SCIENCE CHINA
Information Sciences

• RESEARCH PAPER •

November 2016, Vol. 59 112501:1–112501:13
doi: 10.1007/s11432-015-0616-9

Quantum private comparison based on quantum dense coding

Feng WANG[1,2], Mingxing LUO[2], Huiran LI[2], Zhiguo QU[3*] & Xiaojun WANG[4]

[1]*College of Mathematical Sciences, Dezhou University, Dezhou* 253023*, China;*
[2]*Information Security and National Computing Grid Laboratory, Southwest Jiaotong University, Chengdu* 610031*, China;*
[3]*Jiangsu Engineering Center of Network Monitoring, Nanjing University of Information Science & Technology, Nanjing* 210044*, China;*
[4]*School of Electronic Engineering, Dublin City University, Dublin* 9*, Ireland*

Received February 15, 2016; accepted May 22, 2016; published online September 28, 2016

Abstract A serious problem in cloud computing is privacy information protection. This study proposes a new private comparison protocol using Einstein-Podolsky-Rosen (EPR) pairs. This protocol allows two parties to secretly compare their classical information. Quantum dense coding enables the comparison task to be completed with the help of a classical semi-honest center. A one-step transmission scheme and designed decoy photons can be used against various quantum attacks. The new protocol can ensure fairness, efficiency, and security. The classical semi-honest center cannot learn any information about the private inputs of the players. Moreover, this scheme can be easily generalized using the general EPR pairs in order to improve the transmission efficiency.

Keywords private comparison, multiparty secure computation, classical semi-honesty center, quantum dense coding, general EPR pair

Citation Wang F, Luo M X, Li H R, et al. Quantum private comparison based on quantum dense coding. Sci China Inf Sci, 2016, 59(11): 112501, doi: 10.1007/s11432-015-0616-9

1 Introduction

Privacy information protection has become a very essential requirement, specially using the cloud computing technology. The widespread employment of the cloud computing may be hindered due to various reasons including the privacy information leakage, malicious attacks, unauthorized access, and foraged message [1–4]. To protect private information, sensitive data may be encrypted by the data owner. However, the distribution of the key is very difficult. Quantum states, as special information carriers, have been used to construct various protocols. The first important application is the quantum key distribution (QKD) protocol [5–8] with unconditional security. This great scheme has initiated various kinds of cryptographic protocols such as secure transmission of quantum state [9–12], quantum secret sharing [13–19], quantum direction communication [20–26], and quantum steganography protocols [27–29]; these schemes have been explored for various security systems.

* Corresponding author (email: qzghhh@126.com)

Recently, quantum private comparison (QPC) has attracted great attention because of its special applications in quantum secure computations. QPC protocol aims to securely compare classical secret information of two parties. The classical case has already been discussed in modern cryptography. The first example is the millionaires' problem, which was proposed by Yao [30, 31]. It aims to compare the amount of money of millionaires without revealing their actual wealth. This scheme is slightly changed into general case, where the equality of only two series is compared [32]. Unfortunately, Lo [33] shows that all one-sided two-party computations, which allow only one of the two parties to learn the result, are essentially insecure [33]. To address this problem, special restrictions such as the trust center may be required to perform the private comparison.

The classical private comparison scheme may be extended to the quantum case using quantum entanglement [34, 35]. Until now, many QPC schemes [36–47] have been proposed to improve the security and comparison efficiency. Most of these protocols use the trust or semi-honest center, which can implement the quantum operations, to complete the comparison task. Such legitimate trust centers should execute the protocol faithfully and preserve a record of all intermediate operations. Although this record may be used to infer secret information, it cannot be corrupted by any external attack.

Motivated by the ideas presented in [34–47], a secure QPC protocol should have the following features. First, the secret information is compared by blocks instead of bits to avoid leaking the actual content and reducing the comparison efficiency. Second, the secret information should be encrypted well to prevent the trust center from recognizing the values. Third, any player cannot learn the secret information of another player in case the comparison results is unequal. It means that an inside attacker cannot learn additional information during the comparison procedure compared with the random guess. Finally, the trust center should only send the comparison result (i.e., identical or different) instead of other details to the participants.

With the advancement of quantum theory with respect to quantum entanglement swapping [48, 49] and dense coding [50–52], we can construct a two-party QPC with *a classical semi-honest center*, which can only implement classical cryptography operations. In order to complete the private comparison, we use quantum dense coding based on the Einstein-Podolsky-Rosen (EPR) pairs and its general forms. From the quantum entanglement swapping, the secret comparison is equivalent to comparing two random quantum measurement outcomes. Because these quantum measurement outcomes are random for secret information, they can provide the necessary security from any internal and external attackers. A classical semi-honest center is used to authorize two participants using the classical cryptography techniques, and cannot recover any secret messages. On the other hand, because of the one-time quantum exchanges, our schemes are immune to Trojan horse attacks [53–57] without installing any optical filter devices.

The rest part of this paper is organized as follows. Section 2 describes the entanglement swapping of two EPR pairs and presents the proposed QPC protocol. Section 3 analyzes the security of the proposed scheme with respect to all aspects of attacks. The last section present a simplified general scheme for a qudit case and concludes this paper.

2 QPC protocol using EPR dense coding

This section presents a two-party QPC protocol using EPR pairs.

2.1 Quantum entanglement swapping of Bell states

The entanglement swapping [48, 49] as special quantum phenomenon allows remote parties to generate new entangling systems. The entanglement swapping of two EPR pairs is presented in this section for the convenience of correctness proof in the following section.

In detail, suppose that Alice and Bob prepare an EPR pair of $(\sigma_i \otimes I_2)|\Phi\rangle$ with $|\phi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. Here, (A_1, A_2) denote particles owned by Alice while (B_1, B_2) denote particles owned by Bob. By exchanging the particle A_1 with B_1, a new entanglement is generated between Alice and Bob after performing Bell measurement on particle pair (B_1, A_2) or (A_1, B_2). Their relationships are displayed in

Table 1 The entanglement swapping of Bell states ($0 \leqslant i \neq j \leqslant 3$ and $0 \leqslant k \leqslant 3$)

Two initial Bell states	The resultant
$(\sigma_i \otimes I_2)\|\Phi\rangle(\sigma_i \otimes I_2)\|\Phi\rangle$	$(\sigma_k \otimes I_2)\|\Phi\rangle(\sigma_k \otimes I_2)\|\Phi\rangle$
$(\sigma_i \otimes I_2)\|\Phi\rangle(\sigma_j \otimes I_2)\|\Phi\rangle$	$(\sigma_k \otimes I_2)\|\Phi\rangle(\sigma_{k+i+j \bmod 4} \otimes I_2)\|\Phi\rangle$

Table 2 The entanglement swapping of general Bell states ($0 \leqslant i \neq j \leqslant d-1$ and $0 \leqslant l,\ k \leqslant d-1$)

Two initial Bell states	The resultant
$(U_i \otimes I_d)\|\Phi\rangle(U_i \otimes I_d)\|\Phi\rangle$	$(U_{i+k} \otimes U_l)\|\Phi\rangle(U_{i-k} \otimes U_{-l})\|\Phi\rangle$
$(U_i \otimes I_d)\|\Phi\rangle(U_j \otimes I_d)\|\Phi\rangle$	$(U_{i+k} \otimes U_l)\|\Phi\rangle(U_{j-k \bmod d} \otimes U_{-l})\|\Phi\rangle$

