SCIENCE CHINA
Physics, Mechanics & Astronomy

• Article •

September 2013 Vol. 56 No. 9: 1670–1678
doi: 10.1007/s11433-013-5224-0

Robust and efficient quantum private comparison of equality with collective detection over collective-noise channels

HUANG Wei[1,2*], WEN QiaoYan[1], LIU Bin[1], GAO Fei[1] & SUN Ying[3]

[1] *State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing 100876, China;*
[2] *State Key Laboratory of Information Security, Institute of Software, Chinese Academy of Sciences, Beijing 100190, China;*
[3] *Beijing Electronic Science and Technology Institute, Beijing 100070, China*

Received February 5, 2013; accepted April 26, 2013; published online July 23, 2013

We present a protocol for quantum private comparison of equality (QPCE) with the help of a semi-honest third party (TP). Instead of employing the entanglement, we use single photons to achieve the comparison in this protocol. By utilizing collective eavesdropping detection strategy, our protocol has the advantage of higher qubit efficiency and lower cost of implementation. In addition to this protocol, we further introduce three robust versions which can be immune to collective dephasing noise, collective-rotation noise and all types of unitary collective noise, respectively. Finally, we show that our protocols can be secure against the attacks from both the outside eavesdroppers and the inside participants by using the theorems on quantum operation discrimination.

quantum private comparison of equality, collective detection, collective noise

PACS number(s): 03.67.Dd, 03.67.Hk, 03.67.Pp

Citation: Huang W, Wen Q Y, Liu B, et al. Robust and efficient quantum private comparison of equality with collective detection over collective-noise channels. Sci China-Phys Mech Astron, 2013, 56: 1670–1678, doi: 10.1007/s11433-013-5224-0

1 Introduction

Since the first quantum cryptographic protocol (BB84) was proposed by Bennett and Brassard [1], various branches of quantum cryptography have progressed quickly, including quantum key distribution (QKD) [1–9], quantum secure multiparty computation (QSMC) [10–19] and quantum secure direct communication (QSDC) [20–24], and others. The main function is to provide unconditionally secure information exchange basing on the laws of quantum mechanics.

Secure multiparty computing (SMC), which is also termed secure function evaluation, is to compute a function with private input of each party so that in the end only the evaluation result is known and the private inputs are not exposed. The problem for private comparison of equality (PCE) or the socialist millionaire problem, an important branch of SMC, in that two millionaires want to know whether they happen to be equally rich, but neither millionaire wants to simply disclose their wealth, is an extended problem of the problem of the millionaire, presented by Yao [25], in which two millionaires determine who is richer without knowing the others' actual property value. The problem for PCE was well-studied based on classical cryptography [26,27]. However, the security of such protocols relies on the assumption of computational complexity, which cannot withstand the strong ability of quantum computation.

Quantum private comparison of equality (QPCE) is an attractive application of quantum mechanics, whose security does not rely on computational complexity but simply on the laws of quantum mechanics such as Heisenberg uncertainty principle and quantum no-cloning theorem. QPCE allows two participants (Alice and Bob) to determine whether their secrets are equal without leaking any information about

*Corresponding author (email: huangwei096505@yahoo.cn)

their secrets. In fact, it has been noted that the equality function cannot be securely evaluated with a two-party scenario [28,29], even by using quantum means. Therefore, some additional assumptions (such as a semi-honest third party) should be considered to reach the goal of private comparison. The first QPCE protocol was designed by Yang et al. [30]. Much research focus has been given to QPCE and many correlative protocols have been proposed [30–38]. Summarily, the QPCE protocols presented previously have the following principles.

• A third party (TP) who is at least semi-honest is required to help the two parties (Alice and Bob) accomplish the comparison. A semi-honest TP is a party who always follows the procedure of the protocol. He/she will take a record of all intermediate computations, and will not be corrupted by an outside eavesdropper. However, TP might try to steal the information from the record.

• TP will know the positions of different bit value in the compared information, but he/she will not be able to know the actual bit value of the information.

• All outsiders and the two players should only know the result of the comparison (that is, identical or different), but not the different positions of the information.

Recently, Yang et al. [39] suggested that the above assumption regarding semi-honest TP is unreasonable. They advised that the first one of the above three principles should be replaced by the implementation of a semi-honest TP. This TP cannot be corrupted by others and cannot learn any valuable information about the secrets through active and passive attacks.

Herein we present an efficient QPCE protocol with single photons and collective detection. Collective detection [13,24,40,42] is an efficient (eavesdropping) detection strategy in which eavesdropping detection needs to be taken only once after the whole process of the transmission of the particle. Such detection strategy not only improves the qubit efficiency of the protocol but also reduces the expense of realization as the participants (except for a center) need not to be equipped with the expensive quantum devices, such as the qubit generating machine or qubit measuring machine. With the help of a semi-honest third party (TP), the two distrustful participants (Alice and Bob) in our protocol can securely compare the equivalence of their secrets (X and Y). More importantly, compared with the previous QPCE protocols [30–38], our protocol has the following advantages.

• In most of the previous QPCE protocols [32,35–38], the assumption about TP is that he/she must always follow the procedure of the protocol, he/she will take a record of all intermediate computations, and will not be corrupted by any other one. This assumption seems not to be reasonable for a semi-honest TP since he/she may want to steal the information about the secrets of the participants. In our protocols, the semi-honest TP is assumed to be more powerful, who may misbehave on his/her own but will not conspire with either of the two participants, which is more reasonable. That is to say, the assumption about the TP in our protocol satisfies the principle presented by Yang et al. [39].

• By utilizing collective eavesdropping detection strategy, the cost of realizing this protocol is reduced since the two distrustful participants in this protocol need not to be equipped with qubit generating device or quantum measuring device.

• The qubit efficiency of our protocol is higher than many of the previous QPCE protocols [30–32,34,36–38]. That is to say, to compare the same number of classical bits, our protocol need to use less qubits.

• Compared with the QPCE protocols [30,31,33] which utilize hash function to ensure their security, the security of our protocol is only guaranteed by the laws of quantum mechanics.

