Quantum Information Processing (2019) 18:190
https://doi.org/10.1007/s11128-019-2305-7

Quantum key agreement with Bell states and Cluster states under collective noise channels

Sha-Sha Wang[1] · Dong-Huan Jiang[1] · Guang-Bao Xu[1] · Yong-Hua Zhang[2] · Xiang-Qian Liang[1]

Received: 4 November 2018 / Accepted: 3 May 2019 / Published online: 11 May 2019

Abstract

The collective noises, which include the collective-dephasing noise and the collective-rotation noise, are the topical noises in quantum key agreement (QKA). How to eliminate the influence of the collective noises on quantum communication is a problem to be solved urgently. In this paper, based on logical quantum states, by using controlled-Z, controlled-NOT and unitary operations, two QKA protocols which can be immune to the collective-dephasing noise and the collective-rotation noise are proposed, respectively. The security analysis indicates that these two protocols can resist participant attack and outsider attacks which include Trojan-horse attacks, intercept-resend attack, measure-resend attack and entangle-measure attack. By comparing with the proposed two-party QKA protocols against the collective noises, it is clear that our protocols are more efficient.

Keywords Quantum key agreement · Collective noise · Bell states · Cluster states

1 Introduction

Quantum cryptography has aroused researcher's wide concern after Bennett and Brassard introduced quantum key distribution (QKD) protocol in 1984 [1]. It can realize unconditional security based on theory of quantum mechanisms and quantum principles. Shor et al. [2] proposed a key distribution protocol with entanglement purification and proved the security of BB84. Then, a series of quantum cryptographic protocols were designed, including quantum key distribution [3–6], quantum dialogue [7], quan-

✉ Xiang-Qian Liang
xiangqian.liang@163.com

[1] College of Mathematics and Systems Science, Shandong University of Science and Technology, Qingdao 266590, Shandong, China

[2] College of Computer Science and Engineering, Shandong University of Science and Technology, Qingdao 266590, Shandong, China

tum communication [8], quantum signature [9–12] and so on. Recently, quantum key agreement (QKA) is proposed as a new branch of quantum cryptography. Since QKA protocol can achieve the fairness, it has attracted the attentions of more and more researchers. Different from QKD, QKA allows two-party or multiparty to agree a final shared key fairly.

Zhou et al. [13] first designed a QKA protocol by using quantum teleportation technique. However, it was not a secure QKA protocol as shown by Tsai et al.'s protocol [14]. Later, Chong and Hwang [15] introduced an efficient QKA protocol based on BB84, which used the delayed measurement technique. He et al. [16] put forward a two-party QKA protocol based on five-particle entangled states. It was secure in resisting participant and outsider attacks. However, the above QKA protocols [13–16] only involved two-party case. In addition, some multiparty QKA (MQKA) protocols were proposed. Shi et al. [17] first presented an MQKA protocol based on entanglement swapping and EPR pairs. However, Liu et al. [18] pointed out that Shi et al.'s protocol is unable to resist the participant attack and proposed a new MQKA agreement using single particles. Later, Xu et al. [19] put forward a new three-party and an arbitrary multiparty QKA protocols based on GHZ states without decoy particles. Jiang and Xu [20] proposed an MQKA protocol based on locally indistinguishable orthogonal product states.

Obviously, the above QKA protocols were discussed based on the ideal quantum channel. Actually, when the participants transferred particles through the quantum channel, the particles will be affected by noise. Therefore, the particles will be changed due to noise. Moreover, the attackers may hide his attack by using noise. So it is hard to distinguish whether errors are caused by noise or by attackers. Currently, the influence of the collective noises on quantum communication is a common problem [21–24]. Walton et al. [25] presented the decoherence-free subspace (DFS) which could resist the collective noises because the particles were changeless under the collective noise channels. Huang et al. [22] first introduced two corresponding variables under the collective noise channels. At the same time, Huang et al. [26] presented a QKA protocol which could resist collective decoherence. He et al. [27] proposed two robust QKA protocols with the logical GHZ states. Gao et al. [28] proposed a two-party QKA agreement with Bell states and four-particle GHZ states under collective noise channels. However, there are few QKA protocols resisting the collective noises.

In this paper, two-party QKA protocols are proposed with Bell states and Cluster states under the collective-dephasing noise and collective-rotation noise channels, respectively. The fairness is guaranteed by using the delayed measurement technique. The security is ensured by using the decoy logical particles method. Security analysis indicates that these two protocols can resist the dishonest participant and outside eavesdropper attacks.

The rest of the paper is organized as follows. In Sect. 2, we introduce some preliminary knowledge. In Sect. 3, we propose two QKA protocols against collective noise. In Sects. 4 and 5, we discuss security analysis and efficiency analysis, respectively. In Sect. 6, we give a short conclusion.

2 Preliminaries

This section introduces unitary operations, the collective noises, the logical particles immune to collective-dephasing noise and the logical particles immune to collective-rotation noise.

2.1 The unitary operations and the collective noises

First, the unitary operations used in this paper are denoted as:

$$\begin{aligned} U_0 &= I = |0\rangle\langle 0| + |1\rangle\langle 1|, \\ U_1 &= Z = |0\rangle\langle 0| - |1\rangle\langle 1|, \\ U_2 &= iY = |0\rangle\langle 1| - |1\rangle\langle 0|. \end{aligned}$$

Second, the collective noises include the collective-dephasing noise and the collective-rotation noise. The collective-dephasing noise can be denoted as [29]:

$$U_{dp}|0\rangle = |0\rangle, U_{dp}|1\rangle = e^{i\varphi}|1\rangle.$$

where φ is the noise parameter and it fluctuates with time. In order to make the particles against the collective-dephasing noise, logical particles $|0_{dp}\rangle$ and $|1_{dp}\rangle$ are formed by two physical qubit tensor product states $|01\rangle$ and $|10\rangle$, respectively. They can be denoted as:

$$|0_{dp}\rangle = |01\rangle, |1_{dp}\rangle = |10\rangle.$$

The states $|+_{dp}\rangle$ and $|-_{dp}\rangle$ are described as follows:

$$\begin{aligned} |+_{dp}\rangle &= \frac{1}{\sqrt{2}}(|0_{dp}\rangle + |1_{dp}\rangle) = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle), \\ |-_{dp}\rangle &= \frac{1}{\sqrt{2}}(|0_{dp}\rangle - |1_{dp}\rangle) = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle). \end{aligned}$$

