International Journal of Theoretical Physics (2022) 61: 63
https://doi.org/10.1007/s10773-022-05059-0

Quantum Key Agreement Protocols with GHZ States Under Collective Noise Channels

Ji-hong Guo[1,2,3] · Zhen Yang[1,2,3] · Ming-Qiang Bai[1,2,3] · Zhi-Wen Mo[1,2,3]

Received: 30 December 2021 / Accepted: 14 February 2022 / Published online: 10 March 2022

Abstract
It is necessary to consider the impact of collective noise in quantum key agreement protocols. However, the efficiency of quantum key agreement protocols is generally low under the influence of collective noise. In order to improve the efficiency of the protocols, this paper proposes quantum key agreement protocols that can resist collective noise based on the measurement correlation of logical GHZ states. The efficiency analysis shows that the protocol has a qubit efficiency of 28.57%, which is higher than other protocols. Also, the security analysis proves that the protocols are resistant to external attacks and participant attacks.

Keywords Quantum key agreement · GHZ state · Collective dephasing noise · Collective rotation noise · Qubit efficiency

1 Introduction

With the continuous development of quantum informatics, quantum cryptography [1–6] is constructed based on the basic principles of quantum mechanics, so it has unconditional security in theory. Quantum key agreement (QKA) is an important branch of quantum cryptography. Compared with quantum key distribution (QKD) [7–10], QKA has great research significance because each participant in QKA contributes equally to the final shared key.

In 2004, Zhou et al. [11] presented the first QKA protocol using quantum teleportation, and after that, many QKA protocols [12–15] were proposed one after another. However, most of these QKA protocols are based on quantum communication in an ideal environment. In practical applications, particles are usually affected by noise, and under the cover

✉ Ming-Qiang Bai
baimq@sicnu.edu.cn

1 Institute of Intelligent Information and Quantum Information, Sichuan Normal University, Chengdu, 610068, China

2 National-Local Joint Engineering Laboratory of System Credibility Automatic Verification, Research Center of Sichuan Normal University, Chengdu, 610068, China

3 School of Mathematical Sciences, Sichuan Normal University, Chengdu, 610068, China

of the noise, a malicious attacker can steal information. Therefore, it is necessary to consider the effect of noise on the channel when designing QKA protocols. In 2014, Huang et al. [16] first proposed a QKA protocol to resist collective decoherence. Based on the logical χ states and logical Bell states, He et al. [17] designed two QKA protocols immune to collective noise using measurement correlation and delay measurement techniques for multi-particle entangled states. In 2018, based on four-particle logical GHZ states, Gao et al. [18] presented an improved two-party QKA protocol to resist collective noise with an efficiency of 26.67%. In the same year, Cai et al. [19] proposed two multi-party QKA protocols that are immune to collective noise. In 2019, Yang et al. [20] put forward a two-party QKA protocol based on logical Bell states to resist collective noise with a qubit efficiency of 20%. In the same year, Wang et al. [21] designed two QKA protocols with an efficiency of 25% immune to collective noise, improving the qubit efficiency. In 2020, Tang et al. [22] used logical Bell states to greatly improve the qubit efficiency of the protocol, reaching 27.27%.

To address the efficiency problems in the above QKA protocols immune to collective noise, we propose two-party QKA protocols capable of resisting collective dephasing noise and collective rotational noise, respectively, using the logical GHZ state and its measurement correlation. The safety analysis proves that the protocols are resistant to external attacks as well as participant attacks. Also, the efficiency of our protocols improves by 1.3% over the efficiency of the currently proposed QKA protocols immune to collective noise.

The rest of the article is structured as follows. In Section 2, some basics are presented. Section 3 describes two QKA protocols that are immune to collective noise separately. In Section 4, the security of the protocol is analyzed. The efficiency of qubits in the protocol is calculated in Section 5. Finally, a brief conclusion will be given in Section 6.

2 The Unitary Operations and the Collective Noise

First, the four unitary operations are defined as:

$$\begin{aligned} U_{00} &= I = |0\rangle\langle 0| + |1\rangle\langle 1|, \\ U_{01} &= X = |0\rangle\langle 1| + |1\rangle\langle 0|, \\ U_{10} &= Z = |0\rangle\langle 0| - |1\rangle\langle 1|, \\ U_{11} &= iY = |0\rangle\langle 1| - |1\rangle\langle 0|. \end{aligned} \tag{1}$$

The four Bell states can be denoted as:

$$\begin{aligned} |\phi^{\pm}\rangle &= \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle), \\ |\varphi^{\pm}\rangle &= \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle). \end{aligned} \tag{2}$$

When a unitary operation $U_{i_1 i_2}(i_1 i_2 = 0, 1)$ is performed on the second particle of the Bell state, the Bell state will be transformed into another Bell state. The relationship between the four Bell states and unitary transformation is shown in Table 1.