Currently, almost all the previous QPCE protocols [30–38] have been designed under ideal conditions, hence they cannot withstand channel noise. However in practice, the qubits transmitted in quantum channel often interact with the environment uncontrollably and noises are then introduced in the eavesdropping detection unexpectedly. At present, it is thought that the the noise in a quantum channel is collective [41–47], which indicates the fluctuation of noise is slow in time. Since designing protocols in noisy channel is one of most important elements in quantum cryptography at present, we also present three robust versions of the proposed protocol which can be immune to collective-dephasing noise, collective-rotation noise and all types of unitary collective noise, respectively.

Herein we describe the suggested QPCE protocol and then make a comparison to some of the previously suggested protocols. Testing is then given to determine the robustness of three versions of the protocol under collective noise conditions. Lastly, the security of the system is determined based on quantum operation discrimination.

2 The QPCE protocol with single photons and collective detection

2.1 The proposed QPCE protocol

To ensure the security of particle transmission, we take advantage of the technique of block transmission of particles which has been proposed firstly by Long et al. [20]. The steps of our QPCE protocol in the ideal quantum channel can be described as follows (see also Figure 1).

1. With the help of TP, Alice and Bob generate an n-bit secret key K, by executing the three-party QKD protocol with a dishonest center presented [40]. After that, Alice and Bob calculate the bit strings $X'=X\oplus K$ and $Y'=Y\oplus K$, where X is the secret of Alice and Y is the secret of Bob.

2. TP prepares a sequence of $(n+\delta)$ single photons which are randomly in one of the four states $\{|0\rangle, |1\rangle, |s\rangle, |t\rangle\}$ (denoted as sequence S) and sends the sequence to Alice. Here, $|0\rangle$ and $|1\rangle$ are the up and down eigenstates of the σ_z, $|s\rangle=\frac{1}{2}(|0\rangle-\mathrm{i}|1\rangle)$ and $|t\rangle=\frac{1}{2}(|1\rangle-\mathrm{i}|0\rangle)$. It can be verified that $\{|0\rangle, |1\rangle\}$ and $\{|s\rangle, |t\rangle\}$ form two nonorthogonal unbiased bases, which

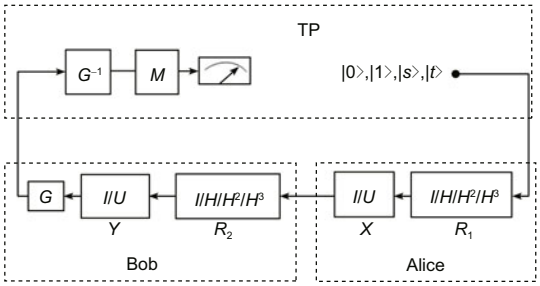

Figure 1 Process of our QPCE protocol in the ideal channel, where M represents one of the four unitary operations $\{I, H^{-1}, U^{-1}, H\}$ and G^{-1} represents the reverse of the permutation function G. TP provides the service for preparing and measuring the states in the sequence. For simplicity, all classical communications are omitted.

means $|\langle 0|1\rangle|=|\langle s|t\rangle|=0$, $|\langle s|0\rangle|^2=|\langle s|1\rangle^2=|\langle t|0\rangle|^2=|\langle t|1\rangle|^2=\frac{1}{2}$.

3. Upon receiving S, Alice first generates a random quaternary string of length $(n+\delta)$, which is denoted as controlling string R_1. Then Alice performs a selected unitary operation in $\{I, H, H^2, H^3\}$ on each photon in S according to R_1, which indicates that Alice performs the operation I, H, H^2, H^3 on the i-th state in S if the value of i-th position in R_1 is 0, 1, 2, 3, respectively. After the operations, each photon in sequence S is randomly transformed to a state in $\{|0\rangle, |1\rangle, |s\rangle, |t\rangle\}$. After that, Alice randomly chooses δ states in sequence S as decoy particles and performs encoding unitary operation I (U) on the i-th state in the remaining n photons if the i-th bit in string X' is 0 (1). Finally, Alice sends the new sequence (denoted as S_1) to Bob. Here

$$U = \mathrm{i}H^2 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \qquad I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$
$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & -\mathrm{i} \\ -\mathrm{i} & 1 \end{pmatrix}. \tag{1}$$

The effect of the operations U and H on the states in the two bases can be described as

$$\begin{aligned} U|0\rangle &= |1\rangle, & U|1\rangle &= |0\rangle, \\ U|s\rangle &= |t\rangle, & U|t\rangle &= |s\rangle, \\ H|0\rangle &= |s\rangle, & H|1\rangle &= |t\rangle, \\ H|s\rangle &= -\mathrm{i}|1\rangle, & H|t\rangle &= -\mathrm{i}|0\rangle. \end{aligned} \tag{2}$$

4. When Bob informs that he has received the sequence S_1, Alice announces the positions of the δ decoy particles in S_1. Then Bob also generates a random quaternary string of length $(n+\delta)$, which is denoted as controlling string R_2. After that, Bob utilizes R_2 and his string Y' to process S_1 in the same procedure as Alice does in step 3, in which the decoys particles are the same ones chosen by Alice. At last, Bob shuffles the processed photons in the sequence with a randomly chosen permutation function G and sends the processed sequence (denoted as S_2) back to TP.

5. After the reception of S_2, TP gives Alice and Bob the notification. Then the three participants can check eavesdropping by the following procedure. (a) Bob first declares the correct positions of the decoy particles, then for each of the decoy particle, Alice and Bob announce the corresponding information of R_1, R_2 in a random sequence determined by TP. That is to say, for each one of the decoy particles, TP will randomly choose one from Alice and Bob to announces the corresponding controlling bit first. (b) With the classical information announced by Alice and Bob, TP first performs operation $I/H^{-1}/U^{-1}/H$ on each decoy particle if the sum of its corresponding values in R_1 and R_2 is 0 or 4/1 or 5/2 or 6/3. At last, TP measures each decoy particle with the same basis as he prepares it. If there is no eavesdropping in the procedure of the protocol, the decoy particle should be the same as TP prepares it. Then TP analyzes the security of the protocol with the measurement outcomes, if there is no error, the procedure of the protocol can proceed, otherwise they abort the protocol.

