Quantum Information Processing (2019) 18:74
https://doi.org/10.1007/s11128-019-2187-8

Two-party quantum key agreement over a collective noisy channel

Yu-Guang Yang[1] · Shang Gao[1] · Dan Li[2] · Yi-Hua Zhou[1] · Wei-Min Shi[1]

Received: 5 October 2018 / Accepted: 16 January 2019 / Published online: 29 January 2019

Abstract

Quantum key agreement (QKA) allows participants to establish a shared key over a quantum channel, and no one of the participants can determine the shared key alone. Actually, particles are usually affected by noise during transmission in the quantum channel, and an aggressor can launch a baleful attack under the cover of noise. In this paper, based on logical Bell states, we propose two robust two-party QKA protocols immune to collective-dephasing noise and collective-rotation noise, respectively. The measurement correlation of quantum entanglement is utilized to establish a shared key. The proposed protocols are globally better in terms of quantum resource cost and qubit efficiency than existing two-party QKA protocols against collective noise. The security analysis demonstrates that they can resist common insider and outsider attacks.

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

1 Introduction

As a combination of classical cryptography and quantum mechanics, quantum cryptography can achieve unconditional security, where the security is provided by quantum physics laws rather than the difficulty of mathematical computation. Quantum cryptography includes many important branches such as quantum key distribution [1–3], quantum secure direct communication [4, 5], quantum secret sharing [6, 7], quantum authentication [8], quantum private comparison [9–11], quantum signature [12–15], quantum private query [16–24] and so on.

✉ Yu-Guang Yang
yangyang7357@bjut.edu.cn

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

[2] College of Computer Science and Technology, Nanjing University of Aeronautics and Astronautics, Nanjing 210016, China

Recently, key agreement has been introduced into quantum cryptography and pursued. It is aimed to establish shared keys among two or more parties where each party contributes its part to the shared key, and the shared key should not be determined fully by any party alone [25]. Since Zhou et al. proposed the first QKA protocol [26], lots of QKA schemes were proposed [27–41].

Most of QKA protocols were presented in the ideal environment [26–41]; that is, it is assumed that there is no noise in the channel. Actually, particles are usually affected by noise during transmission in the quantum channel and an aggressor can launch a baleful attack under the cover of noise. Thus, it is necessary to consider channel noise in the design of QKA protocols. Decoherence-free subspace (DFS) can help to realize reliable particle transmission under collective noise channel [42]. At present, there have been some relevant studies on robust QKA by constructing DF states [43–48]. For example, Cai et al. [43] proposed a multiparty QKA protocol against collective noise. Huang et al. [44] gave a QKA protocol and introduced two corresponding variations against collective noise. Later, they also proposed a robust QKA protocol with DF states [45]. In 2016, based on logical χ states, He et al. [46] presented two QKA protocols immune to collective noise. Using logical five-particle states, He et al. [47] proposed two robust QKA protocols. In 2018, based on four-particle logical GHZ states and logical qubits, Gao et al. [48] presented two QKA protocols under collective noise channel.

In existing schemes against collective noise, we found that these protocols usually have some drawbacks like high quantum resource cost or low efficiency. In this paper, based on logical Bell states, we propose two robust two-party QKA protocols over two kinds of collective noise channels, respectively. Our proposed QKA protocols are globally better in terms of quantum resource cost and qubit efficiency than existing two-party QKA protocols against collective noise.

The rest of this paper is organized as follows. The next section introduces relevant theoretical knowledge. In Sect. 3, we give the description of our QKA protocols in detail. Sections 4 and 5 involve the security analysis and the comparison between ours and other QKA protocols against collective noise in terms of quantum resource cost and qubit efficiency, respectively. Finally, a conclusion is given in Sect. 6.

2 Preliminaries

In this article, we discuss two types of collective noises: the collective-dephasing noise and the collective-rotation noise [42]. The collective-dephasing noise can be depicted as follows:

$$\varpi^{\theta} : |0\rangle \to |0\rangle, \quad \varpi^{\theta} : |1\rangle \to e^{i\theta}|1\rangle. \tag{1}$$

Then, the collective-rotation noise can be formalized by

$$\varpi^{\sigma} : |0\rangle \to \cos\sigma|0\rangle + \sin\sigma|1\rangle, \varpi^{\sigma} : |1\rangle \to -\sin\sigma|0\rangle + \cos\sigma|1\rangle. \tag{2}$$

where θ and σ are the fluctuation factors of the noise with time.

There are two nonorthogonal bases $\{|0\rangle, |1\rangle\}$ (Z-basis) and $\{|+\rangle, |-\rangle\}$ (X-basis), where $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. Four Bell states are defined as

$|\varphi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle)$ and $|\psi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle)$. The four Pauli operations are defined as

$$I = |0\rangle\langle 0| + |1\rangle\langle 1|, \quad X = |1\rangle\langle 0| + |0\rangle\langle 1|, \quad Z = |0\rangle\langle 0| - |1\rangle\langle 1|, \quad iY = |0\rangle\langle 1| - |1\rangle\langle 0|.$$

According to the characteristics of the collective-dephasing noise [42], the subspaces $\left\{\left|0_{dp}\right\rangle, \left|1_{dp}\right\rangle\right\}$ and $\left\{\left|+_{dp}\right\rangle, \left|-_{dp}\right\rangle\right\}$ can form a DFS against the collective-dephasing noise, where $\left|0_{dp}\right\rangle = |01\rangle$, $\left|1_{dp}\right\rangle = |10\rangle$, $\left|\pm_{dp}\right\rangle = \frac{1}{\sqrt{2}}\left(\left|0_{dp}\right\rangle \pm \left|1_{dp}\right\rangle\right) = |\psi^{\pm}\rangle$. Similarly, the subspaces $\{|0_r\rangle, |1_r\rangle\}$ and $\{|+_r\rangle, |-_r\rangle\}$ can form a DFS against the collective-rotation noise, where $|0_r\rangle = |\varphi^{+}\rangle, |1_r\rangle = |\psi^{-}\rangle$, $|\pm_r\rangle = \frac{1}{\sqrt{2}}(|0_r\rangle \pm |1_r\rangle) = \frac{1}{\sqrt{2}}(|\varphi^{+}\rangle \pm |\psi^{-}\rangle)$.

The four logical Bell states are shown as follows:

$$\left|\Phi_{dp}^{+}\right\rangle_{1234} = \frac{1}{\sqrt{2}}\left(\left|0_{dp}\right\rangle\left|0_{dp}\right\rangle + \left|1_{dp}\right\rangle\left|1_{dp}\right\rangle\right)_{1234} = \frac{1}{\sqrt{2}}(|\varphi^{+}\rangle|\varphi^{+}\rangle - |\varphi^{-}\rangle|\varphi^{-}\rangle)_{1324}, \tag{3}$$

$$\left|\Phi_{dp}^{-}\right\rangle_{1234} = \frac{1}{\sqrt{2}}\left(\left|0_{dp}\right\rangle\left|0_{dp}\right\rangle - \left|1_{dp}\right\rangle\left|1_{dp}\right\rangle\right)_{1234} = \frac{1}{\sqrt{2}}(|\varphi^{-}\rangle|\varphi^{+}\rangle - |\varphi^{+}\rangle|\varphi^{-}\rangle)_{1324}, \tag{4}$$

$$\left|\Psi_{dp}^{+}\right\rangle_{1234} = \frac{1}{\sqrt{2}}\left(\left|0_{dp}\right\rangle\left|1_{dp}\right\rangle + \left|1_{dp}\right\rangle\left|0_{dp}\right\rangle\right)_{1234} = \frac{1}{\sqrt{2}}(|\psi^{+}\rangle|\psi^{+}\rangle - |\psi^{-}\rangle|\psi^{-}\rangle)_{1324}, \tag{5}$$

$$\left|\Psi_{dp}^{-}\right\rangle_{1234} = \frac{1}{\sqrt{2}}\left(\left|0_{dp}\right\rangle\left|1_{dp}\right\rangle - \left|1_{dp}\right\rangle\left|0_{dp}\right\rangle\right)_{1234} = \frac{1}{\sqrt{2}}(|\psi^{-}\rangle|\psi^{+}\rangle - |\psi^{+}\rangle|\psi^{-}\rangle)_{1324}, \tag{6}$$