The collective-rotation noise can be denoted as:

$$U_r|0\rangle = \cos\theta|0\rangle + \sin\theta|1\rangle, U_r|1\rangle = -\sin\theta|0\rangle + \cos\theta|1\rangle.$$

The parameter θ is the noise parameter and it fluctuates with time in the quantum channel. In order to make the particles against the collective-rotation noise, logical particles $|0_r\rangle$ and $|1_r\rangle$ are formed by two physical qubit tensor product states $|\Phi^+\rangle$ and $|\Psi^-\rangle$, respectively. They can be denoted as:

$$|0_r\rangle = |\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle), |1_r\rangle = |\Psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle).$$

The states $|+_r\rangle$ and $|-_r\rangle$ are described as follows:

$$|+_r\rangle = \frac{1}{\sqrt{2}}(|0_r\rangle + |1_r\rangle) = \frac{1}{\sqrt{2}}(|\Phi^+\rangle + |\Psi^-\rangle),$$
$$|-_r\rangle = \frac{1}{\sqrt{2}}(|0_r\rangle - |1_r\rangle) = \frac{1}{\sqrt{2}}(|\Phi^+\rangle - |\Psi^-\rangle).$$

2.2 The logical particles immune to collective-dephasing noise

The Bell states used in this paper can be expressed as follows:

$$|\Psi^+\rangle_{12} = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)_{12} = \frac{1}{\sqrt{2}}(|0_{dp}\rangle + |1_{dp}\rangle)_{12},$$
$$|\Psi^-\rangle_{12} = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)_{12} = \frac{1}{\sqrt{2}}(|0_{dp}\rangle - |1_{dp}\rangle)_{12}.$$

where the subscripts 1, 2 denote the first particle and the second particle of the Bell states, respectively.

Take state $|\Psi^+\rangle_{12}$ as an example, when the first and the second particles of $|\Psi^+\rangle_{12}$ pass through the collective-dephasing noise channel, $|\Psi^+\rangle_{12}$ can be expressed in the following equation:

$$|\Psi^+\rangle_{12} = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)_{12}$$
$$\xrightarrow{under\ collective\text{-}dephasing\ noise}$$
$$= \frac{1}{\sqrt{2}}e^{i\varphi}(|01\rangle + |10\rangle)_{12} = e^{i\varphi}|\Psi^+\rangle_{12}.$$

As a result, it is clear that these two Bell states are immune to the collective-dephasing noise.

2.3 The logical particles immune to collective-rotation noise

The Cluster states used in this agreement can be depicted as [30]:

$$|C_1\rangle_{1234} = \frac{1}{2}(|0000\rangle + |0011\rangle + |1100\rangle - |1111\rangle)_{1234},$$
$$|C_2\rangle_{1234} = \frac{1}{2}(|0000\rangle + |0011\rangle - |1100\rangle + |1111\rangle)_{1234},$$
$$|C_3\rangle_{1234} = \frac{1}{2}(-|0001\rangle + |0010\rangle + |1101\rangle + |1110\rangle)_{1234},$$
$$|C_4\rangle_{1234} = \frac{1}{2}(-|0001\rangle + |0010\rangle - |1101\rangle - |1110\rangle)_{1234}.$$

where the subscripts 1, 2, 3, 4 denote the first particle, the second particle, the third particle and the fourth particle of the Cluster states, respectively.

Then, we perform controlled-NOT (CNOT) operation ($CNOT = (|00\rangle\langle 00| + |01\rangle\langle 01| + |10\rangle\langle 11| + |11\rangle\langle 10|)$) on the Cluster states by using the second particle as the control qubit and the fourth particle as the target qubit. Cluster states become the following equations:

$$\begin{aligned}
|C_1\rangle'_{1234} &= U^{2,4}_{CNOT}|C_1\rangle_{1234} = \frac{1}{2}(|0000\rangle + |0011\rangle + |1101\rangle - |1110\rangle)_{1234}\\
&= \frac{1}{\sqrt{2}}(|00\rangle_{12}|0_r\rangle_{34} + |11\rangle_{12}|1_r\rangle_{34}),\\
|C_2\rangle'_{1234} &= U^{2,4}_{CNOT}|C_2\rangle_{1234} = \frac{1}{2}(|0000\rangle + |0011\rangle - |1101\rangle + |1110\rangle)_{1234}\\
&\frac{1}{\sqrt{2}}(|00\rangle_{12}|0_r\rangle_{34} - |11\rangle_{12}|1_r\rangle_{34}),\\
|C_3\rangle'_{1234} &= U^{2,4}_{CNOT}|C_3\rangle_{1234} = \frac{1}{2}(-|0001\rangle + |0010\rangle + |1100\rangle + |1111\rangle)_{1234}\\
&= \frac{1}{\sqrt{2}}(-|00\rangle_{12}|1_r\rangle_{34} + |11\rangle_{12}|0_r\rangle_{34}),\\
|C_4\rangle'_{1234} &= U^{2,4}_{CNOT}|C_4\rangle_{1234} = \frac{1}{2}(-|0001\rangle + |0010\rangle - |1100\rangle - |1111\rangle)_{1234}\\
&= \frac{1}{\sqrt{2}}(-|00\rangle_{12}|1_r\rangle_{34} - |11\rangle_{12}|0_r\rangle_{34}).
\end{aligned}$$

