionally, ECSs are easier to detect. Therefore, we present the following quantum dual signature scheme based on the properties of ECSs and BSs.

3. Quantum dual signature scheme

The schematic representation of the propounded scheme is shown in Fig. 1. There are three participants, the signatory Alice, the verifiers Bob and Charlie. The proposal includes three phases, i.e., initial phase, signing phase, and verification phase, which are described in detail in the following.

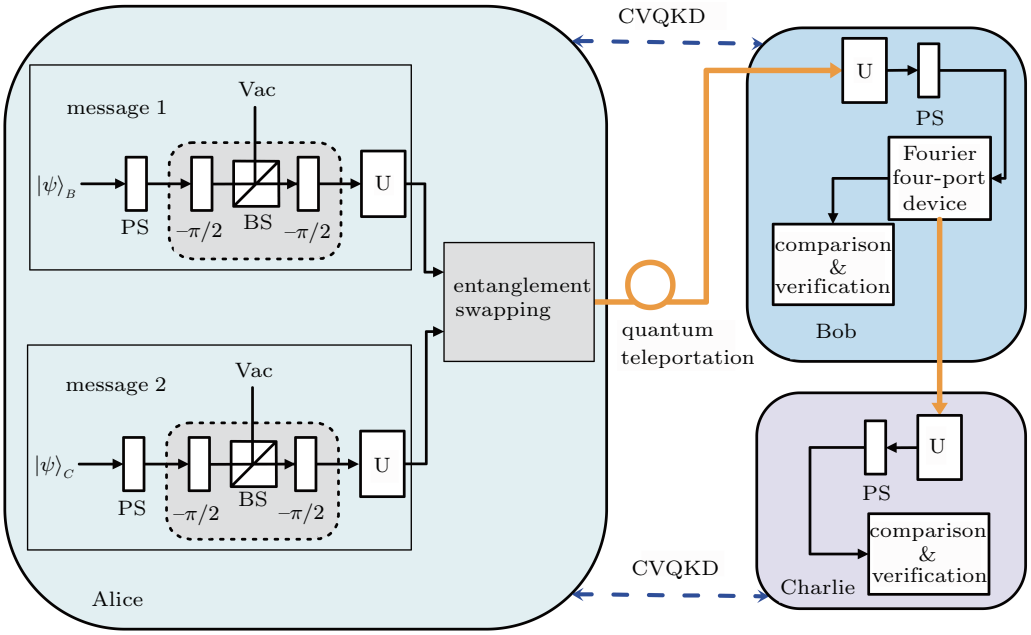


Fig. 1. (color online) Schematic representation of the quantum dual signature scheme. The signatory Alice first signs messages 1 and 2 which are required to be received by Bob and Charlie, respectively. Then she combines the two signatures into a dual signature and sends it to the verifier Bob. Bob verifies the part of the quantum dual signature which is related to message 1 and transmits the rest of the dual signature to Charlie. Subsequently, Charlie completes the verification for the signature of message 2. PS and BS are phase shifter and beam splitter, respectively. The U box stands for performing unitary operations.

3.1. Initial phase

In this phase, Alice generates coherent superposition states, encodes her own message states with the secret keys and acquires corresponding ECSs. The procedures are described below.

Step 1 Alice shares her secret key K_B (K_C) with the verifier Bob (Charlie) by using continuous-variable quantum key distribution (CVQKD) protocols which are demonstrated to be unconditionally secure.[30–33]

Step 2 Alice prepares coherent superposition states

$|\psi\rangle_B = \{|\psi\rangle_{B_i}|\ 1 \le i \le N\}$ and $|\psi\rangle_C = \{|\psi\rangle_{C_i}|\ 1 \le i \le N\}$, where

$$|\psi\rangle_{B_i} = \frac{1}{\sqrt{N_\alpha}}\left(\left|\sqrt{2}\alpha\right\rangle_{B_i} - \left|-\sqrt{2}\alpha\right\rangle_{B_i}\right),$$
$$|\psi\rangle_{C_i} = \frac{1}{\sqrt{N_\alpha}}\left(\left|\sqrt{2}\alpha\right\rangle_{C_i} - \left|-\sqrt{2}\alpha\right\rangle_{C_i}\right),$$

N is the number of message states and N_α is the normalization factor. Then she modulates the message 1 (message 2), i.e., $M_1 = \{M_{1_i}|\ 1 \le i \le N\}$ ($M_2 = \{M_{2_i}|\ 1 \le i \le N\}$), on coherent superposition states $|\psi\rangle_B$ ($|\psi\rangle_C$). Here note that Alice needs to prepare several copies of these coherent superposition states for facilitating comparison and reducing error probability of the verification phase.

Step 3 Alice transforms the secret key K_B into $\{K_B^1, K_B^2, \ldots, K_B^N\}$, where $K_B^i \in \{00, 01, 10, 11\}$. According to these keys, Alice encodes $|\psi\rangle_{B_i}$ into $|\psi\rangle'_{B_i}$ with the phase-shift operation $P(\theta_{B_i}) = \exp(i\theta_{B_i}a^\dagger a)$. Likewise, on the basis of K_C, Alice performs the corresponding operation $P(\theta_{C_i}) = \exp(i\theta_{C_i}a^\dagger a)$ on $|\psi\rangle_{C_i}$ to obtain $|\psi\rangle'_{C_i}$. For simplicity, we define that $\theta_{B_i}(\theta_{C_i}) = 0$ when the key is equal to 00 or 11, while $\theta_{B_i}(\theta_{C_i}) = \pi$ when the key is 01 or 10.