Second, collective noise is divided into collective dephasing noise and collective rotation noise. The influence of collective dephasing noise (U_{dp}) on normal orthogonal basis $|0\rangle$ and $|1\rangle$ can be described as:

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

Bell state	$U_{00} \otimes U_{00}$	$U_{00} \otimes U_{01}$	$U_{00} \otimes U_{10}$	$U_{00} \otimes U_{11}$
$\|\phi^+\rangle$	$\|\phi^+\rangle$	$\|\varphi^+\rangle$	$\|\phi^-\rangle$	$\|\varphi^-\rangle$
$\|\phi^-\rangle$	$\|\phi^-\rangle$	$\|\varphi^-\rangle$	$\|\phi^+\rangle$	$\|\varphi^+\rangle$

$$U_{dp}|0\rangle = |0\rangle, U_{dp}|1\rangle = e^{i\varphi}|1\rangle, \tag{3}$$

where φ is the phase noise parameter that vary with time. In order to eliminate the influence of collective dephasing noise, logical qubits $|0_{dp}\rangle = |01\rangle$ and $|1_{dp}\rangle = |10\rangle$ are proposed. Their superposition states can be denoted as:

$$\begin{aligned} |+_{dp}\rangle &= \frac{1}{\sqrt{2}}(|0_{dp}\rangle + |1_{dp}\rangle), \\ |-_{dp}\rangle &= \frac{1}{\sqrt{2}}(|0_{dp}\rangle - |1_{dp}\rangle). \end{aligned} \tag{4}$$

The influence of collective rotation noise (U_r) on normal orthogonal basis $|0\rangle$ and $|1\rangle$ can be described as:

$$U_r|0\rangle = cos\theta|0\rangle + sin\theta|1\rangle, U_r|1\rangle = -sin\theta|0\rangle + cos\theta|1\rangle, \tag{5}$$

where θ is the rotation noise parameter that vary with time. In order to eliminate the influence of collective rotation noise, logical qubits $|0_r\rangle = |\phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ and $|1_r\rangle = |\psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$ are proposed. Their superposition states are described as follows:

$$\begin{aligned} |+_r\rangle &= \frac{1}{\sqrt{2}}(|0_r\rangle + |1_r\rangle) = \frac{1}{\sqrt{2}}(|\phi^+\rangle + |\psi^-\rangle), \\ |-_r\rangle &= \frac{1}{\sqrt{2}}(|0_r\rangle - |1_r\rangle) = \frac{1}{\sqrt{2}}(|\phi^+\rangle - |\psi^-\rangle). \end{aligned} \tag{6}$$

3 Description of the QKA Protocols Under Collective Noise Channels

3.1 The QKA Protocol Under Collective-dephasing Noise

In both protocols, the following three-particle GHZ states [23] is used as the quantum source, that is

$$\begin{aligned} |\eta\rangle_{123} &= \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)_{123} \\ &= \frac{1}{\sqrt{2}}(|\phi^+\rangle_{12}|+\rangle_3 + |\phi^-\rangle_{12}|-\rangle_3). \end{aligned} \tag{7}$$

According to (7), when performing Bell measurements on particles 1 and 2 in $|\eta\rangle_{123}$ state and peforming X basis measurement on particle 3 respectively, the state $|\eta\rangle_{123}$ will collapse to states $|\phi^+\rangle_{12}|+\rangle_3$ and $|\phi^-\rangle_{12}|-\rangle_3$ with the probability of $\frac{1}{2}$.

Suppose Alice and Bob want to negotiate a common key $K = (K_A^1 \| K_B^1) \| (K_A^2 \| K_B^2) \| \ldots \| (K_A^n \| K_B^n)$. First, Alice and Bob randomly generate their own $2n$ bit keys:

$$K_A = K_A^1 \| K_A^2 \| \ldots \| K_A^n,$$

$$K_B = K_B^1 \| K_B^2 \| \ldots \| K_B^n,$$

where $K_A^i, K_B^i \in \{00, 01, 10, 11\}$ and $i = 1, 2, \ldots, n$. The steps of the protocol are given below.

Step 1 Alice prepares n logical GHZ states $|\eta_{dp}\rangle_{ABC}$:

$$\begin{aligned} |\eta_{dp}\rangle_{ABC} &= \frac{1}{\sqrt{2}}(|0\rangle|0\rangle|0_{dp}\rangle + |1\rangle|1\rangle|1_{dp}\rangle)_{ABC} \\ &= \frac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_B|01\rangle_{C_1C_2} + |1\rangle_A|1\rangle_B|10\rangle_{C_1C_2}), \end{aligned} \tag{8}$$

and divides all particles into three sequences S_1, S_2 and S_3, where sequence S_i is composed of the i-th particle of all $|\eta_{dp}\rangle_{ABC}$ states. In S_3, the logical qubit C is composed of two physical qubits C_1 and C_2. Alice randomly selects enough decoy particles from set $\{|0_{dp}\rangle, |1_{dp}\rangle, |+_{dp}\rangle, |-_{dp}\rangle\}$ and inserts them into sequences S_3 to obtain new sequences S_3^*. Alice sends S_3^* to Bob and retains sequences S_1 and S_2.

Step 2 When Bob receives sequence S_3^*, Alice announces the position of the decoy photons and the corresponding measurement basis $\{|0_{dp}\rangle, |1_{dp}\rangle\}$ or $\{|+_{dp}\rangle, |-_{dp}\rangle\}$. Then, Bob uses the correct measurement basis to measure the corresponding decoy logical particles and tells Alice the measurement results. Alice compares the measurement results with the initial states of the decoy photons and calculates the error rate. If the error rate less than a predetermined threshold, the protocol continues. If the error rate exceeds the threshold, Alice and Bob terminate the agreement and restart.

