Quantum Information Processing (2020) 19:100
https://doi.org/10.1007/s11128-020-2593-y

Two-party quantum key agreement against collective noisy channel

Yi-Hua Zhou[1,2] · Mao-Feng Wang[1,2] · Wei-Min Shi[1,2] · Yu-Guang Yang[1,2] · Jing Zhang[1,2]

Received: 13 May 2019 / Accepted: 18 January 2020 / Published online: 3 February 2020

Abstract
Quantum key agreement (QKA) permits participants to constitute a shared key on a quantum channel, and no participants are able to independently determine the shared key. In fact, particles are frequently affected by channel noise in the transmission process of quantum channel. Under the cover of noise, attackers can launch malicious attacks. In this thesis, on account of the usage of entanglement swapping of GHZ state and logical Bell states, we design two two-party QKA protocols which are immune to collective-dephasing noise and collective-rotation noise, respectively. In comparison with the existing QKA protocols of two parties, the proposed protocols have better quantum resource cost and the qubit efficiency in the global scope. Security analysis reveals that they can resist not only attacks by participants but also external attacks.

Keywords Quantum cryptography · Quantum key agreement · Collective noise · Entanglement swapping · Qubit efficiency

1 Introduction

Quantum cryptography is an interdisciplinary subject which combines classical cryptography with quantum mechanics. It can achieve unconditional security provided by the laws of quantum physics, rather than the difficulties of mathematical calculation. There are plenty of diverse types of cryptographic protocols which have been mentioned before, for instance quantum key distribution (QKD) [1, 2], quantum key agreement (QKA) [3, 4], quantum secret sharing [5, 6], quantum secure direct communication [7, 8], quantum private comparison [9–11],

✉ Mao-Feng Wang
wmf18800133911@163.com

[1] Faculty of Information Technology, Beijing University of Technology, Beijing 100124, China

[2] Beijing Key Laboratory of Trusted Computing, Beijing 100124, China

quantum dialogue [12], quantum signature [13–16], and so on. At present, QKA [3, 4] is one of the most significant elements, which can realize the establishment of a shared key between two and more parties by using the public quantum channel. No party or subgroup can independently identify the shared key [17], so it is dissimilar from the QKD protocol [1], which predetermines the key, and subsequently distributes to other parties.

In Zhou et al. [3] who presented the first QKA protocol, numerous QKA protocols also have been introduced successively [18–31]. According to the BB84, Chong and Hwang [18] engineered an efficient two-party QKA protocol with the assistance of delayed measurement technique. On account of Bell state, a number of researchers also have presented some new two-party QKA protocols, such as Shukla et al.'s protocol [19], Chong et al.'s protocol [20], and Shi et al.'s protocol [21]. In [21], Shi and Zhong broadened the two-party QKA to multi-party QKA (MQKA). In their research, they presented the first multi-party QKA protocol on account of entanglement swapping and EPR pairs. Later, based on GHZ states and without decoy particles, Xu et al. [22] put forward a multi-particle QKA protocol. A large proportion of QKA protocols [18–26] are proposed in the ideal condition, which is that the quantum channel is an ideal channel without noise. Nevertheless, it is well known that quantum cryptographic protocols are inevitably disturbed by channel noise. In the channel of quantum noise, attackers are likely to hide their aggressive behavior with noise. As a result, it is extremely crucial to consider the channel noise in the process of designing the QKA protocol. At the moment, decoherence-free subspace (DFS) [27] which is an effective way to eliminate the influence of collective noise is almost unaffected by collective noise. Huang et al. [28] designed a QKA protocol and brought in two corresponding variations over collective noise. In the same year, Huang et al. [29] also devised a robust QKA protocol which made use of decoherence-free states to against collective decoherence. In 2016, on account of logical χ-states and logical Bell states, He et al. [30] devised two QKA protocols against collective noise. What's more, in 2018, Gao et al. [31] established new QKA protocols which are immune to collective noise on the basis of four-particle logical GHZ states.

In non-ideal channels, in order to solve the problem of communication against noise when there are two or more different kinds of noise at the same time, Wu et al. [43] put forward an idea to construct special particle states that can resist both kinds of noise at the same time. The protocol needs to construct the generalized GHZ state of nine particles, the generalized unitary transformation, and the deceptive state. However, the paper only proposes an idea without the design of the protocol in detail. What's more, because this method uses nine particle entanglement, the quantum resource cost is high and the qubit efficiency is low. Therefore, in our paper, we discuss problems of key negotiation under two kinds of noise in the non-ideal channel, respectively.

In our paper, we put forward two two-party QKA protocols on account of entanglement swapping. Two unrelated three-particle GHZ states are able to establish entanglement correlation just by using two Bell measurements. With the assistance of the entanglement swapping, our proposed QKA protocols

can against two kinds of collective noise channels. Beyond that, in terms of qubit efficiency, we use fewer quantum bits but achieve higher quantum bit efficiency.

The organization of the remainder of this paper is as follows: The second section is used to describe the preliminaries of the whole paper. And Sect. 3 aims to give the description of our two-party QKA protocols in detail. In addition, we make a full analysis of the security of our protocols in Sect. 4. What's more, for the sake of demonstrating the superiority of our protocols, we make a comparison with other QKA protocols against collective noise in regard to qubit efficiency in Sect. 5. At last, a brief conclusion is given in the final section.

2 Preliminaries

2.1 Unitary operations and entanglement swapping

At first, we present four unitary operations which are $U_{00} \equiv I = |0\rangle\langle 0| + |1\rangle\langle 1|$, $U_{01} \equiv X = |0\rangle\langle 1| + |1\rangle\langle 0|$, $U_{10} \equiv Z = |0\rangle\langle 0| - |1\rangle\langle 1|$, and $U_{11} \equiv iY = |0\rangle\langle 1| - |1\rangle\langle 0|$. Two nonorthogonal bases are defined as $\{|0\rangle, |1\rangle\}$ and $\{|+\rangle, |-\rangle\}$, where $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. There are four Bell states $|\phi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle)$ and $|\psi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle)$. After a unitary operation $U_{i_1 i_2}$ $(i_1, i_2 = 0, 1)$ on its second particle, the Bell state is transformed into another Bell state. Table 1 shows the corresponding transformed results.

