Measurement-Device-Independent Quantum Key Agreement against Collective Noisy Channel

Yi-Hua Zhou\textsuperscript{1,2} · Yang Xu\textsuperscript{1,2} · Yu-Guang Yang\textsuperscript{1,2} · Wei-Min Shi\textsuperscript{1,2} · Ze-Song Chen\textsuperscript{1,2}

Received: 25 May 2022 / Accepted: 9 July 2022 / Published online: 23 July 2022
© The Author(s), under exclusive licence to Springer Science+Business Media, LLC, part of Springer Nature 2022

Abstract
Quantum key agreement (QKA) permits participants to constitute a shared key on a quantum channel, while no participants can independently determine the shared key. However, existing Measurement-device-independent (MDI) protocols cannot resist channel noise, and noise-resistant QKA protocols cannot resist side-channel attacks caused by equipment defects. In this paper, we design a MDI-QKA protocol against collective-dephasing noise based on GHZ states. First, in our protocol, Alice and Bob prepare a certain number of GHZ states respectively, and then send two particles of each GHZ state to Charlie for bell measurement. Results are that Alice and Bob can obtain Bell states through entanglement exchange with the help of dishonest Charlie. Meanwhile our protocol can ensure the transmission process noise-resisted. Then, Alice and Bob encode their key components to the particle in their hands and construct logical quantum states against collective noise through additional particles and CNOT operation to implement MDI-QKA. Compared with existing MDI-QKA protocols, our protocol uses logical quantum states during particle transmission, which makes the protocol immune to collective-dephasing noise and thus improves the final key rate. Security analysis shows that our protocol can resist common insider and outsider attacks.

Keywords Quantum cryptography · Quantum key agreement · Collective noise · Measurement-device-independent
1 Introduction

Quantum cryptography combines classical cryptography and quantum mechanics to ensure unconditional security based on quantum laws. Quantum cryptography includes many important branches such as quantum key distribution [1–5], quantum key agreement (QKA) [6, 7], quantum secret sharing [8, 9], quantum secure direct communication (QSDC) [10, 11], quantum dialogue (QD) [12], quantum signature [13–16], and so on. Quantum key agreement (QKA) is an important branch of quantum cryptography. Compared with quantum key distribution (QKD) [1], QKA has great research significance because each participant in QKA contributes equally to the final shared key.

In 2004, Zhou et al. [6] proposed the first quantum key agreement protocol, which uses quantum teleportation to generate share keys. Later, more QKA protocols were proposed [17–25]. However, most of above QKA protocols were presented in the ideal environment. 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 eavesdropper can attack the protocol under the cover of noise. Thus, it is important to consider channel noise in the design of QKA protocols. Decoherence-free subspace (DFS) has been proven to help photons resist collective noise [26]. In 2014, Huang et al. [27] first proposed a QKA protocol to resist collective decoherence. In the same year, Huang et al. [28] designed a QKA protocol and brought in two corresponding variations over collective noise. In 2016, He et al. [29] designed two QKA protocols immune to collective noise based on the logical $\chi$ states and logical Bell states, which uses measurement correlation and delay measurement techniques. In 2018, based on four-particle logical GHZ states, Gao et al. [30] presented an improved two-party QKA protocol to resist collective noise. In 2019, Yang et al. [31] put forward a two-party QKA protocol based on logical Bell states to resist collective noise, which reduces the difficulty of preparing quantum resources. In 2020, Wang et al. [32] designed two QKA protocols based on Logical GHZ states and logical Bell states. In 2022, Bai et al. [33] designed two QKA protocols based on logical GHZ states, which further improves the efficiency of the protocols.

In existing schemes against collective noise, we found that these protocols still provide potential opportunities for some eavesdropping behaviors due to the imperfections of various devices in practical application. Among these imperfections, the defect of measurement equipment is particularly prominent. The solution to this problem is to build a nearly perfect device, which is obviously impractical. Another solution is to design a measurement-device-independent protocol. In 2012, Lo et al. [34] proposed a measurement-device-independent QKD (MID-QKD) protocol, which is independent of measurement devices and all the photons are measured by an untrusted third party.

For side-channel attacks, based on GHZ states, we put forward one two-party MDI-QKA protocol against collective-dephasing noise. Alice and Bob’s unrelated three-particle GHZ states are able to establish entanglement correlation just by using two Bell measurements. Once the encoding is complete, Alice and Bob attach a series of special photons to the particles in their hands, and then convert the two particles into a logical quantum state through the CNOT operation. Then all particles are sent to Charlie for measurement. Alice and Bob decrypt each other’s keys based on the measurements, but Charlie doesn’t know anything about final key. Compared with other protocols, our protocol uses logical quantum states during both particle transfers, greatly improving the key rate. The analysis shows that our proposed protocol can resist various attacks and has high efficiency.
The rest of the paper is organized as follows: In Section 2, we introduce some relevant theoretical knowledge. In Section 3, we describe the concrete steps of our protocol. Analysis is described in Section 4. Efficiency and comparison is given in Section 5. This paper is finally concluded in Section 6.

2 Preliminaries

2.1 Collective Noise and Decoherence-Free Subspaces

Noise has become an important factor affecting the security and accuracy of quantum dialogue. Most practical quantum channels are optical fibers, and optical fibers have birefringence fluctuations. Since the time gap for photons to travel is shorter than that of the noise source. Therefore, when photons transmitting in a quantum channel, they are often affected by noise. These effects can be approximated as a unitary operation $U(t)$ ($t$ represents the quantum-state transmission time) which is the joint unitary noise channel model [35]. Collective noise can be mainly divided into two types: the collective-dephasing noise and the collective-rotation noise [29, 36]. In this article, the collective-dephasing noise can be depicted as follows:

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

Where $\theta$ is the fluctuation factor of the noise with time. When $\theta=0$, the phase is unchanged, and the modulus is also unchanged. Then, the collective-rotation noise can be described as follows:

$$\varpi^\sigma : |0\rangle \rightarrow \cos\sigma|0\rangle + \sin\sigma|1\rangle, \quad \varpi^\sigma : |1\rangle \rightarrow -\sin\sigma|0\rangle + \cos\sigma|1\rangle$$

Where $\sigma$ is also the fluctuation factor of the noise with time.