As shown in the above equations, the third and the fourth particles of $|C_1\rangle'_{1234}$, $|C_2\rangle'_{1234}$, $|C_3\rangle'_{1234}$ and $|C_4\rangle'_{1234}$ are immune to the collective-rotation noise. Take $|C_1\rangle'_{1234}$ as an example, when the third and the fourth particles of $|C_1\rangle'_{1234}$ pass through the collective-rotation noise channel, the state $|C_1\rangle'_{1234}$ can be expressed in the equation:

$$\begin{aligned}
|C_1\rangle'_{1234} &= \frac{1}{\sqrt{2}}(|00\rangle_{12}|\Phi^+\rangle_{34} + |11\rangle_{12}|\Psi^-\rangle_{34})\\
&= \frac{1}{2}[|00\rangle_{12}(|00\rangle + |11\rangle)_{34} + |11\rangle_{12}(|01\rangle - |10\rangle)_{34}]\\
&\xrightarrow{the\ third\ and\ fourth\ particles\ under\ collective\text{-}rotation\ noise}\\
&= \frac{1}{2}[|00\rangle_{12}((cos\theta|0\rangle + sin\theta|1\rangle)_3(cos\theta|0\rangle + sin\theta|1\rangle)_4\\
&\quad + (-sin\theta|0\rangle + cos\theta|1\rangle)_3(-sin\theta|0\rangle + cos\theta|1\rangle)_4)\\
&\quad + |11\rangle_{12}((cos\theta|0\rangle + sin\theta|1\rangle)_3(-sin\theta|0\rangle + cos\theta|1\rangle)_4\\
&\quad - (-sin\theta|0\rangle + cos\theta|1\rangle)_3(cos\theta|0\rangle + sin\theta|1\rangle)_4)]\\
&= \frac{1}{2}[|00\rangle_{12}(cos^2\theta|00\rangle + cos\theta sin\theta|01\rangle + cos\theta sin\theta|10\rangle + sin^2\theta|11\rangle\\
&\quad + sin^2\theta|00\rangle - sin\theta cos\theta|01\rangle - cos\theta sin\theta|10\rangle + cos^2\theta|11\rangle)_{34}]
\end{aligned}$$

$$
\begin{aligned}
&+\frac{1}{2}[|11\rangle_{12}(-cos\theta sin\theta|00\rangle+cos^2\theta|01\rangle-sin^2\theta|10\rangle+cos\theta sin\theta|11\rangle\\
&+cos\theta sin\theta|00\rangle+sin^2\theta|01\rangle-cos^2\theta|10\rangle-cos\theta sin\theta|11\rangle)_{34}]\\
&=\frac{1}{2}[|00\rangle_{12}(|00\rangle+|11\rangle)_{34}+|11\rangle_{12}(|01\rangle-|10\rangle)_{34}]\\
&=|C_1\rangle'_{1234}.
\end{aligned}
$$

Obviously, the third and the fourth particles of state $|C_t\rangle'_{1234}(t=1,2,3,4)$ are unaffected under the collective-rotation noise.

3 The QKA protocols against collective noise

This section is composed of two subsections. In Sect. 3.1, the QKA protocol against collective-dephasing noise is introduced. In Sect. 3.2, the QKA protocol against collective-rotation noise is described.

3.1 The QKA protocol against collective-dephasing noise

Suppose that Alice and Bob want to generate a common key K fairly. First, Alice and Bob randomly generate the bit strings K_A and K_B as their secret keys, respectively.

$$
\begin{aligned}
K_A &= k_A^1||k_A^2||\ldots||k_A^i||\ldots||k_A^n,\\
K_B &= k_B^1||k_B^2||\ldots||k_B^i||\ldots||k_B^n.
\end{aligned}
$$

where $k_A^i, k_B^i \in \{0,1\}$, $k_A^i(k_B^i)$ represents the ith private information of $K_A(K_B)$, for $i=1,2,\ldots,n$. The final key K can be denoted as: $K=H(K_A,K_B)=(k_A^1||k_B^1)||\ldots||(k_A^n||k_B^n)$.

1. Alice and Bob randomly choose the k positive integers which are different, respectively. $N_A=(n_A^1,\ldots,n_A^k)$, $N_B=(n_B^1,\ldots,n_B^k)$, where N_A denotes the set of k positive integers which are selected by Alice, N_B denotes the set of k positive integers which are selected by Bob.
2. Alice and Bob generate n-dimension vectors $\theta_A=(\theta_A^1,\ldots,\theta_A^n)$ and $\theta_B=(\theta_B^1,\ldots,\theta_B^n)$, respectively, where $\theta_A^i=\frac{\pi}{2^{n_A^j-1}}$ and $\theta_B^i=\frac{\pi}{2^{n_B^j-1}}$, $1\le i\le n$; $n_A^j\in N_A, n_B^j\in N_B$.
3. Alice and Bob prepare n states $\{|\psi_A^1\rangle,\ldots,|\psi_A^i\rangle,\ldots,|\psi_A^n\rangle\}$ and $\{|\psi_B^1\rangle,\ldots,|\psi_B^i\rangle,\ldots,|\psi_B^n\rangle\}$ respectively, where $|\psi_A^i\rangle=\{a_1^i,a_2^i\}$ and $|\psi_B^i\rangle=\{b_1^i,b_2^i\}, i=1,2,\ldots,n$. $|\psi_A^i\rangle$ and $|\psi_B^i\rangle$ are the state $|\Psi^+\rangle$. Let a_1^i, b_1^i represent the first particles of $|\Psi^+\rangle$ and a_2^i, b_2^i represent the second particles of $|\Psi^+\rangle$.
4. Alice executes the rotation operation $R(\theta_A^i)$ on a_1^i. Meanwhile, Bob executes the unitary operation $R(\theta_B^i)$ on b_1^i, where $R(\theta_A^i)=cos\theta_A^i(|0\rangle\langle 0|+|1\rangle\langle 1|)+sin\theta_A^i(|1\rangle\langle 0|-|0\rangle\langle 1|)$, $R(\theta_B^i)=cos\theta_B^i(|0\rangle\langle 0|+|1\rangle\langle 1|)+sin\theta_B^i(|1\rangle\langle 0|-|0\rangle\langle 1|)$. After that, Alice and Bob can obtain the new sequences $S'_A=$

$\{|\psi_A^1\rangle', |\psi_A^2\rangle', \ldots, |\psi_A^n\rangle'\}$ and $S'_B = \{|\psi_B^1\rangle', |\psi_B^2\rangle', \ldots, |\psi_B^n\rangle'\}$, respectively, where $S'_A \in \{a_1^{i'}, a_2^i\}$, $S'_B \in \{b_1^{i'}, b_2^i\}$.