Obviously, these four logical Bell states are immune to the collective-dephasing noise. Similarly, the following four logical Bell states are resistant to the collective-rotation noise:

$$|\Phi_r^{+}\rangle_{1234} = \frac{1}{\sqrt{2}}(|0_r\rangle|0_r\rangle + |1_r\rangle|1_r\rangle)_{1234} = \frac{1}{\sqrt{2}}(|\varphi^{+}\rangle|\varphi^{+}\rangle + |\psi^{-}\rangle|\psi^{-}\rangle)_{1324}, \tag{7}$$

$$|\Phi_r^{-}\rangle_{1234} = \frac{1}{\sqrt{2}}(|0_r\rangle|0_r\rangle - |1_r\rangle|1_r\rangle)_{1234} = \frac{1}{\sqrt{2}}(|\varphi^{-}\rangle|\varphi^{-}\rangle + |\psi^{+}\rangle|\psi^{+}\rangle)_{1324}, \tag{8}$$

$$|\Psi_r^{+}\rangle_{1234} = \frac{1}{\sqrt{2}}(|0_r\rangle|1_r\rangle + |1_r\rangle|0_r\rangle)_{1234} = \frac{1}{\sqrt{2}}(|\varphi^{-}\rangle|\psi^{+}\rangle - |\psi^{+}\rangle|\varphi^{-}\rangle)_{1324}, \tag{9}$$

$$|\Psi_r^{-}\rangle_{1234} = \frac{1}{\sqrt{2}}\left(|0_r\rangle|1_r\rangle - \left|1_{dp}\right\rangle|0_r\rangle\right)_{1234} = \frac{1}{\sqrt{2}}(|\varphi^{+}\rangle|\psi^{-}\rangle - |\psi^{-}\rangle|\varphi^{+}\rangle)_{1324}. \tag{10}$$

Let us define the four unitary operations under the collective-dephasing noise as

$$U_{00}^{dp} = I \otimes I, \quad U_{01}^{dp} = Z \otimes I, \quad U_{10}^{dp} = X \otimes X, \quad U_{11}^{dp} = iY \otimes X, \tag{11}$$

and the four unitary operations under the collective-rotation noise as:

$$U_{00}^{r} = I \otimes I, \quad U_{01}^{r} = Z \otimes Z, \quad U_{10}^{r} = Z \otimes X, \quad U_{11}^{r} = I \otimes iY. \tag{12}$$

A logical quantum state against the collective-dephasing noise can be constructed as

$$\begin{aligned}
\left|\Lambda_{dp}\right\rangle &= \left|\Phi_{dp}^{+}\right\rangle_{A_1A_2B_1B_2} \otimes \left|\Phi_{dp}^{+}\right\rangle_{A_3A_4B_3B_4} \\
&= \frac{1}{\sqrt{2}}\left(\left|0_{dp}\right\rangle\left|0_{dp}\right\rangle + \left|1_{dp}\right\rangle\left|1_{dp}\right\rangle\right)_{A_1A_2B_1B_2} \otimes \frac{1}{\sqrt{2}}\left(\left|0_{dp}\right\rangle\left|0_{dp}\right\rangle + \left|1_{dp}\right\rangle\left|1_{dp}\right\rangle\right)_{A_3A_4B_3B_4} \\
&= \frac{1}{4}\left(|\varphi^+\rangle|\varphi^+\rangle|\varphi^+\rangle|\varphi^+\rangle - |\varphi^+\rangle|\varphi^+\rangle|\varphi^-\rangle|\varphi^-\rangle + |\varphi^+\rangle|\varphi^-\rangle|\varphi^+\rangle|\varphi^-\rangle\right. \\
&\quad - |\varphi^+\rangle|\varphi^-\rangle|\varphi^-\rangle|\varphi^+\rangle - |\varphi^-\rangle|\varphi^+\rangle|\varphi^+\rangle|\varphi^-\rangle + |\varphi^-\rangle|\varphi^+\rangle|\varphi^-\rangle|\varphi^+\rangle \\
&\quad - |\varphi^-\rangle|\varphi^-\rangle|\varphi^+\rangle|\varphi^+\rangle + |\varphi^-\rangle|\varphi^-\rangle|\varphi^-\rangle|\varphi^-\rangle + |\psi^+\rangle|\psi^+\rangle|\psi^+\rangle|\psi^+\rangle \\
&\quad - |\psi^+\rangle|\psi^+\rangle|\psi^-\rangle|\psi^-\rangle + |\psi^+\rangle|\psi^-\rangle|\psi^+\rangle|\psi^-\rangle - |\psi^+\rangle|\psi^-\rangle|\psi^-\rangle|\psi^+\rangle \\
&\quad - |\psi^-\rangle|\psi^+\rangle|\psi^+\rangle|\psi^-\rangle + |\psi^-\rangle|\psi^+\rangle|\psi^-\rangle|\psi^+\rangle - |\psi^-\rangle|\psi^-\rangle|\psi^+\rangle|\psi^+\rangle \\
&\quad \left. +|\psi^-\rangle|\psi^-\rangle|\psi^-\rangle|\psi^-\rangle\right)_{A_1A_3A_2A_4B_1B_3B_2B_4} \\
&= \frac{1}{2}\left(\left|\Phi_{dp}^{+}\right\rangle\left|\Phi_{dp}^{+}\right\rangle + \left|\Phi_{dp}^{-}\right\rangle\left|\Phi_{dp}^{-}\right\rangle + \left|\Psi_{dp}^{+}\right\rangle\left|\Psi_{dp}^{+}\right\rangle + \left|\Psi_{dp}^{-}\right\rangle\left|\Psi_{dp}^{-}\right\rangle\right)_{A_1A_3A_2A_4B_1B_3B_2B_4}
\end{aligned}, \tag{13}$$

and the logical quantum state against the collective-rotation noise is given by:

$$\begin{aligned}
|\Lambda_r\rangle &= |\Phi_r^+\rangle_{A_1A_2B_1B_2} \otimes |\Phi_r^+\rangle_{A_3A_4B_3B_4} \\
&= \frac{1}{\sqrt{2}}\left(|\varphi^+\rangle|\varphi^+\rangle + |\psi^-\rangle|\psi^-\rangle\right)_{A_1A_2B_1B_2} \otimes \frac{1}{\sqrt{2}}\left(|\varphi^+\rangle|\varphi^+\rangle + |\psi^-\rangle|\psi^-\rangle\right)_{A_3A_4B_3B_4} \\
&= \frac{1}{2}\left(|\Phi_r^+\rangle|\Phi_r^+\rangle + |\Phi_r^-\rangle|\Phi_r^-\rangle + |\Psi_r^+\rangle|\Psi_r^+\rangle + |\Psi_r^-\rangle|\Psi_r^-\rangle\right)_{A_1A_3A_2A_4B_1B_3B_2B_4},
\end{aligned} \tag{14}$$

where the subscripts A_i and B_i $(i = 1, 2, 3, 4)$ represent physical qubits. So $\left|\Lambda_{dp}\right\rangle$ and $|\Lambda_r\rangle$ are composed of eight physical qubits, respectively.

Table 1 shows the transformations of the four logical Bell states $\left|\Phi_L^+\right\rangle$, $\left|\Phi_L^-\right\rangle$, $\left|\Psi_L^+\right\rangle$, $\left|\Psi_L^-\right\rangle$ under U_{00}^L, U_{01}^L, U_{10}^L, U_{11}^L, respectively. Here, L represents '*dp*' or '*r*.'

3 Description of the QKA protocol

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

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

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

Table 1 Transformations between four logical Bell states

	$\left\|\Phi_L^+\right\rangle$	$\left\|\Phi_L^-\right\rangle$	$\left\|\Psi_L^+\right\rangle$	$\left\|\Psi_L^-\right\rangle$
U_{00}^L	$\left\|\Phi_L^+\right\rangle$	$\left\|\Phi_L^-\right\rangle$	$\left\|\Psi_L^+\right\rangle$	$\left\|\Psi_L^-\right\rangle$
U_{01}^L	$\left\|\Phi_L^-\right\rangle$	$\left\|\Phi_L^+\right\rangle$	$\left\|\Psi_L^-\right\rangle$	$\left\|\Psi_L^+\right\rangle$
U_{10}^L	$\left\|\Psi_L^+\right\rangle$	$\left\|\Psi_L^-\right\rangle$	$\left\|\Phi_L^+\right\rangle$	$\left\|\Phi_L^-\right\rangle$
U_{11}^L	$\left\|\Psi_L^-\right\rangle$	$\left\|\Psi_L^+\right\rangle$	$\left\|\Phi_L^-\right\rangle$	$\left\|\Phi_L^+\right\rangle$

Alice and Bob agree on the coding rules: $\left|\Phi_L^+\right\rangle$:00, $\left|\Phi_L^-\right\rangle$:01, $\left|\Psi_L^+\right\rangle$:10, $\left|\Psi_L^-\right\rangle$:11.