Step 4 Alice inputs $|\psi\rangle'_{B_i}$ and a vacuum state $|0\rangle_{E_i}$ into the BS which is equipped with a pair of $-\pi/2$ phase shifters. As described in Section 2, Alice can acquire an ECS $|\phi\rangle_{BE_i}$, i.e.,

$$|\phi\rangle_{BE_i} = \frac{1}{\sqrt{N'_{\alpha_{BE}}}}(x_B|\alpha\rangle_{B_i}|\alpha\rangle_{E_i} + y_B|-\alpha\rangle_{B_i}|-\alpha\rangle_{E_i}). \quad (13)$$

Similarly, she obtains $|\phi\rangle_{CF_i}$, i.e.,

$$|\phi\rangle_{CF_i} = \frac{1}{\sqrt{N'_{\alpha_{CF}}}}(x_C|\alpha\rangle_{C_i}|\alpha\rangle_{F_i} + y_C|-\alpha\rangle_{C_i}|-\alpha\rangle_{F_i}), \quad (14)$$

where $N'_{\alpha_{BE}}$ and $N'_{\alpha_{CF}}$ are the normalization factors of $|\phi\rangle_{BE_i}$ and $|\phi\rangle_{CF_i}$, respectively. The parameters x_B, y_B, x_C, and y_C are equivalent to 1 or -1.

3.2. Signing phase

This phase gives a specific description of the signature algorithm, i.e., Alice signs the message states by implementing unitary operations and merges these signed messages into a dual signature in the network. The technique used here is entanglement swapping which enables two parties that do not share quantum entanglement to share quantum entanglement with the assistance of a third party.[20] The signing phase is carried out by the following procedures.

Step 1 The expression of $|\phi\rangle_{BE_i}$ and $|\phi\rangle_{CF_i}$ in Eqs. (13) and (14) can be rewritten separately in terms of the orthonormal bases $|+\rangle$ and $|-\rangle$ described in Eqs. (7) and (8), i.e.,

$$|\phi\rangle_{BE_i} = w'_{1_i}|+\rangle_B|+\rangle_E + x'_{1_i}|-\rangle_B|-\rangle_E, \quad (15)$$

$$|\phi\rangle_{CF_i} = w'_{2_i}|+\rangle_C|+\rangle_F + x'_{2_i}|-\rangle_C|-\rangle_F, \quad (16)$$

where

$$w'_{1_i} = \frac{x_B\cos^2\omega + y_B\sin^2\omega}{\sqrt{N'_{\alpha_{BE}}}},$$
$$x'_{1_i} = \frac{x_B\sin^2\omega + y_B\cos^2\omega}{\sqrt{N'_{\alpha_{BE}}}},$$
$$w'_{2_i} = \frac{x_C\cos^2\omega + y_C\sin^2\omega}{\sqrt{N'_{\alpha_{CF}}}}, \quad (17)$$
$$x'_{2_i} = \frac{x_C\sin^2\omega + y_C\cos^2\omega}{\sqrt{N'_{\alpha_{CF}}}}.$$

Alice chooses the operation $U(K_X^i)$ based on her secret key K_X^i, where the subscript $X \in \{B, C\}$. The corresponding relationship between the operation $U(K_X^i)$ and the secret key K_X^i is described in Table 1.

Table 1. The corresponding relationship between the operations and the secret keys.

K_X^i	$U(K_X^i)$
00	$(I)_X$
01	$(-\sigma_x)_X$
10	$(i\sigma_y)_X$
11	$(\sigma_z)_X$

Then Alice implements the corresponding operation on state $|\phi\rangle_{BE_i}$ and derives the signature

$$|\phi\rangle'_{BE_i} = U(K_B^i)|\phi\rangle_{BE_i}$$
$$= \frac{1}{\sqrt{N'_{\alpha_{BE}}}}(|\lambda_1\alpha\rangle_B|\alpha\rangle_E + (-1)^{k_1\oplus 1}|-\lambda_1\alpha\rangle_B|-\alpha\rangle_E), \quad (18)$$

where $\lambda_1 = (-1)^{k_1\oplus k_2}$. k_1 (k_2) stands for the first (second) bit value of K_B^i and the notation $\oplus$ stands for summation mod 2. Therefore, the signature of message 1 is

$$S_B = \{|\phi\rangle'_{BE_i}|\ 1 \le i \le N\}.$$

Similarly, she can also encode the state $|\phi\rangle_{CF_i}$ to obtain the signature

$$|\phi\rangle'_{CF_i} = U(K_C^i)|\phi\rangle_{CF_i}$$
$$= \frac{1}{\sqrt{N'_{\alpha_{CF}}}}(|\lambda_2\alpha\rangle_C|\alpha\rangle_F + (-1)^{k_3\oplus 1}|-\lambda_2\alpha\rangle_C|-\alpha\rangle_F), \quad (19)$$

where $\lambda_2 = (-1)^{k_3\oplus k_4}$. k_3 (k_4) equals the first (second) bit value of K_C^i. We achieve the signature

$$S_C = \{|\phi\rangle'_{CF_i}|\, 1 \le i \le N\}$$

of message 2. Specifically, Alice's two signatures based on different secret keys are shown in Table 2, where $N_1 = 1/\sqrt{N'_{\alpha_{BE}}}$ and $N_2 = 1/\sqrt{N'_{\alpha_{CF}}}$.

Table 2. Alice's signatures based on different secret keys.