A decoherence-free subspace (DFS) is a subspace of a system’s Hilbert space that is invariant to non-unitary dynamics. Alternatively stated, they are a small section of the system Hilbert space where the system is decoupled from the environment and thus its evolution is completely unitary. Due to this character, DFS is utilized against the collective noise [30].

According to the characteristics of the collective-dephasing noise [26], the subspaces $\{|0_{dp}\}, |1_{dp}\rangle\}$ and $\{|+_{dp}\}, |-_dp\rangle\}$ can form a DFS against the collective-dephasing noise, where

$$0_{dp} = |01\rangle, \quad 1_{dp} = |10\rangle, \quad +_{dp} = \frac{1}{\sqrt{2}}\left(|0_{dp}\rangle + |1_{dp}\rangle\right), \quad -_{dp} = \frac{1}{\sqrt{2}}\left(|0_{dp}\rangle - |1_{dp}\rangle\right).$$

2.2 Unitary Operations and Entanglement Swapping

We present four unitary operations which are defined as:

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

We define $U_{00} \equiv I$, $U_{01} \equiv X$, $U_{10} \equiv Z$, $U_{11} \equiv iY$. There are four Bell states, which can be constructed as:
Through the unitary operation $U_{i_1 i_2}$, $i_1, i_2 = 0, 1$, the Bell state can be transformed into another Bell state. Table 1 shows the transformations of the four Bell states $|\phi^\pm\rangle$, $|\psi^\pm\rangle$ under $U_{00}$, $U_{01}$, $U_{10}$, $U_{11}$, respectively.

There are a total of 8 GHZ states, as follows:

$|\psi^1\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$, $|\psi^2\rangle = \frac{1}{\sqrt{2}}(|001\rangle + |110\rangle)$

$|\psi^3\rangle = \frac{1}{\sqrt{2}}(|010\rangle + |101\rangle)$, $|\psi^4\rangle = \frac{1}{\sqrt{2}}(|011\rangle + |100\rangle)$

$|\psi^5\rangle = \frac{1}{\sqrt{2}}(|000\rangle - |111\rangle)$, $|\psi^6\rangle = \frac{1}{\sqrt{2}}(|001\rangle - |110\rangle)$

$|\psi^7\rangle = \frac{1}{\sqrt{2}}(|010\rangle - |101\rangle)$, $|\psi^8\rangle = \frac{1}{\sqrt{2}}(|011\rangle - |100\rangle)$

In our protocol, each participant needs to send two particles to the quantum intermediary, so the first round of transmission requires two particles to be immune to noise. There are a total of 4 GHZ states that satisfy this condition ($|\psi^2\rangle$, $|\psi^3\rangle$, $|\psi^6\rangle$, $|\psi^7\rangle$), and the properties of these four states are similar. Therefore, the three-particle GHZ state we used to resist collective-dephasing noise is $|\text{GHZ}\rangle = \frac{1}{\sqrt{2}}(|010\rangle + |101\rangle)$. It is obvious that the GHZ state $|\text{GHZ}\rangle_{123} = \frac{1}{\sqrt{2}}(|00\rangle_1 |10\rangle_{23} + |11\rangle_1 |01\rangle_{23}) = \frac{1}{\sqrt{2}}(|00\rangle_1 |1_{dp}\rangle_{23} + |11\rangle_1 |0_{dp}\rangle_{23})$ is constant when the second and the third qubits are transmitted through the collective-dephasing noise channel. In this protocol, Alice and Bob prepare a certain amount of GHZ states respectively, $|\text{GHZ}\rangle_{123}$ and $|\text{GHZ}\rangle_{456}$. The joint state of each pair of GHZ states is represented as follows:

| $|\phi^+\rangle$ | $|\phi^-\rangle$ | $|\psi^+\rangle$ | $|\psi^-\rangle$ |
|---|---|---|---|
| $U_{00}$ | $|\phi^+\rangle$ | $|\phi^-\rangle$ | $|\psi^-\rangle$ | $|\psi^+\rangle$ |
| $U_{01}$ | $|\psi^+\rangle$ | $|\psi^-\rangle$ | $|\phi^+\rangle$ | $|\phi^-\rangle$ |
| $U_{10}$ | $|\phi^-\rangle$ | $|\phi^+\rangle$ | $|\psi^-\rangle$ | $|\psi^+\rangle$ |
| $U_{11}$ | $|\psi^-\rangle$ | $|\psi^+\rangle$ | $|\phi^-\rangle$ | $|\phi^+\rangle$ |
\[ |GHZ\rangle_{123} \otimes |GHZ\rangle_{456} = \frac{1}{\sqrt{2}} (|010\rangle + |101\rangle)_{123} \otimes \frac{1}{\sqrt{2}} (|010\rangle + |101\rangle)_{456} \]
\[ = \frac{1}{2\sqrt{2}} \left( |\psi^+\rangle_{14} (|0\rangle_{23} |10\rangle_{56} + |01\rangle_{23} |0\rangle_{56}) + |\psi^-\rangle_{14} (|10\rangle_{23} |10\rangle_{56} - |01\rangle_{23} |01\rangle_{56}) + |\psi^+\rangle_{14} (|10\rangle_{23} |01\rangle_{56} + |01\rangle_{23} |10\rangle_{56}) + |\psi^-\rangle_{14} (|10\rangle_{23} |01\rangle_{56} - |01\rangle_{23} |01\rangle_{56}) \right) \]