Table 1. Pauli matrices σ_i are defined by

$$\sigma_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \sigma_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_2 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad \sigma_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \tag{1}$$

This result may be extended to arbitrary d-level system with normal computation basis $\{|0\rangle, |1\rangle, \ldots, |d-1\rangle\}$. General Bell states, a set of d^2 maximally entangled states, form an orthogonal basis of the space $\mathcal{C}^{d^2}$. The explicit forms of d-level Bell states are defined by $|\varphi(s,t)\rangle = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} \mathrm{e}^{\mathrm{i}2js\pi/d} |j, j+t\rangle$ for $s, t = 0, \ldots, d-1$. Suppose that Alice has Bell state $|\varphi(s_1, t_2)\rangle_{12}$, and Bob has Bell state $|\varphi(s_2, t_2)\rangle_{34}$. The entanglement swapping of two d-level Bell states is defined by the following formula

$$|\varphi(s_1,t_1)\rangle_{12}|\varphi(s_2,t_2)\rangle_{34} = \frac{1}{d}\sum_{k=0}^{d-1}\sum_{l=0}^{d-1} \mathrm{e}^{-\mathrm{i}2kl\pi/d^2} |\varphi(s_1+k, t_2+l)\rangle_{14}|\varphi(s_2-k, t_1-l)\rangle_{32}, \tag{2}$$

where $U_j = \sum_{k=0}^{d-1} |k+j \bmod d\rangle\langle k|$. The relationship of two general Bell states and two measurement outcomes after the entanglement swapping is shown in Table 2.

2.2 QPC protocol progress

Assume that the secretes are of the same length n, otherwise, the result can easily obtained.

All situps are defined as follows.

Goal: Two parties (Alice and Bob) will compare their documents for equivalence with the help of a classical semi-honest center.

Classical semi-honest center: Here, one can only implement classical cryptography operations such as encryption or decryption and does not need to own quantum operation abilities. It also reliably transmits classical messages. A classical computer is a typical example of semi-honest center. It owns the unique identities of all legitimate parties for authentication.

Participant privileges: Both parties can generate EPR pairs $|\Phi\rangle$ and single qubit state set $\mathcal{D}$, and also perform Pauli operations σ_i. The details of $\mathcal{D}$ are explained in the following subsection. The participants can implement an asymmetric encryption function $\mathrm{Ep}_1(\cdot)$ satisfying

$$\mathrm{Ep}_1(\mathrm{Ep}_1(\cdot)_{K_1})_{K_2} \neq \mathrm{Ep}_1(\mathrm{Ep}_1(\cdot)_{K_2})_{K_1} \tag{3}$$

with any two keys K_1 and K_2, and a symmetric encryption function $\mathrm{En}_2(\cdot)$ such as the Advanced Encryption Standard (AES). Alice has a public-secret key pair (K_A, K_A^{-1}) and Bob has a public-secret key pair (K_B, K_B^{-1}). Alice has shared key K_{AS} with the classical semi-honest center while Bob has shared a key K_{BS} with the classical semi-honest center. Both have unique identity information $\mathrm{Identity}_{A(B)}$.

Information encoding: All the Pauli operations σ_i are encoded with two bits $i_1 i_2$.

The proposed protocol can be explained as follows.

S1. This step is used to prepare the physical particles for encoding the information, which is named as "Preparing the EPR" step as shown in Figure 1. Specially, Alice (Bob) prepares an EPR pair sequence $S_A(S_B)$ with $|\Phi\rangle$. She (he) divides these states into two subsequences S_{A1} and S_{A2} (S_{B1} and S_{B2}), which

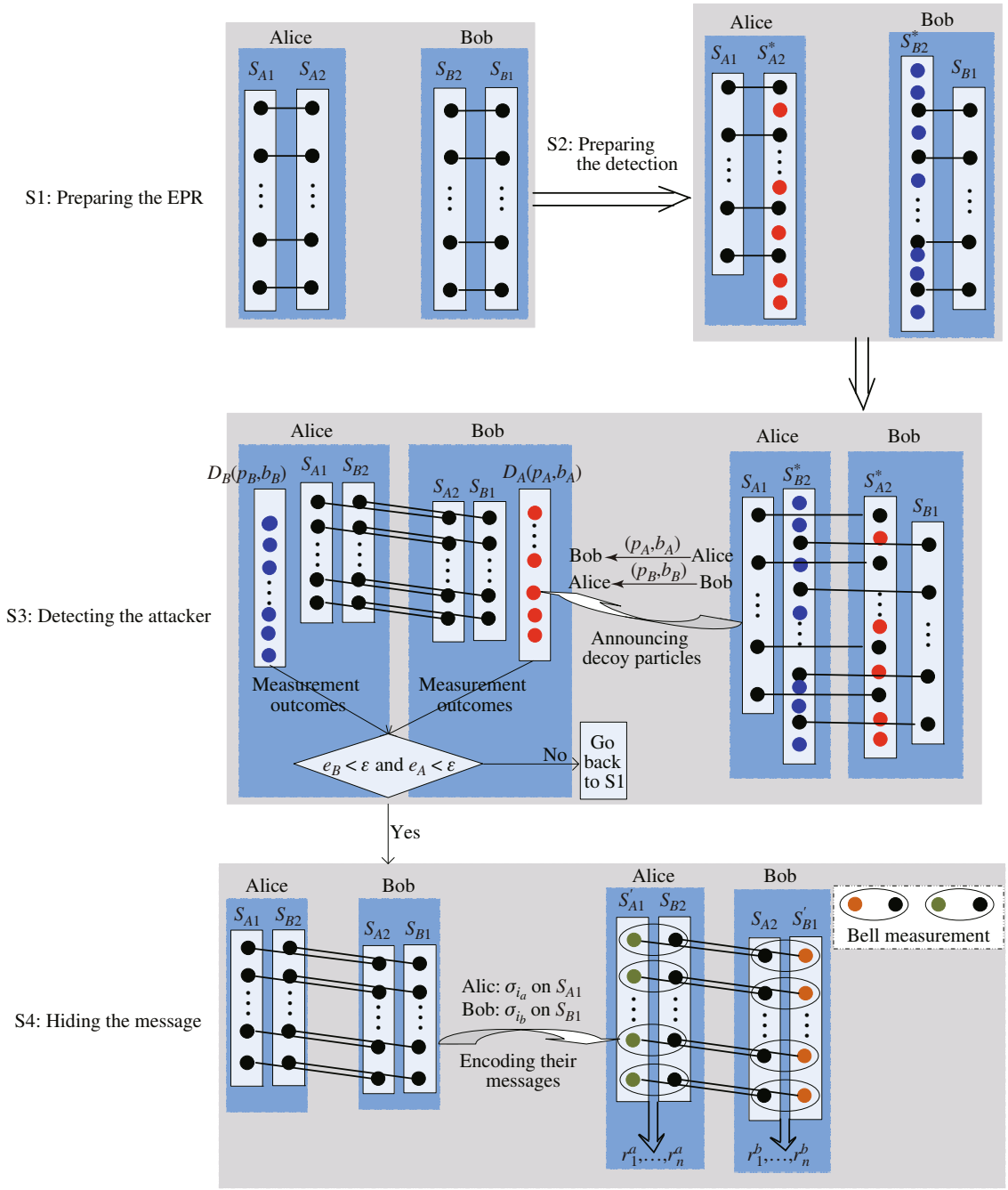

Figure 1 Schematic quantum process of private comparison protocol. ε denotes the error threshold. Red dots and blue dots denote the decoy photons randomly chosen from $\mathcal{D}$ for detecting Eve. σ_{i_a} and σ_{i_b} denote Pauli operations according to bit encodings of massages M_A and M_B, respectively. $e_{A(B)}$ is the error ratio while ε is the error threshold. $r^a_1,\ldots,r^a_n$ and $r^b_1,\ldots,r^b_n$ are the encoding information of measurement outcomes.

include the 1st and the 2nd particles of all states, respectively. These are schematically shown in Figure 1, where the two black dots connected by a line denote an EPR pair.

