International Journal of Theoretical Physics (2023) 62:235
https://doi.org/10.1007/s10773-023-05414-9

RESEARCH

Two-party Quantum Key Agreement with Six-particle Entangled States Against Collective Noise

She-Xiang Jiang[1,2] · Lei Fang[2] · Xian-Jin Fang[2]

Received: 18 March 2023 / Accepted: 19 June 2023 / Published online: 31 October 2023
© The Author(s), under exclusive licence to Springer Science+Business Media, LLC, part of Springer Nature 2023

Abstract
Quantum key agreement (QKA) is an advanced technique that allows multiple parties to share a secret key through cooperation. At present, most QKA protocols have the problems of weak anti-noise ability and low qubit efficiency. In this paper, two improved two-party QKA protocols are proposed using two sets of special logical qubits, which are immune to the collective noise. The main idea of these two protocols is that first, through the measurement correlation of the six-particle entangled states, the communication parties can fairly build a common key. Then, decoy logical qubits and delayed measurement technology are employed to prevent eavesdropping in quantum channels. Security analysis indicates that both protocols are unconditionally secure and capable of resisting internal and external attacks. In addition, compared with existing protocols, both protocols improve the efficiency because they transmit longer qubits.

Keywords Six-particle entangled states · Collective noise · Quantum key agreement · Qubit efficiency · Logical qubits

1 Introduction

With the advent of the Shor algorithm [1] and the further development of quantum computing, the RSA encryption algorithm [2] based on large integer factorization can be easily cracked. There has been an increasing interest in quantum cryptography, a type of encryption that can ensure data security [3, 4]. Quantum cryptography makes use of superposition, entangled state, measurement collapse, and other theories in quantum mechanics to truly realize unconditional security. It can generate dynamic random keys [5, 6] and detect eavesdropping with high probability during communication [7]. QKA is an essential subfield of quantum cryptography. It aims to solve the problem that communication parties negotiate a shared key without the participation of a third party. Unlike quantum key

✉ Lei Fang
15071383712@163.com

[1] Anhui Key Laboratory of Mine Intelligent Equipment and Technology, Anhui University of Science and Technology, Huainan 232001, Anhui, China

[2] School of Computer Science and Engineering, Anhui University of Science and Technology, Huainan 232001, China

distribution (QKD) [8–10], fairness and security are two critical requirements of QKA. In the QKA protocol, each party is required to contribute equally to the ultimate key and cannot decide independently in advance.

Zhou et al. [11] first put forth the QKA protocol in 2004. Since then, numerous QKA protocols have been proposed [12–15]. Nevertheless, the early QKA protocols were all implemented through ideal quantum channels without noise. In real applications, noise typically has an impact on particles, and attackers can launch malicious attacks under cover of it. Therefore, when designing the QKA protocol, noise must be taken into account. In 2003, Walton et al. [16] found that qubits in decoherence-free subspaces (DFS) are not affected by collective noise, which is an ideal strategy to combat noise. In light of Walton et al.'s theory, Huang et al. [17, 18] raised two corresponding variables in the QKA protocol for the first time to immunize collective noise. In 2016, He et al. [19] designed an ingenious QKA protocol against collective noise using logical χ *states* and logical Bell states. Subsequently, in order to improve the qubit efficiency, Gao et al. [20] suggested QKA protocols that are immune to collective noise based on the four-particle entangled GHZ state. Meanwhile, Yang et al. [21] proposed a QKA protocol based on logical Bell states, which is robust to collective noise and superior to most current QKA protocols concerning qubit efficiency and quantum resource cost. In [22], Wang et al. utilized decoy logical qubits to devise a QKA protocol against collective noise, significantly improving qubit efficiency. Due to quantum entanglement swapping technology, Zhou et al. [23] suggested a QKA protocol in 2020 that is resistant to collective noise. Later, qubit efficiency was further enhanced by Guo et al. [24], who presented novel QKA protocols on account of logical GHZ states and their measurement correlation.