K_B^i	K_C^i	$\|\phi\rangle'_{BE}$	$\|\phi\rangle'_{CF}$
00	00	$N_1(\|\alpha\rangle_B\|\alpha\rangle_E - \|-\alpha\rangle_B\|-\alpha\rangle_E)$	$N_2(\|\alpha\rangle_C\|\alpha\rangle_F - \|-\alpha\rangle_C\|-\alpha\rangle_F)$
00	01	$N_1(\|\alpha\rangle_B\|\alpha\rangle_E - \|-\alpha\rangle_B\|-\alpha\rangle_E)$	$N_2(\|-\alpha\rangle_C\|\alpha\rangle_F - \|\alpha\rangle_C\|-\alpha\rangle_F)$
00	10	$N_1(\|\alpha\rangle_B\|\alpha\rangle_E - \|-\alpha\rangle_B\|-\alpha\rangle_E)$	$N_2(\|-\alpha\rangle_C\|\alpha\rangle_F + \|\alpha\rangle_C\|-\alpha\rangle_F)$
00	11	$N_1(\|\alpha\rangle_B\|\alpha\rangle_E - \|-\alpha\rangle_B\|-\alpha\rangle_E)$	$N_2(\|\alpha\rangle_C\|\alpha\rangle_F + \|-\alpha\rangle_C\|-\alpha\rangle_F)$
01	00	$N_1(\|-\alpha\rangle_B\|\alpha\rangle_E - \|\alpha\rangle_B\|-\alpha\rangle_E)$	$N_2(\|\alpha\rangle_C\|\alpha\rangle_F - \|-\alpha\rangle_C\|-\alpha\rangle_F)$
01	01	$N_1(\|-\alpha\rangle_B\|\alpha\rangle_E - \|\alpha\rangle_B\|-\alpha\rangle_E)$	$N_2(\|-\alpha\rangle_C\|\alpha\rangle_F - \|\alpha\rangle_C\|-\alpha\rangle_F)$
01	10	$N_1(\|-\alpha\rangle_B\|\alpha\rangle_E - \|\alpha\rangle_B\|-\alpha\rangle_E)$	$N_2(\|-\alpha\rangle_C\|\alpha\rangle_F + \|\alpha\rangle_C\|-\alpha\rangle_F)$
01	11	$N_1(\|-\alpha\rangle_B\|\alpha\rangle_E - \|\alpha\rangle_B\|-\alpha\rangle_E)$	$N_2(\|\alpha\rangle_C\|\alpha\rangle_F + \|-\alpha\rangle_C\|-\alpha\rangle_F)$
10	00	$N_1(\|-\alpha\rangle_B\|\alpha\rangle_E + \|\alpha\rangle_B\|-\alpha\rangle_E)$	$N_2(\|\alpha\rangle_C\|\alpha\rangle_F - \|-\alpha\rangle_C\|-\alpha\rangle_F)$
10	01	$N_1(\|-\alpha\rangle_B\|\alpha\rangle_E + \|\alpha\rangle_B\|-\alpha\rangle_E)$	$N_2(\|-\alpha\rangle_C\|\alpha\rangle_F - \|\alpha\rangle_C\|-\alpha\rangle_F)$
10	10	$N_1(\|-\alpha\rangle_B\|\alpha\rangle_E + \|\alpha\rangle_B\|-\alpha\rangle_E)$	$N_2(\|-\alpha\rangle_C\|\alpha\rangle_F + \|\alpha\rangle_C\|-\alpha\rangle_F)$
10	11	$N_1(\|-\alpha\rangle_B\|\alpha\rangle_E + \|\alpha\rangle_B\|-\alpha\rangle_E)$	$N_2(\|\alpha\rangle_C\|\alpha\rangle_F + \|-\alpha\rangle_C\|-\alpha\rangle_F)$
11	00	$N_1(\|\alpha\rangle_B\|\alpha\rangle_E + \|-\alpha\rangle_B\|-\alpha\rangle_E)$	$N_2(\|\alpha\rangle_C\|\alpha\rangle_F - \|-\alpha\rangle_C\|-\alpha\rangle_F)$
11	01	$N_1(\|\alpha\rangle_B\|\alpha\rangle_E + \|-\alpha\rangle_B\|-\alpha\rangle_E)$	$N_2(\|-\alpha\rangle_C\|\alpha\rangle_F - \|\alpha\rangle_C\|-\alpha\rangle_F)$
11	10	$N_1(\|\alpha\rangle_B\|\alpha\rangle_E + \|-\alpha\rangle_B\|-\alpha\rangle_E)$	$N_2(\|-\alpha\rangle_C\|\alpha\rangle_F + \|\alpha\rangle_C\|-\alpha\rangle_F)$
11	11	$N_1(\|\alpha\rangle_B\|\alpha\rangle_E + \|-\alpha\rangle_B\|-\alpha\rangle_E)$	$N_2(\|\alpha\rangle_C\|\alpha\rangle_F + \|-\alpha\rangle_C\|-\alpha\rangle_F)$

Step 2 Alice combines her signatures $S_B = \{|\phi\rangle'_{BE_i}|\ 1 \le i \le N\}$ and $S_C = \{|\phi\rangle'_{CF_i}|\ 1 \le i \le N\}$. Alice first combines states E and F in balanced BS and then counts the photon number in mode f or e, as shown in Fig. 2. In accordance with the principle of entanglement swapping, the system B is entangled to the system C, i.e., B and C are projected into the ECS

$$|\phi\rangle_{BC_i} = \begin{cases} N_3[|\lambda_1\alpha\rangle_B|\lambda_2\alpha\rangle_C + \lambda_3|-\lambda_1\alpha\rangle_B|-\lambda_2\alpha\rangle_C], \\ \quad \text{mode } f = 0, \\ N_3[|\lambda_1\alpha\rangle_B|-\lambda_2\alpha\rangle_C + \lambda_3|-\lambda_1\alpha\rangle_B|\lambda_2\alpha\rangle_C], \\ \quad \text{mode } e = 0, \end{cases} \tag{20}$$

where $N_3 = 1/\sqrt{N_{\alpha_{BC}}}$, $N_{\alpha_{BC}}$ is the normalization factor, and $\lambda_3 = (-1)^{k_1 \oplus k_3}$. Because the new state contains both signature information for message 1 and message 2, it is regarded as the dual signature $S_{BC} = \{|\phi\rangle_{BC_i}|1 \le i \le N\}$.

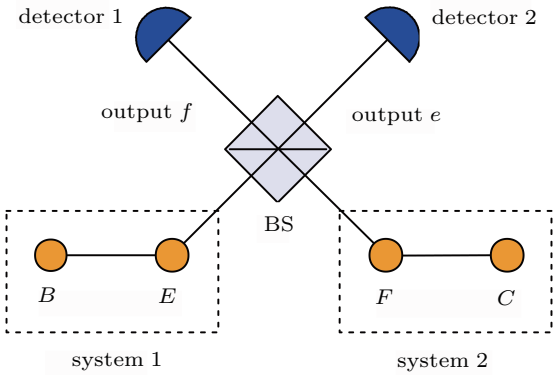


Fig. 2. (color online) Entanglement swapping: in the beginning, there are two entangled links B–E and C–F. Here BS stands for a loss-less 50:50 beam splitter. Detectors 1 and 2 are photon detectors. Modes f and e stand for output modes of the BS. Alice randomly measures mode f or e and then different output states will be achieved. So entanglement between B and C is obtained after the measurement between E and F.