Step (2) Alice prepares a sequence including n quantum states

$$
\begin{aligned}
\left|\Lambda_L\right\rangle &= \left|\Phi_L^+\right\rangle_{A_1A_2B_1B_2} \otimes \left|\Phi_L^+\right\rangle_{A_3A_4B_3B_4} \\
&= \frac{1}{2}\Big(\left|\Phi_L^+\right\rangle\left|\Phi_L^+\right\rangle + \left|\Phi_L^-\right\rangle\left|\Phi_L^-\right\rangle + \left|\Psi_L^+\right\rangle\left|\Psi_L^+\right\rangle + \left|\Psi_L^-\right\rangle\left|\Psi_L^-\right\rangle\Big)_{A_1A_3A_2A_4B_1B_3B_2B_4},
\end{aligned}
$$

where L represents 'dp' or 'r,' and Alice divides these quantum states into two ordered sequences S_A and S_B, where the sequences S_A and S_B are composed of qubits $\left[\left(A_1^1, A_2^1, A_3^1, A_4^1\right), \ldots, \left(A_1^n, A_2^n, A_3^n, A_4^n\right)\right]$ and $\left[\left(B_1^1, B_2^1, B_3^1, B_4^1\right), \ldots, \left(B_1^n, B_2^n, B_3^n, B_4^n\right)\right]$, respectively. Alice prepares decoy logical qubits each of which is randomly in one of the four nonorthogonal logical states $\left\{\left|0_L\right\rangle, \left|1_L\right\rangle, \left|+_L\right\rangle, \left|-_L\right\rangle\right\}$, inserts them into S_B randomly to obtain $S_B^{'}$ and keeps a record of the inserting positions. The number of decoy states can be set to δ which is enough for eavesdropping check. Then, Alice sends $S_B^{'}$ to Bob via the quantum channel and keeps the sequence S_A herself.

Step (3) The first security check for checking eavesdropping. After Bob receives the sequence $S_B^{'}$, Alice announces the positions and the measurement basis of the decoy logical qubits. By utilizing the announced basis, Bob measures the decoy logical qubits and announces their measurement results. Alice computes the error rate by comparing the measurement results and the initial states of the decoy logical qubits. If the error rate is less than the given threshold value ε, they will perform the next step. Otherwise, Alice and Bob will terminate this protocol and restart it.

Step (4) Alice and Bob perform the measurement on qubits $\left(A_1^i, A_3^i, A_2^i, A_4^i\right)$ and $\left(B_1^i, B_3^i, B_2^i, B_4^i\right)$ with the basis $\{ \left|\Phi_L^+\right\rangle, \left|\Phi_L^-\right\rangle, \left|\Psi_L^+\right\rangle, \left|\Psi_L^-\right\rangle \}$ for $i = 1, 2, \ldots, n$, respectively. After the measurement, the quantum states in S_A and S_B collapse into the new quantum state sequences S_A^1 and S_B^1, respectively. Concretely, after the measurement, the state $\left|\Lambda_L\right\rangle$ collapses into one of the four states $\left\{\left|\Phi_L^+\right\rangle\left|\Phi_L^+\right\rangle, \left|\Phi_L^-\right\rangle\left|\Phi_L^-\right\rangle, \left|\Psi_L^+\right\rangle\left|\Psi_L^+\right\rangle, \left|\Psi_L^-\right\rangle\left|\Psi_L^-\right\rangle\right\}$. Alice and Bob can deduce the post-measurement states of each other according to the measurement correlation of Eqs. (13) and (14). According to the coding rules: $\left|\Phi_L^+\right\rangle$:00, $\left|\Phi_L^-\right\rangle$:01, $\left|\Psi_L^+\right\rangle$:10, $\left|\Psi_L^-\right\rangle$:11, Alice and Bob's post-measurement states are translated into a classical bit string $M = M_1||M_2|| \cdots ||M_n$, where $M_i \in \{00, 01, 10, 11\}$ $(i = 1, 2, \ldots, n)$. For example, if the post-measurement state of Alice's and Bob's qubits is $\left|\Phi_L^+\right\rangle$, they can translate it into $M_i = 00$. The similar conclusions can be obtained for other post-measurement states.

Step (5) Alice can encode the key K_A^i by performing the unitary operation $U_{K_A^i}^L$ on her ith post-measurement state in S_A^1 to obtain the encoded quantum state sequence S_A^2. Later, Alice selects a permutation operator Π_n randomly and performs the permutation operator Π_n on S_A^2 to obtain the new quantum state sequence S_A^3. Then, Alice randomly selects δ decoy states from $\left\{|0_L\rangle, |1_L\rangle, |+_L\rangle, |-_L\rangle\right\}$, inserts them into S_A^3 randomly to obtain the new quantum state sequence $S_A^{3'}$ and keeps a record of the inserting positions. Alice sends $S_A^{3'}$ to Bob via the quantum channel.

Step (6) Similar to the first security check, two parties perform the second eavesdropping check after Bob receives the sequence $S_A^{3'}$.

Step (7) Bob informs Alice the value $K_B^{'} = \left\{K_B^1 \oplus M_1, K_B^2 \oplus M_2, \ldots, K_B^n \oplus M_n\right\}$. So according to the value M, Alice can derive the key K_B.

Step (8) Alice publishes the permutation operator Π_n so that Bob applies its inverse permutation on the sequence S_A^3 to obtain S_A^2 and then measures these states. By comparing his measurement results and his post-measurement states obtained in step (4), Bob can deduce K_A according to Table 1. For example, if his post-measurement state in step (4) is $\left|\Phi_L^+\right\rangle$ and his post-measurement state in step (8) is $\left|\Phi_L^-\right\rangle$, Bob can infer Alice's operation $U_{K_A^i}^L$ is U_{01}^L and obtain Alice's key bits $K_A^i = 01$.

Step (9) Alice and Bob compute the shared key $K_{AB} = \left(K_A \oplus K_B\right) || \left(K_A \oplus K_B \oplus M\right)$.

4 Security analysis

In this section, we will discuss the security of the protocol. The security analysis shows that the proposed QKA protocol can resist common attacks from the internal and external attackers. For the outsider eavesdropper Eve, she maybe tries to obtain Alice and Bob's agreement key K_{AB} by taking various attacks including the passive attack and the active attack.

4.1 Outsider attack

4.1.1 Active attack from the outside eavesdropper

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

Trojan horse attacks

Trojan horse attack is a common attack in classical cryptography. Trojan horse attack may be generated from the drawback of construction of the system (e.g., device, computer program, algorithm or protocol). When a Trojan horse is hidden without easy detection in a system, the attacker can break the system and obtain useful information by employing Trojan horses.

Unfortunately, this attack is also available in quantum cryptography [49–53]. Trojan horse attacks are major threats for two-way quantum communication protocols [49–53]. There are several kinds of common Trojan horse attacks such as the general Trojan horse attack [49], the invisible-photon Trojan horse attack [50], the large pulse attack [51] and the delay-photon Trojan horse attack [52, 53]. The first one is the general Trojan horse attack [49], in which Eve sends a light pulse to Alice, same as Bob. The second one is the invisible-photon Trojan horse attack [50]. Its main idea is that Eve inserts an invisible photon in each signal prepared by Bob and sends it to Alice. As Alice's detector cannot click this photon and performs a unitary operation on each signal, Eve can steal the information about Alice's operation by means that she intercepts the signal operated and separates the invisible photon from each signal. With the measurement on the invisible photon, Eve can read out Alice's information. The third one is the so-called large pulse Trojan horse attack [51], in which Eve probes the properties of a component inside Alice or Bob by sending in a bright pulse and analyzing a suitable back-reflected pulse. The last one is the delay-photon Trojan horse attack [52, 53]. Concretely, Eve intercepts the signal transmitted from Bob to Alice and then inserts a fake photon in the signal with a delay time, shorter than the time windows [49]. In this way, Alice cannot detect this fake photon as it does not click Alice's detector. After the operation done by Alice, Eve intercepts the signal again and separates the fake photon. She can get the full information about Alice's operation with measurement. To prevent those attacks, a photon number splitter (PNS:50/50) and a wavelength filter can be used. In practice, PNS is not easy to be implemented with current technology [49], and a photon beam splitter (PBS:50/50) can be used to replace the PNS. In this way, a PBS and a wavelength filter can be used to protect the two-way quantum communication protocols against these types of Trojan horse attacks.