S2. This step is used to prepare the physical particles for detection, which is named as "Preparing for the detection" step, as shown in Figure 1. Specially, Alice and Bob insert many randomly chosen decoy photons, D_A (shown as red dots in Figure 1) and D_B (shown as blue dots in Figure 1), into S_{A2} and S_{B2} respectively; these are used to form new sequences S^*_{A2} and S^*_{B2}, respectively. They send these random sequences to each other via a physical channel. Here, all the positions at which insertion are made, are also random and recorded.

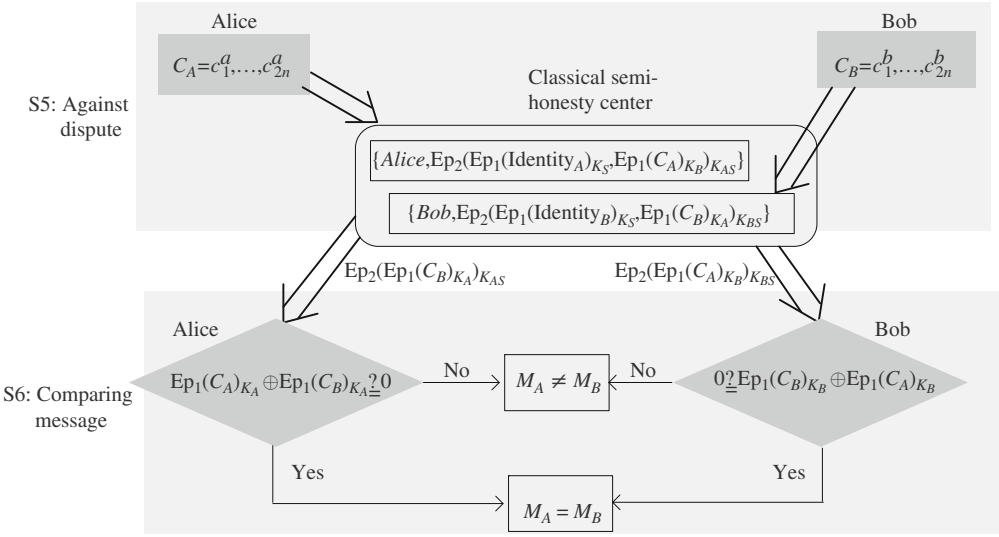

Figure 2 Classical process of private comparison protocol. Identity$_A$ and Identity$_B$ denote the single identity of Alice and Bob respectively. $\mathrm{Ep}_1()$ denotes the asymmetric encrypt function such as RSA while $\mathrm{Ep}_2()$ denotes the symmetric encrypt function such as AES.

S3. This step is used to detect the attackers, which is named as "Detecting the attacker" step, as shown in Figure 1. In detail, Bob (or Alice) first ensures that S^*_{A2} (or S^*_{B2}) has been received by Alice (or Bob) by sending a classical checking message m_A (or m_B) via a classical communication channel, as shown in Figure 1. And then, Alice (or Bob) states the positions (p_A (or p_B), as shown in Figure 1) and the preparation bases (b_A (b_B), as shown in Figure 1) of the decoy states D_A (or D_B) via a classical communication channel. Next, she (he) extracts the other party's particles D_B (or D_A) from S^*_{B2} (or S^*_{A2}) and measures them using the bases b_B (b_A) to obtain the check results R_{D_B} (or R_{D_A}). If there is an attacker, he/she may be detected by Alice or Bob by the comparison of the error rates P_e of R_{D_A} and R_{D_B} to an ideal error threshold ε. If there is no eavesdropper, then the protocol continues; otherwise, they should abort these particles and restart from the step S1.

S4. This step is used to hide the context, which is named as "Hiding the message" step as shown in Figure 1. In detail, note that after the detection step, the two received particle series S^*_{B2} and S^*_{A2} are reduced to S_{B2} and S_{A2}, respectively. The Pauli operations, σ_{i_a} and σ_{i_b}, are performed on the photon series S_{B1} and S_{A1} based on each of the two bits $i_a = i^a_1 i^a_2$ ($i_b = i^b_1 i^b_2$) of the secret message M_A (M_B) to obtain new series S'_{B1} and S'_{A1}, respectively, as shown in Figure 1. After these operations they tell each other from classical communication with massage m_A (m_B). Now, Alice and Bob perform Bell measurement on each pair of the two-particle series (S'_{A1}, S_{B2}) and (S'_{B1}, S_{A2}), respectively. Their measurement outcomes are denoted by $r^a_1, \ldots, r^a_n$ and $r^b_1, \ldots, r^b_n$, which are encoded by the information series $C_A = c^a_1, \ldots, c^a_{2n}$ and $C_B = c^b_1, \ldots, c^b_{2n}$, respectively. Here, $c^a_{2j-1} = r^a_{j,1} \oplus j^a_1$, $c^a_{2j} = r^a_{j,2} \oplus j^a_2$, $c^b_{2j-1} = r^b_{j,1} \oplus j^b_1$, $c^b_{2j} = r^b_{j,2} \oplus j^b_2$, $r^a_j = r^a_{j,1} r^a_{j,2}$, $r^b_j = r^b_{j,1} r^b_{j,2}$, and i represents the ith set of the EPR pair, as shown in Figure 1.

S5. This step is used to against dispute with the help of a classical semi-honest center, which is named as "Against the dispute" step in Figure 2. In detail, Alice sends the ordered messages $\{Alice, \mathrm{Ep}_2(\mathrm{Ep}_1(\mathrm{Identity}_A)_{K_S}, \mathrm{Ep}_1(C_A)_{K_B})_{K_{AS}}\}$ to a classical semi-honest center. Here, Alice denotes the name, and $\mathrm{Ep}_1(\mathrm{Identity_A})_{K_S}$ denotes the encrypted unique identity of Alice using the public key of the classical semi-honesty center, $\mathrm{Ep}_1(C_A)_{K_B}$ denotes the encrypted measurement results using the public key of Bob. These two ciphertexts are re-encrypted using a symmetric system with secret key K_{AS} shared by Alice and the classical semi-honest center. Bob sends the ordered messages $\{Bob, \mathrm{Ep}_2(\mathrm{Ep}_1(\mathrm{Identity}_B)_{K_S}, \mathrm{Ep}_1(C_B)_{K_A})_{K_{BS}}\}$ to the same classical semi-honest center.