The GHZ state is the maximum entanglement state of three particles. In this protocol, the three-particle GHZ state $|G\rangle = \frac{1}{\sqrt{2}}(|010\rangle + |101\rangle)$ is used as a quantum source. At first, we prepare two GHZ states, $|G\rangle_{123} = \frac{1}{\sqrt{2}}(|010\rangle + |101\rangle)_{123}$ and $|G\rangle_{456} = \frac{1}{\sqrt{2}}(|010\rangle + |101\rangle)_{456}$, as Eq. (1), where the subscript i denotes the ith qubit of $|G\rangle_{123}$ and $|G\rangle_{456}$.

Table 1 Relationship between the unitary operations and the transformed Bell states

	$I \otimes U_{00}$	$I \otimes U_{01}$	$I \otimes U_{10}$	$I \otimes U_{11}$
$\|\phi^{\pm}\rangle$	$\|\phi^{\pm}\rangle$	$\|\psi^{\pm}\rangle$	$\|\phi^{\mp}\rangle$	$\|\psi^{\mp}\rangle$
$\|\psi^{\pm}\rangle$	$\|\psi^{\pm}\rangle$	$\|\phi^{\pm}\rangle$	$\|\psi^{\mp}\rangle$	$\|\phi^{\mp}\rangle$

$$
\begin{aligned}
&|G\rangle_{123}\otimes|G\rangle_{456}\\
&=\frac{1}{\sqrt{2}}(|010\rangle+|101\rangle)_{123}\otimes\frac{1}{\sqrt{2}}(|010\rangle+|101\rangle)_{456}\\
&=\frac{1}{2\sqrt{2}}\big(|\phi^+\rangle_{14}(|10\rangle_{23}|10\rangle_{56}+|01\rangle_{23}|01\rangle_{56})\\
&\quad+|\phi^-\rangle_{14}(|10\rangle_{23}|10\rangle_{56}-|01\rangle_{23}|01\rangle_{56})\\
&\quad+|\psi^+\rangle_{14}(|10\rangle_{23}|01\rangle_{56}+|01\rangle_{23}|10\rangle_{56})\\
&\quad+|\psi^-\rangle_{14}(|10\rangle_{23}|01\rangle_{56}-|01\rangle_{23}|10\rangle_{56})\big)\\
&=\frac{1}{2\sqrt{2}}\big(|\phi^+\rangle_{14}(|\phi^+\rangle_{25}|\phi^+\rangle_{36}-|\phi^-\rangle_{25}|\phi^-\rangle_{36})\\
&\quad+|\phi^-\rangle_{14}(|\phi^+\rangle_{25}|\phi^-\rangle_{36}-|\phi^-\rangle_{25}|\phi^+\rangle_{36})\\
&\quad+|\psi^+\rangle_{14}(|\psi^+\rangle_{25}|\psi^+\rangle_{36}-|\psi^-\rangle_{25}|\psi^-\rangle_{36})\\
&\quad+|\psi^-\rangle_{14}(|\psi^+\rangle_{25}|\psi^-\rangle_{36}-|\psi^-\rangle_{25}|\psi^+\rangle_{36})\big)
\end{aligned}
\tag{1}
$$

If one person performs the Bell measurement on the second and the fifth qubits, and the third and the sixth qubits, another one performs measurement on the first and the fourth qubits, separately. According to Eq. (1), the state $|G\rangle_{123}\otimes|G\rangle_{456}$ will collapse into one of the eight states: $\{|\phi^+\rangle_{14}|\phi^+\rangle_{25}|\phi^+\rangle_{36}$, $|\phi^+\rangle_{14}|\phi^-\rangle_{25}|\phi^-\rangle_{36}$, $|\phi^-\rangle_{14}|\phi^+\rangle_{25}|\phi^-\rangle_{36}$, $|\phi^-\rangle_{14}|\phi^-\rangle_{25}|\phi^+\rangle_{36}$, $|\psi^+\rangle_{14}|\psi^+\rangle_{25}|\psi^+\rangle_{36}$, $|\psi^+\rangle_{14}|\psi^-\rangle_{25}|\psi^-\rangle_{36}$, $|\psi^-\rangle_{14}|\psi^+\rangle_{25}|\psi^-\rangle_{36}$, and $|\psi^-\rangle_{14}|\psi^-\rangle_{25}|\psi^+\rangle_{36}\}$. They are able to infer the post-measurement states of each other from the measurement results.

2.2 Collective noise

Practical quantum channels are the mostly optical fibers with fluctuations, uneven media, birefringence fluctuations, etc. Polarized photons will be affected by noise when they are transmitted in optical fibers as information carriers. Due to the fast transmission speed of photons, the noise change can be considered as slow change, that is, the quantum-state transmission time gap is shorter than the noise change time gap, and all photons will be affected by the same noise. These effects can be approximated as an unitary operation $U(t)$ (t represents the quantum-state transmission time) which is the joint unitary noise channel model [41].

In this paper, we discuss two types of collective noise which are the collective-dephasing noise and the collective-rotation noise. Under the collective noise, the changes of N quantum bits can be expressed as $\rho_N \rightarrow [U(t)]^{\otimes N}\rho_N\left[U(t)^{\dagger}\right]^{\otimes N}$, and ρ_N is the density matrix of the quantum system. The effect of unitary operation $U(t)$ can be further approximated as $U|0\rangle=\cos\theta|0\rangle+e^{i\varphi}\sin\theta|1\rangle$, $U|1\rangle=e^{i\Delta}(\cos\theta|1\rangle-e^{i\varphi}\sin\theta|0\rangle)$. The parameters Δ,θ and φ are the fluctuation factors of the noise with time. When the $\theta=0$, Δ,φ takes any value; the corresponding noise is collective-dephasing noise

$U_{\mathrm{dp}}=\begin{pmatrix} 1 & 0 \\ 0 & e^{i\varphi} \end{pmatrix}$. Its effect on the photon horizontal polarization state $|0\rangle$ and vertical polarization state $|1\rangle$ is $U_{\mathrm{dp}}|0\rangle = |0\rangle, U_{\mathrm{dp}}|1\rangle = e^{i\varphi}|1\rangle$. When $\Delta = \varphi = 0$, θ takes any value; the corresponding noise is collective-rotation noise $U_{\mathrm{r}}=\begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix}$. Under the circumstances of collective-rotation noise, the photon undergoes a joint flip which can be expressed as $U_{\mathrm{r}}|0\rangle = \cos\theta|0\rangle + \sin\theta|1\rangle$, $U_{\mathrm{r}}|1\rangle = -\sin\theta|0\rangle + \cos\theta|1\rangle$.

A decoherence-free subspace (DFS) is a subspace of a system's Hilbert space that is invariant to non-unitary dynamics. Alternatively stated, they are a small section of the system Hilbert space where the system is decoupled from the environment, and thus, its evolution is completely unitary. Due to this character, DFS is utilized against the collective noise [27].