Step 3 Alice sends the dual signature S_{BC} to the verifier Bob with the teleportation of ECSs. In order to transmit the ECS $|\phi\rangle_{BC_i}$, we need at least a quantum channel $|D\rangle_{GHI}$ which is a tripartite entangled state.[23] The whole system which consists of the dual signature and quantum channel can be expressed as $|\Psi\rangle = |\phi\rangle_{BC_i}|D\rangle_{GHI}$, where B, C, and G are at Alice's side, and H and I are at Bob's side.[23] Alice successively applies the operation $T_{CB} = P_B B_{CB} P_B$ and $T_{CG} = P_G B_{CG} P_G$ to the whole system. Then, she performs a two-mode number measurement on modes C and G. Subsequently, she transmits the outcome of measurement to Bob through the classical channel. Therefore, Bob can obtain the information of the dual signature after he executes the corresponding unitary operations on particles H and I.[23]

3.3. Verification phase

The verification phase requires Bob (Charlie) to verify the signatures of message 1 (message 2) and judge whether the message states are authentic. This process does not need the participation of the arbitrator, unless there are controversies.

Step 1 Once receiving Alice's dual signature $S_{BC} = \{|\phi\rangle_{BC_i}|\ 1 \le i \le N\}$, Bob randomly chooses n states of them and records their numbers. Since Alice has negotiated with Bob that every quantum dual signature state corresponds to every binary bit in advance. Bob sends the homologous bits of the chosen states and numbers to Alice through a classical channel. Alice generates the signature states based on Bob's binary sequence and compares them with her own signatures. The error rate $\varepsilon_{\text{forgery}} \le \varepsilon_0$ ensures that the following steps can continue to be executed, otherwise the protocol should be terminated, where ε_0 is error rate threshold.

Step 2 Based on K_B^i, Bob implements the operation $U(K_B^i)_{\text{Dec}} \in \{I, -\sigma_x, -\mathrm{i}\sigma_y, \sigma_z\}$ on state B of the dual signature, where the subscript 'Dec' represents that the operation is carried out in the verification phase. The operators I, $-\sigma_x$, $-\mathrm{i}\sigma_y$, and σ_z are chosen when K_B^i are equal to 00, 01, 10, and 11, respectively.

Step 3 Bob performs the operation $P(-\theta_{B_i})$ based on K_B^i and obtains the ECS $|\phi\rangle_{B'C_i}$.

Step 4 Bob gets the decoded message state $|\psi\rangle''_{B_i}$ and the encoded message state $|\psi\rangle_{C_i''}$ which separately relate to message 1 and message 2 by using Fourier multi-port devices.[34] In detail, the multi-port device considered in our scheme has two input optical modes and two output optical modes.

Step 5 Bob transmits $|\psi\rangle_{C_i''}$ to Charlie. Once receiving $|\psi\rangle_{C_i''}$, i.e., the signature of message 2, Charlie applies $U(K_C^i)_{\text{Dec}}$ on it based upon the secret key K_C^i. Likewise, the operators I, $-\sigma_x$, $-\mathrm{i}\sigma_y$, and σ_z severally correspond to 00, 01, 10, and 11. Then Charlie performs the operation $P(-\theta_{C_i})$ and obtains the decoded state $|\psi\rangle''_{C_i}$ of message 2.

Step 6 Bob (Charlie) asks Alice to send the related classical description (binary sequence) of the states of her message 1

(message 2). Then $|\psi\rangle_{B_i}$ and $|\psi\rangle_{C_i}$ are separately acquired by Bob and Charlie based on the relevant descriptions. Bob compares the decoded message states $|\psi\rangle''_{B_i}$ with the initial message states $|\psi\rangle_{B_i}$ by applying BSs.[35] If $|\psi\rangle_{B_i} = |\psi\rangle''_{B_i}$, one of the output modes may contain only the vacuum state. Then Bob gains the parameter

$$F_1 = \begin{cases} 1, & |\psi\rangle_{B_i} = |\psi\rangle''_{B_i}, \\ 0, & |\psi\rangle_{B_i} \neq |\psi\rangle''_{B_i}. \end{cases} \tag{21}$$

Charlie compares $|\psi\rangle_{C_i}$ with $|\psi\rangle''_{C_i}$, and gets the parameter

$$F_2 = \begin{cases} 1, & |\psi\rangle_{C_i} = |\psi\rangle''_{C_i}, \\ 0, & |\psi\rangle_{C_i} \neq |\psi\rangle''_{C_i}. \end{cases} \tag{22}$$

So Bob (Charlie) can draw a conclusion whether the signature is acceptable based on the parameter F_1 (F_2).

4. Security analysis

For the purpose of guaranteeing the security, the quantum signature scheme should satisfy two requirements.[36] One is that the attacker and the disingenuous receiver cannot forge the signature after the completion of signing, and the other is the signatory and the receiver cannot disavow the signature. On the basis of the above security requirements of quantum signature scheme, our protocol provides theoretical security since the attacker cannot obtain the useful information about the secret key and the original message, the signatory is unable to disavow the signatures and the verifiers also cannot deny the received signatures. Subsequently, we analyze the security of the proposed scheme in detail.

4.1. Impossibility of forgery

According to our signature scheme, the two signatures of Alice are S_B and S_C, separately. If the attacker Eve attempts to forge Alice's signatures, she has to be aware of the corresponding secret keys K_B or K_C. For the attacker, there are two ways to get the information about secret keys, i.e., she eavesdrops in the key distribution phase or obtains it from the signature.