S6. This step is used to compare the messages with the help of a classical semi-honest center, which is named as "Comparing the messages" step, as shown in Figure 2. The classical semi-honest center firstly

authorize the identities of the participants by using Identity_A and Identity_B. Then, $\text{Ep}_2(\text{Ep}_1(C_B)_{K_A})_{K_{AS}}$ and $\text{Ep}_2(\text{Ep}_1(C_A)_{K_B})_{K_{BS}}$ are computed by using the shared keys K_{AS} and K_{BS}, respectively. Now, the participants ends the encapsulated message $\text{Ep}_2(\text{Ep}_1(C_B)_{K_A})_{K_{AS}}$ to Alice and $\text{Ep}_2(\text{Ep}_1(C_A)_{K_A})_{K_{BS}}$ to Bob. Finally, Alice computes the exclusive-OR $E_1 = \text{Ep}_1(C_B)_{K_A} \oplus \text{Ep}_1(C_A)_{K_A}$ whereas Bob computes the exclusive-OR $E_2 = \text{Ep}_1(C_A)_{K_B} \oplus \text{Ep}_1(C_B)_{K_B}$. If E_1 and E_2 are consist of only zero bits, the secrets are identical. Otherwise, the secrets are different (i.e., one or more classical bits are 1).

2.3 Correctness

In this QPC protocol, if secrets M_A and M_B satisfy $M_A = M_B$, then by using the entanglement swapping shown in Table 1 it can be easily seen that the measurement results are $C_A = C_B$ in step S4. Moreover, the classical semi-honest center can decrypt Alice's messages $\{Alice, \text{Ep}_2(\text{Ep}_1(\text{Identity}_A)_{K_S}, \text{Ep}_1(C_A)_{K_B})_{K_{AS}}\}$ to obtain Identity_A and $\text{Ep}_1(C_A)_{K_B}$ by using the shared key K_{AS} and secret key K_S^{-1}. Moreover, the classical semi-honest center can decrypt Bob's messages $\{Bob, \text{Ep}_2(\text{Ep}_1(C_B, \text{Identity}_B)_{K_S}, \text{Ep}_1(C_B)_{K_A})_{K_{BS}}\}$ to get Identity_B and $\text{Ep}_1(C_B)_{K_A}$ by using her/his shared key K_{BS} and secret key K_S^{-1}. Now, the classical semi-honest center can encrypt the messages $\text{Ep}_1(C_B)_{K_A}$ and $\text{Ep}_1(C_A)_{K_B}$ to obtain $\text{Ep}_2(\text{Ep}_1(C_B)_{K_A})_{K_{AS}}$ and $\text{Ep}_2(\text{Ep}_1(C_A)_{K_B})_{K_{BS}}$ by using another symmetric encryption; these messages are then sent to Alice and Bob, respectively. Thus, Alice can obtain $\text{Ep}_1(C_B)_{K_A}$ while Bob can obtain $\text{Ep}_1(C_A)_{K_B}$ by decrypting the received cyphertext with their shared key. Furthermore, they can use their public keys to obtain cyphertext $\text{Ep}_1(C_A)_{K_B}$ and $\text{Ep}_1(C_B)_{K_A}$, respectively. Therefore, they can compare their secrets using this protocol.

According to [34, 35], $\eta_E = \frac{q_s}{q_t}$ is used to compare the efficiency, where q_s denotes the compared classical bits, and q_t denotes the qubits generated without considering the decoy qubits. Because two EPR pairs can be used to compare the two bits of secret information between two parties, the qubit efficiency is 50% (i.e., $\eta_E = 50\%$). The proposed QPC protocol requires only a classical semi-honest center and not a quantum semi-honest center [39–53] to complete the task.

3 Security analysis

3.1 Inside attack

In our scheme, the compared secrets may be recovered for an insider (Alice or Bob) iff their final evaluations are zero, which is an essential property for all private comparison schemes. Thus, our scheme exhibits *fairness*.

Dishonest participant—Assume that one participant, e.g., Alice is dishonest and wants to recover Bob's message M_B without foraging the EPRs. First, Alice has to honestly follow from step S1 through S3 in order to avoid star stopping the scheme by Bob. Otherwise, an attack would be detected at step S3 with a nontrivial error probability. Second, in step S4, Alice may perform false Pauli operations σ_j (or no operation that is equivalent to σ_0) on her received particles. After these operations, Bob receives the measurement outcomes C'_B while Alice may forge her measurement outcomes C'_A. Third, because the unique identity (such as the certificate or ID card information) cannot be forged by the assumption, Alice has to use her real identity Identity_A, public keys K_S and K_B, and shared key K_{AS} to complete step S5 with the message $\{Alice, \text{Ep}_2(\text{Ep}_1(\text{Identity}_A)_{K_S}, \text{Ep}_1(C_A)_{K_B})_{K_{AS}}\}$. Finally, even if Alice obtains $\text{Ep}_2(\text{Ep}_1(C_B)_{K_B})_{K_{AS}}$ from the classical semi-honest center, she cannot obtain the original measurement outcomes C_B or the secret M_B. This is because there are four possible measurement outcomes for each measurement under the Bell basis. Thus, the measurement outcomes are random for each Alice's Pauli operation σ_j. Alice cannot recover the Pauli operation σ_j from the measurement outcomes. Based on the explanation above, if one participant wants to recover the other's secret, he/she may choose a random message of length n to complete this scheme honestly. The success probability in this case is only $1/2^n$. This is equivalent to attacking using the random guesses. Thus, our scheme is secure for the dishonest insider attacks. Evidently, the right result can be derived from honest operations.

By contrast, Alice may be dishonest when implementing this scheme by forging the EPR. Specially, assume that Alice uses single particles in the state $\alpha|0\rangle + \beta|1\rangle$ to replace her EPR pairs in step S1. Steps S2 and S3 are performed honestly. Thus, Alice can avoid detection. Now, Alice has only one particle in hand and she may avoid detection by not performing the measurement until Bob announces the completion of measurement. Note that

$$\frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle)(\alpha|0\rangle + \beta|1\rangle) = \frac{1}{\sqrt{2}}[\alpha|0\rangle|00\rangle \pm \beta|1\rangle|11\rangle + \beta|0\rangle|01\rangle \pm \alpha|1\rangle|10\rangle], \tag{4}$$

$$\frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle)(\alpha|0\rangle + \beta|1\rangle) = \frac{1}{\sqrt{2}}[\alpha|0\rangle|10\rangle \pm \beta|1\rangle|01\rangle + \beta|0\rangle|11\rangle \pm \alpha|1\rangle|00\rangle]. \tag{5}$$

Thus, by using the Bell basis, four different measurement outcomes can be obtained with equal probability. This means that Bob's measurement outcomes are random in terms of Alice's Pauli operations even if Alice forges her EPRs. The followed analysis is easy.

Dishonest classical center—Assume that the classical center has been overpowered by an attacker, thus he/she can falsely recover Alice's or Bob's message. In our scheme, the attacker can only receive Alice's message $\{Alice, \mathrm{Ep}_2(\mathrm{Ep}_1(\mathrm{Identity}_A)_{K_S}, \mathrm{Ep}_1(C_A)_{K_B})_{K_{AS}}\}$ and Bob's message $\{Bob, \mathrm{Ep}_2(\mathrm{Ep}_1(C_B, \mathrm{Identity}_B)_{K_S}, \mathrm{Ep}_1(C_B)_{K_A})_{K_{BS}}\}$. Thus by using keys K_S^{-1}, K_{AS} and K_{BS}, the attacker can recover $\mathrm{Identity}_A$, $\mathrm{Identity}_B$, $\mathrm{Ep}_1(C_A)_{K_B}$ and $\mathrm{Ep}_1(C_B)_{K_A}$. The identity information $\mathrm{Identity}_A$ and $\mathrm{Identity}_B$ are trivial if the classical center has been captured by attacker. Moreover, without secret keys K_A^{-1} and K_B^{-1}, dishonest classical center cannot obtained measurement outcomes C_A and C_B. Hence, he/she can recover the secret M_A or M_B. Furthermore, because the classical center can only obtain $\mathrm{Ep}_1(C_B)_{K_A}$ from Bob, and $\mathrm{Ep}_1(C_A)_{K_B}$ from Alice, he/she cannot compare their messages with $\mathrm{Ep}_1(\mathrm{Ep}_1(\cdot)_{K_A})_{K_B} \neq \mathrm{Ep}_1(\mathrm{Ep}_1(\cdot)_{K_B})_{K_A}$. These encrypted messages may be used to solve the disagreement between Alice and Bob.