5. Alice executes unitary operation $U_{t_A^i}$ on $a_1^{i'}$ according to K_A, where the subscript $t_A^i = k_A^i$. So Alice can get the encoded message sequence $S_A^{'*}$. Similarly, Bob executes unitary operation $U_{t_B^i}$ on $b_1^{i'}$ according to K_B, where the subscript $t_B^i = k_B^i$. Then, Bob gets the encoded message sequence $S_B^{'*}$.
6. Alice and Bob prepare $\frac{n}{2}$ decoy logical particles which are randomly selected from $\{|0_{dp}\rangle, |1_{dp}\rangle, |+_{dp}\rangle, |-_{dp}\rangle\}$, respectively. After that, Alice and Bob insert decoy logical particles into the sequences $S_A^{'*}$ and $S_B^{'*}$ to get the new sequences $S_A^{''*}$ and $S_B^{''*}$, respectively. Afterwards, Alice sends the new sequence $S_A^{''*}$ to Bob, and Bob sends the new sequence $S_B^{''*}$ to Alice.
7. After Alice and Bob receive the new sequences $S_B^{''*}$, $S_A^{''*}$, respectively, they inform each other through classical channels. When they confirm that the other party has received the sequence, they disclose the position of the decoy logical particles and the corresponding measurement bases. Then, they measure decoy logical particles by utilizing the correct measurement bases. If the error rate is smaller than the selected threshold, they continue to perform the next step. Otherwise, they give up the protocol.
8. After Alice removes the decoy logical particles, she can obtain the sequence $S_B^{'*}$. Similar to Alice, Bob can also obtain the sequence $S_A^{'*}$. After they confirm that the other party has received the sequence, Alice and Bob announce the unitary operations $R(\theta_A^i)$ and $R(\theta_B^i)$, respectively. Then, Alice executes unitary operation $R^{-1}(\theta_B^i)$ on b_1^i of sequence $S_B^{'*}$. Next, by using Bell measurement, Alice can infer K_B. Similarly, Bob can also conclude K_A by executing unitary operation $R^{-1}(\theta_A^i)$ on a_1^i of sequence $S_A^{'*}$ and Bell measurement. Therefore, they can generate a common key $K = H(K_A, K_B)$, simultaneously.

3.2 The QKA protocol against collective-rotation noise

1. Alice prepares n states $\{|\psi_1\rangle, \ldots, |\psi_i\rangle, \ldots, |\psi_n\rangle\}$ and $\{|\varphi_1\rangle, \ldots, |\varphi_i\rangle, \ldots, |\varphi_n\rangle\}$, respectively, where $|\psi_i\rangle = \{a_1^i, a_2^i, a_3^i, a_4^i\}$, $|\varphi_i\rangle = \{a_5^i, a_6^i\}$. $|\psi_i\rangle$ is the state $|C_1\rangle_{1234}$. Let $a_1^i, a_2^i, a_3^i, a_4^i$ represent the first, second, third, fourth particles of the $|C_1\rangle_{1234}$ state, respectively. If $k_A^i = 0$, $|\varphi_i\rangle = |\Phi^+\rangle$; $k_A^i = 1$, $|\varphi_i\rangle = |\Psi^-\rangle$. Let a_5^i, a_6^i represent the first, second particles of the state $|\varphi_i\rangle$. $|\varphi_i\rangle$ denotes of the message qubits $|\Phi^+\rangle$ or $|\Psi^-\rangle$. Then, Alice performs two CNOT operations and a controlled-Z (CZ) operation $(CZ = (|00\rangle\langle 00| + |01\rangle\langle 01| + |10\rangle\langle 10| - |11\rangle\langle 11|))$ on the n Cluster states and the message qubits, where a_2^i as the control bit, and a_4^i, a_6^i as the target bit of the CNOT operation, respectively. And, a_1^i is treated as the control qubit, and a_5^i is the target qubit of the CZ operation, respectively. After that, $|C_1\rangle_{1234}$ is entangled with the message qubits. The result states can be showed as follows:

$$
\begin{aligned}
|C_1^{(0)}\rangle_{123456} &= CZ(1,5)CNOT(2,6)CNOT(2,4)|C_1\rangle_{1234}\otimes|\Phi^+\rangle_{56}\\
&= CZ(1,5)CNOT(2,6)|C_1\rangle'_{1234}\otimes|\Phi^+\rangle_{56}\\
&= CZ(1,5)CNOT(2,6)\frac{1}{\sqrt{2}}(|00\rangle_{12}|\Phi^+\rangle_{34}|\Phi^+\rangle_{56}\\
&\quad+|11\rangle_{12}|\Psi^-\rangle_{34}|\Phi^+\rangle_{56})\\
&= \frac{1}{\sqrt{2}}(|00\rangle_{12}|\Phi^+\rangle_{34}|\Phi^+\rangle_{56}+|11\rangle_{12}|\Psi^-\rangle_{34}|\Psi^-\rangle_{56}),\\
|C_1^{(1)}\rangle_{123456} &= CZ(1,5)CNOT(2,6)CNOT(2,4)|C_1\rangle_{1234}\otimes|\Psi^-\rangle_{56}\\
&= CZ(1,5)CNOT(2,6)|C_1\rangle'_{1234}\otimes|\Psi^-\rangle_{56}\\
&= CZ(1,5)CNOT(2,6)\frac{1}{\sqrt{2}}(|00\rangle_{12}|\Phi^+\rangle_{34}|\Psi^-\rangle_{56}\\
&\quad+|11\rangle_{12}|\Psi^-\rangle_{34}|\Psi^-\rangle_{56})\\
&= \frac{1}{\sqrt{2}}(|00\rangle_{12}|\Phi^+\rangle_{34}|\Psi^-\rangle_{56}+|11\rangle_{12}|\Psi^-\rangle_{34}|\Phi^+\rangle_{56}).
\end{aligned}
$$

2. Alice prepares $\frac{n}{2}$ decoy logical particles which are randomly selected from $\{|0_r\rangle, |1_r\rangle, |+_r\rangle, |-_r\rangle\}$. Then, Alice inserts $\frac{n}{2}$ decoy logical particles into the sequence $S_{A(34)} = \{a_3^i, a_4^{i'}\}$ to obtain the new sequence $S'_{A(34)}$. After that, Alice transmits $S'_{A(34)}$ to Bob.
3. After Alice confirms that Bob has received the sequence $S'_{A(34)}$, she discloses the position of the decoy logical particles and the corresponding measurement bases. Then, Bob measures decoy logical particles by utilizing the correct measurement bases. If the error rate is smaller than the selected threshold, they continue to perform the next step. Otherwise, they give up the protocol.
4. After Bob removes the decoy logical particles, he can get the sequence $S_{A(34)}$. Then, Bob executes unitary operation $U_{2t_B^i}$ on $a_4^{i'}$ according to K_B, where the superscript $t_B^i = k_B^i$. So Bob can gain the encoded message sequence $S^*_{A(34)}$. Then, Bob inserts $\frac{n}{2}$ decoy logical particles into $S^*_{A(34)}$ to get the new sequence $S^{**}_{A(34)}$. After that, Bob performs a permutation operator $\prod_n$ on $S^{**}_{A(34)}$, and makes $\prod_n S^{**}_{A(34)} = S^{**'}_{A(34)}$. Last, Bob transmits $S^{**'}_{A(34)}$ to Alice.