However, due to the unconditionally secure CVQKD,[37–41] it is impossible to eavesdrop the secret keys shared between the signatory and verifiers. Moreover, quantum one-time pad algorithm also ensures the security. On one hand, for preventing the recipient or the eavesdropper from forging a message in the quantum signature process, we should ensure that only Alice knows the complete information about message states. If the attacker obtains the signature, she is ignorant of the signature algorithm. Thus Eve cannot infer the secret key from the signature. On the other hand, according to the characteristics of entanglement, once Eve tries to measure the signature to get the information of the keys, the entangled state may collapse and the forgery behavior can be discovered definitely and then honest correspondents may give up this communication. So Eve fails to deduce the key.

In the worst situation, if Eve gets K_B (K_C), she still has no information about the message states that were distributed to Bob (Charlie) without destroying the entanglement states. Moreover, if Eve tampers with the signature, the following example shows that the forgery can be definitely detected.

Example

(i) If $K_B^i = K_C^i = 00$ and there is no attack by Eve, we get the dual signature in the case of mode $e = 0$,

$$|\phi\rangle_{BC_i} = \frac{1}{\sqrt{N_{\alpha_{BC}}}}(|\alpha\rangle_B|-\alpha\rangle_C + |-\alpha\rangle_B|\alpha\rangle_C). \tag{23}$$

(ii) If Eve forges Alice's signature

$$\frac{1}{\sqrt{N'_{\alpha_{BE}}}}(|\alpha\rangle_B|\alpha\rangle_E - |-\alpha\rangle_B|-\alpha\rangle_E)$$

with

$$\frac{1}{\sqrt{N'_{\alpha_{BE}}}}(|\alpha\rangle_B|\alpha\rangle_E + |-\alpha\rangle_B|-\alpha\rangle_E)$$

and mode $e = 0$, the dual signature becomes

$$|\phi\rangle_{BC_i} = \frac{1}{\sqrt{N_{\alpha_{BC}}}}(|\alpha\rangle_B|-\alpha\rangle_C - |-\alpha\rangle_B|\alpha\rangle_C). \tag{24}$$

Comparing Eq. (23) with Eq. (24), it is easy to know that if Eve tampers with Alice's signatures, the entangled state of B and C may be changed. Supposing $K_B^i = K_C^i = 00$, as shown in Table 3, the states of legal communication are shown in case 0. There are fifteen cases for Eve's forgery and three cases (5, 10, and 15) may be successful. So the probability of forging a single state is $P = 3/15 = 1/5$. What is more, for another fifteen kinds of groups of secret keys, the probability is also $1/5$. Thus, the probability of forging the entire signature is

$$\varepsilon_{\text{forgery}} = \binom{n}{m}\left(\frac{1}{5}\right)^m\left(\frac{4}{5}\right)^{n-m}, \tag{25}$$

where m is the number of states which are forged by Eve successfully. n is the total number of states which are chosen in the step 1 of the verification phase. Obviously, the probability $\varepsilon_{\text{forgery}}$ satisfies the binomial distribution and the binomial coefficient $\binom{n}{m}$ is given by the expression $n!/m!(n-m)!$. As shown in Fig. 3, for each n, $\varepsilon_{\text{forgery}}$ has a maximum value which indicates the success probability of forgery in the best case. However, the optimal forgery probability is smaller when n is larger. Obviously, it is difficult to forge the entire signature since the value of $\varepsilon_{\text{forgery}}$ approaches 0 when $n \to \infty$. It is also necessary to define a forgery threshold ε_0. Once the error rate $\varepsilon_{\text{forgery}}$ exceeds the threshold ε_0, the scheme should be discontinued.

Table 3. The quantum dual signatures under different conditions.