According to the characteristics of the collective-dephasing noise [27], the subspaces $\{|0_{\mathrm{dp}}\rangle, |1_{\mathrm{dp}}\rangle\}$ and $\{|+_{\mathrm{dp}}\rangle, |-_{\mathrm{dp}}\rangle\}$ are able to constitute a DFS which is immune to collective-dephasing noise, where $|0_{\mathrm{dp}}\rangle = |01\rangle$, $|1_{\mathrm{dp}}\rangle = |10\rangle$, $|\pm_{\mathrm{dp}}\rangle = \frac{1}{\sqrt{2}}(|0_{\mathrm{dp}}\rangle \pm |1_{\mathrm{dp}}\rangle)) = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle)$. In the same way, the subspaces $\{|0_{\mathrm{r}}\rangle, |1_{\mathrm{r}}\rangle\}$ and $\{|+_{\mathrm{r}}\rangle, |-_{\mathrm{r}}\rangle\}$ are able to constitute a DFS which is immune to collective-rotation noise, where $|0_{\mathrm{r}}\rangle = |\phi^+\rangle$, $|1_{\mathrm{r}}\rangle = |\psi^-\rangle$, $|\pm_{\mathrm{r}}\rangle = \frac{1}{\sqrt{2}}(|0_{\mathrm{r}}\rangle \pm |1_{\mathrm{r}}\rangle)$ $= \frac{1}{\sqrt{2}}(|\phi^+\rangle \pm |\psi^-\rangle)$.

It is obvious that GHZ state $|G\rangle_{123} = \frac{1}{\sqrt{2}}(|0\rangle_1|10\rangle_{23} + |1\rangle_1|01\rangle_{23}) = \frac{1}{\sqrt{2}}\left(|0\rangle_1\left|1_{\mathrm{dp}}\right\rangle_{23} + |1\rangle_1\left|0_{\mathrm{dp}}\right\rangle_{23}\right)$ is constant when the second and the third qubits are transmitted through the collective-dephasing noise channel. We can prepare that GHZ-like state $|L\rangle_{123} = \frac{1}{\sqrt{2}}(|001\rangle - |010 + |100 + |111\rangle)_{123} = \frac{1}{\sqrt{2}}\left(|0\rangle_1|1_{\mathrm{r}}\rangle_{23} + |1\rangle_1|0_{\mathrm{r}}\rangle_{23}\right)$ is constant when the second and the third qubits are transmitted through the collective-rotation noise channel.

3 Description of the QKA protocols against collective noise

Before the start of the protocol, both parties shall carry out identity authentication [42] to ensure that they are not impersonated by the intruder Eve.

3.1 The QKA protocol against collective-dephasing noise

Step 1 Alice and Bob randomly generate their own $2n$-bit secret keys:

$$K_A = \left\{K_A^1, K_A^2, \ldots, K_A^n\right\}, \quad K_B = \left\{K_B^1, K_B^2, \ldots, K_B^n\right\},$$

where $K_A^i, K_B^i \in \{00, 01, 10, 11\}$ and $i = 1, 2, \ldots, n$.

Step 2 Alice is going to generate a sequence of $2n$ GHZ states $|G\rangle = \frac{1}{\sqrt{2}}(|010\rangle + |101\rangle)$. Then, use $|G\rangle_{123} \otimes |G\rangle_{456}$ as a quantum source. According to Eq. (1), Alice remains particles 1 and 4, sends particles 2, 5 and 3, 6 to Bob. After that, Alice and Bob measure the particles they hold by Bell measurement, respectively. After measurement, the particles collapse to the Bell state, different Bell states correspond to different encodings. Alice and Bob negotiate the coding scheme as shown in Table 2.

Alice distributes $2n$ GHZ states into two ordered sequences named S_A and S_B, she takes the first qubits to constitute a new sequence $S_A = \{q_1^i\}$, and the rest of the qubits are used to establish the other sequence $S_B = \{q_2^i, q_3^i\}$, for $i = 1, 2, \ldots, 2n$. At the same time, $2n$ GHZ states are divided into q_1, q_2, q_3. Then, the sequence of q_1 contains the first particle of GHZ states, and the quantity of this sequence is $2n$. Beyond that, the sequence of q_2 contains the second particle of the GHZ state, and the sequence q_3 contains a third particle of the GHZ state. Alice prepares m decoy logical qubits which are both randomly selected from $\{|0_{dp}\rangle, |1_{dp}\rangle, |+_{dp}\rangle, |-_{dp}\rangle\}$. After that, Alice inserts them into S_B randomly to obtain $S_B^{'}$ and keeps a record of the inserting positions. Then, Alice sends them to Bob and maintains the sequence S_A.

Step 3 After that, Bob accepts the sequence $S_B^{'}$; Alice indicates the location and the measurement basis of the decoy logical qubits. Afterward, Bob measures the decoy logical qubits with the announced bases. And he reports the measurement results to Alice. Alice compares the measurement results with initial states of the decoy logical qubits in order to calculate the error rate. In this process, if the error rate is less than the given threshold value, they will continue to perform the next step. If not, they will give up this protocol and restart it.

Step 4 On the basis of Eq. (1), n pair GHZ states $|G\rangle$ means there are n $|G\rangle_{123} \otimes |G\rangle_{456}$ as the quantum source, the sequence of q_1 contains the first and the fourth particle, the sequence of q_2 contains the second and the fifth particle, the sequence of q_3 contains the third and the sixth particle. Then, Alice performs Bell measurement on qubits $\{q_1^{2j-1}, q_1^{2j}\}$; Bob measures the qubits $\{q_2^{2j-1}, q_2^{2j}\}$ and $\{q_3^{2j-1}, q_3^{2j}\}$, for $j = 1, 2, \ldots, n$. After the measurement, the state $|G_{123} \otimes |G_{456}$ will collapses into one of the four states as shown in Eq. (1). On the basis of the measurement correlation of Eq. (1), Alice and Bob are able to deduce the post-measurement states of each other. Later, according to the coding rules negotiated by Step 1, the post-measurement status of Alice and Bob is converted into a classic bit string $M = M_1||M_2||\cdots||M_n$, where $M_i \in \{00, 01, 10, 11\}$ $(i = 1, 2, \ldots, n)$. Since both sides can infer each other's state, they have a common M.