Conspiracy attacking—Assume that one participant, e.g., Alice and the classical center are conspiring to recover Bob's message. First, by performing the first three steps, S1–S3, correctly, Alice can avoid the stopping of the scheme by Bob. If Alice forges her Pauli operations in step S4, she obtains fake measurement outcomes C'_A, moreover, Bob can also obtain fake measurement outcomes C'_B. The classical center obtains Bob's identity information $\mathrm{Identity}_B$ and encrypted measurement outcomes $\mathrm{Ep}_1(C'_B)_{K_A}$. By cooperating with each other, they can decrypt $\mathrm{Ep}_1(C'_B)_{K_A}$ and obtain C'_B, which is useless for recovering Bob's secret M_B. Similarly, if Alice forges her EPRs, they can jointly obtain random measurement outcomes C'_B, which are useless.

Dispute—If two participants disagree regarding their comparison results, the classical semi-honest center first authorizes their identities by using $\mathrm{Identity}_A$ and $\mathrm{Identity}_B$. Then, the participants can announce their messages $\{\mathrm{Ep}_1(C_A)_{K_B}, \mathrm{Identity}_A\}$ and $\{\mathrm{Ep}_1(C_B)_{K_A}, \mathrm{Identity}_B\}$. They can obtain the final judgement by using their private keys. However, there is an issue that if one participant wants to cheat the other participant using a forged message, they can complete all steps. All of them may obtain an incorrect result and the dishonest participant can avoid disagreement. This is also unavoidable for all privacy comparison schemes.

3.2 Entangle-measuring attack

Assume that Eve wants to retrieve useful information from the transmitted qubit sequences by performing entangle-measuring attack. She first prepares ancillary qubits $L = \{|L_1\rangle, |L_2\rangle, \ldots, |L_{2n}\rangle\}$ and then entangles them into the transmitted sequences through an appropriate unitary operation U_E. However, any nontrivial operations on decoy qubits for Eve will lead to different results. Take $\mathcal{D} = \{|\pm i\rangle := \frac{1}{\sqrt{2}}(|0\rangle \pm i|1\rangle),\ |\pm\rangle := \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)\}$ as an example. Here, the entangled operation is defined by

$$U_E|\pm i\rangle|L_i\rangle = \frac{1}{2}[|+i\rangle(a|e_{00}\rangle + b|e_{01}\rangle \pm c|e_{10}\rangle \pm d|e_{11}\rangle) + |-i\rangle(a|e_{00}\rangle - b|e_{01}\rangle \pm c|e_{10}\rangle \mp d|e_{11}\rangle), \tag{6}$$

$$U_E|\pm\rangle|L_i\rangle = \frac{1}{2}[|+\rangle(a|e_{00}\rangle + b|e_{01}\rangle \pm c|e_{10}\rangle \pm d|e_{11}\rangle) + |-\rangle(a|e_{00}\rangle - b|e_{01}\rangle \pm c|e_{10}\rangle \mp d|e_{11}\rangle). \tag{7}$$

Here, $|L_i\rangle$ is an initial state of Eve's ancillary qubit, and $|e_{00}\rangle$, $|e_{01}\rangle$, $|e_{10}\rangle$ and $|e_{11}\rangle$ are four distinguishable quantum states, where the coefficients satisfy $|a^2| + |b^2| = |c^2| + |d^2| = 1$. If the decoy photon is $|\pm i\rangle$ or $|\pm\rangle$, Eve has to let $(a|e_{00}\rangle + b|e_{01}\rangle \pm c|e_{10}\rangle \pm d|e_{11}\rangle) = (a|e_{00}\rangle - b|e_{01}\rangle \pm c|e_{10}\rangle \mp d|e_{11}\rangle) = 0|0\rangle$ to pass through the eavesdropping check. If these situations are all conformed, we have $a = b = c = d = 0$, which is impossible. Thus, Eve's attack will be successfully detected during the public discussion.

Generally, to successfully detect an attacker in this case, the participants should choose different basis states from at least two different bases to generate the decoy state set $\mathcal{D}$.

Of course, if a dishonest participant wants to disturb their scheme, this is easy to complete by using incorrect Pauli operations or forging EPRs with right decoy photons. However, this attack is meaningless for them because the same goal may be completed by no reply of the dishonest participant. The secret information remains secure under this case.

3.3 Disturb-attack

This attack is designed to disturb the progress without being detected. In the following, we will evaluate the success probability for Eve if he/she only takes special quantum operations on the transmitted qubits.

If $\mathcal{D} = \{|0\rangle, |1\rangle, |\pm\rangle\}$ is used as the decoy state set, Eve may implement special operations on the transmitted qubits to disturb the progress. Note that the computation basis $|0\rangle$, $|1\rangle$ is unchanged under the Pauli matrix σ_3. Thus, if Eve performs $\sigma = \mathrm{diag}(1, \pm i)$ on the transmitted qubits originating from Alice or Bob, she can obtain the following qubit set $\{|0\rangle, |1\rangle, |\pm i\rangle\}$, which can be detected with a probability of $1/2 \times 1/2 = 1/4$ per qubit. If the attack on the decoy state is not detected fortunately, we need to determine the effect on the transmitted particles of EPRs. From Table 1, it can be seen that Eve has performed this attacking operation on the transmitted qubits, two legitimate parties may obtain different measurement results from the same input states or they may obtain the same result for different input states. It means that an attacker may affect the correctness of this comparison scheme.

Similarly, if $\mathcal{D} = \{|\pm i\rangle, |\pm\rangle\}$ is used, in general, Eve can obtain

$$\frac{1}{2}((a \mp a^* + (b \pm b^*)i)|+i\rangle + (a \pm a^* - (b \mp b^*)i)|-i\rangle), \tag{8}$$

$$\frac{1}{2}((a \mp a^* + b \pm b^*)|+\rangle + (a \pm a^* - b \pm b^*)|-\rangle) \tag{9}$$

by using a general qubit operation

$$\begin{pmatrix} a & b \\ b^* & -a^* \end{pmatrix}. \tag{10}$$

Under the assumption of the uniform distribution of decoy states, the total error probability is

$$\begin{aligned} P_e =& \frac{1}{4} \times \frac{1}{4}(4(\mathrm{Re}(a) + \mathrm{Im}(b))^2) + \frac{1}{4} \times \frac{1}{4}(4(\mathrm{Re}(a) - \mathrm{Im}(b))^2) \\ &+ \frac{1}{4} \times \frac{1}{4}(4(\mathrm{Re}(a)^2 + \mathrm{Im}(b)^2)) + \frac{1}{4} \times \frac{1}{4}(4(\mathrm{Im}(a)^2 + \mathrm{Re}(b)^2)) \\ =& \frac{1}{4} + \frac{1}{2}a^2 + \frac{1}{2}\mathrm{Im}(b)^2 + \frac{1}{2}a\mathrm{Im}(b) \geqslant \frac{1}{4} \end{aligned} \tag{11}$$

from general assumptions $\mathrm{Im}(a) = 0$ and $a^2 + |b|^2 = 1$, as shown in Figure 3. Here, Re and Im denote the real and imagine parts respectively. From this figure, P_e is monotonously increasing along a^2 and $\mathrm{Im}(b)$. The lower bound is achieved when $a = \mathrm{Im}(b) = 0$, i.e., $b = 1$. Thus, this decoy state set is similar to the first case $\mathcal{D} = \{|0\rangle, |1\rangle, |\pm\rangle\}$.