Case	K_B^i	K_C^i	$\|\phi\rangle'_{BC}$	
			$f=0$	$e=0$
0	00	00	$N_3(\|\alpha\rangle_B\|\alpha\rangle_C+\|-\alpha\rangle_B\|-\alpha\rangle_C)$	$N_3(\|\alpha\rangle_B\|-\alpha\rangle_C+\|-\alpha\rangle_B\|\alpha\rangle_C)$
1	00	01	$N_3(\|\alpha\rangle_B\|-\alpha\rangle_C+\|-\alpha\rangle_B\|\alpha\rangle_C)$	$N_3(\|\alpha\rangle_B\|\alpha\rangle_C+\|-\alpha\rangle_B\|-\alpha\rangle_C)$
2	00	10	$N_3(\|\alpha\rangle_B\|-\alpha\rangle_C-\|-\alpha\rangle_B\|\alpha\rangle_C)$	$N_3(\|\alpha\rangle_B\|\alpha\rangle_C-\|-\alpha\rangle_B\|-\alpha\rangle_C)$
3	00	11	$N_3(\|\alpha\rangle_B\|\alpha\rangle_C-\|-\alpha\rangle_B\|-\alpha\rangle_C)$	$N_3(\|\alpha\rangle_B\|-\alpha\rangle_C-\|-\alpha\rangle_B\|\alpha\rangle_C)$
4	01	00	$N_3(\|-\alpha\rangle_B\|\alpha\rangle_C+\|\alpha\rangle_B\|-\alpha\rangle_C)$	$N_3(\|\alpha\rangle_B\|\alpha\rangle_C+\|-\alpha\rangle_B\|-\alpha\rangle_C)$
5	01	01	$N_3(\|-\alpha\rangle_B\|-\alpha\rangle_C+\|\alpha\rangle_B\|\alpha\rangle_C)$	$N_3(\|\alpha\rangle_B\|-\alpha\rangle_C+\|-\alpha\rangle_B\|\alpha\rangle_C)$
6	01	10	$N_3(\|-\alpha\rangle_B\|-\alpha\rangle_C-\|\alpha\rangle_B\|\alpha\rangle_C)$	$N_3(\|\alpha\rangle_B\|-\alpha\rangle_C-\|-\alpha\rangle_B\|\alpha\rangle_C)$
7	01	11	$N_3(\|-\alpha\rangle_B\|\alpha\rangle_C-\|\alpha\rangle_B\|-\alpha\rangle_C)$	$N_3(\|\alpha\rangle_B\|\alpha\rangle_C-\|-\alpha\rangle_B\|-\alpha\rangle_C)$
8	10	00	$N_3(\|-\alpha\rangle_B\|\alpha\rangle_C-\|\alpha\rangle_B\|-\alpha\rangle_C)$	$N_3(\|\alpha\rangle_B\|\alpha\rangle_C-\|-\alpha\rangle_B\|-\alpha\rangle_C)$
9	10	01	$N_3(\|-\alpha\rangle_B\|-\alpha\rangle_C-\|\alpha\rangle_B\|\alpha\rangle_C)$	$N_3(\|\alpha\rangle_B\|-\alpha\rangle_C-\|-\alpha\rangle_B\|\alpha\rangle_C)$
10	10	10	$N_3(\|-\alpha\rangle_B\|-\alpha\rangle_C+\|\alpha\rangle_B\|\alpha\rangle_C)$	$N_3(\|\alpha\rangle_B\|-\alpha\rangle_C+\|-\alpha\rangle_B\|\alpha\rangle_C)$
11	10	11	$N_3(\|-\alpha\rangle_B\|\alpha\rangle_C+\|\alpha\rangle_B\|-\alpha\rangle_C)$	$N_3(\|\alpha\rangle_B\|\alpha\rangle_C+\|-\alpha\rangle_B\|-\alpha\rangle_C)$
12	11	00	$N_3(\|\alpha\rangle_B\|\alpha\rangle_C-\|-\alpha\rangle_B\|-\alpha\rangle_C)$	$N_3(\|\alpha\rangle_B\|-\alpha\rangle_C-\|-\alpha\rangle_B\|\alpha\rangle_C)$
13	11	01	$N_3(\|\alpha\rangle_B\|-\alpha\rangle_C-\|-\alpha\rangle_B\|\alpha\rangle_C)$	$N_3(\|\alpha\rangle_B\|\alpha\rangle_C-\|-\alpha\rangle_B\|-\alpha\rangle_C)$
14	11	10	$N_3(\|\alpha\rangle_B\|-\alpha\rangle_C+\|-\alpha\rangle_B\|\alpha\rangle_C)$	$N_3(\|\alpha\rangle_B\|\alpha\rangle_C+\|-\alpha\rangle_B\|-\alpha\rangle_C)$
15	11	11	$N_3(\|\alpha\rangle_B\|\alpha\rangle_C+\|-\alpha\rangle_B\|-\alpha\rangle_C)$	$N_3(\|\alpha\rangle_B\|-\alpha\rangle_C+\|-\alpha\rangle_B\|\alpha\rangle_C)$

If the receiver Bob is malicious and attempts to forge Alice's signature, he is obliged to know Charlie's secret key K_C. However, his forgery fails since he cannot obtain the secret key K_C and has no idea of message 2. Besides, Charlie cannot forge the signature of message 1 since he has no chance of access to message 1's signature. He also could not forge message 2's signature, because he knows nothing about the message states of message 2. Based on the analysis, we can conclude that any forgery would fail.

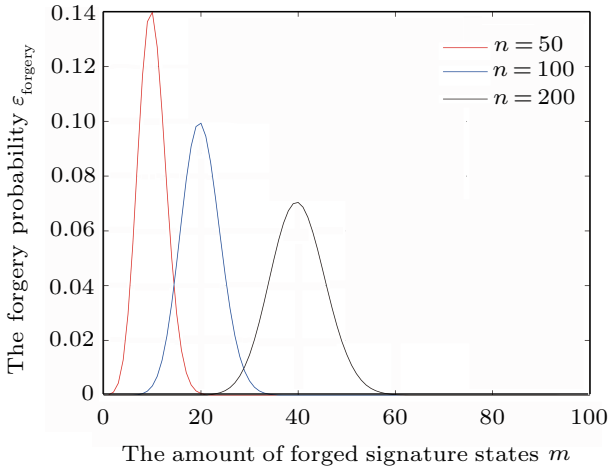


Fig. 3. (color online) The forgery probability as a function of the amount of forged signature states. The three curves in lines correspond to $n=50$, 100, and 200. It shows that $\varepsilon_{\text{forgery}}$ has a maximum value for each n. But the optimal forgery probability is smaller when n is larger.

4.2. Impossibility of disavowal by the signatory

In the proposed scheme, Alice signs messages 1 and 2 and integrates the two signatures to generate a dual signature, which includes the information of K_B (K_C) that is only distributed between Alice and Bob (Charlie). Thereby, it is easy to discover whether Alice disavows the signature or not. Furthermore, Alice may either recognize or disavow the signature, so the probability of disavowing a signature state is $1/2$. Thus the probability of disavowal for the signature by Alice is

$$\varepsilon_{\text{disavowal}} = \binom{N}{l}\left(\frac{1}{2}\right)^{l}\left(\frac{1}{2}\right)^{N-l}, \tag{26}$$

where l is the amount of signature states which are disavowed by the signatory. N stands for the length of signature. Similarly, the probability $\varepsilon_{\text{disavowal}}$ satisfies the binomial distribution and the binomial coefficient

$$\binom{N}{l} = \frac{N!}{l!(N-l)!}.$$

From Fig. 4, we also conclude that $\varepsilon_{\text{disavowal}}$ can be very small when N is large enough. If $\varepsilon_{\text{disavowal}}$ exceeds the disavowal threshold ε_1, it is concluded that Alice disavows her signature.

In particular, when there are disputations between signatory and verifiers, a trusted arbitrator is required. Alice just needs to transmit her messages and the corresponding signatures to the arbitrator. For example, if the signature which belongs to Alice can be decoded by Alice's secret key, the signature has been executed by Alice, otherwise, Bob, Charlie or the attacker has forged the signature. It is apparent that the arbitrator plays an important role in judging whether Alice has disavowed her signatures when there are disputes or disagreements.