Step 3 After security detection, Bob discards the decoy particles and returns to sequence S_3. A $CNOT$ operation uses C_1 as the control qubit and C_2 as the target qubit. After $CNOT$ operation, each logic GHZ state $|\eta_{dp}\rangle_{ABC}$ is converted to

$$\begin{aligned} |\eta_{dp}^*\rangle_{ABC} &= CNOT(C_1, C_2)|\eta_{dp}\rangle_{ABC} \\ &= \frac{1}{\sqrt{2}}(|0001\rangle + |1111\rangle)_{ABC_1C_2} \\ &= \frac{1}{\sqrt{2}}(|\eta\rangle_{ABC_1}) \otimes |1\rangle_{C_2}. \end{aligned} \tag{9}$$

Alice, Bob share n $|\eta_{dp}^*\rangle$ states. Alice performs Bell measurement on the corresponding particles in sequences S_1 and S_2, while Bob performs X basis measurement on the particles C_1 in sequence S_3, Alice and Bob negotiate coding rules, $|+\rangle \rightarrow 00$, $|-\rangle \rightarrow 11$. Bob records the measurement results as $H_B = H_B^1 \| H_B^2 \| \ldots \| H_B^n$, where H_B^i is Bob's i-th measurement result, and $H_B^i \in \{00, 11\}$. Due to the measurement correlation of η state, Alice and Bob can infer each other's measurement results. Alice knows Bob's measured value H_B, Bob knows the initial Bell states of the corresponding particles in sequences S_1, S_2.

Step 4 Alice performs unitary transformation $U_{i_1 i_2}$ on the i^{th} particle in the sequence S_2 according to her own key $K_A^i (i = 1, 2, \ldots, n)$ to obtain a new sequence S_2^*. The subscripts $i_1 i_2$ corresponds to the values of $K_A^i (i = 1, 2, \ldots, n)$. Then, S_1, S_2^* form new Bell states. According to the new Bell states, Alice prepares their corresponding logical Bell states $S_{1(1)}$, $S_{2(1)}^*$ as follows. Logical Bell states $S_{1(1)}$, $S_{2(1)}^*$ are composed of logical qubits A(two physical qubits A_1 and A_2) and logical qubits B(two physical qubits B_1 and B_2). Alice performs a permutation operation $\prod_n$ on $S_{1(1)}$ to obtain a randomized sequence $S_{1(1)}^*$. Then, Alice randomly selects enough decoy photons from set $\{|0_{dp}\rangle, |1_{dp}\rangle\}$ or $\{|+_{dp}\rangle, |-_{dp}\rangle\}$ and inserts sequences $S_{1(1)}^*$ and $S_{2(1)}^*$ to obtain two new sequences $S_{1(1)}^{**}$ and $S_{2(1)}^{**}$. Finally, she sends the two new sequences to Bob.

$$
\begin{aligned}
|\phi_{dp}^+\rangle_{A_1A_2B_1B_2} &= \frac{1}{\sqrt{2}}(|0_{dp}\rangle|0_{dp}\rangle + |1_{dp}\rangle|1_{dp}\rangle)_{A_1A_2B_1B_2} \\
&= \frac{1}{\sqrt{2}}(|\phi^+\rangle|\phi^+\rangle - |\phi^-\rangle|\phi^-\rangle)_{A_1B_1A_2B_2} \\
|\phi_{dp}^-\rangle_{A_1A_2B_1B_2} &= \frac{1}{\sqrt{2}}(|0_{dp}\rangle|0_{dp}\rangle - |1_{dp}\rangle|1_{dp}\rangle)_{A_1A_2B_1B_2} \\
&= \frac{1}{\sqrt{2}}(|\phi^-\rangle|\phi^+\rangle - |\phi^+\rangle|\phi^-\rangle)_{A_1B_1A_2B_2}
\end{aligned} \tag{10}
$$

$$
\begin{aligned}
|\psi_{dp}^+\rangle_{A_1A_2B_1B_2} &= \frac{1}{\sqrt{2}}(|0_{dp}\rangle|1_{dp}\rangle + |1_{dp}\rangle|0_{dp}\rangle)_{A_1A_2B_1B_2} \\
&= \frac{1}{\sqrt{2}}(|\psi^+\rangle|\psi^+\rangle - |\psi^-\rangle|\psi^-\rangle)_{A_1B_1A_2B_2} \\
|\psi_{dp}^-\rangle_{A_1A_2B_1B_2} &= \frac{1}{\sqrt{2}}(|0_{dp}\rangle|1_{dp}\rangle - |1_{dp}\rangle|0_{dp}\rangle)_{A_1A_2B_1B_2} \\
&= \frac{1}{\sqrt{2}}(|\psi^-\rangle|\psi^+\rangle - |\psi^+\rangle|\psi^-\rangle)_{A_1B_1A_2B_2}.
\end{aligned} \tag{11}
$$

Step 5 After Bob receives sequences $S_{1(1)}^{**}$ and $S_{2(1)}^{**}$, Alice and Bob perform the second eavesdropping detection. The second eavesdropping detection is the same as the first eavesdropping detection. If the error rate is lower than the predetermined threshold, both parties continue the following steps. Otherwise, they will terminate the agreement and start again.

Step 6 Bob publicly announces the value of K_B^*, where $K_B^* = K_B \oplus H_B = (K_B^1 \oplus H_B^1) \| (K_B^2 \oplus H_B^2) \| \ldots \| (K_B^n \oplus H_B^n)$, through the classical channel. According to the value of H_B, Alice can calculate K_B and get the shared key K.