$$
\begin{aligned}
U_0|C_1^{(0)}\rangle_{123456} &= I^4\frac{1}{\sqrt{2}}(|00\rangle_{12}|\Phi^+\rangle_{34}|\Phi^+\rangle_{56}+|11\rangle_{12}|\Psi^-\rangle_{34}|\Psi^-\rangle_{56})\\
&= \frac{1}{\sqrt{2}}(|00\rangle_{12}|\Phi^+\rangle_{34}|\Phi^+\rangle_{56}+|11\rangle_{12}|\Psi^-\rangle_{34}|\Psi^-\rangle_{56})\\
&= \frac{1}{\sqrt{2}}(|C_1\rangle'_{1256}|+_r\rangle_{34}+|C_2\rangle'_{1256}|-_r\rangle_{34}),\\
U_2|C_1^{(0)}\rangle_{123456} &= iY^4\frac{1}{\sqrt{2}}(|00\rangle_{12}|\Phi^+\rangle_{34}|\Phi^+\rangle_{56}+|11\rangle_{12}|\Psi^-\rangle_{34}|\Psi^-\rangle_{56})
\end{aligned}
$$

$$
\begin{aligned}
&= \frac{1}{\sqrt{2}}(|11\rangle_{12}|\Phi^{+}\rangle_{34}|\Psi^{-}\rangle_{56} - |00\rangle_{12}|\Psi^{-}\rangle_{34}|\Phi^{+}\rangle_{56})\\
&= \frac{1}{\sqrt{2}}(|C_4\rangle'_{1256}|+_r\rangle_{34} + |C_3\rangle'_{1256}|-_r\rangle_{34}),\\
U_0|C_1^{(1)}\rangle_{123456} &= I^4\frac{1}{\sqrt{2}}(|00\rangle_{12}|\Phi^{+}\rangle_{34}|\Psi^{-}\rangle_{56} + |11\rangle_{12}|\Psi^{-}\rangle_{34}|\Phi^{+}\rangle_{56})\\
&= \frac{1}{\sqrt{2}}(|00\rangle_{12}|\Phi^{+}\rangle_{34}|\Psi^{-}\rangle_{56} + |11\rangle_{12}|\Psi^{-}\rangle_{34}|\Phi^{+}\rangle_{56})\\
&= \frac{1}{\sqrt{2}}(|C_3\rangle'_{1256}|+_r\rangle_{34} + |C_4\rangle'_{1256}|-_r\rangle_{34}),\\
U_2|C_1^{(1)}\rangle_{123456} &= iY^4\frac{1}{\sqrt{2}}(|00\rangle_{12}|\Phi^{+}\rangle_{34}|\Psi^{-}\rangle_{56} + |11\rangle_{12}|\Psi^{-}\rangle_{34}|\Phi^{+}\rangle_{56})\\
&= \frac{1}{\sqrt{2}}(|11\rangle_{12}|\Phi^{+}\rangle_{34}|\Phi^{+}\rangle_{56} - |00\rangle_{12}|\Psi^{-}\rangle_{34}|\Psi^{-}\rangle_{56})\\
&= \frac{1}{\sqrt{2}}(|C_2\rangle'_{1256}|+_r\rangle_{34} + |C_1\rangle'_{1256}|-_r\rangle_{34}).
\end{aligned}
$$

5. Bob performs eavesdropping detection as Alice does in step 3.
6. Alice discloses K_A. Bob concludes the final key $K = H(K_A, K_B)$.
7. Bob declares the permutation operator $\prod_n$. Then, Alice can obtain the encoded message sequence $S^{*}_{A(34)}$. Next, Alice performs CNOT operation $U^{2,6}_{CNOT}$, measures the particles $\{a^i_1, a^i_2, a^i_5, a^i_6\}$ by using Cluster states, and measures the particles $\{a^i_3, a^i_4\}$ with logical *X*-basis. The result states are denoted as follows:

$$
\begin{aligned}
U^{2,6}_{CNOT}U_0|C_1^{(0)}\rangle_{123456} &= \frac{1}{\sqrt{2}}(U^{2,6}_{CNOT}|C_1\rangle'_{1256}|+_r\rangle_{34} + U^{2,6}_{CNOT}|C_2\rangle'_{1256}|-_r\rangle_{34})\\
&= \frac{1}{\sqrt{2}}(|C_1\rangle_{1256}|+_r\rangle_{34} + |C_2\rangle_{1256}|-_r\rangle_{34}),\\
U^{2,6}_{CNOT}U_2|C_1^{(0)}\rangle_{123456} &= \frac{1}{\sqrt{2}}(U^{2,6}_{CNOT}|C_4\rangle'_{1256}|+_r\rangle_{34} + U^{2,6}_{CNOT}|C_3\rangle'_{1256}|-_r\rangle_{34})\\
&= \frac{1}{\sqrt{2}}(|C_4\rangle_{1256}|+_r\rangle_{34} + |C_3\rangle_{1256}|-_r\rangle_{34}),\\
U^{2,6}_{CNOT}U_0|C_1^{(1)}\rangle_{123456} &= \frac{1}{\sqrt{2}}(U^{2,6}_{CNOT}|C_3\rangle'_{1256}|+_r\rangle_{34} + U^{2,6}_{CNOT}|C_4\rangle'_{1256}|-_r\rangle_{34})\\
&= \frac{1}{\sqrt{2}}(|C_3\rangle_{1256}|+_r\rangle_{34} + |C_4\rangle_{1256}|-_r\rangle_{34}),\\
U^{2,6}_{CNOT}U_2|C_1^{(1)}\rangle_{123456} &= \frac{1}{\sqrt{2}}(U^{2,6}_{CNOT}|C_2\rangle'_{1256}|+_r\rangle_{34} + U^{2,6}_{CNOT}|C_1\rangle'_{1256}|-_r\rangle_{34})\\
&= \frac{1}{\sqrt{2}}(|C_2\rangle_{1256}|+_r\rangle_{34} + |C_1\rangle_{1256}|-_r\rangle_{34}).
\end{aligned}
$$

By Table 1, Alice infers the secret key K_B and the final key $K = H(K_A, K_B)$.