Generally, Eve can perform one unitary (not-identity) operation such that any state of one basis is unchanged up to a global phase (in geometry she can choose another basis such that each initial state and its changed state have the same inner product). Hence, to improve the security against this attack, legitimate parties need to generate a larger decoy set with more than two different quantum bases.

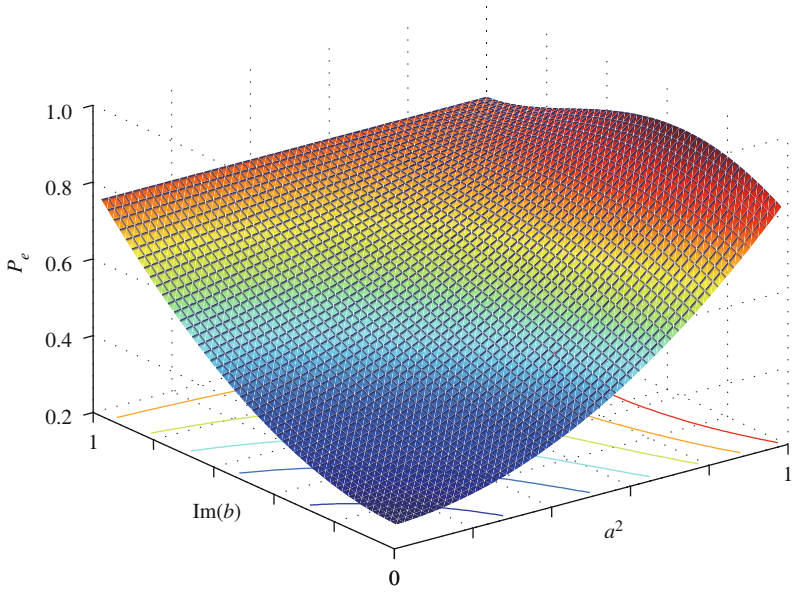

Figure 3 The total error probability P_e. Here we assume $a \in R$ and $a^2 + |b|^2 = 1$.

3.4 Other attacks

Trojan horse attack. There are two kinds of Trojan horse attacks that have been widely discussed in quantum photonic protocols, i.e., the invisible photon eavesdropping (IPE) attack [43–45] and the delay-photon attack [46, 47]. In general, the first one can be prevented by filtering the invisible photons using wavelength optical device. The second attack can be prevented by using a photon number splitters. Thus, the delay-photon attack is equivalent to an unreasonably high rate of the multi-photon signal. However, these quantum operations can be completed within the decoy photons. Therefore, the detection of the Trojan horse attack does not reduce the transmission efficiency.

Intercept-resend attack. In our QPC protocol, many random chosen decoy qubits are hidden at random positions of the EPR sequences S_{A2} and S_{B2}. Eve cannot obtain the preparation bases of these decoy states and the position information before her announcement in step S3. Thus, if a wrong basis is used to measure and resend these particles by Eve, an error will be introduced in the detection step with a nontrivial error probability of $1/|\mathcal{D}|$. Hence, the error ratio from the detection measurement is $1-(1/|\mathcal{D}|)^k \approx 1$ for $k \to \infty$ and $|\mathcal{D}| > 1$, where k is the total number of decoy states.

If a classical attacker wants to recover the secrets M_A and M_B, he/she can obtain the transmitted classical messages

$$\{Alice, \mathrm{Ep}_2(\mathrm{Ep}_1(C_A, \mathrm{Identity}_A)_{K_S}, \mathrm{Ep}_1(C_A)_{K_B})_{K_{AS}}\}$$

and

$$\{Bob, \mathrm{Ep}_2(\mathrm{Ep}_1(C_B, \mathrm{Identity}_B)_{K_S}, \mathrm{Ep}_1(C_B)_{K_A})_{K_{BS}}\}.$$

Because K_{AS} and K_{BS} are secret keys, the classical attacker can not decrypt these ciphertexts. Even if these secret keys are revealed to the attacker, he/she can obtain $\mathrm{Ep}_1(\mathrm{Identity}_A)_{K_S}$, $\mathrm{Ep}_1(C_A)_{K_B}$, $\mathrm{Ep}_1(\mathrm{Identity}_B)_{K_S}$, and $\mathrm{Ep}_1(C_B)_{K_A}$. Because the attacker does not know private keys K_S^{-1}, K_A^{-1} and K_B^{-1}, he/she cannot obtain the measurement results C_A and C_B. Thus, the attacker cannot compare their secrets or recover the secrets of Alice and Bob.

4 Discussion and conclusion

The proposed QPC protocol can be easily extended with general EPR pairs $|\varphi(0,0)\rangle$ and single qudit state set $\mathcal{D}$, and qudit operations $U(j)$. In fact, using the d-dimensional representation (dit) of the secrets

$M_A(M_B)$ and general Bell measurement basis $\{|\varphi(s,t)\rangle\}_{s,t=0}^{d-1}$, the secrets can be encoded in the first dit of each measurement outcome t_1t_2 from (2). Thus, only the first dit subseries can be used to encode information series $C_A = c_1^a, \ldots, c_n^a$ and $C_B = c_1^b, \ldots, c_n^b$ respectively, where $c_j^a = r_j^a + j^a \bmod d$ and $c_j^b = d - r_j^b - j^b \bmod d$ are used in step S4 of the generalized scheme. The following steps are easily extended. The main differences from the qubit case are the information transformation in step S4 and the different comparison (using minus operation) in step S6. Because two dits may be exchanged using one qudit' transmission, the comparison efficiency is $\frac{1}{2}\log_2 d$ bits/qudit. The proof of the security is similar to the qubit case. In practice, the qudit scheme is more difficult to implement even if its efficiency is higher. There may be a trade-off with the experimental equipment.

The efficiency of the theoretical scheme in Section 2 may be reduced if the experimental conditions are considered. In fact, the ideal EPR pair may be become a mixed state or a less-entangled state with the effect of various noises. Thus, the ideal detection error ratio should be ensured by recovering the maximally entangled EPR pairs from mixed states or less-entangled states. Different methods have been explored for addressing these problems. One is the entanglement purification [58] that can be used to distill the high quality mixed state from the low quality mixed states [59–61]. The other is the entanglement concentration [62] in which the maximally entangled state may be probabilistically recovered from the less-entangled state [63–70]. If photons are used in our scheme and are lost, the quantum state amplification should be considered to increase the probability of the single photon state [71–74].