Step 7 Alice publicly announces the permutation operation $\prod_n$, and Bob performs the corresponding inverse permutation on the sequence $S_{1(1)}^*$ to obtain the original sequence $S_{1(1)}$. Next, Bob performs Bell measurements on the particles A_1, B_1 and A_2, B_2 in sequences $S_{1(1)}$ and $S_{2(1)}^*$. Based on the measurement results, Bob can know the logical Bell states constituted by $S_{1(1)}$ and $S_{2(1)}^*$, thus know the Bell states constituted by S_1, S_2^*. According to the initial Bell states, Bob can calculate K_A and generate the shared key K.

3.2 The QKA Protocol Under Collective-Rotation Noise

As the first QKA protocol, Alice and Bob want to negotiate a common key K. The negotiation steps are as follows.

Step 1 Alice prepares n logical GHZ states $|\eta_r\rangle_{ABC}$:

$$\begin{aligned}|\eta_r\rangle_{ABC} &= \frac{1}{\sqrt{2}}(|0\rangle|0\rangle|0_r\rangle + |1\rangle|1\rangle|1_r\rangle)_{ABC} \\ &= \frac{1}{2}(|0\rangle_A|0\rangle_B|\phi^+\rangle_{C_1C_2} + |1\rangle_A|1\rangle_B|\varphi^-\rangle_{C_1C_2}),\end{aligned} \tag{12}$$

and divides all particles into three sequences S_1, S_2 and S_3, where sequence S_i is composed of the i-th particle of all $|\eta_r\rangle_{ABC}$ states. In S_3, the logical qubit C is composed of two physical qubits C_1 and C_2. Meanwhile, all the physical qubits C_1 form the sequence S_{31} and C_2 form S_{32}. Alice randomly selects enough decoy particles from set $\{|0_r\rangle, |1_r\rangle, |+_r\rangle, |-_r\rangle\}$ and inserts them into sequences S_3 to obtain new sequences S_3^*. Alice sends S_3^* to Bob and retains sequences S_1 and S_2.

Step 2 When Bob receives sequence S_3^*, Alice announces the position of the decoy particles and the corresponding measurement basis $\{|0_r\rangle, |1_r\rangle\}$ or $\{|+_r\rangle, |-_r\rangle\}$. Then, Bob uses the correct measurement basis to measure the corresponding decoy logical particles and tells Alice the measurement results. Alice compares the measurement results with the initial states of the decoy particles and calculates the error rate. If the error rate less than a predetermined threshold, the protocol continues. If the error rate exceeds the threshold, Alice and Bob terminate the agreement and restart.

Step 3 After security detection, Bob discards the decoy particles and recovers sequence S_3. At this point, Alice, Bob share n $|\eta_r\rangle$ states, Alice performs Z basis measurement on the corresponding particles in sequences S_1 and S_2, while Bob performs Bell measurement on the particles C_1 and C_2 in S_{31} and S_{32}, Alice and Bob negotiate coding rules, $|00\rangle \rightarrow 00$, $|11\rangle \rightarrow 11$, $|01\rangle \rightarrow 01$, $|10\rangle \rightarrow 10$. Alice records the measurement results as $H_A = H_A^1 \| H_A^2 \| \ldots \| H_A^n$, where H_A^i is the i-th measurement of Alice. Due to the measurement correlation of $|\eta\rangle_{ABC}$, Alice and Bob can infer each other's measurement results. That is to say, Bob knows Alice's measured value H_A. Alice knows the initial Bell states consisting of the corresponding particles in sequence S_3.

Step 4 Bob performs the $U_{i_1 i_2}$ operation on the particles C_2 of the sequence S_{32}, according to his own key $K_B^i (i = 1, 2, \ldots, n)$ to obtain a new sequence S_{32}^*. The subscripts $i_1 i_2$ corresponds to the values of $K_B^i (i = 1, 2, \ldots, n)$. Then, S_{31}, S_{32}^* form new Bell states. According to the new Bell states, Bob prepares their corresponding logical Bell states $S_{3(1)}$, $S_{3(2)}^*$ as follows. Logical Bell states $S_{3(1)}$, $S_{3(2)}^*$ are composed of logical qubit C_1(two physical qubits C_{11} and C_{12}) and logical qubit C_2(two physical qubits C_{21} and C_{22}). Then, Bob performs a permutation operation $\prod_n$ on $S_{3(1)}$ to obtain a randomized sequence $S_{3(1)}^*$ and randomly selects enough decoy photons from set $\{|0_r\rangle, |1_r\rangle, |+_r\rangle, |-_r\rangle\}$ inserts sequences $S_{3(1)}^*$ and $S_{3(2)}^*$ to obtain

two new sequences $S^{**}_{3(1)}$ and $S^{**}_{3(2)}$. Finally, he sends the two sequences to Alice.