If Charlie performs the Bell measurement on the second and the fifth qubits, and the third and the sixth qubits, according to Eq. (5), the state \( |GHZ\rangle_{123} \otimes |GHZ\rangle_{456} \) will collapse into one of the eight states: \( \{ |\phi^+\rangle_{14} |\phi^+\rangle_{25} |\phi^+\rangle_{36}, |\phi^+\rangle_{14} |\phi^-\rangle_{25} |\phi^-\rangle_{36}, |\phi^-\rangle_{14} |\phi^+\rangle_{25} |\phi^-\rangle_{36}, |\phi^-\rangle_{14} |\phi^-\rangle_{25} |\phi^+\rangle_{36}, |\psi^+\rangle_{14} |\psi^+\rangle_{25} |\psi^+\rangle_{36}, |\psi^+\rangle_{14} |\psi^-\rangle_{25} |\psi^-\rangle_{36}, |\psi^-\rangle_{14} |\psi^+\rangle_{25} |\psi^-\rangle_{36}, |\psi^-\rangle_{14} |\psi^-\rangle_{25} |\psi^+\rangle_{36} \} \).

Alice and Bob are able to deduce the post-measurement states of each other from the measurement results announced by Charlie.

### 3 Description of the MDI-QKA Protocol against Collective-Dephasing Noise

The MDI-QKA protocol is illustrated in Fig. 1. The detailed steps are given below.

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

\[ K_A = \{ K^1_A, K^2_A, \ldots, K^n_A \}, K_B = \{ K^1_B, K^2_B, \ldots, K^n_B \} \]

Where \( K^i_A, K^i_B \in \{ 00, 01, 10, 11 \} \) and \( i = 1, 2, \ldots, n \).

**Step 2** Alice prepares \( 2n + \delta \) \( |GHZ\rangle \) particles as described in Section 2, which are expressed as: \( \{ |P_1(1), P_1(2), P_2(3), \ldots, P_{2n+\delta}(1), P_{2n+\delta}(2) \} \}. \) \( \delta \) is a very small number that can be ignored, and \( \delta \) particles are used for security check.) Then, Alice divides the GHZ particles into two sequences, which are as follows:

\[ S_{A_1} : \{ P_1(1), P_2(1), \ldots, P_{2n+\delta}(1) \} \]

\[ S_{A_2} : \{ P_1(2)P_1(3), P_2(2)P_2(3), \ldots, P_{2n+\delta}(2)P_{2n+\delta}(3) \} \]

In the sequence \( S_{A_1} \), each element consists of two particles. Alice randomly selects \( m \) decoy particles from set \( \{ 0_{dp}, 1_{dp}, 1_{dp}, 1_{dp} \} \) and inserts them into sequences \( S_{A_1} \) to obtain new sequences \( S^*_A \). Alice sends \( S^*_{A_1} \) to Charlie and retains sequences \( S^*_{A_1} \).
**Step 3** In the same way, Bob prepares $2n + \delta |GHZ\rangle_{B_1B_2B_3}$ states and obtains sequences $S_{B_1}$ and $S_{B_2}$. Similarly, Bob randomly inserts $m$ logical decoy particles into sequences $S_{B_2}$ to obtain new sequences $S_{B_2}^\ast$. Bob sends $S_{B_2}^\ast$ to Charlie and retains sequences $S_{B_1}$.

**Step 4** After Charlie receives the sequence $S_{A_2}^\ast$ and $S_{B_2}^\ast$, he makes Bell measurements of the first particle of each element in sequence $S_{A_2}^\ast$ and the first particle of the corresponding ele-
moment in sequence \( S_{B_2}^* \). Also, Charlie makes joint Bell measurements for the second particle of each element of the sequence \( S_{A_2}^* \) and \( S_{B_2}^* \). After measuring all the particles, Charlie announces the results in order.

Step 5 Security Checking. After Charlie announces the Bell measurement outcomes, Alice and Bob announce the specific locations of the logical decoy particles in their sequences through classical channel. The source of the photon pairs in Charlie’s hand can be divided into three situations, as shown in Table 2.

In Table 2, two pairs of photons in case (1) are both from the entangled pair of Alice and Bob, and Charlie’s Bell measurement is equivalent to allowing the photons in different entangled pairs to achieve entanglement swapping. Such photon pairs are most cases, and will be discarded because only a small number of single photons are inserted. In order to make the security test effective, Alice and Bob only use the photons in case (2) to analyze the security of the step 2–4. The details are as follows:

\[
|0_{dp}\rangle_{12} |0_{dp}\rangle_{34} = \frac{1}{4} \left( |\psi^+\rangle + |\psi^-\rangle \right)_{13} \otimes \left( |\phi^+\rangle - |\phi^-\rangle \right)_{1324}
\]

(6)

\[
|1_{dp}\rangle_{12} |1_{dp}\rangle_{34} = \frac{1}{4} \left( |\psi^+\rangle - |\psi^-\rangle \right)_{13} \otimes \left( |\phi^+\rangle + |\phi^-\rangle \right)_{1324}
\]

(7)

\[
|0_{dp}\rangle_{12} |1_{dp}\rangle_{34} = \frac{1}{4} \left( |\psi^+\rangle + |\psi^-\rangle \right)_{13} \otimes \left( |\phi^+\rangle - |\phi^-\rangle \right)_{1324}
\]

(8)

\[
|+_{dp}\rangle_{12} |+_{dp}\rangle_{34} = \frac{1}{\sqrt{2}} \left( |0_{dp}\rangle + |1_{dp}\rangle \right)_{12} \otimes \frac{1}{\sqrt{2}} \left( |0_{dp}\rangle + |1_{dp}\rangle \right)_{34}
\]

(9)

\[
= \frac{1}{2} \left( (|01\rangle + |10\rangle)_{12} \otimes (|01\rangle + |10\rangle)_{34} \right)
\]

\[
= \frac{1}{2} \left( (|0101\rangle + |0110\rangle + |1001\rangle + |1101\rangle)_{1324} \right)
\]

\[
= \frac{1}{2} \left( (|0011\rangle + |0110\rangle + |1001\rangle + |1100\rangle)_{1324} \right)
\]