In the proposed QKA protocol, since each particle is transmitted only once via the quantum channel. Thus, the proposed QKA protocol can resist Trojan horse attacks.

Intercept-resend attack

In this paper, the decoy particles are chosen randomly from four nonorthogonal logical quantum states $\left\{|0_L\rangle, |1_L\rangle, |+_L\rangle, |-_L\rangle\right\}$ and then randomly inserted into the transmitted sequences. Eve does not know the positions and the states of the decoy logical qubits before the eavesdropping check. If Eve performs the intercept-resend attack and measures it randomly with the basis $\left\{|0_L\rangle, |1_L\rangle\right\}$ or $\left\{|+_L\rangle, |-_L\rangle\right\}$, similar to the BB84 protocol [1], her attack will be discovered with the probability of $1-\left(\frac{3}{4}\right)^{\delta}$. Here, δ denotes the number of decoy logical qubits.

Entangle-measure attack

In this attack, Eve uses an auxiliary particle to interact with the travel particles and measures the auxiliary particle to get some useful information. Later, it will be shown that Eve cannot achieve any information about the message in the condition that no errors are to occur. In the eavesdropping process, Eve adds the ancilla $|E\rangle$ and performs the unitary operation U on the transmitted logical qubits and her ancillary qubits $|E\rangle$. Here, we take the collective-dephasing noise as an example. The similar conclusion can be obtained for the collective-rotation noise. The most general operation U Eve can do can be written as:

$$U\left(\left|0_{dp}\right\rangle|E\rangle\right)=a_{00}|00\rangle\left|e_0e_0\right\rangle+a_{01}|01\rangle\left|e_0e_1\right\rangle+a_{10}|10\rangle\left|e_1e_0\right\rangle+a_{11}|11\rangle\left|e_1e_1\right\rangle, \tag{15}$$

$$U\left(\left|1_{dp}\right\rangle|E\rangle\right)=b_{00}|00\rangle\left|e_0^{'}e_0^{'}\right\rangle+b_{01}|01\rangle\left|e_0^{'}e_1^{'}\right\rangle+b_{10}|10\rangle\left|e_1^{'}e_0^{'}\right\rangle+b_{11}|11\rangle\left|e_1^{'}e_1^{'}\right\rangle, \tag{16}$$

$$\begin{aligned}U\left(\left|+_{dp}\right\rangle|E\rangle\right)&=\frac{1}{\sqrt{2}}\left(U\left(\left|0_{dp}\right\rangle|E\rangle\right)+U\left(\left|1_{dp}\right\rangle|E\rangle\right)\right)\\&=\frac{1}{2}\left[\left|\varphi^+\right\rangle\left(a_{00}\left|e_0e_0\right\rangle+a_{11}\left|e_1e_1\right\rangle+b_{00}\left|e_0^{'}e_0^{'}\right\rangle+b_{11}\left|e_1^{'}e_1^{'}\right\rangle\right)\right.\\&\quad+\left|\varphi^-\right\rangle\left(a_{00}\left|e_0e_0\right\rangle-a_{11}\left|e_1e_1\right\rangle+b_{00}\left|e_0^{'}e_0^{'}\right\rangle-b_{11}\left|e_1^{'}e_1^{'}\right\rangle\right)\\&\quad+\left|\psi^+\right\rangle\left(a_{01}\left|e_0e_1\right\rangle+a_{10}\left|e_1e_0\right\rangle+b_{01}\left|e_0^{'}e_1^{'}\right\rangle+b_{10}\left|e_1^{'}e_0^{'}\right\rangle\right)\\&\quad\left.+\left|\psi^-\right\rangle\left(a_{01}\left|e_0e_1\right\rangle-a_{10}\left|e_1e_0\right\rangle+b_{01}\left|e_0^{'}e_1^{'}\right\rangle-b_{10}\left|e_1^{'}e_0^{'}\right\rangle\right)\right],\end{aligned} \tag{17}$$

$$\begin{aligned}U\left(\left|-_{dp}\right\rangle|E\rangle\right)&=\frac{1}{\sqrt{2}}\left(U\left(\left|0_{dp}\right\rangle|E\rangle\right)-U\left(\left|1_{dp}\right\rangle|E\rangle\right)\right)\\&=\frac{1}{2}\left[\left|\varphi^+\right\rangle\left(a_{00}\left|e_0e_0\right\rangle+a_{11}\left|e_1e_1\right\rangle-b_{00}\left|e_0^{'}e_0^{'}\right\rangle+b_{11}\left|e_1^{'}e_1^{'}\right\rangle\right)\right.\\&\quad+\left|\varphi^-\right\rangle\left(a_{00}\left|e_0e_0\right\rangle-a_{11}\left|e_1e_1\right\rangle-b_{00}\left|e_0^{'}e_0^{'}\right\rangle-b_{11}\left|e_1^{'}e_1^{'}\right\rangle\right)\\&\quad+\left|\psi^+\right\rangle\left(a_{01}\left|e_0e_1\right\rangle+a_{10}\left|e_1e_0\right\rangle-b_{01}\left|e_0^{'}e_1^{'}\right\rangle+b_{10}\left|e_1^{'}e_0^{'}\right\rangle\right)\\&\quad\left.+\left|\psi^-\right\rangle\left(a_{01}\left|e_0e_1\right\rangle-a_{10}\left|e_1e_0\right\rangle-b_{01}\left|e_0^{'}e_1^{'}\right\rangle-b_{10}\left|e_1^{'}e_0^{'}\right\rangle\right)\right],\end{aligned} \tag{18}$$

where $\left|e_ie_j\right\rangle$ and $\left|e_i^{'}e_j^{'}\right\rangle$ $(i,j\in\{0,1\})$ are the pure ancilla's states determined uniquely by the unitary operation U. According to the normalization and orthogonality of quantum states, it should be satisfied, i.e.,

$$\begin{aligned}&\langle E|\left\langle 0_{dp}\right|U^+U\left|1_{dp}\right\rangle|E\rangle\\&\quad=\left(a_{00}|00\rangle\left|e_0e_0\right\rangle+a_{01}|01\rangle\left|e_0e_1\right\rangle+a_{10}|10\rangle\left|e_1e_0\right\rangle+a_{11}|11\rangle\left|e_1e_1\right\rangle\right)^+\\&\left(b_{00}|00\rangle\left|e_0^{'}e_0^{'}\right\rangle+b_{01}|01\rangle\left|e_0^{'}e_1^{'}\right\rangle+b_{10}|10\rangle\left|e_1^{'}e_0^{'}\right\rangle+b_{11}|11\rangle\left|e_1^{'}e_1^{'}\right\rangle\right)=0.\end{aligned} \tag{19}$$

According to the unitary property, $UU^{+} = I$, it should be satisfied, i.e.,

$$\sum_{i,j=0,1} \left|a_{ij}\right|^{2} \left\langle e_{i}e_{j}|e_{i}e_{j}\right\rangle = 1, \quad \sum_{i,j=0,1} \left|b_{ij}\right|^{2} \left\langle e_{i}^{'}e_{j}^{'}|e_{i}^{'}e_{j}^{'}\right\rangle = 1. \tag{20}$$