Table 1 The relationship among message bits, unitary operations and measurement results

K_A	Message qubits	K_B	Unitary operation	The result of Cluster states measurement	The result of logical X-basis measurement
0	$\|\Phi^+\rangle$	0	I	$\|C_1\rangle$	$\|+_r\rangle$
0	$\|\Phi^+\rangle$	0	I	$\|C_2\rangle$	$\|-_r\rangle$
0	$\|\Phi^+\rangle$	1	iY	$\|C_4\rangle$	$\|+_r\rangle$
0	$\|\Phi^+\rangle$	1	iY	$\|C_3\rangle$	$\|-_r\rangle$
1	$\|\Psi^-\rangle$	0	I	$\|C_3\rangle$	$\|+_r\rangle$
1	$\|\Psi^-\rangle$	0	I	$\|C_4\rangle$	$\|-_r\rangle$
1	$\|\Psi^-\rangle$	1	iY	$\|C_2\rangle$	$\|+_r\rangle$
1	$\|\Psi^-\rangle$	1	iY	$\|C_1\rangle$	$\|-_r\rangle$

4 Security analysis

The QKA protocol mainly involves two kinds of attacks: participant attack and outsider attacks (Trojan-horse attacks, Intercept-resend attack, Measure-resend attack and Entangle-measure attack). In order to prove the security of these protocols, we will discuss them according to these two kinds of attacks.

4.1 Participant attack

In the protocol against collective-dephasing noise, we ensure the security of the sequences $S_A^{'*}$ and $S_B^{'*}$ by inserting decoy logical particles in step 6 and performing eavesdropping check in step 7. Because Alice (Bob) obtains the $K_B(K_A)$ after she (he) sends the encoded message sequences to Bob (Alice), she (he) cannot change the final key as she (he) expected. Therefore, this protocol can resist the participant attack.

In the protocol against collective-rotation noise, the delayed measurement technique guarantees that Alice obtains K_B after he announces K_A. Thus, Alice cannot change K_A according to K_B. On the other hand, because Bob obtains K_A after he sends the encoded message sequence $S_{A(34)}^*$, he cannot change the final key as he expected. Therefore, this protocol can also resist the participant attack.

4.2 Outsider attack

Trojan-horse attacks: In the protocol against collective-dephasing noise, because each qubit in quantum channel is delivered only once, the protocol is immune to two kinds of Trojan-horse attacks [31]. However, in the protocol against collective-rotation noise, the same particles are delivered more than once. In order to avoid Trojan-horse attacks, Alice and Bob can use the qubit number splitter (PNS: 50/50) and wavelength filter. They can divide each signal into two pieces by using qubit number splitter. If a multiqubit signal appears an irrational high rate, the attack can be found [32,33].

Intercept-resend attack: Take the protocol against collective-dephasing noise as an example, when Eve wants to perform the intercept-resend attack on the sequences $S_A^{''*}$

and $S_B^{''*}$, she must intercept the two sequences in step 6 and send the two pseudo-random sequences to Bob and Alice, respectively. However, Eve does not know the position of the decoy logical particles and the corresponding measurement bases before the eavesdropping check. Therefore, when performing the eavesdropping check in step 7, the probability of detecting the intercept-resend attack is $1-(\frac{1}{2})^{\frac{n}{2}}$, where $\frac{n}{2}$ denotes the number of decoy logical particles.

Measure-resend attack: Take the protocol against collective-dephasing noise as an example, when Eve performs the measure-resend attack on the sequences $S_A^{''*}$ and $S_B^{''*}$ in step 6, Eve does not know the position of the decoy logical particles and the corresponding measurement bases before the eavesdropping check. Thus, Eve's measurement would change the states of decoy logical particles in the sequences $S_A^{''*}$ and $S_B^{''*}$. When performing the eavesdropping check in step 7, the probability of discovering Eve's attack is $1-(\frac{3}{4})^{\frac{n}{2}}$, where $\frac{n}{2}$ denotes the number of decoy logical particles.

Entangle-measure attack: In these two protocols, suppose that Eve executes entangle-measure attack by using the unitary operation $\hat{U}_E$. We can get the results as follows:

$$\begin{aligned}
\hat{U}_E|0_{dp}\rangle|\varepsilon\rangle_E &= a_{00}|00\rangle|\varepsilon_{00}\rangle_E + a_{01}|01\rangle|\varepsilon_{01}\rangle_E + a_{10}|10\rangle|\varepsilon_{10}\rangle_E + a_{11}|11\rangle|\varepsilon_{11}\rangle_E,\\
\hat{U}_E|1_{dp}\rangle|\varepsilon\rangle_E &= b_{00}|00\rangle|\varepsilon'_{00}\rangle_E + b_{01}|01\rangle|\varepsilon'_{01}\rangle_E + b_{10}|10\rangle|\varepsilon'_{10}\rangle_E + b_{11}|11\rangle|\varepsilon'_{11}\rangle_E,\\
\hat{U}_E|+_{dp}\rangle|\varepsilon\rangle_E &= \frac{1}{\sqrt{2}}(\hat{U}_E|0_{dp}\rangle|\varepsilon\rangle_E + \hat{U}_E|1_{dp}\rangle|\varepsilon\rangle_E)\\
&= \frac{1}{2}[|\Phi^+\rangle(a_{00}\varepsilon_{00}\rangle_E + a_{11}|\varepsilon_{11}\rangle_E + b_{00}|\varepsilon'_{00}\rangle_E + b_{11}|\varepsilon'_{11}\rangle_E)\\
&\quad + |\Phi^-\rangle(a_{00}|\varepsilon_{00}\rangle_E - a_{11}|\varepsilon_{11}\rangle_E + b_{00}|\varepsilon'_{00}\rangle_E - b_{11}|\varepsilon'_{11}\rangle_E)\\
&\quad + |\Psi^+\rangle(a_{01}|\varepsilon_{01}\rangle_E + a_{10}|\varepsilon_{10}\rangle_E + b_{01}|\varepsilon'_{01}\rangle_E + b_{10}|\varepsilon'_{10}\rangle_E)\\
&\quad + |\Psi^-\rangle(a_{01}||\varepsilon_{01}\rangle_E - a_{10}|\varepsilon_{10}\rangle_E + b_{01}|\varepsilon'_{01}\rangle_E - b_{10}|\varepsilon'_{10}\rangle_E)],\\
\hat{U}_E|-_{dp}\rangle|\varepsilon\rangle_E &= \frac{1}{\sqrt{2}}(\hat{U}_E|0_{dp}\rangle|\varepsilon\rangle_E - \hat{U}_E|1_{dp}\rangle|\varepsilon\rangle_E)\\
&= \frac{1}{2}[|\Phi^+\rangle(a_{00}|\varepsilon_{00}\rangle_E + a_{11}|\varepsilon_{11}\rangle_E - b_{00}|\varepsilon'_{00}\rangle_E - b_{11}|\varepsilon'_{11}\rangle_E)\\
&\quad + |\Phi^-\rangle(a_{00}|\varepsilon_{00}\rangle_E - a_{11}|\varepsilon_{11}\rangle_E - b_{00}|\varepsilon'_{00}\rangle_E + b_{11}|\varepsilon'_{11}\rangle_E)\\
&\quad + |\Psi^+\rangle(a_{01}|\varepsilon_{01}\rangle_E + a_{10}|\varepsilon_{10}\rangle_E - b_{01}|\varepsilon'_{01}\rangle_E - b_{10}|\varepsilon'_{10}\rangle_E)\\
&\quad + |\Psi^-\rangle(a_{01}|\varepsilon_{01}\rangle_E - a_{10}|\varepsilon_{10}\rangle_E - b_{01}|\varepsilon'_{01}\rangle_E + b_{10}|\varepsilon'_{10}\rangle_E)].
\end{aligned}$$

where $|a_{00}|^2+|a_{01}|^2+|a_{10}|^2+|a_{11}|^2=1$, $|b_{00}|^2+|b_{01}|^2+|b_{10}|^2+|b_{11}|^2=1$. $|\varepsilon\rangle_E$ denotes an ancillary system. If Eve does not want to be detected in the eavesdropping check, the $\hat{U}_E$ must satisfy four conditions: $a_{01}=b_{10}=1$, $a_{00}=a_{10}=a_{11}=0$, $b_{00}=b_{01}=b_{11}=0$ and $|\varepsilon_{01}\rangle_E=|\varepsilon'_{10}\rangle_E$. Obviously, Eve does not introduce any errors only when the ancillary state and the target particle $\{|0_{dp}\rangle, |1_{dp}\rangle\}$ are product states. That is, she cannot obtain useful information about K_A and K_B. Thus, the two protocols can resist the outsider attacks.

5 Efficiency analysis

Cabello [34] introduced the qubit efficiency which is given as

$$\eta = \frac{c}{q+b},$$

where c, q, b denote the length of the final key, the number of the used particles, and the number of classical bits exchanged for decoding of the message, respectively.

In the protocol against collective-dephasing noise, the length of the final key $K = H(K_A, K_B) = (k_A^1||k_B^1)||\ldots||(k_A^n||k_B^n)$ is $c_1 = 2n$. Alice and Bob prepare n quantum states, and use $\frac{n}{2}$ decoy logical particles in step 6 respectively, where a quantum state and a decoy logical particle are composed of two particles, respectively. Therefore, the number of the used particles is $q_1 = 4n + \frac{n}{2} \cdot 2 \cdot 2 = 6n$. Alice and Bob encode their private information by using unitary operation on n-bit single particle sequences in step 5, respectively. So the number of classical bits exchanged for decoding of the message is $b_1 = 2n$. Thus, the qubit efficiency of the protocol against collective-dephasing noise is calculated as

$$\eta_1 = \frac{c_1}{q_1 + b_1} = \frac{2n}{\left(4n + \frac{n}{2} \cdot 2 \cdot 2\right) + 2n} = \frac{2}{8} = 25\%.$$

In the protocol against collective-rotation noise, the length of the final key $K = H(K_A, K_B) = (k_A^1||k_B^1)||\ldots||(k_A^n||k_B^n)$ is $c_2 = 2n$. Alice prepares n four-particle states and n two-particle states, and uses $\frac{n}{2}$ decoy logical particles in step 2 and step 4, where a decoy logical particle is composed of two particles. Therefore, the number of the used particles is $q_2 = 4n + 2n + 2 \cdot (\frac{n}{2} + \frac{n}{2}) = 8n$. Alice encodes her private information by using unitary operation on n-bit single particle sequences in step 4. So the number of classical bits exchanged for decoding of the message is $b_2 = n$. Thus, the qubit efficiency of the protocol against collective-rotation noise is calculated as

$$\eta_2 = \frac{c_2}{q_2 + b_2} = \frac{2n}{\left(4n + 2n + 2 \cdot \left(\frac{n}{2} + \frac{n}{2}\right)\right) + n} = \frac{2}{9} \approx 22.22\%.$$

Table 2 Comparison between our protocols and the other two-party protocols against the collective noises

QKA protocol	Quantum resource	Quantum measurement basis	Qubit efficiency (%)
Huang et al.'s protocol [22]	Logical Bell states	Z-basis and X-basis	16.67
Huang et al.'s protocol [26]	Four-qubit DF states	$ZZXX$-basis and $XZXZ$-basis	10
He et al.'s protocol [23]	Logical χ-states	ZZ-basis and Bell basis	21.05
He et al.'s protocol [27]	Logical GHZ states	ZZ-basis and Bell basis	21.05
Our first protocol	Bell states	Bell basis	25
Our second protocol	Cluster states	Cluster basis and logical X-basis	22.22

The comparison between our protocols and the other two-party protocols against the collective noises is shown in Table 2. From Table 2, we conclude that our agreements are more efficient.

6 Conclusion

The influence of the collective noises on quantum communication is a common problem. However, there are few QKA protocols resisting the collective noises. In this paper, based on logical quantum states, we propose two QKA protocols which can be immune to the collective-dephasing noise and the collective-rotation noise, respectively. By using the decoy logical particles method [35–42], the security of the protocols are guaranteed. By comparison between our protocols and the other two-party protocols against collective noise, it is quite obvious that our protocols are more efficient.