To sum up, based on the quantum dense coding of two EPR pairs, we show that two legitimate parties can successfully compare the classical secrets with a classical semi-honest center. From the entanglement swapping of the EPR pairs, the secrets are hidden within the random measurement results. Thus the followed transmission scheme may provide necessary security for internal or external attackers. Furthermore, the qubit scheme is extended to general qudit case. In this case, the encryption is different from the qubit case because of the different entanglement swapping. The new scheme is more efficient than the qubit case with the same security while it is more difficult to implement in experiment. Thus one may trade off them in practice. Compared with previous QPC schemes [34, 35], two participants have no shared secrets. Different from the QPC with triplet entanglements [37], W state [38, 43] or χ state [41, 42], our scheme is based on Bell states. In our schemes, the semi-honest center has no information about the secret and the comparison result [37]. In recent protocol [38, 39], two participants and the trust center need to prepare Bell states, and the private comparison task is fulfilled by utilizing the entanglement swapping between Bell states of the participants and semi-honest center. This scheme has a loophole that the trust center could launch the measurement attack to obtain all secrets without being detected [40]. Since the quantum part is uninvolved the semi-honest center, our schemes can avoid this attack. Compared with the QPC based on the quantum operation discrimination [43] or the combination of decoherence-free states and error-correcting code [45], our schemes are based on the entanglement swapping of Bell states. Different from previous quantum trust center [24–32] or quantum semi-honest center [43–47], our schemes take use of the classical semi-honest center, which is more flexible in implementation. These schemes can be used to justify their disagreements by the semi-honest center. Of course, since we have used the classical asymmetric encryptions, the powerful attacker may obtain the measurement outcomes C_A and C_B if these classical cryptography systems are cracked. Thus, they know the comparison result. However, from the randomness of the C_A and C_B in terms of the secrets M_A and M_B, the powerful attacker cannot know the secret messages. Under this assumptions, our schemes are secure in terms of the secrets.

Acknowledgements This work was supported by National Natural Science Foundation of China (Grant Nos. 61303039, 61373131), Natural Science Foundation of Shandong Province (Grant No. ZR2015FL024), Fundamental Research Funds for the Central Universities (Grant No. 2682014CX095), PAPD and CICAEET Funds, Open Foundation of Jiangsu Engineering Center of Network Monitoring (Nanjing University of Information Science & Technology) (Grant No. KJR1502), Open Foundation of China-USA Computer Science Center (Grant No. KJR16012), and Science Foundation Ireland (SFI) under the International Strategic Cooperation Award (Grant No. SFI/13/ISCA/2845).

Conflict of interest The authors declare that they have no conflict of interest.

References

1 Fu Z J, Sun X M, Liu Q, et al. Achieving efficient cloud search services: multi-keyword ranked search over encrypted cloud data supporting parallel computing. IEICE Trans Commun, 2015, 98: 190–200
2 Li J, Li X L, Yang B, et al. Segmentation-based image copy-move forgery detection scheme. IEEE Trans Inform Forens Secur, 2015, 10: 507–518
3 Ren Y J, Shen J, Wang J, et al. Mutual verifiable provable data auditing in public cloud storage. J Internet Technol, 2015, 16: 317–324
4 Xia Z H, Wang X H, Sun X M, et al. A secure and dynamic multi-keyword ranked search scheme over encrypted cloud data. IEEE Trans Parall Distrib Syst, 2015, 27: 340–352
5 Bennett C H, Brassard G. Quantum cryptography: public key distribution and coin tossing. In: Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, 1984. 175–179
6 Zhou C, Bao W S, Fu X Q. Decoy-state quantum key distribution for the heralded pair coherent state photon source with intensity fluctuations. Sci China Inf Sci, 2010, 53: 2485–2494
7 Qian X D, He G Q, Zeng G H. Realization of error correction and reconciliation of continuous quantum key distribution in detail. Sci China Ser-F: Inf Sci, 2009, 52: 1598–1604
8 Bennett C H, Brassard G, Crepeau C, et al. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. Phys Rev Lett, 1993, 70: 1895–1899
9 Bouwmeester D, Pan J W, Mattle K, et al. Experimental quantum teleportation. Nature, 1997, 390: 575–579
10 Furusawa A, Søensen J L, Braunstein S L, et al. Unconditional quantum teleportation. Science, 1998, 282: 706–709
11 Bennett C H, DiVincenzo D P, Shor P Q, et al. Remote state preparation. Phys Rev Lett, 2001, 87: 077902
12 Luo M X, Deng Y, Chen X B, et al. The faithful remote preparation of general quantum states. Quantum Inform Process, 2013, 12: 279–294
13 Hillery M, Buzek V, Berthiaume A. Quantum secret sharing. Phys Rev A, 1999, 59: 1829–1834
14 Cleve R, Gottesman D, Lo H K. How to share a quantum secret. Phys Rev Lett, 1999, 83: 648–651
15 Guo G P, Guo G C. Quantum secret sharing without entanglement. Phys Lett A, 2003, 310: 247–251
16 Xiao L, Long G L, Deng F G, et al. Efficient multiparty quantum-secret-sharing schemes. Phys Rev A, 2004, 69: 052307
17 Qin S J, Gao F, Wen Q Y, et al. Improving the security of multiparty quantum secret sharing against an attack with a fake signal. Phys Lett A, 2006, 357: 101–103
18 Xu J, Chen H W, Liu W J, et al. Selection of unitary operations in quantum secret sharing without entanglement. Sci China Inf Sci, 2011, 54: 1837–1842
19 Wang T Y, Wen Q Y. Security of a kind of quantum secret sharing with single photons. Quantum Inform Comput, 2011, 11: 434–443
20 Boström K, Felbinger T. Deterministic secure direct communication using entanglement. Phys Rev Lett, 2002, 89: 187902
21 Deng F G, Long G L, Liu X S. Two-step quantum direct communication protocol using the Einstein-Podolsky-Rosen pair block. Phys Rev A, 2003, 68: 042317
22 Wang C, Deng F-G, Li Y-S, et al. Quantum secure direct communication with high-dimension quantum superdense coding. Phys Rev A, 2005, 71: 044305
23 Lin S, Wen Q Y, Gao F, et al. Quantum secure direct communication with χ-type entangled states. Phys Rev A, 2008, 78: 064304
24 Liu Z H, Chen H W, Liu W J, et al. Deterministic secure quantum communication without unitary operation based on highdimensional entanglement swapping. Sci China Inf Sci, 2012, 55: 360–367
25 Zheng C, Long G F. Quantum secure direct dialogue using Einstein-Podolsky-Rosen pairs. Sci China Phys Mech Astro, 2014, 57: 1238–1243
26 Zou X F, Qiu D W. Three-step semiquantum secure direct communication protocol. Sci China Phys Mech Astro, 2014, 57: 1696–1702
27 Qu Z G, Chen X B, Zhou X J, et al. Novel quantum steganography with large payload. Opt Commun, 2010, 283: 4782–4786
28 Qu Z G, Chen X B, Luo M X, et al. A large payload of novel quantum steganography with χ-type entangled state. Opt Commun, 2011, 284: 2075–2082
29 Xu S J, Chen X B, Niu X X, et al. High-efficiency quantum steganography based on the tensor product of Bell states. Sci China Phys Mech Astro, 2013, 56: 1745–1754
30 Yao A C. Protocols for secure computations. In: Proceedings of the 23rd Annual Symposium on Foundations of Computer Science, Chicago, 1982. 160–164
31 Yao A C. How to generate and exchange secrets. In: Proceedings of the 27th Annual Symposium on Foundations of Computer Science, Toronto, 1986. 162–167
32 Boudot F, Schoenmakers B, Traore J. A fair and efficient solution to the socialist millionaires problem. Discret Appl Math, 2001, 111: 23–36
33 Lo H K. Insecurity of quantum secure computations. Phys Rev A, 1997, 56: 1154–1162