Table 2 The source of sequence \( (S_{A_2}^*, S_{B_2}^*) \) and the use of Bell measurements in every situation

| Every situation | Source of \( S_{A_2}^* \) | Source of \( S_{B_2}^* \) | Functions         |
|-----------------|-----------------|-----------------|-----------------|
| (1)             | entanglement    | entanglement    | Entanglement swapping |
| (2)             | decoy photon    | decoy photon    | security check   |
| (3)             | entanglement    | decoy photon    | discard          |
|                 | decoy photon    | entanglement    | discard          |
\begin{align}
\left|-d_p\right\rangle_{12} \left|-d_p\right\rangle_{34} &= \frac{1}{\sqrt{2}} \left(\left|0_{dp}\right\rangle - \left|1_{dp}\right\rangle\right)_{12} \bigotimes \frac{1}{\sqrt{2}} \left(\left|0_{dp}\right\rangle - \left|1_{dp}\right\rangle\right)_{34} \\
&= \frac{1}{4\sqrt{2}} \left(\left|\phi^+\right\rangle \left|\phi^-\right\rangle - \left|\phi^-\right\rangle \left|\phi^+\right\rangle - \left|\psi^+\right\rangle \left|\psi^-\right\rangle + \left|\psi^-\right\rangle \left|\psi^+\right\rangle\right)_{1324} 
\end{align}

\begin{align}
\left|+d_p\right\rangle_{12} \left|-d_p\right\rangle_{34} &= \frac{1}{\sqrt{2}} \left(\left|0_{dp}\right\rangle + \left|1_{dp}\right\rangle\right)_{12} \bigotimes \left|01\right\rangle_{34} = \frac{1}{\sqrt{2}} \left(\left|0011\right\rangle + \left|1001\right\rangle\right)_{1234} \\
&= \frac{1}{\sqrt{2} \sqrt{2}} \left(\left|\phi^+\right\rangle \left|\phi^-\right\rangle + \left|\phi^-\right\rangle \left|\phi^+\right\rangle - \left|\phi^-\right\rangle \left|\phi^+\right\rangle - \left|\phi^+\right\rangle \left|\phi^-\right\rangle\right)_{1324} 
\end{align}

\begin{align}
\left|+d_p\right\rangle_{12} \left|0_{dp}\right\rangle_{34} &= \frac{1}{\sqrt{2}} \left(\left|0_{dp}\right\rangle + \left|1_{dp}\right\rangle\right)_{12} \bigotimes \left|01\right\rangle_{34} = \frac{1}{\sqrt{2}} \left(\left|0011\right\rangle + \left|1001\right\rangle\right)_{1234} \\
&= \frac{1}{\sqrt{2} \sqrt{2}} \left(\left|\phi^+\right\rangle \left|\phi^-\right\rangle + \left|\phi^-\right\rangle \left|\phi^+\right\rangle - \left|\phi^-\right\rangle \left|\phi^+\right\rangle - \left|\phi^+\right\rangle \left|\phi^-\right\rangle\right)_{1324} 
\end{align}

Alice and Bob have a total of 16 combinations of decoy photons. Take the above 8 equations as an example. For those logical decoy photons with different preparation basis, Bell measurement will lead to any one of all possible Bell measurements for logical photons, as shown in Eqs. (12) and (13), it is not useful for security check and analysis. There are six cases similar to the above, namely \(\left|+d_p\right\rangle_{12} \left|1_{dp}\right\rangle_{34}, \left|-d_p\right\rangle_{12} \left|0_{dp}\right\rangle_{34}, \left|0_{dp}\right\rangle_{12} \left|+d_p\right\rangle_{34}, \left|1_{dp}\right\rangle_{12} \left|-d_p\right\rangle_{34}, \left|1_{dp}\right\rangle_{12} \left|+d_p\right\rangle_{34}\) and \(\left|1_{dp}\right\rangle_{12} \left|-d_p\right\rangle_{34}\). The decomposition of two pairs of logical photons with identical basis in terms of Bell state are shown as Eqs. (6), (7), (8), (9), (10) and (11). From Eqs. (6) and (7), we see that the decoy photon states \(\left|0_{dp}\right\rangle_{12} \left|0_{dp}\right\rangle_{34}\) and \(\left|1_{dp}\right\rangle_{12} \left|1_{dp}\right\rangle_{34}\) are indistinguishable under the bell measurement. Similar indistinguishable cases are quantum states \(\left|0_{dp}\right\rangle_{12} \left|1_{dp}\right\rangle_{34}, \left|1_{dp}\right\rangle_{12} \left|0_{dp}\right\rangle_{34}\), \(\left|1_{dp}\right\rangle_{12} \left|+d_p\right\rangle_{34}, \left|+d_p\right\rangle_{12} \left|1_{dp}\right\rangle_{34}\), \(\left|1_{dp}\right\rangle_{12} \left|-d_p\right\rangle_{34}, \left|-d_p\right\rangle_{12} \left|+d_p\right\rangle_{34}\). To sum up, we choose Eqs. (6), (8), (9) and (10) for security checks, which can be completely distinguished. There are only some specific combinations of Bell measurements. According to the decoy photon states and positions and states published by Alice and Bob and the above equations, Alice and Bob can check the channel’s security and Charlie's honesty. This method is similar to the detection method of the general MDI-QKD protocol. The behavior of the eavesdropper Eve or dishonest Charlie would cause some errors when he chooses the wrong measurement basis. Alice and Bob analyze and compare the measurements announced by Charlie based on the initial positions and states of the decoy photons. Then they calculate the error rate, if the error rate is less than the given threshold value, they will continue to perform the next step. If not, they will give up this protocol and restart it.