6. After they have confirmed that the processes above is secure, Bob publishes the function G. With the information of G, TP recovers the remaining n photons in sequence S_2 in correct order. Then Alice and Bob announce the corresponding information of R_1, R_2 for the remaining n photons. That is to say, Alice (Bob) publishes the rest n bits of his/her controlling strings R_1 (R_2). With the classical information announced by Alice and Bob, TP first performs operation $I/H^{-1}/U^{-1}/H$ on each of the remaining states if the sum of its corresponding values in R_1 and R_2 is 0 or 4/1 or 5/2 or 6/3. After that, TP measures each of the photons with the same basis as he prepares it. If TP finds a state which is different from its initial state, he publishes that X and Y is not equal. Otherwise, he continues to measure the remaining particles until he finds all the photons are the same as the initial states he prepared and publishes that X is equal to Y.

In this protocol, with the help of a semi-honest TP, Alice and Bob can compare the equivalence of their secrets with single photons. In step 6, TP begins to measure states after both Alice and Bob have announced the remaining n bits of their controlling strings (R_1 and R_2), hence neither of them can know the positions of different bit value in the compared secrets. In other words, if TP announces that X and Y is not equal, they cannot know the positions of different bit value. Moreover, the participants should set up the filter and the beam splitter to prevent the Trojan horse attacks [48,49].

2.2 The comparison between our protocol and some of the previous QPCE protocols

The qubit efficiency is defined as $\eta = n_s/n_q$, where n_s denotes the length of classical secrets compared in the protocol and n_q represents the total number of qubits used in the protocol. It should be noted that the security of quantum cryptographic protocols is based on the error rate analysis with the theories in statistics. Hence the proportion of the detection particles in the transmitted particles should not be small and usually the proportion is set at 50%. As usual, we suppose the propor-

tion of the decoy particles in the transmitted particles is 50% in the following comparison. In our protocol, to compare two secrets of length n, $2n$ photons are used to generate an n-bit key and $2n$ (δ=n) photons are used to comparing the secrets, hence the qubit efficiency of our protocol is $n/(2n+2n)$=25%.

In the first QPCE protocol presented by Yang et al. [30,31], to compare two secrets of length n, TP generate at least $2n$ qubits in EPR pairs and $2n$ decoy qubits, also two participants generate $2n$ decoy qubits. In addition, the two participants generate at least $2l$ qubits to execute a QKD protocol. Hence the qubit efficiency of the protocols [30,31] is $n/(6n + 2l)$ <17%. In the protocol presented elsewhere [32], to compare two secrets of length $4n$, TP generates $8n$ qubits in $2n$ χ-type states for comparison, $8n$ qubits in $2n$ χ-type state for eavesdropping check. Also the two participants generates at least $4n$ qubits to establish two n-bit classical keys with TP. Hence the qubit efficiency of this protocol is $4n/(8n + 8n + 4n)$=20%. In the QPCE protocol presented by Liu et al. [34], to compare two secrets of length n, TP generates $4n$ qubits in n χ-type states and $2n$ decoy qubits, also the participants generates $4n$ qubits to establish two n-bit classical keys. Therefore, the qubit efficiency of this protocol is $n/(4n + 4n + 2n)$=10%. In the QPCE protocol proposed by Chen et al. [36], to compare two secrets of length n, TP generates $6n$ qubits in $2n$ GHZ states. Unfortunately, Lin et al. [37] pointed out that this protocol is not secure. In the improved version [37], TP generates $3n$ qubits in n GHZ states and $2n$ decoy qubits. Therefore, the qubit efficiency of the protocols [36,37] is $n/(3n + 2n)$=20%. In the QPCE protocol propose by Liu et al. [38], to compare two secrets of length $2n$, the two participants generate $6n$ qubits in $2n$ GHZ states, $4n$ decoy qubit for eavesdropping check. Also they use at least $8n$ qubits to establish two $2n$-bit classical keys. Hence the qubit efficiency of this protocol is $2n/(6n+4n+8n) \approx 11\%$. From the above analysis, we can see that the qubit efficiency of our protocol is higher than most of the previous QPCE protocols. More details are shown in Table 1.

3 Robust versions of the proposed protocol over collective-noise channels

At present, designing protocols in noisy channel is one of the key areas in quantum cryptography. Hence in this section, we will propose three robust versions of our protocol, which can be secure against collective-dephasing noise, collective-rotation noise and all types of unitary collective noise, respectively. For each one of the three protocols, the steps are identical as described in sect. 2.1. For simplicity, we only give the bases and unitary operations with which the protocol can be used in the corresponding collective-noise channel. It should be noted that that in each of the three fault-tolerant QPCE protocols, the three participants can generate the secret classical key K, by executing the three-party QKD protocol over corresponding collective-noise channel [42].

Table 1 Comparison among the QPCE protocols

Protocol	Qubit efficiency	Utilizing entanglement
Protocols in refs. [30,31]	< 17%	yes (EPR pairs)
Protocols in refs. [36,37]	20%	yes (GHZ states)
Protocol in ref. [32]	20%	yes (χ-type states)
Protocol in ref. [34]	10%	yes (χ-type states)
Protocol in ref. [38]	≈11%	yes (GHZ states)
Our protocol	25%	no (single photons)

3.1 The version over collective-dephasing channel

The collective-dephasing noise can be described as a unitary operation U satisfying

$$U|0\rangle = |0\rangle, \qquad U|1\rangle = \mathrm{e}^{\mathrm{i}\phi}|1\rangle, \tag{3}$$

where ϕ is the noise parameter which fluctuates with time. In general, the logical qubit encoded into two physical qubit product states in eq. (4) can withstand this collective-dephasing noise as the two logical qubits acquire the same phase factor $\mathrm{e}^{\mathrm{i}\phi}$ through the collective-dephasing channel

$$|0\rangle_L = |0\rangle|1\rangle, \qquad |1\rangle_L = |1\rangle|0\rangle. \tag{4}$$

For secure communication, at least two nonorthogonal measuring bases (MBs) are needed. One of the bases can be $\{|0\rangle_L, |1\rangle_L\}$, and the other one can be chosen as $\{|s\rangle_L, |t\rangle_L\}$, where

$$|s\rangle_L = \frac{1}{\sqrt{2}}(|0\rangle_L - \mathrm{i}|1\rangle_L), \quad |t\rangle_L = \frac{1}{\sqrt{2}}(|1\rangle_L - \mathrm{i}|0\rangle_L). \tag{5}$$