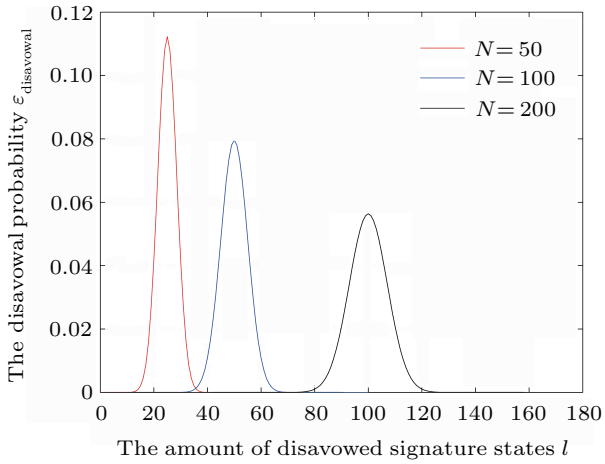


Fig. 4. (color online) The disavowal probability as a function of the amount of disavowed signature states. The three curves in lines correspond to $N = 50$, 100, and 200. Similarly, $\varepsilon_{\text{disavowal}}$ has a maximum value for each N and the optimal disavowal probability is smaller with N being larger.

4.3. Impossibility of denial by the verifiers

The verifier Bob cannot deny his behavior. After the operation of entanglement swapping, Alice sends the dual signature S_{BC} to Bob. It is clear that Bob knows the secret keys K_B and he performs some operations on the dual signature during the verification phase. He is willing to verify the signature meaning that he received the dual signature which contains information of Alice's signatures, and he has verified the signature indeed without later denying his involvement and actions. In the same way, Charlie also fails to deny. Based on K_C, Charlie performs measurements and operations after receiving the signature of message 2. So he cannot deny his behaviors.

According to the above analysis, we can determine that the proposed signature scheme can provide us theoretical security.

5. Extension

In the real life, a merchant often trades with some multiple customers and every customer has several different bank accounts. Thus the quantum dual signature scheme which contains more than three participants is discussed in this section. As shown in the following Fig. 5, Alice$_i$ $(2 \leq i \leq n)$ is a customer, Bob is business, and Charlie$_j$ $(2 \leq j \leq m)$ is bank. In the case that all Alice and Charlies are connected to Bob, thus any Alice to reach any Charlie should pass through Bob, namely, any Alice can correspond with any Charlie with the help of Bob.

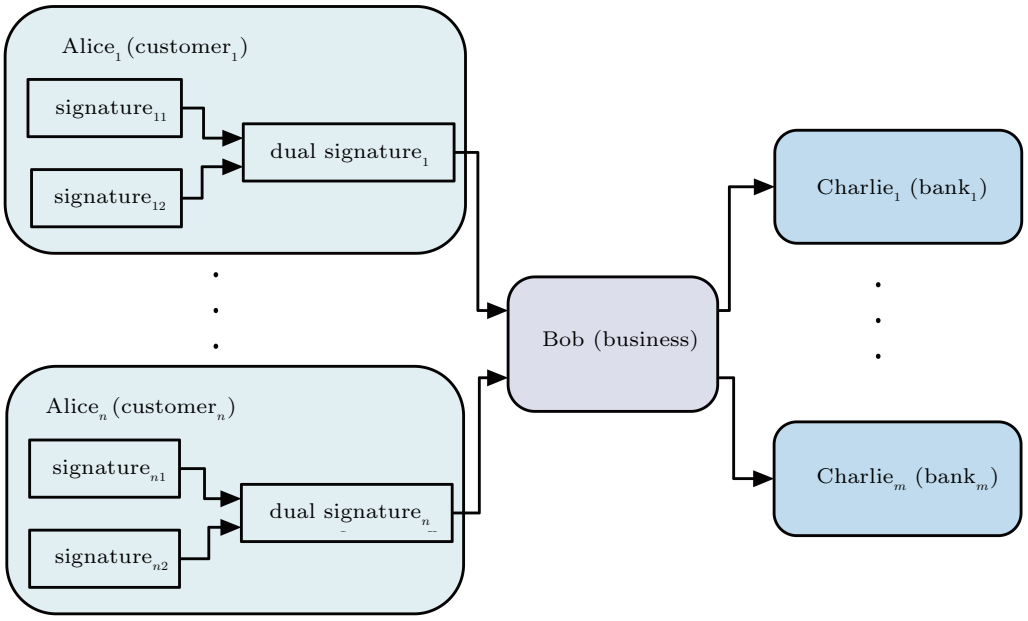


Fig. 5. (color online) Schematic representation of the quantum dual signature scheme which involves multiple participants in the network. Alice$_i$ $(2 \leq i \leq n)$ is a customer who signs her own two messages and generates a dual signature by applying entanglement swapping. Bob is the business who verifies the order information's signature. Charlie$_j$ $(2 \leq j \leq m)$ is the bank who verifies the signature of payment information of the corresponding customer.

The multi-party quantum dual signature scheme also includes three phases, i.e., the initial phase, the signing phase and the verification phase. The main difference between the multi-party quantum dual signature scheme and the three-party one is that Alice$_i$ needs to notify Bob of the trading bank in advance in the initial phase. We assume that Alice$_i$ wants to pay the order with her account in the bank Charlie$_j$. The extensional scheme is briefly described as follows.

Step 0 Alice$_i$ informs Bob that she wants to trade with him, and indicates to him which bank she wants to use through the classical channel. If Bob agrees to the transaction, he severally establishes the quantum channels with Alice$_i$ and the corresponding bank Charlie$_j$.

Step 1 Alice$_i$ encrypts message 1 (2) by using the shared

secret key with the verifier Bob (Charlie$_j$).

Step 2 Alice$_i$ generates the ECSs based on encrypted message states and then signs the ECSs by implementing unitary operations.

Step 3 Alice$_i$ combines the signatures of messages 1 and 2 into the dual signature and sends the proceeding dual signature to Bob.

Step 4 Bob extracts and verifies message 1's signature and transmits message 2's signature to Charlie$_j$.