**Step 6** Let \(K_{A_1}^i K_{A_2}^i = K_{A_1}^i K_{B_1}^i K_{B_2}^i = K_{B_1}^i\). After security check, Alice and Bob will discard the photons in \(S_{A_i}\) and \(S_{B_i}\) that are not entangled, which are these photons in case (3) and (4) in the Table 2. There are about 2n photons remaining in the sequence \(S_{A_i}\) and \(S_{B_i}\). Alice selects the first half of the n particles in the sequence \(S_{A_i}\) and encodes her key \(K_A\) through four unitary operations \(U_{K_{A_1}^i K_{A_2}^i}\), where \(i = 1, 2, \ldots, n\). At the same time, Bob also performs random unitary operations on his half of the corresponding particles for pre-
venting Eve to perform the intercept and resend attack. Similarly, Bob encodes the key \( K_B \) by performing the unitary operation \( U_{1^{k_1} 3^{k_2}} \) on the remaining \( n \) particles and Alice performs random unitary operations on the corresponding particles.

**Step 7** After the encoding operation is completed, Alice and Bob respectively prepare 2\( n \) single photons whose initial state is \( |1\rangle \), namely sequence \( S_{A_1} \) and \( S_{B_1} \). Then, Alice performs the CNOT operations on the sequences \( S_{A_1} \) and \( S_{A_3} \). Specifically, the particles in the sequence \( S_{A_1} \) are used as the control qubits and the particles in the sequence \( S_{A_3} \) are used as the target qubits, respectively. After these CNOT operations, Alice obtains a new sequence \( S^*_{A_1} \), which is composed of particles of sequence \( S_{A_1} \) and \( S_{A_3} \). At the same time, Bob performs the same operation on the sequences \( S_{B_1} \) and \( S_{B_3} \) and obtains a new sequence \( S^*_{B_1} \). At this time, the sequences \( S^*_{A_1} \) and \( S^*_{B_1} \) can resist collective-dephasing noise. Specifically, suppose that an entangled state of the sequence \( S_{A_1} \) and \( S_{B_1} \) is \( |\phi^+\rangle \). The whole process is as follows:

\[
\text{CNOT}(A_1, A_3) \text{CNOT}(B_1, B_3) |\phi^+\rangle_{A_1 B_1} \otimes |11\rangle_{A_3 B_3} = \text{CNOT}(A_1, A_3) \text{CNOT}(B_1, B_3) \left( \frac{1}{\sqrt{2}} (|0011\rangle + |1100\rangle)_{A_1 B_1 A_3 B_3} \right) \\
= \frac{1}{\sqrt{2}} (|0011\rangle + |1100\rangle)_{A_1 B_1 A_3 B_3} = \frac{1}{\sqrt{2}} (|0101\rangle + |1010\rangle)_{A_1 A_3 B_1 B_3} = \frac{1}{\sqrt{2}} (|\phi^+\rangle |\phi^+\rangle - |\phi^-\rangle |\phi^-\rangle)_{A_1 A_3 B_1 B_3}
\]

From Eq. (14), the particles of \( A_1 \) and \( A_3 \) form a logical state against collective-dephasing noise. Also, the particles of \( B_1 \) and \( B_3 \) can resist collective-dephasing noise, too. The other three cases are as follows:

\[
\text{CNOT}(A_1, A_3) \text{CNOT}(B_1, B_3) |\phi^-\rangle_{A_1 B_1} \otimes |11\rangle_{A_3 B_3} = \frac{1}{\sqrt{2}} (|0101\rangle - |1010\rangle)_{A_1 A_3 B_1 B_3} = \frac{1}{\sqrt{2}} (|\phi^-\rangle |\phi^+\rangle - |\phi^+\rangle |\phi^-\rangle)_{A_1 A_3 B_1 B_3}
\]

\[
\text{CNOT}(A_1, A_3) \text{CNOT}(B_1, B_3) |\psi^+\rangle_{A_1 B_1} \otimes |11\rangle_{A_3 B_3} = \frac{1}{\sqrt{2}} (|0110\rangle + |1001\rangle)_{A_1 A_3 B_1 B_3} = \frac{1}{\sqrt{2}} (|\psi^+\rangle |\psi^+\rangle - |\psi^-\rangle |\psi^-\rangle)_{A_1 A_3 B_1 B_3}
\]

\[
\text{CNOT}(A_1, A_3) \text{CNOT}(B_1, B_3) |\psi^-\rangle_{A_1 B_1} \otimes |11\rangle_{A_3 B_3} = \frac{1}{\sqrt{2}} (|0110\rangle - |1001\rangle)_{A_1 A_3 B_1 B_3} = \frac{1}{\sqrt{2}} (|\psi^-\rangle |\psi^+\rangle - |\psi^+\rangle |\psi^-\rangle)_{A_1 A_3 B_1 B_3}
\]

Finally, Alice and Bob send the sequences \( S^*_{A_1} \) and \( S^*_{B_1} \) to Charlie.

**Step 8** After Charlie receives the sequences \( S^*_{A_1} \) and \( S^*_{B_1} \), he performs two joint Bell measurements on the sequences \( S_{A_1}, S_{B_1} \) and the sequences \( S_{A_3}, S_{B_3} \). Then Charlie announces the measurement results. According to the results published by Charlie and Eqs. (14), (15), (16) and (17), Alice and Bob can deduce each other’s keys. Finally, Alice and Bob calculate the share key \( K_{AB} = K_A \oplus K_B \).
Step 9 The Second Security Checking. After Alice and Bob get the share key $K_{AB}$, Alice and Bob choose random m-bit keys to compare to check the key integrity. (m is a very small number that can be ignored.) Ensure that the negotiation process is not destroyed through the second round of security checks.

4 Analysis

According to [37], a secure quantum key agreement protocol should meet the following four conditions.

(C1) Correctness. At the end of the protocol, each participant gets the correct agreement key.
(C2) Security. No external eavesdropper can obtain any information about the agreement key without being detected.
(C3) Fairness. All participants equally influence the agreement key, that is, any nontrivial subset of the participants cannot determine the agreement key alone.
(C4) Privacy. The inputs of the participants can be kept secret.