It can be easily shown that $\{|0\rangle_L, |1\rangle_L\}$ and $\{|s\rangle_L, |t\rangle_L\}$ form two nonorthogonal unbiased bases. The encoding operation (U_{dp}) and control operation (H_{dp}) for our robust QPC protocol over collective-dephasing channel can be chosen as follows

$$U_{dp} = \mathrm{i}H_{dp}^2 = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}, I = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix},$$
$$H_{dp} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 & 0 & -\mathrm{i} \\ 0 & 1 & -\mathrm{i} & 0 \\ 0 & -\mathrm{i} & 1 & 0 \\ -\mathrm{i} & 0 & 0 & 1 \end{pmatrix}. \tag{6}$$

The effect of the operations U_{dp} and H_{dp} on the states in the two bases can be described as

$$\begin{aligned} &U_{dp}|0\rangle_L = |1\rangle_L, && U_{dp}|1\rangle_L = |0\rangle_L; \\ &U_{dp}|s\rangle_L = |t\rangle_L, && U_{dp}|t\rangle_L = |s\rangle_L; \\ &H_{dp}|0\rangle_L = |s\rangle_L, && H_{dp}|1\rangle_L = |t\rangle_L; \\ &H_{dp}|s\rangle_L = -\mathrm{i}|1\rangle_L, && H_{dp}|t\rangle_L = -\mathrm{i}|0\rangle_L. \end{aligned} \tag{7}$$

Thus, we can obtain our QPCE protocol over collective-dephasing channel by substituting the bases and unitary operations in the protocol proposed in sect. 2.1. Concretely, the two bases used in the protocol presented in sect. 2.1 should be replaced with bases $\{|0\rangle_L, |1\rangle_L\}$ and $\{|s\rangle_L, |t\rangle_L\}$, and also the two unitary operations, U and H, should be replaced with U_{dp} and H_{dp}, respectively.

3.2 The version over collective-rotation channel

The collective-rotation noise can be described as a unitary operation U satisfying

$$U|0\rangle = \cos\theta|0\rangle + \sin\theta|1\rangle,$$
$$U|1\rangle = -\sin\theta|0\rangle + \cos\theta|1\rangle. \quad (8)$$

where θ is the parameter of noise which fluctuates with time. The two Bell states $|\Phi^+\rangle=\frac{1}{\sqrt{2}}(|00\rangle+|11\rangle)$ and $|\Psi^-\rangle=\frac{1}{\sqrt{2}}(|01\rangle-|10\rangle)$ can keep invariant under such type of collective noise. Therefore, logical qubits under collective-rotation noise can be chosen as

$$|0_r\rangle_L = |\Phi^+\rangle, \quad |1_r\rangle_L = |\Psi^-\rangle. \quad (9)$$

For secure communication, at least two nonorthogonal measuring bases (MBs) are required. One of the bases is $\{|0_r\rangle_L, |1_r\rangle_L\}$, the other is $\{|s_r\rangle_L, |t_r\rangle_L\}$, where

$$|s_r\rangle_L = \frac{1}{\sqrt{2}}(|0_r\rangle_L - \mathrm{i}|1_r\rangle_L), \quad |t_r\rangle_L = \frac{1}{\sqrt{2}}(|1_r\rangle_L - \mathrm{i}|0_r\rangle_L). \quad (10)$$

It can be shown that $\{|0_r\rangle_L, |1_r\rangle_L\}$ and $\{|s_r\rangle_L, |t_r\rangle_L\}$ form two nonorthogonal unbiased bases. The encoding operation (U_r) and control operation (H_r) for our robust QPC protocol over collective-rotation channel can be chosen as

$$H_r = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & -\mathrm{i} & 0 & 0 \\ -\mathrm{i} & 1 & 0 & 0 \\ 0 & 0 & 1 & \mathrm{i} \\ 0 & 0 & \mathrm{i} & 1 \end{pmatrix},$$
$$U_r = \mathrm{i}H_r^2 = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & -1 & 0 \end{pmatrix}. \quad (11)$$

The effect of the two unitary operations on the states in the two bases can be described as

$$U_r|0_r\rangle_L = |1_r\rangle_L, \quad U_r|1_r\rangle_L = |0_r\rangle_L,$$
$$U_r|s_r\rangle_L = |t_r\rangle_L, \quad U_r|t_r\rangle_L = |s_r\rangle_L,$$
$$C_r|0_r\rangle_L = |s_r\rangle_L, \quad C_r|1_r\rangle_L = |t_r\rangle_L,$$
$$C_r|s_r\rangle_L = -\mathrm{i}|1_r\rangle_L, \quad C_r|t_r\rangle_L = -\mathrm{i}|0_r\rangle_L. \quad (12)$$

Thus, we can obtain our QPCE protocol over collective-rotation channel by substituting the bases and unitary operations in the protocol proposed in Sect. 2.1. Concretely, the two bases used in the protocol presented in Sect. 2.1 should be replaced with bases $\{|0_r\rangle_L, |1_r\rangle_L\}$ and $\{|s_r\rangle_L, |t_r\rangle_L\}$, and also the two unitary operations, U and H, should be replaced with U_r and H_r, respectively.

3.3 The version over all types of unitary collective noise channels

Thus far, we have introduced the bases and unitary operations which are needed in our protocols over collective-dephasing channel and collective-rotation channel, respectively. Here we will introduce the bases and operations which can be used in our protocol over all types of unitary collective noise.

It is known that the singlet $|\psi^-\rangle$ is one of the decoherence free (DF) state [41,47] which can stay invariant under any n-lateral unitary transformation. That is to say, $U^{\otimes n}|\psi^-\rangle = |\psi^-\rangle$, where $U^{\otimes n} = U \otimes ... \otimes U$ denotes the tensor product of n unitary transformations U. According to the conclusion given by Cabello [47], at least 4 qubits are needed to fully protect one arbitrary logical qubit against all types of unitary collective noise. Therefore, a natural choice of the orthogonal basis in the 4-qubit DF subspace is $\{|\bar{0}\rangle_L, |\bar{1}\rangle_L\}$, where

$$\begin{aligned} |\bar{0}\rangle_L &= |\psi^-\rangle_{12}|\psi^-\rangle_{34} \\ &= \frac{1}{2}(|0101\rangle + |1010\rangle - |0110\rangle - |1001\rangle)_{1234}, \\ |\bar{1}\rangle_L &= \frac{1}{2\sqrt{3}}(2|0011\rangle + 2|1100\rangle - |0101\rangle - |1010\rangle \\ &\quad -|0110\rangle - |1001\rangle)_{1234}. \end{aligned} \quad (13)$$

For secure communication, we choose another basis as $\{|\bar{s}\rangle_L, |\bar{t}\rangle_L\}$, where

$$|\bar{s}\rangle_L = \frac{1}{\sqrt{2}}(|\bar{0}\rangle_L - \mathrm{i}|\bar{1}\rangle_L), \quad |\bar{t}\rangle_L = \frac{1}{\sqrt{2}}(|\bar{1}\rangle_L - \mathrm{i}|\bar{0}\rangle_L). \quad (14)$$

It can be easily verified that $\{|\bar{0}\rangle_L, |\bar{1}\rangle_L\}$ and $\{|\bar{s}\rangle_L, |\bar{t}\rangle_L\}$ form two nonorthogonal unbiased bases.