For every transmitted decoy logical quantum state, the action of Eve's eavesdropping will introduce an error rate

$$P_{e}^{0} = 1 - \left|\langle E|\left\langle 0_{dp}\right|U\left(\left|0_{dp}\right\rangle|E\rangle\right)\right|^{2} = 1 - \left|a_{01}\right|^{2}\langle e_{0}e_{1}|e_{0}e_{1}\rangle, \tag{21}$$

$$P_{e}^{1} = 1 - \left|\langle E|\left\langle 1_{dp}\right|U\left(\left|1_{dp}\right\rangle|E\rangle\right)\right|^{2} = 1 - \left|b_{10}\right|^{2}\left\langle e_{1}^{'}e_{0}^{'}|e_{1}^{'}e_{0}^{'}\right\rangle, \tag{22}$$

$$\begin{aligned} P_{e}^{+} &= 1 - \left|\langle E|\left\langle +_{dp}\right|U\left(\left|+_{dp}\right\rangle|E\rangle\right)\right|^{2} \\ &= 1 - \frac{1}{4}\left(a_{01}^{*}\langle e_{0}e_{1}| + a_{10}^{*}\langle e_{1}e_{0}| + b_{01}^{*}\left\langle e_{0}^{'}e_{1}^{'}\right| + b_{10}^{*}\left\langle e_{1}^{'}e_{0}^{'}\right|\right) \\ &\quad \left(a_{01}\left|e_{0}e_{1}\right\rangle + a_{10}\left|e_{1}e_{0}\right\rangle + b_{01}\left|e_{0}^{'}e_{1}^{'}\right\rangle + b_{10}\left|e_{1}^{'}e_{0}^{'}\right\rangle\right), \end{aligned} \tag{23}$$

$$\begin{aligned} P_{e}^{-} &= 1 - \left|\langle E|\left\langle -_{dp}\right|U\left(\left|-_{dp}\right\rangle|E\rangle\right)\right|^{2} \\ &= 1 - \frac{1}{4}\left(a_{01}^{*}\langle e_{0}e_{1}| - a_{10}^{*}\langle e_{1}e_{0}| - b_{01}^{*}\left\langle e_{0}^{'}e_{1}^{'}\right| - b_{10}^{*}\left\langle e_{1}^{'}e_{0}^{'}\right|\right) \\ &\quad \left(a_{01}\left|e_{0}e_{1}\right\rangle - a_{10}\left|e_{1}e_{0}\right\rangle - b_{01}\left|e_{0}^{'}e_{1}^{'}\right\rangle - b_{10}\left|e_{1}^{'}e_{0}^{'}\right\rangle\right), \end{aligned} \tag{24}$$

where P_{e}^{0}, P_{e}^{1}, P_{e}^{+} and P_{e}^{-} are the error rate introduced by Eve's eavesdropping on decoy logical quantum states $\left|0_{L}\right\rangle, \left|1_{L}\right\rangle, \left|+_{L}\right\rangle, \left|-_{L}\right\rangle$, respectively. In other words, P_{e}^{0}, P_{e}^{1}, P_{e}^{+} and P_{e}^{-} are the probabilities of the decoy logical quantum states being changed after Eve applies the unitary operation U on the decoy logical quantum states $\left|0_{L}\right\rangle, \left|1_{L}\right\rangle, \left|+_{L}\right\rangle, \left|-_{L}\right\rangle$ and her ancillary qubits $|E\rangle$ in Eqs. (15)–(18), respectively.

Eve is supposed to be clever enough to prevent Alice and Bob from detecting her eavesdropping by finding the discrepancy in the error rates of quantum states, i.e.,

$$P_{e}^{0} = P_{e}^{1} = P_{e}^{+} = P_{e}^{-} = p_{e}. \tag{25}$$

If Eve tries to achieve the eavesdropping without being detected, then the error rate p_{e} has to be zero in the ideal environment. From Eqs. (19) to (25), we obtain the following equations

$$\begin{aligned} &\left|a_{01}\right|^{2}\langle e_{0}e_{1}|e_{0}e_{1}\rangle = 1, \quad \left|b_{10}\right|^{2}\left\langle e_{1}^{'}e_{0}^{'}|e_{1}^{'}e_{0}^{'}\right\rangle = 1 \\ &\left|e_{0}e_{0}\right\rangle = \left|e_{1}e_{0}\right\rangle = \left|e_{1}e_{1}\right\rangle = \mathrm{O}, \quad \left|e_{0}^{'}e_{0}^{'}\right\rangle = \left|e_{0}^{'}e_{1}^{'}\right\rangle = \left|e_{1}^{'}e_{1}^{'}\right\rangle = \mathrm{O}. \end{aligned} \tag{26}$$

As a result, from Eq. (26), we find that the whole system involving the transmitted logical qubits and her ancillary photons $|E\rangle$ in Eqs. (15)–(18) are in a tensor-product state. This implies that it is impossible for Eve to pass the two security checks by entangling the ancilla with the travel particles and measuring it without introducing any error. Thus, Eve cannot derive the useful information about M and K_A.

4.1.2 Passive attack from the outside eavesdropper

After the information $K_{\mathrm{B}}^{'}$ is published, Eve may attempt to gain the shared secret key. However, she cannot get any information about the measurement results of M and infer Alice or Bob's secret key. So it is not possible for Eve to obtain the final shared secret key.

4.2 Participant attack

The participant attack is first proposed by Gao et al. [54–56]. The participant attack means that the legal participant instead of the outsider eavesdropper may be dishonest and try to perform an attack for his own purpose. The purpose of the participant is different for different quantum cryptography protocols. For example, for QKA protocols, the dishonest participant may hope to control the shared secret key and determine it fully by himself alone.

Next, we will analyze the security against possible malicious Alice or Bob. Assume Bob is dishonest. In this case, Alice is assumed to be honest. Although Bob can decode K_A by measuring the particles once they are received, and then decide the corresponding K_B to generate his favorite K_{AB}, without the correct permutation operator Π_n of Alice, he can only decode K_A accurately with the probability $\frac{1}{n!}$. Even though Bob uses the wrong permutation operator Π_n, he can also obtain two bits of K_A correctly with probability 1/4. Accordingly, to control the 2n-bit shared key K_{AB} as well as to perform the security check (via 2m-bit checking sets C), Bob succeeds only with the probability $\left(\frac{1}{4}\right)^n$, which is negligible.

Next we assume Alice is dishonest. In this case, Bob is assumed to be honest. Upon receiving K_B from Bob in step (6), if Alice wants to control K_{AB}, she needs to modify her key K_A appropriately. However, Alice can only get the key K_B after Alice has sent the encoded message qubits.

Therefore, Alice or Bob's participant attack will not succeed.

5 Comparison with other two-party QKA protocols against collective noise

In this section, we consider the Cabello's qubit efficiency [57] of our QKA protocols. It is defined as $\eta = \frac{c}{q+b}$, where c, q and b are the number of the agreement classical bits, the number of qubits used and the number of classical bits exchanged for decoding, respectively. Let n be the number of eight-particle states and δ be the number of decoy states in each transmitted quantum sequence, the qubit efficiency of our first QKA protocol is $\eta = \frac{4n}{8n+4\delta+4\delta+n+2n}$. Let $\delta = n$, we have $\eta = \frac{4}{19} = 21.05\%$.

Table 2 gives the comparisons among several kinds of two-party QKA protocols against collective noise. There are so many indicators for evaluating the performance of QKA protocols such as the difficulty of preparing quantum states, quantum resource cost, the difficulty of necessary quantum operations, quantum efficiency, one-way or two-way quantum communication and so on. Therefore, it is rather difficult to evaluate the performance of QKA protocols precisely and quantitatively and it is also very difficult to provide a precise weight to the importance of these indicators. It is more rational to evaluate the performance of QKA protocols in a qualitative way.

As is shown in Table 2, although the proposed protocol does not have the highest qubit efficiency in existing two-party QKA schemes against collective noise, they are globally better in terms of quantum resource cost and qubit efficiency. We define the meaning of a protocol being 'globally better in terms of quantum resource cost and qubit efficiency' in a qualitative way. Concretely, we first rank the QKA protocols in Table 2 in terms of each indicator. For example, we rank the QKA protocols in terms of the size of the qubit efficiency and also rank the QKA protocols in terms of the difficulty of performing measurements and so on. Then, we sum the ranks of all the indicators of each QKA protocol and make a rank. If the value is smallest for some QKA protocol, it shows that this protocol is globally the best. The rest can be done in the same manner. Therefore, in terms of the qubit efficiency, our proposed protocol is runner-up. However, in other aspects such as the preparation of quantum states, the difficulty of performing measurements, it is easier to implement our protocol than other QKA protocols against collective noise. Therefore, our protocol is globally better in terms of quantum resource cost and qubit efficiency.

Table 2 Comparisons among several kinds of QKA protocols against collective noise

	Quantum resource	Quantum measurement basis	Operation	Qubit efficiency (%)
[44]	Logical Bell states	Z-basis and X-basis	CNOT	16.67
[45]	Four-qubit DF states	$ZZXX$-basis and $XZXZ$-basis	Permutation	10
[46]	Logical χ-states	ZZ-basis and BSM	CNOT and permutation	21.05
[47]	Logical five-particle states	ZZ-basis and BSM	CNOT and permutation	20
[48]	Logical GHZ states and logical Bell states	Z-basis, X-basis and BSM	CNOT	26.67
Ours	Logical Bell states	Logical BSM	Permutation	21.05

6 Conclusion

Based on logical Bell states, we propose two QKA protocols against the collective-dephasing noise and the collective-rotation noise, respectively. Compared with existing two-party QKA protocols against collective noise, the proposed protocols are globally better in terms of quantum resource cost and qubit efficiency. The security analysis shows that the proposed protocols are secure enough and can effectively resist common insider and outsider attacks.