Table 2 Relationship between the Bell states and the encodings

Raw keybits	Alice's measurement result	Bob's measurement result
00	$\|\phi^+\rangle$	$\|\phi^+\|\phi^+\rangle$ or $\|\phi^-\|\phi^-\rangle$
01	$\|\phi^-\rangle$	$\|\phi^+\|\phi^-\rangle$ or $\|\phi^-\|\phi^+\rangle$
10	$\|\psi^+\rangle$	$\|\psi^+\rangle\|\psi^+\rangle$ or $\|\psi^-\rangle\|\psi^-\rangle$
11	$\|\psi^-\rangle$	$\|\psi^+\rangle\|\psi^-\rangle$ or $\|\psi^-\rangle\|\psi^+\rangle$

Step 5 Let $K_{A_1}^i K_{A_2}^i = K_A^i$. Alice can encode the key K_A by performing the unitary operation $U_{K_{A_1}^i K_{A_2}^i}$ on the post-measurement qubits $\{q_1^{2j}\}$; it means the even number of particles in the q_1 sequence, where $i, j = 1, 2, \ldots, n$. Obtain the encoded quantum-state sequence which is able to be denoted as S_D^*. The qubit sequence $\{q_1^{2j-1}\}$ is denoted as S_C. Consequently, the corresponding two particles in S_C and S_D^* constitute a new Bell state. On account of the new Bell states, Alice prepares the corresponding logical Bell states as follows:

$$
\begin{aligned}
|\phi_{\mathrm{dp}}^+\rangle_{C_1C_2D_1D_2} &= \frac{1}{\sqrt{2}}\left(|0_{\mathrm{dp}}\rangle|0_{\mathrm{dp}}\rangle + |1_{\mathrm{dp}}\rangle|1_{\mathrm{dp}}\rangle\right)_{C_1C_2D_1D_2} \\
&= \frac{1}{\sqrt{2}}\left(|\phi^+\rangle|\phi^+\rangle - |\phi^-\rangle|\phi^-\rangle\right)_{C_1D_1C_2D_2} \\
|\phi_{\mathrm{dp}}^-\rangle_{C_1C_2D_1D_2} &= \frac{1}{\sqrt{2}}\left(|0_{\mathrm{dp}}\rangle|0_{\mathrm{dp}}\rangle - |1_{\mathrm{dp}}\rangle|1_{\mathrm{dp}}\rangle\right)_{C_1C_2D_1D_2} \\
&= \frac{1}{\sqrt{2}}\left(|\phi^-\rangle|\phi^+\rangle - |\phi^+\rangle|\phi^-\rangle\right)_{C_1D_1C_2D_2} \\
|\psi_{\mathrm{dp}}^+\rangle_{C_1C_2D_1D_2} &= \frac{1}{\sqrt{2}}\left(|0_{\mathrm{dp}}\rangle|1_{\mathrm{dp}}\rangle + |1_{\mathrm{dp}}\rangle|0_{\mathrm{dp}}\rangle\right)_{C_1C_2D_1D_2} \\
&= \frac{1}{\sqrt{2}}\left(|\psi^+\rangle|\psi^+\rangle - |\psi^-\rangle|\psi^-\rangle\right)_{C_1D_1C_2D_2} \\
|\psi_{\mathrm{dp}}^-\rangle_{C_1C_2D_1D_2} &= \frac{1}{\sqrt{2}}\left(|0_{\mathrm{dp}}\rangle|1_{\mathrm{dp}}\rangle - |1_{\mathrm{dp}}\rangle|0_{\mathrm{dp}}\rangle\right)_{C_1C_2D_1D_2} \\
&= \frac{1}{\sqrt{2}}\left(|\psi^-\rangle|\psi^+\rangle - |\psi^+\rangle|\psi^-\rangle\right)_{C_1D_1C_2D_2}
\end{aligned}
\tag{2}
$$

The new sequences $S_C{}^{(1)}$ and $S_D^*{}^{(1)}$ are made up of logical qubits C (two physical qubits C_1 and C_2) and logical qubits D (two physical qubits D_1 and D_2) separately. Later, Alice selects a permutation operator Π_n randomly and performs the permutation operator Π_n on $S_C^{(1)}$ to obtain the new quantum-state sequence $S_C^{(2)}$. Soon after, Alice randomly selects m decoy states from $\{|0_{\mathrm{dp}}\rangle, |1_{\mathrm{dp}}\rangle, |+_{\mathrm{dp}}, |-_{\mathrm{dp}}\}$, and randomly inserts them into $S_C^{(2)}$ and $S_D^{*(1)}$ in order to obtain the new quantum-state sequence $S_C{}^{(2)\prime}$ and $S_D^*{}^{(1)\prime}$. Alice sends the sequences $S_C{}^{(2)\prime}$ and $S_D^*{}^{(1)\prime}$ to Bob.

Step 6 It is similar to Step 3; when Bob receives the sequences $S_C{}^{(2)\prime}$ and $S_D^*{}^{(1)\prime}$, two parties perform a second eavesdropping check.

Step 7 Bob declares the value $K_B^{'} = K_B \oplus M = \{K_B^1 \oplus M_1, K_B^2 \oplus M_2, \ldots, K_B^n \oplus M_n\}$. On account of the value M, Alice is able to derive the key K_B. Beyond that, Alice is able to compute the shared key $K_{AB} = (K_A \oplus K_B)||(K_A \oplus K_B \oplus M)$.

Step 8 Alice announces the permutation operator Π_n. Bob who wants to obtain the sequence $S_C{}^{(1)}$ applies its inverse permutation to the sequence $S_C^{(2)}$. He associates the sequence $S_C{}^{(1)}$ with the sequence $S_D^*{}^{(1)}$ in order to obtain n logical Bell

states. After that, he carries out the Bell measurements on the particles C_1, D_1 as well as the particles C_2, D_2, respectively. In the light of Eq. (2), Bob deduces the physical Bell state corresponding to each pair of particles in $S_C{}^{(1)}$ and $S_D^{*}{}^{(1)}$. What's more, on the basis of Table 1, Bob is able to deduce K_A. Beyond that, Bob can figure the shared key $K_{AB} = (K_A \oplus K_B)||(K_A \oplus K_B \oplus M)$.

3.2 The QKA protocol against collective-rotation noise

Step 1 Alice and Bob randomly generate their $2n$-bit secret keys:

$$K_A = \left\{K_A^1, K_A^2, \ldots, K_A^n, K_B\right\} = \left\{K_B^1, K_B^2, \ldots, K_B^n\right\},$$

where $K_A^i, K_B^i \in \{00, 01, 10, 11\}$ and $i = 1, 2, \ldots, n$.