$$\begin{aligned}
|\phi_r^+\rangle_{C_{11}C_{12}C_{21}C_{22}} &= \frac{1}{\sqrt{2}}(|0_r\rangle|0_r\rangle + |1_r\rangle|1_r\rangle)_{C_{11}C_{12}C_{21}C_{22}} \\
&= \frac{1}{\sqrt{2}}(|\phi^+\rangle|\phi^+\rangle + |\psi^-\rangle|\psi^-\rangle)_{C_{11}C_{21}C_{12}C_{22}} \\
|\phi_r^-\rangle_{C_{11}C_{12}C_{21}C_{22}} &= \frac{1}{\sqrt{2}}(|0_r\rangle|0_r\rangle - |1_r\rangle|1_r\rangle)_{C_{11}C_{12}C_{21}C_{22}} \\
&= \frac{1}{\sqrt{2}}(|\phi^-\rangle|\phi^-\rangle + |\psi^+\rangle|\psi^+\rangle)_{C_{11}C_{21}C_{12}C_{22}} \\
|\psi_r^+\rangle_{C_{11}C_{12}C_{21}C_{22}} &= \frac{1}{\sqrt{2}}(|0_r\rangle|1_r\rangle + |1_r\rangle|0_r\rangle)_{C_{11}C_{12}C_{21}C_{22}} \\
&= \frac{1}{\sqrt{2}}(|\phi^-\rangle|\psi^+\rangle - |\psi^+\rangle|\phi^-\rangle)_{C_{11}C_{21}C_{12}C_{22}} \\
|\psi_r^-\rangle_{C_{11}C_{12}C_{21}C_{22}} &= \frac{1}{\sqrt{2}}(|0_r\rangle|1_r\rangle - |1_r\rangle|0_r\rangle)_{C_{11}C_{12}C_{21}C_{22}} \\
&= \frac{1}{\sqrt{2}}(|\phi^+\rangle|\psi^-\rangle - |\psi^-\rangle|\phi^+\rangle)_{C_{11}C_{21}C_{12}C_{22}}. \qquad (13)
\end{aligned}$$

Step 5 After Alice receives sequences $S^{**}_{3(1)}$ and $S^{**}_{3(2)}$, Alice and Bob perform the second eavesdropping detection. The second eavesdropping detection is the same as the first eavesdropping detection. If the error rate is lower than the predetermined threshold, both parties continue the following steps. Otherwise, they will terminate the agreement and start again.

Step 6 Alice tells Bob the value of K^*_A, where $K^*_A = K_A \oplus H_A = (K^1_A \oplus H^1_A)\|(K^2_A \oplus H^2_A)\| \ldots \|(K^n_A \oplus H^n_A)$. According to the value of H_A, Bob can infer K_A and calculate the shared key K of both parties.

Step 7 Bob publicly announces the permutation operation $\prod_n$, and Alice performs the corresponding inverse permutation operation on the sequence $S^*_{3(1)}$ to obtain the original sequence $S_{3(1)}$. Next, Alice performs Bell measurements on the particles C_{11}, C_{21} and C_{12}, C_{22} in sequences $S_{3(1)}$ and $S^*_{3(2)}$. Based on the measurement results, Bob is able to know the logical Bell states constituted by $S_{3(1)}$ and $S^*_{3(2)}$, thus know the Bell states constituted by S_{31}, S^*_{32}. According to the initial Bell states, Bob can calculate K_A and generate the shared key K.

4 Security Analysis

In the above QKA protocols, the transmitted particles are logical particles that immune to noise interference. Therefore, the two QKA protocols can resist collective dephasing noise and collective rotation noise respectively. In this section, we will discuss the security of the two protocols. The QKA protocol mainly involves two kinds of attacks, including participant attacks and outsider attacks, the outsider attacks include Trojan-horse attack, Intercept-resend attack, Measure-resend attack and Entangle-measure attack. The security analysis will show that the proposed QKA protocols can completely resist these attacks.

Participant attacks The delay measurement technique ensures that Bob cannot know the key K_A before he announces K^*_B, so he cannot change his key K_B according to K_A.

Therefore, he cannot successfully execute the participant attack. On the other hand, Alice can only deduce K_B after sending the encoded information to Bob, so he can't change K_A according to K_B. Thus, Alice can't execute participant attack either.

Trojan-horse attack Trojan attacks mainly include invisible photonic eavesdropping(IPE) and delayed photonic Trojan attacks [24]. Our propose first protocol under collective-dephasing is a one-way QKA protocol. All particles are transmitted only once in the channel, the Trojan-horse attacker has no chance to extract the spy photons from the particle sequences. But in the second protocol under collective-rotation, since the sequence S_3 is transmitted twice in the quantum channel, it is possible to receive a Trojan horse attack during the transmission. Fortunately, current technology is well able to defend against such attacks. To be protected from Eve's IPE attack, a filter is added before all of Bob's devices so that Eve's invisible photons will be eavesdropped, and a photon splitter (PNS) is able to split each signal into two parts, thus enabling protection from delayed photon Trojan-horse attacks. In conclusion, in our protocols, an outside eavesdropper Eve is unable to get the agreement key by performing Trojan-horse attack.

Intercept-resend attack Take the QKA protocol under collective dephasing noise as an example. If Eve executes the intercept-resend attack, he intercepts S_3^* firstly, and then sends the prepared sequence to Bob. However, Eve does not know the position of the decoy particles in sequence S_3^* and the measurement basis used, so the sequences forged by Eve cannot pass the first security detection. Similarly, when Eve intercepts S_1^{**} and S_2^{**}, its malicious behavior will also be found in the second security detection. When m decoy particles are used to detect this eavesdropping attack, the probability of Eve attack being found is $1-\frac{1}{2^m}$.