Suppose W is the 4-qubit Hilbert space whose dimension is 16, then we can easily find an orthonormal basis $|\bar{0}\rangle_L, |\bar{1}\rangle_L, ..., |\bar{15}\rangle$ for W by using the Gram-Schmidt procedure. For simplicity, here we do not give the concrete form of the states $|\bar{2}\rangle_L, |\bar{3}\rangle_L, ..., |\bar{15}\rangle$ since the well-known Gram-Schmidt method is not complicated. After getting all the states of the orthonormal basis, we can construct the required operations $\bar{U}$ and $\bar{H}$ for our QPC protocol over all types of unitary collective-noise channels by utilizing the method presented in ref. [42]. The form of the operations $\bar{U}$ and $\bar{H}$ are

$$\bar{U} = |\bar{0}\rangle\langle\bar{1}| + |\bar{1}\rangle\langle\bar{0}| + O, \quad \bar{H} = \frac{\sqrt{2U}}{1+\mathrm{i}}. \quad (15)$$

As described elsewhere [42], we have many feasible choices for the from of O, such as $O = |\bar{2}\rangle\langle\bar{2}| + ... + |\bar{15}\rangle\langle\bar{15}|$ and $O = |\bar{2}\rangle\langle\bar{3}| + |\bar{3}\rangle\langle\bar{4}| + ... + |\bar{15}\rangle\langle\bar{2}|$. For example, when $O = |\bar{2}\rangle\langle\bar{3}| + |\bar{3}\rangle\langle\bar{4}| + ... + |\bar{15}\rangle\langle\bar{2}|$, the effect of the operations $\bar{U}$ and $\bar{C}$ on the states in the two bases can be described as

$$\bar{U}|\bar{0}\rangle_L = |\bar{1}\rangle_L, \quad \bar{U}|\bar{1}\rangle_L = |\bar{0}\rangle_L,$$
$$\bar{U}|\bar{s}\rangle_L = |\bar{t}\rangle_L, \quad \bar{U}|\bar{t}\rangle_L = |\bar{s}\rangle_L,$$
$$\bar{H}|\bar{0}\rangle_L = |\bar{s}\rangle_L, \quad \bar{H}|\bar{1}\rangle_L = |\bar{t}\rangle_L,$$
$$\bar{H}|\bar{s}\rangle_L = -\mathrm{i}|\bar{1}\rangle_L, \quad \bar{H}|\bar{t}\rangle_L = -\mathrm{i}|\bar{0}\rangle_L. \quad (16)$$

To protect the communication from all types of unitary collective noise, the two bases used in the protocol presented in sect. 2.1 need be replaced with bases $\{|\bar{0}\rangle_L, |\bar{1}\rangle_L\}$ and $\{|\bar{s}\rangle_L, |\bar{t}\rangle_L\}$, and also the two unitary operations, U and H, need be replaced with $\bar{U}$ and $\bar{H}$, respectively.

Thus far, we have already introduced the required bases and unitary operations for our QPCE protocols which can withstand collective-dephasing noise, collective-rotation noise and all types of unitary collective noise, respectively. For simplicity, we do not describe the three protocols in detail, since the steps of these three protocols are identical as the steps of the protocol in the ideal channel given in sect. 2.1.

4 Security analysis

For simplicity, we analyze the security of the QPCE protocol over collective-dephasing channel in detail. As for the security of the other three QPCE protocols, it can be shown in same manner as the case with collective-dephasing noise.

Suppose Eve is an evil attacker (outsider attacker or a dishonest participant) who wants to eavesdrop the the secret of the participant (Alice or Bob) secret without being noted. Eve can intercept the legal states sent to the receiver and resend the states that she prepared instead, or she can entangle the legal states with her additional particles [50]. In the proposed protocol, two participants first encrypt their secrets with their private key K by utilizing classical one-time pad. Then they compare the ciphertext of their secrets instead of comparing the secrets directly. Since the ciphertext are encoded in the operations that the participants performed on the states in our protocols, the action to eavesdrop a secret of the participant is equivalent to discriminate the operations he/him performed. As each of the bits in the secret of the participants (X and Y) and controlling strings (R_1 and R_2) will be used only once in the execution of our protocol, here we introduce some useful conclusions on quantum operation discrimination [51,52] as follow.

Theorem 4.1 Under the condition that the device can be accessed only once, the minimum error probability to discriminate the two operations U_1 and U_2 is given as [40,51]

$$P_E = \frac{1}{2}\left[1 - \sqrt{1 - 4p_1p_2r(U_1^\dagger U_2)^2}\right]. \tag{17}$$

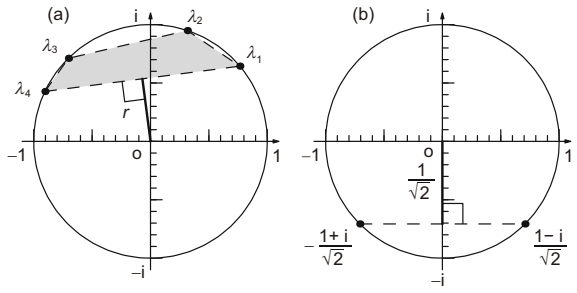

Figure 2 (a) Definition of the function $r(U)=r$, where λ_1, λ_2, λ_3 and λ_4 are eigenvalues of the matrix U and r is the distance between polygon $\lambda_1\lambda_2\lambda_3\lambda_4$ and the origin of the complex plane o and($r = 0$ when o is in/on the polygon). (b) shows an example, i.e., $r(U_{dp}^\dagger H_{dp})$.