In this protocols, the inputs of participants are random bits and do not contain any private information. Therefore, when analyzing the securities of our protocol, we ignore the privacy requirement and focus on the first three conditions C1–C3.

4.1 Correctness

Let’s take our protocol as an example. In step 4, the two Bell measurements published by Charlie are $|\psi^+\rangle_2|\psi^+\rangle_3$. According to Eq. (5), the corresponding particles of sequence $S_{A_1}$ and sequence $S_{B_1}$ collapse to $|\psi^+\rangle_{14}$. Suppose this particle is in the first half of the sequence $S_{A_1}$ and The key of Alice at the corresponding position is $K_{iA}^i = 01$. Suppose that the random unitary operation chosen by Bob is $U_{10}$. According to Table 1, The joint state $|\psi^+\rangle$ will collapse into $|\phi^-\rangle$. Finally, after Charlie publishes the measurement results $|\phi^-\rangle |\phi^+\rangle$, according to Eq. (16), everyone knows the joint state is $|\phi^-\rangle$. Since Charlie doesn’t know what unitary operation Bob has done, he can’t deduce the key $K_{iA}^i$. However, Bob can deduce Alice’s encoding operation $U_{01}$ based on the unitary operation he did. In the same way, Alice can also deduce Bob’s key. At the end of the protocol, Alice and Bob can get each other’s correct key. Therefore, our proposed protocol is correct.

4.2 Security

In the above QKA protocol, the transmitted particles are logical particles that immune to noise interference. Therefore, our QKA protocols can resist collective dephasing noise. In this section, we will discuss the security of our protocol. The common attack methods are Trojan-horse attack, intercept–resend, measure–resend and fake bell measurement attack. The analysis of various attack methods is as follows.
4.2.1 Trojan-Horse Attack

Trojan Horse attack is a physical attack that uses the physical characteristics and special devices of photons to obtain photon states. This attack mainly exists in two-way communication protocols. In our scheme, the four quantum information flows are: Alice → Charlie; Bob → Charlie; Alice → Charlie; Bob → Charlie. One-way quantum communication protocol refers to only one party transfers the quantum information flow to the other, and no returned information. Therefore, our protocol is a one-way quantum communication protocol and Trojan horse attack will be naturally resisted in this protocol.

4.2.2 Intercept–Resend Attack

If outsider eavesdropper Eve executes the intercept-resend attack, he intercepts the sequences $S_{A_2}^*$ and $S_{B_2}^*$ in the first photon transmission process, and then sends the prepared sequence to Charlie. However, Eve does not know the position of the decoy particles in sequences $S_{A_2}^*$ and $S_{B_2}^*$ and the measurement basis used, so the sequences forged by Eve cannot pass the first security detection. The probability of Eve attack being found is $1 - \left( \frac{1}{16} \right)^m$. (m refers to the number of decoy particles.) If intercepts the sequences $S_{A_1}^*$ and $S_{B_1}^*$ in the second photon transmission process, Eve cannot obtain any information because he does not know the unitary operation performed by Bob. If he sends the prepared sequence to Charlie, he can only destroy the progress of the protocol without obtaining any keys. To avoid the interruption from Eve or Charlie, Alice and Bob perform the second round of security checking. Therefore, intercept–resend attack will be naturally resisted in this protocol.

4.2.3 Measure–Resend Attack

Similar to intercept–resend, if Eve intercepts and measures the sequences $S_{A_2}^*$ and $S_{B_2}^*$ in the first photon transmission process, because eve does not know the specific position and initial state of the decoy photons in the sequences, when eve chooses the wrong measurement basis, his measurement will change the state of the decoy photon, causing certain errors. Eve’s attack will definitely be discovered in the first round of security checks. The probability of Eve attack being found is $1 - \left( \frac{1}{16} \right)^m$. (m refers to the number of decoy particles.) If intercepts the sequences $S_{A_1}^*$ and $S_{B_1}^*$ in the second photon transmission process, Eve cannot obtain any information because he does not know the unitary operation performed by Bob. At this time, Eve has the same function as Charlie, but is only responsible for measuring the sequence, but cannot obtain any key.

4.2.4 Fake Bell Measurement Attack

In our agreement, Charlie is an untrusted third party. Compared with Eve, the internal eavesdropper Charlie has more advantage in acquiring information about entangled particles. In Step 4, Charlie does not perform Bell measurement on the corresponding sequences $(S_{A_2}, S_{B_2})$ and $(S_{A_1}, S_{B_1})$, but announces fake Bell measurement results. However, he does not know the specific position and initial state of the decoy photons in the sequences $S_{A_2}^*$ and
If Charlie announces fake Bell measurement results in Step 8, his dishonesty behavior must be detected because Alice and Bob will perform the second security check. The probability of Charlie attack being found is \( 1 - \left( \frac{1}{16} \right)^m \). (m refers to the number of decoy particles and number of keys published in the second round of security check.)

In summary, our protocol can resist various types of attacks and ensure the security of the protocol.

### 4.3 Fairness

The key encoding phase is at step 6, Alice and Bob simultaneously encode their own keys in their halves of the particle. The final measurement publication is at step 8. At this point both Alice and Bob have no particles in their hands. Taking Alice as an example, she has encoded her own key into sequence \( S_{A_1} \) in step 6, and in step 8, she can only decode to obtain Bob’s key. Alice can’t know Bob’s key before step 8, so she can’t decide the key by herself before the encoding operation. Similarly, Bob cannot decide the shared key by himself. Therefore, Our protocol can achieve fairness.