Measure-resend attack Take the first protocol as an example. Suppose Eve can perform measure-resend attacks on particles in sequences S_3^*, S_1^{**} and S_2^{**} respectively. However, the measurement of Eve will affect the status of decoy particles in S_3^*, S_1^{**} and S_2^{**}. In the first and second security tests, the probability of Eve attack being found is $1-(\frac{3}{4})^m$ (m refers to the number of decoy particles).

Entangle-measure attack In both protocols, assuming that Eve wants to perform an entangle-measure attack on the protocol using his pre-prepared auxiliary particles, he needs to perform the operation $\widehat{U}$ on the intercepted quantum state. As an example, the process and results of the QKA protocol for immune collective dephasing noise are as follows.

$$\widehat{U}(|0_{dp}\rangle|E\rangle) = a_{00}|00\rangle|e_{00}\rangle + a_{01}|01\rangle|e_{01}\rangle + a_{10}|10\rangle|e_{10}\rangle + a_{11}|11\rangle|e_{11}\rangle \tag{14}$$

$$\widehat{U}(|1_{dp}\rangle|E\rangle) = b_{00}|00\rangle|e_{00}^*\rangle + b_{01}|01\rangle|e_{01}^*\rangle + b_{10}|10\rangle|e_{10}^*\rangle + b_{11}|11\rangle|e_{11}^*\rangle \tag{15}$$

$$\begin{aligned}\widehat{U}(|+_{dp}\rangle|E\rangle) &= \frac{1}{\sqrt{2}}(\widehat{U}|0_{dp}\rangle|E\rangle + \widehat{U}|1_{dp}\rangle|E\rangle)\\ &= \frac{1}{2}[|\phi^+\rangle(a_{00}|e_{00}\rangle + a_{11}|e_{11}\rangle + b_{00}|e_{00}^*\rangle + b_{11}|e_{11}^*\rangle)\\ &\quad +|\phi^-\rangle(a_{00}|e_{00}\rangle - a_{11}|e_{11}\rangle + b_{00}|e_{00}^*\rangle - b_{11}|e_{11}^*\rangle)\\ &\quad +|\psi^+\rangle(a_{01}|e_{01}\rangle + a_{10}|e_{10}\rangle + b_{01}|e_{01}^*\rangle + b_{10}|e_{10}^*\rangle)\\ &\quad +|\psi^-\rangle(a_{01}|e_{01}\rangle - a_{10}|e_{10}\rangle + b_{01}|e_{01}^*\rangle - b_{10}|e_{10}^*\rangle)]\end{aligned} \tag{16}$$

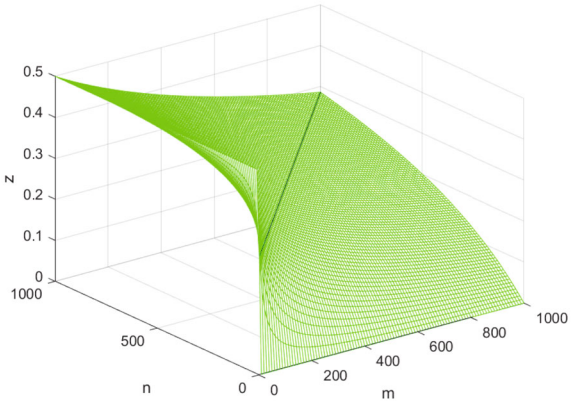

Fig. 1 Effect of changes in the number of decoy particles and quantum states on the qubit efficiency

$$\begin{aligned}\widehat{U}(|-_{dp}\rangle|E\rangle) &= \frac{1}{\sqrt{2}}(\widehat{U}|0_{dp}\rangle|E\rangle - \widehat{U}|1_{dp}\rangle|E\rangle)\\ &= \frac{1}{2}[|\phi^+\rangle(a_{00}|e_{00}\rangle + a_{11}|e_{11}\rangle - b_{00}|e^*_{00}\rangle - b_{11}|e^*_{11}\rangle)\\ &\quad +|\phi^-\rangle(a_{00}|e_{00}\rangle - a_{11}|e_{11}\rangle - b_{00}|e^*_{00}\rangle + b_{11}|e^*_{11}\rangle)\\ &\quad +|\psi^+\rangle(a_{01}|e_{01}\rangle + a_{10}|e_{10}\rangle - b_{01}|e^*_{01}\rangle - b_{10}|e^*_{10}\rangle)\\ &\quad +|\psi^-\rangle(a_{01}|e_{01}\rangle - a_{10}|e_{10}\rangle - b_{01}|e^*_{01}\rangle + b_{10}|e^*_{10}\rangle)]. \end{aligned} \tag{17}$$

Where, $|e_{00}\rangle$, $|e_{01}\rangle$, $|e_{10}\rangle$, $|e_{11}\rangle$, $|e^*_{00}\rangle$, $|e^*_{01}\rangle$, $|e^*_{10}\rangle$, $|e^*_{11}\rangle$ are pure states determined by unitary transformation $\widehat{U}$, and $|a_{00}|^2+|a_{01}|^2+|a_{10}|^2+|a_{11}|^2 = 1$, $|b_{00}|^2+|b_{01}|^2+|b_{10}|^2+|b_{11}|^2 = 1$. If Eve wants to successfully pass the security detection, the following equations must hold.