For future work, there are several open questions. Firstly, here we only proved the security of the proposed QKA protocol against common inside and outside attacks, and its security has not been studied by strict mathematical proof. It would be interesting to study how to give a mathematical proof of the proposed QKA protocol [58–131]. Therefore, we take it as an open problem and will make the further study in the future. Secondly, we only proposed a two-party QKA protocol, and the generalization to multiparty QKA has not been studied. Therefore, it is also interesting to study how to construct robust multiparty QKA protocols. Finally, in the proposed protocols, the quantum resource cost and qubit efficiency are not optimal. Therefore, the optimization of the proposed protocols should be performed in the future.

Acknowledgements This work was supported by the National Natural Science Foundation of China (Grant No. 61572053); Beijing Natural Science Foundation (Grant No. 4182006); the National Natural Science Foundation of China (Grant Nos. 61671087, U1636106, 61602019, 61571226, 61701229,61702367); Natural Science Foundation of Jiangsu Province, China (Grant No. BK20170802); Jiangsu postdoctoral science foundation.

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. IEEE, New York (1984)
2. Ekert, A.: Quantum cryptography based on Bell's theorem. Phys. Rev. Lett. **67**, 661–664 (1991)
3. Bennett, C.H.: Quantum cryptography using any two nonorthogonal states. Phys. Rev. Lett. **68**, 3121–3124 (1992)
4. Boström, K., Felbinger, T.: Deterministic secure direct communication using entanglement. Phys. Rev. Lett. **89**, 187902 (2002)
5. Deng, F.G., Long, G.L., Liu, X.S.: Two-step quantum direct communication protocol using the Einstein–Podolsky–Rosen pair block. Phys. Rev. A **68**, 042317 (2003)
6. Hillery, M., Bužek, V., Berthiaume, A.: Quantum secret sharing. Phys. Rev. A **59**, 1829–1834 (1999)
7. Karlsson, A., Koashi, M., Imoto, N.: Quantum entanglement for secret sharing and secret splitting. Phys. Rev. A **59**, 162–168 (1999)
8. Dušek, M., Haderka, O., Hendrych, M., Myska, R.: Quantum identification system. Phys. Rev. A **60**, 149–156 (1999)
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, 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)
13. 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)
14. Jiang, D.-H., Xu, Y.-L., Xu, G.-B.: Arbitrary quantum signature based on local indistinguishability of orthogonal product states. Int. J. Theor. Phys. (2019). https://doi.org/10.1007/s10773-018-03995-4
15. Wang, T.-Y., Cai, X.Q., Ren, Y.L., Zhang, R.L.: Security of quantum digital signature. Sci. Rep. **5**, 9231 (2015)
16. Gao, F., Liu, B., Huang, W., Wen, Q.Y.: Postprocessing of the oblivious key in quantum private query. IEEE. J. Sel. Top. Quant. **21**, 6600111 (2015)
17. Wei, C.Y., Wang, T.Y., Gao, F.: Practical quantum private query with better performance in resisting joint-measurement attack. Phys. Rev. A **93**, 042318 (2016)
18. Yang, Y.-G., Liu, Z.-C., Chen, X.-B., Zhou, Y.-H., Shi, W.-M.: Robust QKD-based private database queries based on alternative sequences of single-qubit measurements. Sci. Chin. Phys. Mech. Astron. **60**(12), 120311 (2017)
19. Yang, Y.-G., Liu, Z.-C., Li, J., Chen, X.-B., Zuo, H.-J., Zhou, Y.-H., Shi, W.-M.: Quantum private query with perfect user privacy against a joint-measurement attack. Phys. Lett. A **380**(48), 4033–4038 (2016)
20. Yang, Y.-G., Liu, Z.C., Chen, X.B., Cao, W.F., Zhou, Y.H., Shi, W.M.: Novel classical post-processing for quantum key distribution-based quantum private query. Quantum Inf. Process. **15**, 3833–3840 (2016)
21. Gao, F., Liu, B., Wen, Q.-Y.: Flexible quantum private queries based on quantum key distribution. Opt. Exp. **20**, 17411–17420 (2012)
22. Yang, Y.-G., Sun, S.-J., Xu, P., Tian, J.: Flexible protocol for quantum private query based on B92 protocol. Quantum Inf. Process. **13**, 805–813 (2014)
23. Gao, F., Qin, S.J., Huang, W., Wen, Q.Y.: Quantum private query: a new kind of practical quantum cryptographic protocols. Sci. China-Phys. Mech. Astron. **62**, 070301 (2019)
24. Yang, Y.-G., Guo, X.-P., Xu, G., Chen, X.-B., Li, J., Zhou, Y.-H., Shi, W.-M.: Reducing the communication complexity of quantum private database queries by subtle classical post-processing with relaxed quantum ability. Comput. Secur. **81**, 15–24 (2019)
25. Diffie, W., Hellman, M.: New directions in cryptography. IEEE Trans. Inf. Theory **22**, 644–654 (1976)
26. Zhou, N., Zeng, G., Xiong, J.: Quantum key agreement protocol. Electron. Lett. **40**(18), 1149 (2004)
27. Tsai, C.W., Hwang, T.: On quantum key agreement protocol, Technical Report, CS-I-E, NCKU, Taiwan, ROC, 2009
28. Chong, S.K., Hwang, T.: Quantum key agreement protocol based on BB84. Opt. Commun. **283**, 1192–1195 (2010)
29. He, Y.F., Ma, W.P.: Two-party quantum key agreement with five-particle entangled states. Int. J. Quantum Inf. **15**(03), 1750018 (2017)
30. Cai, B., Guo, G., Lin, S.: Multi-party quantum key agreement with teleportation. Mod. Phys. Lett. B **31**(10), 1750102 (2017)
31. Cao, H., Ma, W.: Multiparty quantum key agreement based on quantum search algorithm. Sci. Rep. **7**, 45046 (2017)
32. Shi, R.H., Zhong, H.: Multi-party quantum key agreement with Bell states and Bell measurements. Quantum Inf. Process. **12**, 921–932 (2013)
33. Liu, B., Gao, F., Huang, W., Wen, Q.-Y.: Multiparty quantum key agreement with single particles. Quantum Inf. Process. **12**, 1797–1805 (2013)
34. 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)
35. 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)