Step 5 Charlie$_j$ verifies the signature of message 2 and judges whether the message is falsified.

The unconditional security of our extensional scheme can also be guaranteed. Moreover, it is obvious that the multi-party quantum dual signature scheme is preferably applicable to the network. It also has the important application value in the e-commerce system for its unconditional security.

6. Conclusion

A quantum dual signature scheme based on the ECSs and entanglement swapping is presented in this paper, in which a signatory and two verifiers are considered. The signatory Alice signs two different messages 1 and 2 which are separately sent to two diverse verifiers Bob and Charlie. Alice aggregates those two signatures to generate a quantum dual signature with entanglement swapping. In order to make this scheme suitable for the practical application, the signature verified by Charlie is forwarded by Bob. The verifier Bob (Charlie) can judge whether the signature of message 1 (2) is authentic and valid. Based on the security analysis with quantum properties, any attacker who attempts to counterfeit the signature would be detected, and the important rules impossible to forge, disavow or deny for the signature protocol are observed, thus our protocol can guarantee the security unconditionally. The three-party scheme can also be extended to the multi-party scheme which contains more than three participants, and the extensional scheme can remain safe. Furthermore, the proposed schemes are quite appropriate for the e-payment system if they involve further theoretical and technical supports.

References

[1] Zeng G and Keitel C H 2002 *Phys. Rev. A* **65** 042312
[2] Greenberger D, Hentschel K and Weinert F 2009 *Compendium of Quantum Physics: Concepts, Experiments, History and Philosophy* (Berlin: Springer)
[3] Zeng G, Lee M, Guo Y and He G Q 2007 *Int. J. Quantum Infor.* **5** 553
[4] Gottesman D and Chuang I 2001 arXiv: 0105032 [quant-ph]
[5] Curty M and Lütkenhaus N 2008 *Phys. Rev. A* **77** 046301
[6] Zeng G 2008 *Phys. Rev. A* **78** 016301
[7] Wen X and Liu Y 2007 *The First International Symposium on Data, Privacy, and E-Commerce*, November 1–3, 2007, Chengdu, China, p. 496
[8] Shi J, Shi R, Tang Y and Lee M H 2011 *Quantum Infor. Process.* **10** 653
[9] Shi J, Shi R, Guo Y, Peng X, Lee M H and Park D 2012 *Int. J. Theor. Phys.* **51** 1038
[10] Shi J, Shi R, Guo Y, Peng X and Tang Y 2013 *Sci. China-Infor. Sci.* **56** 052115
[11] Dunjko V, Wallden P and Andersson E 2014 *Phys. Rev. Lett.* **112** 040502
[12] Wang C, Liu J W and Shang T 2014 *Chin. Phys. B* **23** 060309
[13] Shang T, Zhao X J, Wang C and Liu J W 2015 *Quantum Infor. Process.* **14** 393
[14] Zhou D L and Kuang L M 2009 *Chin. Phys. B* **18** 1328
[15] Wang X and Sanders B C 2001 *Phys. Rev. A* **65** 012303
[16] Zhang Y M, Li X W, Yang W and Jin G R 2013 *Phys. Rev. A* **88** 043832
[17] Van Enk S J and Hirota O 2001 *Phys. Rev. A* **64** 022313
[18] Chao W and Hu Z 2011 *International Conference on Intelligence Science and Information Engineering*, 2011, p. 85
[19] Zhang C Y and Chao W 2011 *International Symposium on Intelligence Information Processing and Trusted Computing*, October 22–23, 2011, Wuhan, China, p. 245
[20] Sangouard N, Simon C, Gisin N, Laurat J, Tualle-Brouri R and Grangier P 2010 *J. Opt. Soc. Am. B* **27** A137
[21] Weedbrook C, Pirandola S, García-Patrón R, Cerf N J, Ralph T C, Shapiro J H and Lloyd S 2012 *Rev. Mod. Phys.* **84** 621
[22] Braunstein S L and Van Loock P 2005 *Rev. Mod. Phys.* **77** 513
[23] Wang X 2001 *Phys. Rev. A* **64** 022302
[24] Cai X H, Guo J R, Nie J H and Jia J P 2006 *Chin. Phys.* **15** 488
[25] Kim M S, Son W, Bužek V and Knight P L 2002 *Phys. Rev. A* **65** 032323
[26] Liao J Q and Kuang L M 2006 *Chin. Phys.* **15** 2246
[27] Zhou D L and Kuang L M 2009 *Chin. Phys. B* **18** 1328
[28] Jeong H, Kim M S and Lee J 2001 *Phys. Rev. A* **64** 052308
[29] Joo J and Ginossar E 2015 arXiv: 1509.02859 [quant-ph]
[30] Grosshans F and Grangier P 2002 *Phys. Rev. Lett.* **88** 057902
[31] Yang J, Xu B, Peng X and Guo H 2012 *Phys. Rev. A* **85** 052302
[32] Walk N, Ralph T C, Symul T and Lam P K 2013 *Phys. Rev. A* **87** 020303
[33] Gong L H, Song H C, He C S, Liu Y and Zhou N R 2014 *Phys. Scr.* **89** 035101
[34] Vourdas A and Dunningham J A 2005 *Phys. Rev. A* **71** 013809
[35] Andersson E, Curty M and Jex I 2006 *Phys. Rev. A* **74** 022304
[36] Li Q, Chan W H and Long D Y 2009 *Phys. Rev. A* **79** 054307
[37] Lodewyck J, Bloch M, and Grangier P 2007 *Phys. Rev. A* **76** 042305
[38] García-Patrón R and Cerf N J 2006 *Phys. Rev. Lett.* **97** 190503
[39] Li Y, Zhang J, Zhang J X and Zhang T C 2006 *Chin. Phys.* **15** 1766
[40] He G Q, Zhu S W, Guo H B and Zeng G H 2008 *Chin. Phys. B* **17** 1263
[41] Zhu J, He G Q and Zeng G H 2007 *Chin. Phys.* **16** 1364