$$\begin{cases} a_{00}|00\rangle|e_{00}\rangle + a_{10}|10\rangle|e_{10}\rangle + a_{11}|11\rangle|e_{11}\rangle = 0\\ b_{00}|00\rangle|e_{00}\rangle + b_{11}|11\rangle|e_{11}\rangle + b_{01}|01\rangle|e_{01}\rangle = 0\\ |\phi^+\rangle(a_{00}|e_{00}\rangle + a_{11}|e_{11}\rangle + b_{00}|e^*_{00}\rangle + b_{11}|e^*_{11}\rangle)+\\ |\phi^-\rangle(a_{00}|e_{00}\rangle - a_{11}|e_{11}\rangle + b_{00}|e^*_{00}\rangle - b_{11}|e^*_{11}\rangle)+\\ |\psi^-\rangle(a_{01}|e_{01}\rangle - a_{10}|e_{10}\rangle + b_{01}|e^*_{01}\rangle - b_{10}|e^*_{10}\rangle)] = 0\\ |\phi^+\rangle(a_{00}|e_{00}\rangle + a_{11}|e_{11}\rangle - b_{00}|e^*_{00}\rangle - b_{11}|e^*_{11}\rangle)+\\ |\phi^-\rangle(a_{00}|e_{00}\rangle - a_{11}|e_{11}\rangle - b_{00}|e^*_{00}\rangle + b_{11}|e^*_{11}\rangle)+\\ |\psi^+\rangle(a_{01}|e_{01}\rangle + a_{10}|e_{10}\rangle - b_{01}|e^*_{01}\rangle - b_{10}|e^*_{10}\rangle) = 0. \end{cases} \tag{18}$$

According to (18), $|a_{00}| = |a_{10}| = |a_{11}| = |b_{00}| = |b_{01}| = |b_{11}| = 0$, $|e_{01}\rangle = |e^*_{10}\rangle$. Obviously, if Eve doesn't want to be found in the security detection, he won't get any information about the shared key. Therefore, the protocol can resist entangle-measure attacks.

Table 2 Comparison of our protocol and the other QKA protocols

QKA protocol	Quantum resource	Quantum measurement basis	Efficiency
Huang's [15]	Logical Bell states	Single particles	16.67%
He's [17]	Logical χ states	Bell basis and single particles	21.05%
Yang's [20]	Logical Bell states	Logical Bell basis	21.05%
Wang's [21]	Bell states	Bell basis and cluster basis	25%
Gao's [18]	Logical χ states	Bell basis and single particles	26.67%
Tang's [22]	Logical Bell states	X-basis and Bell-basis	27.27%
Ours	Logical GHZ states	X-basis and Bell-basis	28.57%

5 Efficiency Analysis

In QKA protocol, Cabello's [25] method is used to evaluate qubit efficiency which is defined as

$$\eta = \frac{c}{q+b}, \tag{19}$$

where c is the number of classical bits negotiated, q is the number of qubits (including the number of decoy particles) used in the protocol and b is the number of classical bits exchanged for decoding the message. In the proposed QKA protocol, the number of classical bits negotiated is $c = 4n$, the total number of qubits used in the protocol is $q = 6n + 2m + 4m$, Bob decodes Alice's key by U-transformations, so the number of classical bits exchanged for decoding the message is $2n$. Therefore, the qubit efficiency of this protocol is as follows: $\eta = \frac{4n}{6n+2m+4m+2n}$, where m refers to the number of decoy particles, n refers to the number of quantum states. As shown in the Fig. 1. when $m < n$, on the left side of the line $m = n$, this case is considered as an unclassified condition and should be excluded. When $m > n$, the value of the qubit efficiency in this case becomes lower. The value of the qubit efficiency reaches the optimal value only when $m = n$, i.e. $\eta = \frac{2}{7} = 28.57\%$. The comparison between this protocol and the existing secure QKA protocols that are resistant to collective noise is shown in the Table 2. Obviously, our protocols have higher qubit efficiency.

6 Conclusion

In this paper, two QKA protocols immune to collective dephasing noise and collective rotation noise are proposed by exploiting the measurement correlation of three-particle GHZ states, respectively. The qubit efficiency reaches 28.57%, which improves the efficiency. Besides, the proposed protocols only use Bell measurements and X basis measurements, which can be easily implemented in the existing technology. Finally, the security analysis also shows that the proposed protocols are resistant to external attacks and internal participants attacks. Using the logical GHZ state, our proposed QKA protocols immune to collective noise is more efficient than previous protocols. But in fact, this efficiency is still extremely low. Therefore, how to improve the efficiency of QKA protocols that are immune to noise may be the next step we should consider.

Acknowledgements This work is supported by the National Natural Science Foundation of China (Grant No.11671284) and Sichuan Science and Technology Program(Grant NO.2020YFG0290).

Author Contributions In fact, all of the authors' contributions to this paper are important. The specific contributions are as follows. The first author played a major role in the conceptualization and writing of the article. The second author worked mainly on the overall framework and language of the article. The third and fourth authors mainly guided the article in terms of its core ideas and expertise.

Data Availability The datasets generated during and/or analysed during the current study are available from the corresponding author on reasonable request.