36. Sun, Z.W., Yu, J.P., Wang, P.: Efficient multi-party quantum key agreement by cluster States. Quantum Inf. Process. **15**, 373–384 (2016)
37. He, Y.-F., Ma, W.-P.: Quantum key agreement protocols with four-qubit cluster states. Quantum Inf. Process. **14**, 3483–3498 (2015)
38. Sun, Z.W., Zhang, C., Wang, P., Yu, J.P., Zhang, Y., Long, D.Y.: Multi-party quantum key agreement by an entangled six-qubit state. Int. J. Theor. Phys. **55**, 1920–1929 (2016)
39. Huang, W., Wen, Q.-Y., Liu, B., Su, Q., Gao, F.: Cryptanalysis of a multi-party quantum key agreement protocol with single particles. Quantum Inf. Process. **13**, 1651–1657 (2014)
40. Huang, W., Su, Q., Xu, B.J., Liu, B., Fan, F., Jia, H.Y., Yang, Y.H.: Improved multiparty quantum key agreement in travelling mode. Sci. Chin. Phys. Mech. Astron. **59**(12), 120311 (2016)
41. 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)
42. 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)
43. Cai, B., Guo, G., Lin, S., Zuo, H., Yu, C.: Multipartite quantum key agreement over collective noise channels. IEEE Photonics J. **10**(1), 1–11 (2018)
44. 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)
45. Huang, W., Su, Q., Wu, X., Li, Y.B., Sun, Y.: Quantum key agreement against collective decoherence. Int. J. Theor. Phys. **53**, 2891 (2014)
46. He, Y.F., Ma, W.P.: Two-party quantum key agreement against collective noise. Quantum Inf. Process. **15**, 5023–5035 (2016)
47. He, Y.-F., Ma, W.-P.: Two quantum key agreement protocols immune to collective noise. Int. J. Theor. Phys. **56**, 328–338 (2017)
48. Gao, H., Chen, X.G., Qian, S.R.: Two-party quantum key agreement protocols under collective noise channel. Quantum Inf. Process. **17**, 140 (2018)
49. Gisin, N., Fasel, S., Kraus, B., Zbinden, H., Ribordy, G.: Trojan-horse attacks on quantum-key distribution systems. Phys. Rev. A **73**, 022320 (2006)
50. Cai, Q.Y.: Eavesdropping on the two-way quantum communication protocols with invisible photons. Phys. Lett. A **351**, 23–25 (2006)
51. Vakhitov, A., Makarov, V., Hjelme, D.R.: Large pulse attack as a method of conventional optical eavesdropping in quantum cryptography. J. Mod. Opt. **48**, 2023–2038 (2001)
52. 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)
53. Deng, F.G., Zhou, P., Li, X.H., et al.: Robustness of two-way quantum communication protocols against Trojan horse attack. arXiv:quant-ph/0508168
54. Gao, F., Qin, S.J., Wen, Q.Y., Zhu, F.C.: A simple participant attack on the Brádler–Dušek protocol. Quantum Inf. Comput. **7**, 329–334 (2007)
55. Gao, F., Guo, F.Z., Wen, Q.Y., Zhu, F.C.: Comment on "Experimental demonstration of a quantum protocol for byzantine agreement and liar detectio". Phys. Rev. Lett. **101**, 208901 (2008)
56. 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)
57. Cabello, A.: Quantum key distribution in the Holevo limit. Phys. Rev. Lett. **85**, 5635–5638 (2000)
58. Jiang, D.-H., Wang, X.-J., Xu, G.-B., Lin, J.-Q.: A denoising-decomposition model combining TV minimisation and fractional derivatives. East Asia J. Appl. Math. **8**, 447–462 (2018)
59. Li, L., Wang, Z., Li, Y.X., Shen, H., Lu, J.W.: Hopf bifurcation analysis of a complex-valued neural network model with discrete and distributed delays. Appl. Math. Comput. **330**, 152–169 (2018)
60. Liang, X., Gao, F., Zhou, C.-B., Wang, Z., Yang, X.-J.: An anomalous diffusion model based on a new general fractional operator with the Mittag-Leffler function of Wiman type. Adv. Differ. Eqn. **2018**, 25 (2018)
61. Wang, J., Liang, K., Huang, X., Wang, Z., Shen, H.: Dissipative fault-tolerant control for nonlinear singular perturbed systems with Markov jumping parameters based on slow state feedback. Appl. Math. Comput. **328**, 247–262 (2018)
62. Zhou, J.P., Sang, C.Y., Li, X., Fang, M.Y., Wang, Z.: H∞ consensus for nonlinear stochastic multi-agent systems with time delay. Appl. Math. Comput. **325**, 41–58 (2018)
63. Hu, Q.Y., Yuan, L.: A plane wave method combined with local spectral elements for nonhomogeneous Helmholtz equation and time-harmonic Maxwell equations. Adv. Comput. Math. **44**(1), 245–275 (2018)

64. Liu, F.: Rough maximal functions supported by subvarieties on Triebel-Lizorkin spaces, Revista de la Real Academia de Ciencias Exactas. Fisicas y Naturales. Serie A. Math. **112**(2), 593–614 (2018)
65. Wang, W., Zhang, T.Q.: Caspase-1-mediated pyroptosis of the predominance for driving CD4++ T cells death: a nonlocal spatial mathematical model. Bull. Math. Biol. **80**(3), 540–582 (2018)
66. Li, H.J., Zhu, Y.L., Liu, J., Wang, Y.: Consensus of second-order delayed nonlinear multi-agent systems via node-based distributed adaptive completely intermittent protocols. Appl. Math. Comput. **326**, 1–15 (2018)
67. Cui, Y.J., Ma, W.J., Sun, Q., Su, X.W.: New uniqueness results for boundary value problem of fractional differential equation. Nonlinear Anal. Model. Control **23**(1), 31–39 (2018)
68. Cui, Y.J., Ma, W.J., Wang, X.Z., Su, X.W.: Uniqueness theorem of differential system with coupled integral boundary conditions. Electron. J. Qual. Theory Differ. Equ. **9**, 1–10 (2018)
69. Ma, W.-X.: Conservation laws by symmetries and adjoint symmetries. Discrete. Contin. Dyn. Syst. Ser. S **11**(4), 707–721 (2018)
70. Ma, W.-X., Yong, X.L., Zhang, H.-Q.: Diversity of interaction solutions to the (2+1)-dimensional Ito equation. Comput. Math. Appl. **75**(1), 289–295 (2018)
71. Ma, W.-X., Zhou, Y.: Lump solutions to nonlinear partial differential equations via Hirota bilinear forms. J. Differ. Equ. **264**(4), 2633–2659 (2018)
72. McAnally, M., Ma, W.-X.: An integrable generalization of the D-Kaup–Newell soliton hierarchy and its bi-Hamiltonian reduced hierarchy. Appl. Math. Comput. **323**, 220–227 (2018)
73. Lu, C.N., Fu, C., Yang, H.W.: Time-fractional generalized boussinesq equation for rossby solitary waves with dissipation effect in stratified fluid and conservation laws as well as exact solutions. Appl. Math. Comput. **327**, 104–116 (2018)
74. Liu, F.: Continuity and approximate differentiability of multisublinear fractional maximal functions. Math. Inequal. Appl. **21**(1), 25–40 (2018)
75. Wang, J., Cheng, H., Li, Y., et al.: The geometrical analysis of a predator-prey model with multistate dependent impulsive. J. Appl. Anal. Comput. **8**(2), 427–442 (2018)
76. Chen, J., Zhang, T., Zhang, Z.Y., Lin, C., Chen, B.: Stability and output feedback control for singular Markovian jump delayed systems. Math. Control Relat. Fields **8**(2), 475–490 (2018)
77. Xu, X.-X., Sun, Y.-P.: Two symmetry constraints for a generalized Dirac integrable hierarchy. J. Math. Anal. Appl. **458**, 1073–1090 (2018)
78. Shen, H., Song, X.N., Li, F., Wang, Z., Chen, B.: Finite-time L2-L∞ filter design for networked Markov switched singular systems: a unified method. Appl. Math. Comput. **321**(15), 450–462 (2018)
79. Wang, Z., Wang, X.H., Li, Y.X., Huang, X.: Stability and Hopf bifurcation of fractional-order complex-valued single neuron model with time delay. Int. J. Bifurc. Chaos **27**(13), 1750209 (2017)
80. Zhang, Y., Dong, H.H., Zhang, X.E., Yang, H.W.: Rational solutions and lump solutions to the generalized (3+1)-dimensional Shallow Water-like equation. Comput. Math. Appl. **73**, 246–252 (2017)
81. Zhang, S.Q., Meng, X.Z., Zhang, T.H.: Dynamics analysis and numerical simulations of a stochastic non-autonomous predator-prey system with impulsive effects. Nonlinear Anal: Hybrid Syst. **26**, 19–37 (2017)
82. Zhang, R.Y., Xu, F.F., Huang, J.C.: Reconstructing local volatility using total variation. Acta Math. Sin.-English Ser. **33**(2), 263–277 (2017)
83. Liu, F.: A remark on the regularity of the discrete maximal operator. Bull. Aust. Math. Soc. **95**, 108–120 (2017)
84. Liu, F.: Integral operators of Marcinkiewicz type on Triebel-Lizorkin spaces. Math. Nachr. **290**, 75–96 (2017)
85. Tian, Z.L., Tian, M.Y., Liu, Z.Y., Xu, T.Y.: The Jacobi and Gauss-Seidel-type iteration methods for the matrix equation AXB = C. Appl. Math. Comput. **292**, 63–75 (2017)
86. Song, Q.L., Dong, X.Y., Bai, Z.B., Chen, B.: Existence for fractional Dirichlet boundary value problem under barrier strip conditions. J. Nonlinear Sci. Appl. **10**, 3592–3598 (2017)
87. Liu, F., Wu, H.X.: On the regularity of maximal operators supported by submanifolds. J. Math. Anal. Appl. **453**, 144–158 (2017)
88. Liu, F., Wu, H.X.: Regularity of discrete multisublinear fractional maximal functions. Sci. China Math. **60**(8), 1461–1476 (2017)
89. Liu, F., Wu, H.X.: Endpoint regularity of multisublinear fractional maximal functions. Can. Math. Bull. **60**(3), 586–603 (2017)