Step 2 Alice prepares a sequence of $2n$ GHZ-like states $|L\rangle_{123} = \frac{1}{\sqrt{2}}(|001\rangle - |010 + |100 + |111\rangle)_{123}$. Use $|L\rangle_{123} \otimes |L\rangle_{456}$ as a quantum source:

$$\begin{aligned}
&|L_{123} \otimes |L_{456} \\
&= \frac{1}{\sqrt{2}}(|001\rangle - |010 + |100 + |111\rangle)_{123} \\
&\otimes \frac{1}{\sqrt{2}}(|001\rangle - |010 + |100 + |111\rangle)_{456} \\
&= \frac{1}{\sqrt{2}}\left(|0\rangle_1|\psi^-\rangle_{23} + |1\rangle_1|\phi^+\rangle_{23}\right) \\
&\otimes \frac{1}{\sqrt{2}}\left(|0\rangle_4|\psi^-\rangle_{56} + |1\rangle_4|\phi^+\rangle_{56}\right) \\
&= \frac{1}{2\sqrt{2}}\left(|\phi^+\rangle_{14}\left(|\phi^+\rangle_{25}|\phi^+\rangle_{36} + |\psi^-\rangle_{25}|\psi^-\rangle_{36}\right)\right. \\
&+ |\phi^-{}_{14}\left(-|\phi^-\rangle_{25}|\phi^-\rangle_{36} - |\psi^+\rangle_{25}|\psi^+\rangle_{36}\right) \\
&+ |\psi^+{}_{14}\left(|\phi^-\rangle_{25}|\psi^+\rangle_{36} - |\psi^+\rangle_{25}|\phi^-\rangle_{36}\right) \\
&\left.+|\psi^-{}_{14}\left(-|\phi^+\rangle_{25}|\psi^-\rangle_{36} + |\psi^-\rangle_{25}|\phi^+\rangle_{36}\right)\right)
\end{aligned} \tag{3}$$

Table 3 Relationship between the Bell states and the encodings

Raw keybits	Alice's measurement result	Bob's measurement result
00	$\|\phi^+\rangle$	$\|\phi^+\|\phi^+\rangle$ or $\|\psi^-\rangle\|\psi^-\rangle$
01	$\|\phi^-\rangle$	$\|\phi^-\|\phi^-\rangle$ or $\|\psi^+\rangle\|\psi^+\rangle$
10	$\|\psi^+\rangle$	$\|\phi^-\|\psi^+\rangle$ or $\|\psi^+\rangle\|\phi^-\rangle$
11	$\|\psi^-\rangle$	$\|\phi^+\|\psi^-\rangle$ or $\|\psi^-\rangle\|\phi^+\rangle$

Similar to protocol 3.1, Alice and Bob negotiate the coding scheme as shown in Table 3.

Alice separates these GHZ-like states into two ordered sequences S_A and S_B; she takes the first qubits to form a new sequence $S_A=\{q_1^i\}$ and the remaining qubits form the another sequence $S_B=\{q_2^i, q_3^i\}$, for $i=1, 2,\ldots, 2n$. Alice prepares m decoy logical qubits which are randomly selected from $\{|0_{dp}\rangle, |1_{dp}\rangle, |+_{dp}\rangle, |-_{dp}\rangle\}$, whereafter Alice inserts them into S_B randomly to obtain $S_B^{'}$ and keeps a record of the inserting positions. After that, Alice sends them to Bob and keeps the sequence S_A.

Steps 3–4 These steps are almost identical to Steps 3–4 of protocol against collective-dephasing noise.

Step 5 Alice is able to encode the key K_A by performing the unitary operation $U_{K_{A_1}^i K_{A_2}^i}$ on the post-measurement qubits $\{q_1^{2j}\}$, where $i, j=1, 2, \ldots, n$. And she could obtain the encoded quantum-state sequence which is recorded as S_D^*. What's more, the qubit sequence $\{q_1^{2j-1}\}$ is denoted as S_C. As a consequence, the corresponding two particles in S_C and S_D^* constitute a new Bell state. On account of the new Bell states, Alice prepares the corresponding logical Bell states as follows:

$$
\begin{aligned}
|\phi^+\rangle_{rA_1A_2B_1B_2} &= \frac{1}{\sqrt{2}}\left(|0_r\rangle|0_r\rangle + |1_r\rangle|1_r\rangle\right)_{A_1A_2B_1B_2} \\
&= \frac{1}{\sqrt{2}}\left(|\phi^+\rangle|\phi^+\rangle + |\psi^-\rangle|\psi^-\rangle\right)_{A_1B_1A_2B_2} \\
|\phi^-\rangle_{rA_1A_2B_1B_2} &= \frac{1}{\sqrt{2}}\left(|0_r\rangle|0_r\rangle - |1_r\rangle|1_r\rangle\right)_{A_1A_2B_1B_2} \\
&= \frac{1}{\sqrt{2}}\left(|\phi^-\rangle|\phi^-\rangle + |\psi^+\rangle|\psi^+\rangle\right)_{A_1B_1A_2B_2} \\
|\psi^+\rangle_{rA_1A_2B_1B_2} &= \frac{1}{\sqrt{2}}\left(|0_r\rangle|1_r\rangle + |1_r\rangle|0_r\rangle\right)_{A_1A_2B_1B_2} \\
&= \frac{1}{\sqrt{2}}\left(|\phi^-\rangle|\psi^+\rangle - |\psi^+\rangle|\phi^-\rangle\right)_{A_1B_1A_2B_2} \\
|\psi^-\rangle_{rA_1A_2B_1B_2} &= \frac{1}{\sqrt{2}}\left(|0_r\rangle|1_r\rangle - |1_r\rangle|0_r\rangle\right)_{A_1A_2B_1B_2} \\
&= \frac{1}{\sqrt{2}}\left(|\phi^+\rangle|\psi^-\rangle - |\psi^-\rangle|\phi^+\rangle\right)_{A_1B_1A_2B_2}
\end{aligned}
\tag{4}
$$

The new sequences $S_C{}^{(1)}$ and $S_D^{*}{}^{(1)}$ are made up of logical qubits C (two physical qubits C_1 and C_2) and logical qubits D (two physical qubits D_1 and D_2), respectively. Later, Alice selects a permutation operator Π_n randomly and performs the permutation operator Π_n on $S_C{}^{(1)}$, in order to obtain the new quantum-state sequence $S_C{}^{(2)}$. Soon after, Alice randomly selects m decoy states from $\{|0_{dp}, |1_{dp}, |+_{dp}, |-_{dp}\}$, and randomly inserts them into $S_C^{(2)}$ and $S_D^{*}{}^{(1)}$ to obtain the new quantum-state sequence $S_C{}^{(2)'}$ and $S_D^{*}{}^{(1)'}$. In the end, Alice sends the sequences $S_C{}^{(2)'}$ and $S_D^{*}{}^{(1)'}$ to Bob.