Here, $r(U_1^\dagger U_2)$ represents the distance between the origin of the complex plane and the polygon (line segment if the operations are single qubit operations) whose vertices are the eigenvalues of the unitary operator $U_1^\dagger U_2$ (Figure 2(a)), and $U^\dagger$ denotes the adjoint matrix of U. For example, the eigenvalues of the operation $U_{dp}^\dagger H_{dp}$ are $\frac{1-i}{\sqrt{2}}$, $\frac{1-i}{\sqrt{2}}$, $\frac{-1-i}{\sqrt{2}}$, $\frac{-1-i}{\sqrt{2}}$, hence $r(U_{dp}^\dagger H_{dp})=1/\sqrt{2}$ (Figure 2(b)) and the minimum error probability to discriminate U_{dp} and H_{dp} is $\frac{1}{2}$-$\frac{\sqrt{2}}{4}$.

Corollary 4.2 Under the condition that the device can be accessed only once, two unitary operations U_1 and U_2 can be discriminate precisely if and only if $r(U_1^\dagger U_2) = 0$.

Theorem 4.3 The quantum operations $\delta_1, \cdots, \delta_n$ can be unambiguously discriminated by a single use if and only if for any $i = 1, \cdots, n$, $\mathrm{supp}(\delta_i) \nsubseteq \mathrm{supp}(S_i)$, where $\mathrm{supp}(\delta)$ denotes the support of a quantum operation δ and $S_i=\{\delta_j: j \neq i\}$ [52].

4.1 Outside attack

In the QPCE protocol over collective-dephasing channel, the unitary operations performed by both Alice and Bob can be regarded as four unitary operations as a whole (actually there should be eight combinations, but some are equal to each other when the global phase factors are ignored, e.g., $H_{dp}^2 U_{dp}=-\mathrm{i}I$), i.e., I, U_{dp}, H_{dp}, $H_{dp}U_{dp}$. According to Theorem 1, we can show that these four operations cannot be precisely discriminated. Take the operations U_{dp} and H_{dp} as an example, the eigenvalues of the operation $U_{dp}^\dagger H_{dp}$ are $\frac{1-i}{\sqrt{2}}$, $\frac{1-i}{\sqrt{2}}$, $\frac{-1-i}{\sqrt{2}}$, $\frac{-1-i}{\sqrt{2}}$, therefore, $r(U_{dp}^\dagger H_{dp}) = 1/\sqrt{2}$ (see Figure 3(b)) and the minimum error probability to discriminate U_{dp} and H_{dp} is given as

$$P_e = \frac{1}{2}\left[1 - \sqrt{1 - (1/\sqrt{2})^2}\right] \approx 0.15. \tag{18}$$

Also with this theorem, we can find that the minimum error probability to discriminate I and H_{dp} (I and $H_{dp}U_{dp}$, U and $H_{dp}U_{dp}$) is also $P_e(\approx 0.15)$, which indicates that these operations cannot be discriminated precisely. Moreover, we can also obtain the same conclusion according to Theorem 3. It is readily apparent that $H_{dp} = \frac{1}{\sqrt{2}}(1 \cdot I - \mathrm{i} \cdot U_{dp} + 0 \cdot H_{dp}U_{dp})=\frac{1}{\sqrt{2}}(I - \mathrm{i}U_{dp})$, which indicates $\mathrm{supp}\{H_{dp}\} \subseteq \mathrm{supp}\{I, U_{dp}, H_{dp}U_{dp}\}$. Therefore, these four operations cannot be discriminated precisely.

As the secrets of the participants secrets are encoded in the unitary operations they performed, if an outside attacker wants to obtain a secret of the participant (Alice of Bob) without arousing any errors in the eavesdropping check, he should be capable of discriminating the four operations, that is, I, U_{dp}, H_{dp}, $H_{dp}U_{dp}$, precisely with a single use. However, from the above analysis, such four operations cannot be unambiguously discriminated in this condition. Therefore, no matter what attack strategies (such as intercept-resend attack, measurement-resend attack, entanglement-measure at-

tack and dense-coding attack) an eavesdropper takes, his action will inevitably be found in the eavesdropping check.

In order to protect the proposed protocol from the Trojan horse attacks, such as the delay-photon Trojan horse attack and the invisible photon eavesdropping (IPE) Trojan horse attack, the filter and beam splitter which can eliminate the spy states, are utilized in our scheme [48,49]. Therefore, the eavesdropper can obtain none of the useful information by utilizing these attacks.

In addition, we consider another type of special attack for two-way communication, that is, denial of service (DOS) attack. In such attack strategy, an outside eavesdropper tries to make the comparison result inconsistent with the the actual situation, by randomly performing the encoding operation U_{dp} or the identity operation I in the process of the scheme, without being noticed. However, it can never succeed in our protocol since she/he cannot determine the positions of the decoy particles used in the final eavesdropping detection, and hence his/her disturbing operations will introduce errors in the measurement outcomes of some checking states. Next, we will consider the inside participant attack, including the attack by Alice, Bob and TP.

4.2 Participant attack

It is known that not all of the participants in a quantum cryptographic protocol are credible. A dishonest participant has more power to attack the scheme than an outside eavesdropper. First, he can know partial information legally. Second, he can tell a lie in the process of eavesdropping detection in order to avoid introducing errors. Hence we now concentrate our attention on the participant attacks in what follows. We consider the following three kinds of participant attacks. The first one is that Bob tries to eavesdrop on the secret of Alice, and the second is that Alice want to know the secret from Bob. Finally we consider that TP wants to obtains the secrets of the two participants.

4.2.1 Bob attempts to obtain the secret of Alice

We first consider the attacks by Bob in which he wants to get the secret of Alice without being noted. In this protocol, the four operations that Alice performed on the states cannot be discriminated precisely, hence the attack strategies such as entanglement-measure attack, dense-coding attack [50] and measurement-resend attack cannot be utilized to obtain the secret of Alice without introducing any errors, since he may mistake other operations for the correct one with certain probability.