References

1. Gottesman, D.: Phys. Rev. A **61**, 042311 (2000). https://doi.org/10.1103/PhysRevA.61.042311
2. Zhang, J.Z., Li, Y., Man, Z.X.: Phys. Rev. A **71**, 044301 (2005). https://doi.org/10.1103/PhysRevA.71.044301
3. Deng, G.F., Long, G.L., Liu, X.S.: Phys. Rev. A **68**, 042317 (2003). https://doi.org/10.1103/PhysRevA.68.042317
4. Jiang, D.H., Xu, Y.L., Xu, G.B.: Int. J. Theor. Phys. **58**(3), 1036 (2019). https://search.ebscohost.com/login.aspx?direct=true&db=aph&AN=134870032&lang=zh-cn&site=ehost-live
5. Wang, T.Y., Wen, Q.Y., Chen, X.B.: Opt. Commun. **283**(24), 5261 (2010). https://doi.org/10.1016/j.optcom.2010.07.022. https://www.sciencedirect.com/science/article/pii/S0030401810007583
6. Guo, G., Guo, G.: Phys. Lett. A **310**(4), 247 (2003). https://search.ebscohost.com/login.aspx?direct=true&db=aph&AN=9446107&lang=zh-cn&site=ehost-live
7. Allati, A., Baz, M., Hassouni, Y.: Quantum Inf. Process **10**(5), 589 (2011). https://search.ebscohost.com/login.aspx?direct=true&db=aph&AN=65020733&lang=pt-br&site=ehost-live
8. Lo, H., Chau, H.: Science **283**(5410), 2050 (1999). https://search.ebscohost.com/login.aspx?direct=true&db=aph&AN=1703227&lang=zh-cn&site=ehost-live
9. Bourennane, M., Karlsson, A., Björk, G.: Phys. Rev. A **64**, 012306 (2001). https://doi.org/10.1103/PhysRevA.64.012306
10. Gao, F., Guo, F., Wen, Q., Zhu, F.: Phys. Lett. A **349**(1-4), 53 (2006). https://search.ebscohost.com/login.aspx?direct=true&db=aph&AN=19338818&lang=zh-cn&site=ehost-live
11. Zhou, N., Zeng, G., Xiong, J.: Electron. Lett. (Inst. Eng. Technol.) **40**(18), 1149 (2004). https://search.ebscohost.com/login.aspx?direct=true&db=buh&AN=14329439&lang=zh-cn&site=ehost-live
12. Chong, S.K., Hwang, T.: Opt. Commun. **283**(6), 1192 (2010). https://doi.org/10.1016/j.optcom.2009.11.007. https://www.sciencedirect.com/science/article/pii/S0030401809011316
13. Tsai, C.W., Chong, S.K., Hwang, T.: Nephron Clinical Practice, pp 47–49 (2010)
14. Shi, R.H., Zhong, H.: Quantum Inf. Process. **12**(2), 921 (2013). https://search.ebscohost.com/login.aspx?direct=true&db=aph&AN=84695721&lang=zh-cn&site=ehost-live
15. Huang, W., Wen, Q.Y., Liu, B., Gao, F., Sun, Y.: Quantum Inf. Process. **13**(3), 649 (2014). https://search.ebscohost.com/login.aspx?direct=true&db=aph&AN=94231656&lang=zh-cn&site=ehost-live
16. Huang, W., Su, Q., Wu, X., Li, Y.B., Sun, Y.: Int. J. Theor. Phys. **53**(9), 2891 (2014). https://search.ebscohost.com/login.aspx?direct=true&db=aph&AN=97460852&lang=zh-cn&site=ehost-live
17. He, Y.F., Ma, W.P.: Quantum Inf. Process. **15**(12), 5023 (2016). https://search.ebscohost.com/login.aspx?direct=true&db=aph&AN=119629325&lang=zh-cn&site=ehost-live
18. Gao, H., Chen, X.G., Qian, S.R.: Quantum Inf. Process. **17**(6), 1 (2018). https://search.ebscohost.com/login.aspx?direct=true&db=aph&AN=129928283&lang=pt-br&site=ehost-live
19. Cai, B.B., Guo, G.D., Lin, S., Zuo, H.J., Yu, C.H.: IEEE Photon. J. **10**(1), 1 (2018). https://doi.org/10.1109/JPHOT.2018.2797535
20. Yang, Y.G., Gao, S., Li, D., Zhou, Y.H., Shi, W.M.: Quantum Inf. Process. **18**(3), 1 (2019). https://search.ebscohost.com/login.aspx?direct=true&db=aph&AN=135041039&lang=zh-cn&site=ehost-live
21. Wang, S.S., Jiang, D.H., Xu, G.B., Zhang, Y.H., Liang, X.Q.: Quantum Inf. Process. **18**(6), 190 (2019). https://doi.org/10.1007/s11128-019-2305-7
22. Tang, J., Shi, L., Wei, J.: Ad. Lasers Optoelectron. **40**(18), 1149 (2020). https://search.ebscohost.com/login.aspx?direct=true&db=buh&AN=14329439&lang=zh-cn&site=ehost-live
23. Ye, T.Y.: Int. J. Theor. Phys. **53**(11), 3719 (2014). https://search.ebscohost.com/login.aspx?direct=true&db=aph&AN=98676669&lang=pt-br&site=ehost-live

24. Li, X.H., Deng, F.G., Zhou, H.Y.: Phys. Rev. A **74**, 054302 (2006). https://doi.org/10.1103/PhysRevA.74.054302
25. Cabello, A.: Phys. Rev. Lett. **85**, 5635 (2000). https://doi.org/10.1103/PhysRevLett.85.5635