Steps 6–8 These steps are almost the same as Steps 6–8 of protocol against collective-dephasing noise.

4 Security analysis

In section four, we intend to discuss the security of the protocol. As can be seen from the security analysis, the two QKA protocols which we have proposed before are able to resist common attacks from the internal and external attackers.

Since the protocol only transmits logical qubits in quantum channels, these are not attacked by the collective-dephasing noise and the collective-rotation noise [32], respectively.

4.1 Participant attack

Gao et al. [33–35] first proposed the concept of participant attack which refers to some legitimate participants who may be dishonest rather than external eavesdroppers. Additionally, they try to conduct an attack for their own purposes. For diverse quantum cryptographic protocols, the purpose of the participants is diverse. For instance, for a QKA protocol, the dishonest participant might intend to control the shared key and decide it entirely by himself alone.

At first, it can be assumed that Bob is dishonest and Alice is honest. Due to delayed measurement technology [36], even if Bob got decode K_A by measuring the particles before he announces $K_B^{'} = K_B \oplus M$, he could not get the correct K_A because he still did not know the permutation operation Π_n. Therefore, the participant attack of Alice will not succeed. Then, we assume that Alice is dishonest and Bob is honest. Before Alice sends the encoded message qubits, she cannot obtain $K_B^{'}$. So for Alice there is no way to control K_{AB}. Therefore, Bob's participant attack will not succeed.

4.2 Outsider attack

Suppose Eve wants to get the shared key, she has to eavesdrop the information of M and K_A. The possible main attacks are the Trojan horse attacks, the intercept-resend attack, the measure-resend attack, the entangle-measure attack, and the double CNOT attack.

Trojan horse attacks: In the two proposed QKA protocols, each photon can only be transmitted once via the quantum channel. Thus, our two QKA protocols are immune to Trojan horse attacks [37, 38].

Intercept-resend attack: In our two protocols, we randomly select the decoy logical qubits from two nonorthogonal bases $\{|0_{dp}\rangle, |1_{dp}\rangle\}$(or $\{|0_r\rangle, |1_r\rangle\}$) and $\{|+_{dp}\rangle, |-_{dp}\rangle$(or $|+_r\rangle, |-_r\rangle$) and then randomly insert into all the transmitted sequences. Eve does not recognize the positions and the states of the corresponding decoy logical qubits before the eavesdropping checks. If Eve performs the interception-resend attack, based on the characteristics of decoy logical states, we will know the probability that her attack will be found is $1 - \left(\frac{1}{2}\right)^m$ (m denotes the number of decoy logical qubits). Therefore, Eve's attack cannot pass the eavesdropping checks.

Measure-resend attack: If Eve conducts the measure-resend attack, because Eve does not know the positions and the states of the corresponding decoy logical qubits,

his measure will change the states of the decoy logical qubits. It will be discovered with the probability of $1-\left(\frac{3}{4}\right)^m$. Hence, m denotes the number of decoy logical qubits.

Entangle-measure attack: In order to implement the entangle-measure attack, Eve needs to entangle the transmitted logical qubits with her auxiliary photons $|E\rangle$. Eve performs the unitary operation U to the transmitted logical qubits and her ancillary photons $|E\rangle$. We suppose that $|e_0e_0\rangle, |e_0e_1\rangle, |e_1e_0\rangle, |e_1e_1\rangle, |e_0'e_0'\rangle, |e_0'e_1'\rangle, |e_1'e_0'\rangle, |e_1'e_1'\rangle$ are probe states. Hence, we take the collective-dephasing noise as an example. And we can get the results as follows:

$$
\begin{aligned}
U(|0_{\mathrm{dp}}|E\rangle) &= a_{00}|00\rangle|e_0e_0\rangle + a_{01}|01\rangle e_0e_1\rangle + a_{10}|10\rangle|e_1e_0\rangle + a_{11}|11\rangle|e_1e_1\rangle,\\
U(|1_{\mathrm{dp}}|E\rangle) &= b_{00}|00\rangle|e_0'e_0'\rangle + b_{01}|01\rangle|e_0'e_1'\rangle + b_{10}|10\rangle|e_1'e_0'\rangle + b_{11}|11\rangle|e_1'e_1'\rangle,\\
U(|+_{\mathrm{dp}}|E\rangle) &= \frac{1}{\sqrt{2}}[U(|0_{\mathrm{dp}}|E\rangle) + U(|1_{\mathrm{dp}}|E\rangle)]\\
&= \frac{1}{2}\big[|\phi^+(a_{00}|e_0e_0\rangle) + a_{11}|e_1e_1\rangle + b_{00}|e_0'e_0'\rangle + b_{11}|e_1'e_1'\rangle\\
&\quad + |\phi^-(a_{00}|e_0e_0\rangle) - a_{11}|e_1e_1\rangle + b_{00}|e_0'e_0'\rangle - b_{11}|e_1'e_1'\rangle\\
&\quad + |\psi^+(a_{01}|e_0e_1\rangle) + a_{10}|e_1e_0\rangle + b_{01}|e_0'e_1'\rangle + b_{10}|e_1'e_0'\rangle\\
&\quad + |\psi^-(a_{01}|e_0e_1\rangle) - a_{10}|e_1e_0\rangle + b_{01}|e_0'e_1'\rangle - b_{10}|e_1'e_0'\rangle\big],\\
U(|-_{\mathrm{dp}}|E\rangle) &= \frac{1}{\sqrt{2}}[U(|0_{\mathrm{dp}}|E\rangle) - U(|1_{\mathrm{dp}}|E\rangle)]\\
&= \frac{1}{2}\big[|\phi^+(a_{00}|e_0e_0\rangle) + a_{11}|e_1e_1\rangle - b_{00}|e_0'e_0'\rangle - b_{11}|e_1'e_1'\rangle\\
&\quad + |\phi^-(a_{00}|e_0e_0\rangle) - a_{11}|e_1e_1\rangle - b_{00}|e_0'e_0'\rangle + b_{11}|e_1'e_1'\rangle\\
&\quad + |\psi^+(a_{01}|e_0e_1\rangle) + a_{10}|e_1e_0\rangle - b_{01}|e_0'e_1'\rangle - b_{10}|e_1'e_0'\rangle\\
&\quad + |\psi^-(a_{01}|e_0e_1\rangle) - a_{10}|e_1e_0\rangle - b_{01}|e_0'e_1'\rangle + b_{10}|e_1'e_0'\rangle\big]
\end{aligned}
\tag{5}
$$