Acknowledgements This work is supported by the National Natural Science Foundation of China (61402265) and the Fund for Postdoctoral Application Research Project of Qingdao (01020120607).

References

1. Bennett, C.H., Brassard, G.: Public-key distribution and coin tossing. In: Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, India, pp. 175–179 (1984)
2. Shor, P.W., Preskill, J.: Simple proof of security of the BB84 quantum key distribution protocol. Phys. Rev. Lett. **85**, 441 (2000)
3. Hwang, W.Y.: Quantum key distribution with high loss: toward global secure communication. Phys. Rev. Lett. **91**, 057901 (2003)
4. Lo, H.K., Ma, X.F., Chen, K.: Decoy state quantum key distribution. Phys. Rev. Lett. **94**, 230504 (2005)
5. Cerf, N.J., Bourennane, M., Karlsson, A., Gisin, N.: Security of quantum key distribution using d-level systems. Phys. Rev. Lett. **88**, 127902 (2002)
6. Lo, H.K., Curty, M., Qi, B.: Measurement-device-independent quantum key distribution. Phys. Rev. Lett. **108**, 130503 (2012)
7. Chang, C.H., Yang, C.W., Hzu, G.R., Hwang, T., Kao, S.H.: Quantum dialogue protocols over collective noise using entanglement of GHZ state. Quantum Inf. Process. **15**, 2971–2991 (2016)
8. Yang, C.W., Tsai, C.W., Hwang, T.: Fault tolerant deterministic quantum communications using GHZ states over collective-noise channels. Quantum Inf. Process. **12**, 3043–3055 (2013)
9. Zhang, K.J., Zhang, W.W., Li, D.: Improving the security of arbitrated quantum signature against the forgery attack. Quantum Inf. Process. **12**, 2655–2669 (2013)
10. Cao, H.J., Zhang, J.F., Liu, J., Li, Z.Y.: A new quantum proxy multi-signature scheme using maximally entangled seven-qubit states. Int. J. Theor. Phys. **55**, 774–780 (2016)
11. Xu, G.B., Zhang, K.J.: A novel quantum group signature scheme without using entangled states. Quantum Inf. Process. **14**, 2577–2587 (2015)
12. Fan, L., Zhang, K.J., Qin, S.J., Guo, F.Z.: A novel quantum blind signature scheme with four-particle GHZ states. Int. J. Theor. Phys. **55**, 1028–1035 (2016)
13. Zhou, N., Zeng, G., Xiong, J.: Quantum key agreement protocol. Electron. Lett. **40**, 1149 (2004)
14. Tsai, C., Hwang, T.: On quantum key agreement protocol. Technical Report, C-S-I-E, NCKU, Taiwan (2009)
15. Chong, S.K., Hwang, T.: Quantum key agreement protocol based on BB84. Opt. Commun. **283**, 1192–1195 (2010)
16. He, Y.F., Ma, W.P.: Two-party quantum key agreement with five-particle entangled states. Int. J. Quantum Inf. **15**(03), 1750018 (2017)

17. Shi, R.H., Zhong, H.: Multi-party quantum key agreement with bell states and bell measurements. Quantum Inf. Process. **12**, 921–932 (2013)
18. Liu, B., Gao, F., Huang, W., Wen, Q.Y.: Multiparty quantum key agreement with single particles. Quantum Inf. Process. **12**, 1797–1805 (2013)
19. 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)
20. Jiang, D.H., Xu, G.B.: Multiparty quantum key agreement protocol based on locally indistinguishable orthogonal product states. Quantum Inf. Process. **17**, 180 (2018)
21. 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)
22. 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)
23. He, Y.F., Ma, W.P.: Two-party quantum key agreement against collective noise. Quantum Inf. Process. **15**, 5023–5035 (2016)
24. Chang, C.H., Yang, C.W., Hwang, T.: Trojan horse attack free fault-tolerant quantum key distribution protocols using GHz states. Int. J. Theor. Phys. **55**(9), 1–12 (2016)
25. Walton, Z.D., Abouraddy, A.F., Sergienko, A.V., Saleh, B.E.A., Teich, M.C.: Decoherence free subspaces in quantum key distribution. Phys. Rev. Lett. **91**, 087901 (2003)
26. Huang, W., Su, Q., Wu, X., Li, Y.B., Sun, Y.: Quantum key agreement against collective decoherence. Int. J. Theor. Phys. **53**, 2891–2901 (2014)
27. He, Y.F., Ma, W.P.: Two robust quantum key agreement protocols based on logical GHz states. Mod. Phys. Lett. **B31**(3), 1750015 (2017)
28. Gao, H., Chen, X.G., Qian, S.R.: Two-party quantum key agreement protocols under collective noise channel. Quantum Inf. Process. **17**, 140 (2018)
29. Li, X.H., Deng, F.G., Zhou, H.Y.: Efficient quantum key distribution over a collective noise channel. Phys. Rev. A **78**, 022321 (2008)
30. Shukla, V., Kothari, C., Banerjee, A., Pathak, A.: On the group-theoretic structure of a class of quantum dialogue protocols. Phys. Lett. A **377**, 518–527 (2013)
31. 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**(5), 361–364 (2006)
32. 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**(4), 440–450 (2005)
33. 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)
34. Cabello, A.: Quantum key distribution in the Holevo limit. Phys. Rev. Lett. **85**, 5633–5638 (2000)
35. 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)
36. Wang, Y.H.: Beyond regular semigroups. Semigroup Forum **92**(2), 414–448 (2016)
37. 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)
38. 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)
39. Zhao, W.C., Li, J., Meng, X.Z.: Dynamical analysis of SIR epidemic model with nonlinear pulse vaccination and lifelong immunity. Discrete Dyn. Nat. Soc. **2015**, 848623 (2015)
40. Cui, Y.J., Zou, Y.M.: An existence and uniqueness theorem for a second order nonlinear system with coupled integral boundary value conditions. Appl. Math. Comput. **256**, 438–444 (2015)
41. Jiang, D.H., Xu, Y.L., Xu, G.B.: Arbitrary Quantum Signature Based on Local Indistinguishability of Orthogonal Product States. Int. J. Theor. Phys. **58**, 1036–1045 (2019)
42. 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)