In step 4, if Bob replaces the states (in S_1), on which Alice has encode her secret, with some states prepared by himself and processes the remaining decoy particles following the protocol, he will introduces no error in the eavesdropping check in step 5. However, by utilizing this strategy, he can obtain no information on the secret of Alice with the stolen states in his hand even after Alice reveals R_1. The reason is that Bob does not know the initial state of each the particle in S, which are randomly in one of the four states $\{|0\rangle_L, |1\rangle_L, |s\rangle_L, |t\rangle_L\}$. Hence for each one of the stolen states, he does not know which basis he can use to measure it. Even if he uses the correct basis, he still cannot judge weather Alice has performed operation U_{dp} on the state with the measurement outcome, since he does not know its initial state. In addition, if Bob intercepts S and sends Alice a sequence of states prepared by himself instead. When Alice sends the sequence to him after performing her operations, Bob preserves the processed sequence and sends S back to TP. In eavesdropping check, when Alice is required to publish the corresponding bit in R_1 for a decoy particle first, Bob can publish a fake value as the corresponding bit in R_2 to disguise his eavesdropping action. However, when TP requires him to publish first, his attack will be found with certain probability. In step 5, for each of the decoy particles, which one of Alice and Bob should be first to announce the corresponding controlling bit is randomly determined by TP, hence the intercept-resend attack is considered noneffective.

4.2.2 Alice attempts to obtain the secret of Bob

Now let us consider that Alice is a dishonest participant who wants to steal the secret from Bob. In this situation, also the four operations that Bob performed on the states cannot be discriminated precisely, hence the attack strategies such as entanglement-measure, dense-coding attack [50] and measurement-resend attack cannot be effective.

Then we consider the intercept-resend attack from Alice. In the proposed protocol, Alice is more powerful than Bob since the positions of the decoy states are chosen by herself. If Bob does not shuffles the states in the sequence after his operations in step 4, Alice can learn the information about the secret of Bob without being noted. That is, after she receives the sequence S, she replaces the states in S with the states prepared by herself except for the ones chosen as decoy states and sends the new sequence to Bob. After Bob performs his operations on the states in the sequence and sends them out, Alice intercepts the travelling sequence and replaces the states which are encoded with the secret from Bob also except for the decoys states. This means that the eavesdropping done by Alice does not disturb any one of the decoy states, hence she can obtain the secret from Bob with the information of R_2 announced by Bob and his action will not be noted in the eavesdropping check. However in this protocol, in order to prevent Alice from eavesdropping his secret in this way, Bob shuffles the states in the sequence with a permutation function G after his unitary operations. As Alice has no idea of the function G, he cannot know the correct positions of the decoy states, hence he will probably send TP the incorrect decoy states. In the procedure of eavesdropping check, if TP asks Alice to publish the corresponding bit in R_1 first, her eavesdropping action will be found by TP with

certain probability.

4.2.3 TP attempts to deduce the the secrets of the participants.

Different from most of the previous QPCE protocols [32,35–38], the TP in our protocol is assumed to be a semi-honest party, who may misbehave on its own but will not conspire with either of the two participants. That is to say, the TP in our protocols is more powerful since his/her is allowed to do anything to steal the information about the secrets of the participants by his/her own. However, TP cannot obtain any information about X and Y except for the comparison result in our protocol. First, the two participants in our protocol encoded their secrets with their shared key K by utilizing the classical one-time pad. Second, the encrypted secrets (X' and Y') are encoded in the operations performed by the participants (Alice and Bob). Since these operations cannot be precisely discriminated and K is private to Alice and Bob, TP can obtain none of the useful information about the secrets of the two participants (except for the comparison result for each bit) unless he/she cooperates with one of the two participants (Alice or Bob).

Thus, we have shown that the proposed protocol, which can resist collective-dephasing noise, is secure against both the outside attack and participant attack. As for the protocol over the ideal channel (collective-rotation channel, all types of unitary collective-noise channels), we can also show the security of it just in the same way, since the operations $\{I, H, U, HU\}$ ($\{I, H_r, U_r, H_rU_r\}$, $\{I, \bar{H}, \bar{U}, \bar{H}\bar{U}\}$) cannot be discriminated precisely according to the theorems given above [42,51,52]. For simplicity, here we do not describe detailed proofs.

5 Conclusions

Herein, we proposed a new QPCE protocol with single photons by utilizing collective detection. Our protocols have the following merits. Firstly, the assumption about TP in our protocols is more reasonable compared with the protocols presented elsewhere [32,35–38]. Secondly, by utilizing the collective detection, the qubit efficiency of our protocol is higher than those of the protocols described by others [30–32,34,36–38], also the cost of realizing this protocol is reduced since the two participants in this protocol need not to be equipped with qubit generating device or quantum measuring device. Thirdly, compared with the QPCE protocols [30,31,33] which employs hash function to guarantee their security, the security of our protocol is only guaranteed by the laws of quantum mechanics. Moreover, the three proposed versions of our protocol can combat with the errors over collective-dephasing channel, collective-rotation channel and all types of unitary collective-noise channels, respectively.

This work was supported by the National Natural Science Foundation of China (Grant Nos. 61272057, 61170270, 61100203, 61003286, 61121061 and 61103210), the Program for New Century Excellent Talents in Universities (Grant No. NCET-10-0260), the Specialized Research Fund for the Doctoral Program of Higher Education (Grant No. 20090005110010), the Natural Science Foundation of Beijing (Grant Nos. 4112040 and 4122054), the Fundamental Research Funds for the Central Universities (Grant No. 2011YB01), and the BUPT Excellent Ph.D. Students Foundation (Grant No. CX201217).