where $|a_{00}|^2+|a_{01}|^2+|a_{10}|^2+|a_{11}|^2=1$, $|b_{00}|^2+|b_{01}|^2+|b_{10}|^2+|b_{11}|^2=1$. If Eve does not intend to be detected by eavesdropping check, then U must meet four conditions: $a_{01}=b_{10}=1$, $a_{00}=a_{10}=a_{11}=0$, $b_{00}=b_{01}=b_{11}=0$ and $a_{01}|e_0e_1\rangle = b_{10}|e_1'e_0'\rangle$, because Eve cannot distinguish the auxiliary photons $a_{01}|e_0e_1\rangle$ from $b_{10}|e_1'e_0'\rangle$, that is, she cannot acquire useful information about K_A and M. Thus, our two protocols can resist the entangle-measure attack.

Double CNOT attack: As for the double CNOT attack mentioned in Gu et al. [44], Eve prepares state $|00\rangle$ in advance. When Alice and Bob transmit information, a CNOT attack is used for logical quantum bits in the channel. The attack result is shown in Eq. (6):

$$
\begin{aligned}
&\mathrm{CNOT}(1,3)\mathrm{CNOT}(2,4)|01\rangle_{12}\otimes|00\rangle_{34}=|0101\rangle_{1234},\\
&\mathrm{CNOT}(1,3)\mathrm{CNOT}(2,4)|10\rangle_{12}\otimes|00\rangle_{34}=|1010\rangle_{1234},\\
&\mathrm{CNOT}(1,3)\mathrm{CNOT}(2,4)\frac{1}{\sqrt{2}}(01\rangle+|10\rangle)_{12}\otimes|00\rangle_{34}=\frac{1}{\sqrt{2}}(|0101\rangle+|1010\rangle)_{1234},\\
&\mathrm{CNOT}(1,3)\mathrm{CNOT}(2,4)\frac{1}{\sqrt{2}}(01\rangle-|10\rangle)_{12}\otimes|00\rangle_{34}=\frac{1}{\sqrt{2}}(0101-|1010\rangle)_{1234},
\end{aligned}
\tag{6}
$$

Eve introduced entanglement in the CNOT attack on $|\pm_{dp}$, so after a CNOT attack, the entanglement error will be detected in the eavesdropping detection of Step 3. So the protocol we designed can successfully withstand double CNOT attack. And the final key acquisition depends on the classic bit string M measured in the middle. The composition of M is determined by the states held by both Alice and Bob. So the protocol we designed can successfully withstand double CNOT attack.

5 Efficiency analysis

Cabello [39] introduced the qubit efficiency of a QKA protocol is widely applied, which is given as $\eta=\frac{c}{q+b}$, where c, q, and b denote the number of the agreement classical bits, the number of qubits used, and the number of classical bits exchanged for decoding the message, respectively. Let n be the number of GHZ states and m be the number of decoy states in each transmitted quantum sequence, the qubit efficiency of our two QKA protocols is $\eta=\frac{4n}{8n+4m+4m+n+2n}$. Let $m=n$, we have $\eta=\frac{4}{17}=23.53\%$. The comparison between our protocols and several kinds of others two-party protocols against collective noise is shown in Table 4. As shown in Table 4, our protocol has better global performance in terms of quantum resource cost and qubit efficiency.

Table 4 Comparison between our protocols and the proposed two-party protocols

	Quantum resource	Quantum measurement basis	Qubit efficiency (%)
Huang et al. [28]	Logical Bell states	Z-basis and X-basis	16.67
He et al. [30]	Logical χ-states	ZZ-basis and BSM	21.05
Yang et al. [40]	Logical Bell states	Logical BSM	21.05
Ours	Logical GHZ states and logical Bell states	Logical BSM	23.53

6 Conclusion

On account of logical GHZ states and logical Bell states, we propose two two-party QKA protocols against the collective-dephasing noise and the collective-rotation noise, respectively. As we can see from the security analysis, the proposed protocol is sufficiently secure to effectively protect against common internal and external attacks. Furthermore, compared with the existing two-party QKA protocol, the protocols proposed in this paper have a higher advantage in the cost of quantum resources and the efficiency of qubits.

For future work, I have two thoughts: Firstly, we only proposed the two-party QKA protocol, which can be studied for the multi-party QKA protocol. Secondly, the protocol we propose is to assume that there is only one kind of noise exists in the channel. If there are two kinds of noise in the channel, it is interesting to study how to construct QKA protocols. Therefore, this is the direction of our future research.

Acknowledgements This work is supported by Beijing Natural Science Foundation (Grant Nos. 4182006, 4162005) and National Natural Science Foundation of China (Grant Nos. 61572053, 61472048, 61671087, U1636106, 61602019, 61502016).

References

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, pp. 175–179. New York: IEEE (1984)
2. Bennett, C.H.: Quantum cryptography using any two nonorthogonal states. Phys. Rev. Lett. **68**, 3121–3124 (1992)
3. Zhou, N., Zeng, G., Xiong, J.: Quantum key agreement protocol. Electron. Lett. **40**(18), 1149 (2004)
4. Hsueh, C.C., Chen, C.Y. In: Proceedings of the 14th Information Security Conference (ISC 2004), pp. 236–242. National Taiwan University of Science and Technology, Taipei (2004)
5. Hillery, M., Bužek, V., Berthiaume, A.: Quantum secret sharing. Phys. Rev. A **59**, 1829–1834 (1999)
6. Karlsson, A., Koashi, M., Imoto, N.: Quantum entanglement for secret sharing and secret splitting. Phys. Rev. A **59**, 162–168 (1999)
7. Boström, K., Felbinger, T.: Deterministic secure direct communication using entanglement. Phys. Rev. Lett. **89**, 187902 (2002)
8. Long, G.L., Liu, X.S.: Theoretically efficient high-capacity quantum-key-distribution scheme. Phys. Rev. A **65**, 032302 (2002)
9. 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. **42**(5), 055305 (2009)
10. Yang, Y.G., Cao, W.F., Wen, Q.Y.: Secure quantum private comparison. Phys. Scr. **80**(6), 065002 (2009)
11. Chen, X.B., Xu, G., Niu, X.X., Wen, Q.Y., Yang, Y.X.: An efficient protocol for the private comparison of equal information based on the triplet entangled state and single particle measurement. Opt. Commun. **283**(7), 1561–1565 (2010)
12. Yang, C.-W., Hwang, T.: Quantum dialogue protocols immune to collective noise. Quantum Inf. Process. **12**(6), 2131 (2013)
13. Yang, Y.-G., Liu, Z.-C., Li, J., Chen, X.-B., Zuo, H.-J., Zhou, Y.-H., Shi, W.-M.: Theoretically extensible quantum digital signature with starlike cluster states. Quantum Inf. Process. **16**(1), 1–15 (2017)
14. Yang, Y.-G., Lei, H., Liu, Z.-C., Zhou, Y.-H., Shi, W.-M.: Arbitrated quantum signature scheme based on cluster states. Quantum Inf. Process. **15**(6), 2487–2497 (2016)