34 Yang Y G, Wen Q Y. An efficient two-party quantum private comparison protocol with decoy photons and two-photon entanglement. J Phys A-Math Theor, 2009, 42: 055305
35 Yang Y G, Cao W F, Wen Q Y. Secure quantum private comparison. Phys Scr, 2009, 80: 065002
36 Lin J, Tseng H Y, Hwang T. Intercept-resend attacks on Chen et al.'s quantum private comparison protocol and the improvements. Opt Commun, 2011, 284: 2412–2414
37 Chen X B, Xu G, Niu X X, et al. An efficient protocol for the private comparison of equal information based on the triplet entangled state and single-particle measurement. Opt Commun, 2010, 283: 1561–1565
38 Liu W J, Liu C, Wang H B, et al. Secure quantum private comparison of equality based on asymmetric W state. Int J Theor Phys, 2014, 53: 1804–1813
39 Tseng H Y, Lin J, Hwang T. New quantum private comparison protocol using EPR pairs. Quantum Inf Proc, 2012, 11: 373–384
40 Liu W J, Liu C, Chen H W, et al. Cryptanalysis and improvement of quantum private comparison protocol based on bell entangled states. Commun Theor Phys, 2014, 62: 210–214
41 Liu W, Wang Y B, Jiang Z T, et al. A protocol for the quantum private comparison of equality with χ-type state. Int J Theor Phys, 2012, 51: 69–77
42 Xu G A, Chen X B, Wei Z H, et al. An efficient protocol for the quantum private comparison of equality with a four-qubit cluster state. Int J Quantum Inf, 2012, 10: 1250045
43 Liu W, Wang Y B, Jiang Z T. An efficient protocol for the quantum private comparison of equality with W state. Opt Commun, 2011, 284: 3160–3163
44 Liu B, Gao F, Jia H Y, et al. Efficient quantum private comparison employing single photons and collective detection. Quantum Inf Proc, 2013, 12: 887–897
45 Li Y B, Qin S J, Yuan Z, et al. Quantum private comparison against decoherence noise. Quantum Inf Proc, 2013, 12: 2191–2205
46 Zhang W W, Zhang K J. Cryptanalysis and improvement of the quantum private comparison protocol with semi-honest third party. Quantum Inf Proc, 2013, 12: 1981–1990
47 Chen X B, Su Y, Niu X X, et al. Efficient and feasible quantum private comparison of equality against the collective amplitude damping noise. Quantum Inf Proc, 2013, 12: 2871–2875
48 Zukowski M, Zeilinger A, Horne M A, et al. Event-ready-detectors Bell experiment via entanglement swapping. Phys Rev Lett, 1993, 71: 4287–4290
49 Pan J W, Bouwmeester D, Weinfurter H, et al. Experimental entanglement swapping: entangling photons that never interacted. Phys Rev Lett, 1998, 80: 3891–3894
50 Barencoa A, Ekerta A K. Dense coding based on quantum entanglement. J Mod Opt, 1995, 42: 1253–1259
51 Yeo Y, Chua W K. Teleportation and dense coding with genuine multipartite entanglement. Phys Rev Lett, 2006, 96: 060502
52 Shadman Z, Kampermann H, Macchiavello C, et al. Optimal super dense coding over noisy quantum channels. New J Phys, 2010, 12: 073042
53 Cai Q Y. Eavesdropping on the two-way quantum communication protocols with invisible photons. Phys Lett A, 2006, 351: 23–25
54 Deng F G, Li X H, Zhou H Y, et al. Improving the security of multiparty quantum secret sharing against Trojan horse attack. Phys Rev A, 2006, 73: 049901
55 Qin S J, Wen Q Y, Zhu F C. Cryptanalysis of multiparty quantum secret sharing of quantum state using entangled states. Chin Phys Lett, 2008, 25: 3551–3554
56 Li X H, Deng F G, Zhou H Y. Improving the security of secure direct communication based on the secret transmitting order of particles. Phys Rev A, 2006, 74: 054302
57 Yang C W, Hwang T, Luo Y P. Enhancement on quantum blind signature based on two-state vector formalism. Quantum Inf Proc, 2013, 12: 109–117
58 Bennett C H, Brassard G, Popescu S, et al. Purification of noisy entanglement and faithful teleportation via noisy channels. Phys Rev Lett, 1996, 76: 722–725
59 Sheng Y B, Zhou L. Deterministic entanglement distillation for secure double-server blind quantum computation. Sci Rep, 2015, 5: 7815
60 Sheng Y B, Zhou L. Deterministic polarization entanglement purification using time-bin entanglement. Laser Phys Lett, 2014, 11: 085203
61 Sheng Y B, Zhou L, Long G L. Hybrid entanglement purification for quantum repeaters. Phys Rev A, 2013, 88: 022302
62 Bennett C H, Bernstein H J, Popescu S, et al. Concentrating partial entanglement by local operations. Phys Rev A, 1996, 53: 2046–2052
63 Zhao Z, Yang T, Chen Y A, et al. Experimental realization of entanglement concentration and a quantum repeater. Phys Rev Lett, 2003, 90: 207901
64 Sheng Y B, Zhou L, Zhao S M, et al. Efficient single-photon-assisted entanglement concentration for partially entangled photon pairs. Phys Rev A, 2012, 85: 012307
65 Ren B C, Du F F, Deng F G. Hyperentanglement concentration for two-photon four-qubit systems with linear optics. Phys Rev A, 2013, 88: 012302
66 Zhao Z, Pan J W, Zhan M S. Practical scheme for entanglement concentration. Phys Rev A, 2001, 64: 014301
67 Sheng Y B, Deng F G, Zhou H Y. Nonlocal entanglement concentration scheme for partially entangled multipartite

systems with nonlinear optics. Phys Rev A, 2008, 77: 062325
68 Shi B S, Jiang Y K, Guo G C. Optimal entanglement purification via entanglement swapping. Phys Rev A, 2000, 62: 054301
69 Luo M X, Chen X B, Yang Y X, et al. Hyperentanglement concentration for n-photon $2n$-qubit systems with linear optics. J Opt Soc Amer B-Opt Phys, 2014, 31: 67–74
70 Luo M X, Li H R, Wang X. Efficient atomic and photonic multipartite W state concentration via photonic faraday rotation. Eur Phys J D, 2014, 68: 190
71 Chrzanowski H M, Walk N, Assad S M, et al. Measurement-based noiseless linear amplification for quantum communication. Nat Photon, 2014, 8: 333–338
72 Eleftheriadou E, Barnett S M, Jeffers J. Quantum optical state comparison amplifier. Phys Rev Lett, 2013, 111: 213601
73 Kocsis S, Xiang G Y, Ralph T C, et al. Heralded noiseless amplification of a photon polarization qubit. Nat Phys, 2013, 9: 23–28
74 Zhou L, Sheng Y B. Recyclable amplification protocol for the single-photon entangled state. Laser Phys Lett, 2015, 12: 045203