### 5 Efficiency Analysis

Now let’s discuss the efficiency of our protocol. According to [38], the reference index of efficiency can be defined as follows:

\[
\eta = \frac{c}{q + b}
\]  

(18)

In the formula, \( c \) represents the shared key bits generated by the protocol, \( q \) represents the total quantum bits utilized in the protocol, and \( b \) represents the classical bits used for decoding (excluding the classical bits used for eavesdropping detection). In the proposed MDI-QKA protocol, the number of classical bits negotiated is \( c = 2n \), the total number of qubits used in the protocol is \( q = 6n + 6n + 4n \). Because \( m \) is much smaller than \( n \), compared to \( n \), the proportion is significantly smaller of number of decoy photons which are used for entanglement detection and it can be neglected theoretically. Because Alice and Bob deduce each other’s key through the bell measurement published by Charlie, the number of classical bits exchanged for decoding the message is \( 2n \). Therefore, the qubit efficiency of this protocol is as follows \( \eta = \frac{2n}{6n + 6n + 4n + 2n} = 11.1\% \). Because there is no MDI-QKA protocol against collective noise of the same type for comparison, we select several other two-party protocols against collective noise and MDI protocols that are not immune to noise to compare with ours. The comparison is shown in Table 3.

As is shown in Table 3, although existing two-party QKA protocols against collective noise have higher quantum efficiency, these protocols cannot resist side-channel attacks caused by equipment defects. Similarly, existing two-party MDI protocols are not suitable for noisy channels. In the MDI protocols, many errors will be introduced due to the influence of collective noise, which will cause the participants to think that the protocol is under attack, and affect the final key rate. However, our protocol is not only resistant to side-channel attacks, but also immune to collective-dephasing noise, which has good qubit efficiency.
Table 3  Comparisons among several kinds of QKA protocols against collective noise

| Protocols          | Quantum resource                                    | Measurement-device-independent | Immune to noise | Qubit efficiency(%) |
|--------------------|------------------------------------------------------|--------------------------------|-----------------|--------------------|
| Huang et al. [28]  | Logical Bell states                                  | No                             | Yes             | 16.67%             |
| Yang et al. [31]   | Logical Bell states                                  | No                             | Yes             | 21.05              |
| Wang et al. [32]   | Logical GHZ states and logical Bell states           | No                             | Yes             | 13.3               |
| Shi. [39]          | Bell states                                          | Yes                            | No              | 10                 |
| ours               | Logical GHZ states and single photons                | Yes                            | Yes             | 11.1               |
6 Conclusion

Based on GHZ states and single photons, we propose one QKA protocol against the collective-dephasing noise. Alice and Bob conduct key agreement through entanglement exchange in the GHZ state with the help of dishonest Charlie. After encoding is complete, Alice and Bob will attach a series of special photons to the particles in their hands and perform CNOT operations to resist noise. In comparison with the existing MDI-QKA protocols of two parties, our protocol uses logical quantum states during both particle transmissions, which makes the protocol immune to collective-dephasing noise, greatly improving the final key rate. Also, our proposed protocol only uses Bell measurements and common quantum gate operations, which can be easily implemented in the existing technology. Through the security analysis, it can be seen that the proposed protocol has sufficient security to effectively defend against common internal and external attacks. Besides, the proposed protocol is better in terms of quantum resource cost and actual experiment.

For future work, I have two thoughts: Firstly, the advantages of our proposed protocol in terms of efficiency are not obvious, so in the next step we will refer to other protocols and improve our protocol to improve the overall quantum efficiency. Secondly, because the existing protocols against collective noise do not have much work on measurement-device-independent aspect, we next try to improve our protocol and apply it to other related fields, such as quantum secret sharing, quantum secure direct communication (QSDC) and quantum dialogue, etc. Therefore, this is the direction of our future research.

Acknowledgments This work was supported by the National Natural Science Foundation of China under grant No. 62071015.