15. Wang, T.-Y., Wei, Z.L.: One-time proxy signature based on quantum cryptography. Quantum Inf. Process. **11**, 455–463 (2012)
16. Wang, T.-Y., Cai, X.Q., Ren, Y.L., Zhang, R.L.: Security of quantum digital signature. Sci. Rep. **5**, 9231 (2015)
17. Diffie, W., Hellman, M.: New directions in cryptography. IEEE Trans. Inf. Theory **22**, 644–654 (1976)
18. Chong, S.K., Hwang, T.: Quantum key agreement protocol based on BB84. Opt. Commun. **283**(6), 1192–1195 (2010)
19. Shukla, C., Alam, N., Pathak, A.: Protocols of quantum key agreement solely using Bell states and Bell measurement. Quantum Inf. Process. **13**, 2391–2405 (2014)
20. Chong, S.K., Tsai, C.W., Hwang, T.: Improvement on quantum key agreement protocol with maximally entangled states. Int. J. Theor. Phys. **50**, 1793–1802 (2011)
21. Shi, R.H., Zhong, H.: Multi-party quantum key agreement with Bell states and Bell measurements. Quantum Inf. Process. **12**, 921–932 (2013)
22. Xu, G.B., Wen, Q.Y., Gao, F., Qin, S.J.: Novel multiparty quantum key agreement protocol with GHZ states. Quantum Inf. Process. **13**, 2587–2594 (2014)
23. He, Y.F., Ma, W.P.: Two-party quantum key agreement with five-particle entangled states. Int. J. Quantum Inf. **15**(03), 1750018 (2017)
24. Cai, B., Guo, G., Lin, S.: Multi-party quantum key agreement with teleportation. Mod. Phys. Lett. B **31**(10), 1750102 (2017)
25. Cao, H., Ma, W.: Multiparty quantum key agreement based on quantum search algorithm. Sci. Rep. **7**, 45046 (2017)
26. Sun, Z.W., Zhang, C., Wang, B.H., Li, Q., Long, D.Y.: Improvements on "multiparty quantum key agreement with single particles". Quantum Inf. Process. **12**, 3411–3420 (2013)
27. Kwiat, P.G., Berglund, A.J., Altepeter, J.B., White, A.G.: Experimental verification of decoherence-free subspaces. Science (New York, N.Y.) **290**(5491), 498–501 (2000)
28. Huang, W., Wen, Q.Y., Liu, B., Gao, F., Sun, Y.: Quantum key agreement with EPR pairs and single particle measurements. Quantum Inf. Process. **13**, 649–663 (2014)
29. Huang, W., Su, Q., Wu, X., Li, Y.B., Sun, Y.: Quantum key agreement against collective decoherence. Int. J. Theor. Phys. **53**, 2891 (2014)
30. He, Y.F., Ma, W.P.: Two-party quantum key agreement against collective noise. Quantum Inf. Process. **15**, 5023–5035 (2016)
31. Gao, H., Chen, X.G., Qian, S.R.: Two-party quantum key agreement protocols under collective noise channel. Quantum Inf. Process. **17**, 140 (2018)
32. Walton, Z.D., Abouraddy, A.F., Sergienko, A.V., et al.: Decoherence-free subspaces in quantum key distribution. Phys. Rev. Lett. **91**, 087901 (2003)
33. Gao, F., Qin, S.J., Wen, Q.Y., et al.: A simple participant attack on the Bradler–Dusek protocol. Quantum Inf. Comput. **7**(4), 329–334 (2007)
34. Gao, F., Guo, F.Z., Wen, Q.Y., Zhu, F.C.: Comment on "Experimental demonstration of a quantum protocol for byzantine agreement and liar detection". Phys. Rev. Lett. **101**, 208901 (2008)
35. Qin, S., Gao, F., Wen, Q., Zhu, F.: Improving the security of multiparty quantum secret sharing against an attack with a fake signal. Phys. Lett. A **357**, 101–103 (2006)
36. Deng, F.G., Long, G.L., Wang, Y., Xiao, L.: Increasing the efficiencies of random-choice-based quantum communication protocols with delayed measurement. Chin. Phys. Lett. **21**, 2097 (2004)
37. Deng, F.G., Li, X.H., Zhou, H.Y., Zhang, Z.J.: Improving the security of multiparty quantum secret sharing against Trojan horse attack. Phys. Rev. A **72**, 044302 (2005)
38. 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 **74**, 054302 (2006)
39. Cabello, A.: Quantum key distribution in the Holevo limit. Phys. Rev. Lett. **85**, 5635–5638 (2000)
40. Yang, Y.G., Gao, S., Li, D., et al.: Two-party quantum key agreement over a collective noisy channel. Quantum Inf. Process. **18**, 74 (2019)
41. Xiangbin, Wang: Fault tolerant quantum key distribution protocol with collective random unitary noise. Phys. Rev. A **72**(5), 762–776 (2005)
42. Zhou, N., Zeng, G., Zeng, W., et al.: Cross-center quantum identification scheme based on teleportation and entanglement swapping. Opt. Commun. **254**(4–6), 380–388 (2005)
43. Gui-Tong, Wu, Nan-Run, Zhou, Li-Hua, Gong, et al.: Quantum dialogue protocols with identification over collection noisy channel without information leakage. Acta Phys. Sin. **63**(6), 060302 (2014)

44. Jun, G., Po-Hua, L., Tzonelih, H.: Double C-NOT attack and counterattack on 'Three-step semi-quantum secure direct communication protocol'. Quantum Inf. Process. **17**(7), 182 (2018)