1 Bennett C H, Brassard G. Quantum cryptography: Public key distribution and coin tossing. In: Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing. New York: IEEE, 1984. 175–179
2 Ekert A K. Quantum cryptography based on Bell's theorem. Phys Rev Lett, 1991, 67: 661–663
3 Wen K, Long G L. Modified Bennett-Brassard 1984 quantum key distribution protocol with two-way classical communications. Phys Rev A, 2005, 72: 022336
4 Deng F G, Long G L. Controlled order rearrangement encryption for quantum key distribution. Phys Rev A, 2003, 68: 042315
5 Cai Q Y. Eavesdropping on the two-way quantum communication protocols with invisible photons. Phys Lett A, 2006, 351: 23–25
6 Tan Y G, Cai Q Y. Practical decoy state quantum key distribution with finite resource. Eur Phys J D, 2010, 56: 449–455
7 Lu Z X, Yu L, Li K, et al. Reverse reconciliation for continuous variable quantum key distribution. Sci China-Phys Mech Astron, 2010, 53: 101–105
8 Gao F, Wen Q Y, Qin S J, et al. Quantum asymmetric cryptography with symmetric keys. Sci China Ser G-Phys Mech Astron, 2009, 52: 1925–1931
9 Huang W, Guo F Z, Huang Z, et al. Three-particle QKD protocol against a collective noise. Opt Commun, 2011, 284: 536–540
10 Cleve R, Gottesman D, Lo H K. How to share a quantum secret. Phys Rev Lett, 1999, 83: 648–651
11 Hillery M, Buz ek V, Berthiaume A. Quantum secret sharing. Phys Rev A, 1999, 59: 1829–1834
12 Karlsson A, Koashi M, Imoto N. Quantum entanglement for secret sharing and secret splitting. Phys Rev A, 1999, 59: 162–168
13 Lin S, Wen Q Y, Qin S J, et al. Multiparty quantum secret sharing with collective eavesdropping-check. Opt Commun, 2009, 282: 4455–4459
14 Yang Y G, Chai H P, Wang Y, et al. Fault tolerant quantum secret sharing against collective-amplitude-damping noise. Sci China-Phys Mech Astron, 2011, 54: 1619–1624
15 Wang T Y, Wen Q Y. Security of a kind of quantum secret sharing with single photons. Quant Inf Comput, 2011, 11: 0434–0443
16 Tsai C W, Hwang T. Multi-party quantum secret sharing based on two special entangled states. Sci China-Phys Mech Astron, 2012, 55: 460–464
17 Li Q, Long D Y, Chan W H, et al. Sharing a quantum secret without a trusted party. Quantum Inf Process, 2011, 10: 97–106
18 Shi R H, Huang L S, Yang W, et al. Asymmetric multi-party quantum state sharing of an arbitrary m-qubit state. Quantum Inf Process, 2011, 10: 53–61
19 Jia H Y, Wen Q Y, Song T T, et al. Quantum protocol for millionaire problem. Opt Commun, 2011, 284: 545–549
20 Long G L, Liu X. Theoretically efficient high-capacity quantum-key-distribution scheme. Phys Rev A, 2002, 65: 032302
21 Boström K, Felbinger T. Deterministic secure direct communication using entanglement. Phys Rev Lett, 2002, 89: 187902
22 Gu B, Zhang C Y, Cheng G S, et al. Robust quantum secure direct

communication with a quantum one-time pad over a collective-noise channel. Sci China-Phys Mech Astron, 2011, 54: 942–947

23 Long G L, Deng F G, Wang C, et al. Quantum secure direct communication and deteministic secure quantum communication. Front Phys China, 2007, 2: 251–272

24 Huang W, Wen Q Y, Liu B, et al. Deterministic secure quantum communication with collective detection using single photons. Int J Theor Phys, 2012, 51: 2787–2797

25 Yao A. Protocols for secure computations. In: Proceedings of 23rd IEEE Symposium on Foundations of Computer Science (FOCS' 82). Washington: IEEE, 1982

26 Boudot F, Schoenmakers B, Traore J. A fair and efficient solution to the socialist millionaires problem. Discr Appl Math, 2001, 111: 23–36

27 Qin J, Zhang Z F, Feng D G, et al. A protocol of comparing information without leaking. J Softw, 2004, 15: 421–427

28 Lo H K. Insecurity of quantum secure computations. Phys Rev A, 1997, 56: 1154–1162

29 Buhrman H, Christandl M, Schaffner C. Complete insecurity of quantum protocols for classical two-party computation. Phys Rev Lett, 2012, 109: 160501

30 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

31 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, 2010, 43: 209801

32 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

33 Liu B, Gao F, Jia H Y, et al. Efficient quantum private comparison employing single photons and collective detection. Quantum Inf Process, 2012, 12: 887–897

34 Liu W, Wang Y B, Jiang Z T, et al. New quantum private comparison protocol using χ-type state. Int J Theor Phys, 2012, 51: 1953–1960

35 Tseng H Y, Lin J, Hwang T, New quantum private comparison protocol using EPR pairs. Quantum Inf Process, 2012, 11: 373–384

36 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, 2009, 283: 1161–1165

37 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: 2212–2214

38 Liu W, Wang Y B. Quantum private comparison based on GHZ entangled. Int J Theor Phys, 2012, 51: 3596–3604

39 Yang, Y G, Xia J, Jia X, et al. Comment on quantum private comparison protocols with a semi-honest third party. Quantum Inf Process, 2013, 12: 877–885

40 Liu B, Gao F, Wen Q Y. Single-photon multiparty quantum cryptographic protocols with collective detection. IEEE J Quant Electron, 2011, 47: 1383–1390

41 Zanardi P, Rasetti M. Noiseless quantum codes. Phys Rev Lett, 1997, 79: 3306

42 Huang W, Wen Q Y, Liu B, et al. A general method for constructing unitary operations for protocols with collective detection and new QKD protocols against collective noise. arXiv:1210.1332v2

43 Duan L M, Guo G C. Reducing decoherence in quantum-computer memory with all quantum bits coupling to the same environment. Phys Rev A, 1998, 57: 737–741

44 Boileau J C, Gottesman D, Laflamme R, et al. Robust polarization-based quantum key distribution over a collective-noise channel. Phys Rev Lett, 2004, 92: 017901

45 Huang W, Wen Q Y, Jia H Y, et al. Fault tolerant quantum secure direct communication with quantum encryption against collective noise. Chin Phys B, 2012, 21: 100308

46 Li X H, Deng F G, Hong Y Z. Efficient quantum key distribution over a collective noise channel. Phys Rev A, 2008, 78: 022321

47 Cabello A. Six-qubit permutation-based decoherence-free orthogonal basis. Phys Rev A, 2007, 75: 020301

48 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

49 Cai Q Y. Eavesdropping on the two-way quantum communication protocols with invisible photons. Phys Lett A, 2006, 351: 23–25

50 Gao F, Qin S J, Guo F Z, et al. Dense-coding attack on three-party quantum key distribution protocols. IEEE J Quant Electron, 2011, 47: 630–635

51 D'Ariano G M, Presti P L, Paris M G A. Using entanglement improves the precision of quantum measurements. Phys Rev Lett, 2001, 87: 270404

52 Wang G M, Ying M S. Unambiguous discrimination among quantum operations. Phys Rew A, 2006, 73: 042301