References

1. Bennett, C. H. and Brassard, G.: Quantum Cryptography: Public Key Distribution and Coin Tossing. In: Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India, 175–179 (1984). 10.1016/j.tcs.2014.05.025
2. Ekert, A.K.: Quantum cryptography based on Bell’s theorem. Phys. Rev. Lett. 67, 661–663 (1991). https://doi.org/10.1103/PhysRevLett.67.661
3. Bennett, C.H.: Quantum cryptography using any two nonorthogonal states. Phys. Rev. Lett. 68, 3121–3124 (1992). https://doi.org/10.1103/PhysRevLett.68.3121
4. Grosshans, F., Van Assche, G., Wenger, J., Cerf, N.J., Grangier, P.: Quantum key distribution using gaussian-modulated coherent states. Nature. 421, 238–241 (2003). https://doi.org/10.1038/nature01289
5. Wang, T.Y., Wen, Q.Y., Chen, X.B.: Cryptanalysis and improvement of a multi-user quantum key distribution protocol. Opt. Commun. 283(24), 5261–5263 (2010). https://doi.org/10.1016/j.optcom.2010.07.022
6. Zhou, N., Zeng, G., Xiong, J.: Quantum key agreement protocol. Electron. Lett. 40(18), 1149–1150 (2004). https://doi.org/10.1049/el:20045183
7. Chong, S.K., Hwang, T.: Quantum key agreement protocol based on BB84. Opt. Commun. 283(6), 1192–1195 (2010). https://doi.org/10.1016/j.optcom.2009.11.007
8. Hillery, M., Bužek, V., Berthiaume, A.: Quantum secret sharing. Phys. Rev. A. 59, 1829–1834 (1999). https://doi.org/10.1103/PhysRevA.59.1829
9. Karlsson, A., Koashi, M., Imoto, N.: Quantum entanglement for secret sharing and secret splitting. Phys. Rev. A. 59, 162–168 (1999). https://doi.org/10.1103/PhysRevA.59.162
10. Boström, K., Felbinger, T.: Deterministic secure direct communication using entanglement. Phys. Rev. Lett. 89, 187902 (2002). https://doi.org/10.1103/PhysRevLett.89.187902
11. Long, G.L., Liu, X.S.: Theoretically efficient high-capacity quantum-key-distribution scheme. Phys. Rev. A. 65, 032302 (2002). https://doi.org/10.1103/PhysRevA.65.032302
12. Nguyen, B.A.: Quantum dialogue. Phys. Lett. A. 328(1), 6–10 (2004). https://doi.org/10.1016/j.physleta.2004.06.009
13. Yang, Y.-G., Liu, Z.-C., Li, J., Chen, X.-B., Zuo, H.-J., Zhou, Y.-H., Shi, W.-M.: Theoretically extensible quantum digital signature with starlike cluster states. Quantum Inf. Process. 16(1), 1–15 (2017). https://doi.org/10.1007/s11128-016-1458-x
14. Yang, Y.-G., Lei, H., Liu, Z.-C., Zhou, Y.-H., Shi, W.-M.: Arbitrated quantum signature scheme based on cluster states. Quantum Inf. Process. 15(6), 2487–2497 (2016). https://doi.org/10.1007/s11128-016-1293-0
15. Wang, T.-Y., Wei, Z.L.: One-time proxy signature based on quantum cryptography. Quantum Inf. Process. 11, 455–463 (2012). https://doi.org/10.1007/s11128-011-0258-6
16. Wang, T.-Y., Cai, X.Q., Ren, Y.L., Zhang, R.L.: Security of quantum digital signatures for classical messages. Sci. Rep. 5, 9231 (2015). https://doi.org/10.1038/srep09231
17. Liu, S.L., Zheng, D., Chen, K.F.: Analysis of information leakage in quantum key agreement. J. Shanghai Jiaotong Univ. (Sci.). E-11(2), 219–223 (2006). https://doi.org/10.1007/s002540100348
18. Shi, R.H., Zhong, H.: Multi-party quantum key agreement with bell states and bell measurements. Quantum Inf. Process. 12, 921–932 (2013). https://doi.org/10.1007/s11128-012-0443-2
19. Liu, B., Gao, F., Huang, W., Wen, Q.-Y.: Multiparty quantum key agreement with single particles. Quantum Inf. Process. 12, 1797–1805 (2013). https://doi.org/10.1007/s11128-012-0492-6
20. Xu, G.-B., Wen, Q.-Y., Wu, X., Li, Y.B., Sun, Y.: Quantum key agreement against collective decoherence. Quantum Inf. Process. 13(12), 2587–2594 (2014). https://doi.org/10.1007/s11128-014-0816-9
21. Shu, D.S., Ma, W.P., Wang, L.L.: Two-party quantum key agreement with four-qubit cluster states. Quantum Inf. Process. 13, 2313–2324 (2014). https://doi.org/10.1007/s11128-014-0785-z
22. Sun, Z.W., Yu, J.P., Wang, P.: Efficient multi-party quantum key agreement by cluster states. Quantum Inf. Process. 15, 373–384 (2016). https://doi.org/10.1007/s11128-015-1155-1
23. He, Y.F., Ma, W.P.: Two-party quantum key agreement based on four-particle GHZ states. Int. J. Theor. Phys. 14, 1650007 (2017). https://doi.org/10.1142/S0219749916500076
24. He, Y.F., Ma, W.P.: Two-party quantum key agreement with five-particle entangled states. Int. J. Quantum Inf. 15, 1750018 (2017). https://doi.org/10.1142/S0219749917500186
25. Gu, J., Hwang, T.: Improvement of "novel multiparty quantum key agreement protocol with GHZ states". Int. J. Theor. Phys. 56, 3108–3116 (2017). https://doi.org/10.1007/s10773-017-3478-4
26. 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). https://doi.org/10.1126/science.290.5491.498
27. 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). https://doi.org/10.1007/s10773-014-2087-8
28. Huang, W., Wen, Q.-Y., Liu, B., Gao, F., Sun, Y.: Quantum key agreement with EPR pairs and single particle measurements. Quantum Inf. Process. 13, 649–663 (2014). https://doi.org/10.1007/s11128-013-0680-z
29. He, Y.F., Ma, W.P.: Two-party quantum key agreement against collective noise. Quantum Inf. Process. 15, 5023–5035 (2016). https://doi.org/10.1007/s11128-016-1436-3
30. Gao, H., Chen, X.G., Qian, S.R.: Two-party quantum key agreement protocols under collective noise channel. Quantum Inf. Process. 17, 140 (2018). https://doi.org/10.1007/s11128-018-1910-1
31. Yang, Y.G., Gao, S., Li, D., et al.: Two-party quantum key agreement over a collective noisy channel. Quantum Inf. Process. 18, 74 (2019). https://doi.org/10.1007/s11128-019-2187-8
32. Wang, M.F., Zhou, Y.H., Yang, Y.G., et al.: Two-party quantum key agreement against collective noisy channel. Quantum Inf. Process. 19, 100 (2020). https://doi.org/10.1007/s11128-020-2593-y
33. Bai, M.Q., Guo, J.H., Yang, Z., Mo, Z.W.: Quantum key agreement protocols with GHZ states under collective noise channels. Int. J. Theor. Phys. 61, 63 (2022). https://doi.org/10.1007/s10773-022-05059-0
34. Lo, H.K., Curty, M., Qi, B.: Measurement-device-independent quantum key distribution. Phys. Rev. Lett. 108, 130503 (2012). https://doi.org/10.1103/PhysRevLett.108.130503
35. Wang, X.B.: Fault tolerant quantum key distribution protocol with collective random unitary noise. Phys. Rev. A. 72(5), 762–776 (2005). https://doi.org/10.1103/PhysRevA.72.050304
36. 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). https://doi.org/10.1007/s10773-016-3028-5
37. Lin, S., Zhang, X., Guo, G.-D., Wang, L.-L., Liu, X.-F.: Multiparty quantum key agreement. Phys. Rev. A. 104, 042421 (2021). https://doi.org/10.1103/PhysRevA.104.042421

38. Cabello, A.: Quantum key distribution in the Holevo limit. Phys. Rev. Lett. 85, 5633–5638 (2000). https://doi.org/10.1103/PhysRevLett.85.5635

39. Shi, G.F.: Measurement-device-independent quantum dialogue. Chinese Physics B. 30(10), 100303 (2021). https://doi.org/10.1088/1674-1056/ac140a

Publisher’s Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.