90. Liu, F., Mao, S.Z.: On the regularity of the one-sided Hardy-Littlewood maximal functions. Czech. Math. J. **67**(142), 219–234 (2017)
91. Liu, F.: On the Triebel-Lizorkin space boundedness of Marcinkiewicz integrals along compound surfaces. Math. Inequal. Appl. **20**(2), 515–535 (2017)
92. Li, X.Y., Zhao, Q.L.: A new integrable symplectic map by the binary nonlinearization to the super AKNS system. J. Geom. Phys. **121**, 123–137 (2017)
93. Cheng, W., Xu, J.F., Cui, Y.J.: Positive solutions for a system of nonlinear semipositone fractional q-difference equations with q-integral boundary conditions. J. Nonlinear Sci. Appl. **10**, 4430–4440 (2017)
94. Xu, X.-X., Sun, Y.-P.: An integrable coupling hierarchy of Dirac integrable hierarchy, its Liouville integrability and Darboux transformation. J. Nonlinear Sci. Appl. **10**, 3328–3343 (2017)
95. Liu, Y.Q., Sun, H.G., Yin, X.L., Xin, B.G.: A new Mittag-Leffler function undetermined coefficient method and its applications to fractional homogeneous partial differential equations. J. Nonlinear Sci. Appl. **10**, 4515–4523 (2017)
96. Chen, J.C., Zhu, S.D.: Residual symmetries and soliton-cnoidal wave interaction solutions for the negative-order Korteweg-de Vries equation. Appl. Math. Lett. **73**, 136–142 (2017)
97. Zhang, X.E., Chen, Y., Zhang, Y.: Breather, lump and X soliton solutions to nonlocal KP equation. Comput. Math. Appl. **74**(10), 2341–2347 (2017)
98. Zhang, J.B., Ma, W.X.: Mixed lump-kink solutions to the BKP equation. Comput. Math. Appl. **74**, 591–596 (2017)
99. Zhao, H.Q., Ma, W.X.: Mixed lump-kink solutions to the KP equation. Comput. Math. Appl. **74**, 1399–1405 (2017)
100. Liu, F., Wu, H.X.: Singular integrals related to homogeneous mappings in Triebel-Lizorkin spaces. J. Math. Inequal. **11**(4), 1075–1097 (2017)
101. Liu, F.: Rough singular integrals associated to surfaces of revolution on Triebel-Lizorkin spaces. Rocky Mt. J. Math. **47**(5), 1617–1653 (2017)
102. Zhao, Q.L., Li, X.Y.: A bargmann system and the involutive solutions associated with a new 4-order lattice hierarchy. Anal. Math. Phys. **6**(3), 237–254 (2016)
103. Wang, Y.H.: Beyond regular semigroups. Semigroup Forum **92**(2), 414–448 (2016)
104. Zhang, J.K., Wu, X.J., Xing, L.S., Zhang, C.: Bifurcation analysis of five-level cascaded H-bridge inverter using proportional-resonant plus time-delayed feedback. Int. J. Bifurc. Chaos **26**(11), 1630031 (2016)
105. Zhang, T.Q., Meng, X.Z., Zhang, T.H.: Global analysis for a delayed siv model with direct and environmental transmissions. J. Appl. Anal. Comput. **6**(2), 479–491 (2016)
106. Meng, X.Z., Wang, L., Zhang, T.H.: Global dynamics analysis of a nonlinear impulsive stochastic chemostat system in a polluted environment. J. Appl. Anal. Comput. **6**(3), 865–875 (2016)
107. Cui, Y.J.: Uniqueness of solution for boundary value problems for fractional differential equations. Appl. Math. Lett. **51**, 48–54 (2016)
108. Meng, X.Z., Zhao, S.N., Feng, T., Zhang, T.H.: Dynamics of a novel nonlinear stochastic Sis epidemic model with double epidemic hypothesis. J. Math. Anal. Appl. **433**(1), 227–242 (2016)
109. Yin, C., Cheng, Y.H., Zhong, S.M., Bai, Z.B.: Fractional-order switching type control law design for adaptive sliding mode technique of 3d fractional-order nonlinear systems. Complexity **21**(6), 363–373 (2016)
110. Liu, F., Mao, S.Z., Wu, H.X.: On rough singular integrals related to homogeneous mappings. Collectanea Math. **67**(1), 113–132 (2016)
111. Liu, F., Chen, T., Wu, H.X.: A note on the endpoint regularity of the Hardy-littlewood maximal functions. Bull. Aust. Math. Soc. **94**(1), 121–130 (2016)
112. Liu, F., Fu, Z.W., Zheng, Y.P., Yuan, Q.: A rough marcinkiewicz integral along smooth curves. J. Nonlinear Sci. Appl. **9**(6), 4450–4464 (2016)
113. Liu, F., Wang, F.: Entropy-expansiveness of geodesic flows on closed manifolds without conjugate points. Acta Math. Sin.-English Ser. **32**(4), 507–520 (2016)
114. Cui, Y.J.: Existence of solutions for coupled integral boundary value problem at resonance. Publ. Mathe-Debrecen **89**(1–2), 73–88 (2016)
115. Cui, Y.J., Zou, Y.M.: Existence of solutions for second-order integral boundary value problems. Nonlinear Anal. Model. Control **21**(6), 828–838 (2016)
116. Dong, H.H., Guo, B.Y., Yin, B.S.: Generalized fractional supertrace identity for Hamiltonian structure of Nls-Mkdv hierarchy with self-consistent sources. Anal. Math. Phys. **6**(2), 199–209 (2016)

117. Liu, F., Wu, H.X.: L-p bounds for marcinkiewicz integrals associated to homogeneous mappings. Monatshefte für Mathematik **181**(4), 875–906 (2016)
118. Li, X.P., Lin, X.Y., Lin, Y.Q.: Lyapunov-Type conditions and stochastic differential equations driven by G-brownian motion. J. Math. Anal. Appl. **439**(1), 235–255 (2016)
119. Liu, F., Zhang, D.Q.: Multiple singular integrals and maximal operators with mixed homogeneity along compound surfaces. Math. Inequal. Appl. **19**(2), 499–522 (2016)
120. Zhao, Y., Zhang, W.H.: Observer-based controller design for singular stochastic Markov jump systems with state dependent noise. J. Syst. Sci. Complex. **29**(4), 946–958 (2016)
121. Ma, H.J., Jia, Y.M.: Stability analysis for stochastic differential equations with infinite Markovian switchings. J. Math. Anal. Appl. **435**(1), 593–605 (2016)
122. Zhang, T.Q., Ma, W.B., Meng, X.Z., Zhang, T.H.: Periodic solution of a prey-predator model with nonlinear state feedback control. Appl. Math. Comput. **266**, 95–107 (2015)
123. Liu, F., Zhang, D.Q.: Parabolic marcinkiewicz integrals associated to polynomials compound curves and extrapolation. Bull. Korean Math. Soc. **52**(3), 771–788 (2015)
124. Ling, S.T., Cheng, X.H., Jiang, T.S.: An algorithm for coneigenvalues and coneigenvectors of quaternion matrices. Adv. Appl. Clifford Algebras **25**(2), 377–384 (2015)
125. Liu, F., Wu, H.X., Zhang, D.Q.: L-p bounds for parametric marcinkiewicz integrals with mixed homogeneity. Math. Inequal. Appl. **18**(2), 453–469 (2015)
126. Liu, F., Wu, H.X.: On the regularity of the multisublinear maximal functions. Can. Math. Bull. **58**(4), 808–817 (2015)
127. Gao, M., Sheng, L., Zhang, W.H.: Stochastic H-2/H-infinity control of nonlinear systems with time-delay and state-dependent noise. Appl. Math. Comput. **266**, 429–440 (2015)
128. Li, Y.X., Huang, X., Song, Y.W., Lin, J.N.: A new fourth-order memristive chaotic system and its generation. Int. J. Bifurc. Chaos **25**(11), 1550151 (2015)
129. Xu, X.X.: A deformed reduced semi-discrete Kaup-Newell equation, the related integrable family and darboux transformation. Appl. Math. Comput. **251**, 275–283 (2015)
130. Li, X.Y., Zhao, Q.L., Li, Y.X., Dong, H.H.: Binary bargmann symmetry constraint associated with 3×3 discrete matrix spectral problem. J. Nonlinear Sci. Appl. **8**(5), 496–506 (2015)
131. Yu, J., Li, M.Q., Wang, Y.L., He, G.P.: A decomposition method for large-scale box constrained optimization. Appl. Math. Comput. **231**, 9–15 (2014)