In recent years, some researchers have focused on multi-party quantum key agreement (MQKA). Wang et al. [25] proposed a three-party QKA protocol using quantum Fourier transform. Later, Yang et al. [26] proposed a tree-type MQKA protocol, which increased the number of participants to N parties. This year, Zhao et al. [27] established a MQKA protocol using non-maximally entangled states with unknown parameters for the first time, which is more suitable for real-world situations. However, the research on MQKA protocol is still in the initial stage due to its low efficiency and inability to resist collective noise.

The scheme described in this essay can further boost qubit efficiency while resisting collective noise. This scheme utilizes six-particle entangled states, decoy logical qubits [29–32], and delayed measurement technology [13, 28] to provide two QKA protocols immune to different types of collective noise. Both protocols are based on the measurement correlation of six-particle entangled states, allowing two participants to establish a shared key fairly. Eavesdroppers cannot successfully carry out Trojan horse attacks [33–35] since each particle is sent only once in our protocols. Internal and external attacks have shown our two QKA protocols to be secure. Furthermore, both protocols have excellent qubit efficiency.

The remainder of this essay is arranged as follows. The second section introduces theoretical knowledge of our protocols, including the four unitary operations, six-particle entangled states, and collective noise. Our protocols are fully explained in the next section. The security and efficiency analyses are the main topics of Sections 4 and 5, respectively. Last but not least, we draw a conclusion in Section 6.

2 Theoretical Knowledge

2.1 Unitary Operations and Quantum Entangled States

The Z-basis is well known to consist of $\{|0\rangle||1\rangle\}$, and the X-basis is known to consist of $\{|+\rangle||-\rangle\}$, where $|+\rangle = 1/\sqrt{2}(|0\rangle + |1\rangle)$ and $|-\rangle = 1/\sqrt{2}(|0\rangle - |1\rangle)$. The four unitary operations are denoted as $U_{00} \equiv I = |0\rangle\langle 0| + |1\rangle\langle 1|$, $U_{01} \equiv X = |0\rangle\langle 1| + |1\rangle\langle 0|$, $U_{10} \equiv Z = |0\rangle\langle 0| - |1\rangle\langle 1|$, and $U_{11} \equiv iY = |0\rangle\langle 1| - |1\rangle\langle 0|$. Then we introduce four Bell states which are described as $|\Psi^{\pm}\rangle = 1/\sqrt{2}(|01\rangle \pm |10\rangle)$ and $|\Phi^{\pm}\rangle = 1/\sqrt{2}(|00\rangle \pm |11\rangle)$. After a unitary operation $U_{i_1 i_2}(i_1, i_2 = 0, 1)$ is applied to a Bell state's second particle, it will change into another Bell state. The results of the transformation between four Bell states are shown in Table 1.

This paper uses the six-particle entangled state [36] as the quantum resource, defined as

$$
\begin{aligned}
|\psi\rangle_{ABCDEF} = \frac{1}{\sqrt{32}}&(|000000\rangle + |111111\rangle + |000011\rangle + |111100\rangle + |000101\rangle + |111010\rangle + \\
&|000110\rangle + |111001\rangle + |001001\rangle + |110110\rangle + |001111\rangle + |110000\rangle + \\
&|010001\rangle + |101110\rangle + |010010\rangle + |101101\rangle + |011000\rangle + |100111\rangle + \\
&|011101\rangle + |100010\rangle - |001010\rangle - |110101\rangle - |001100\rangle - |110011\rangle + \\
&|010100\rangle + |101011\rangle + |010111\rangle + |101000\rangle + |011011\rangle + |100100\rangle + \\
&|011110\rangle + |100001\rangle)_{ABCDEF} \\
=\frac{1}{8}&\big[(|000\rangle_{ABEF} + |0110\rangle_{ABEF} - |1001\rangle_{ABEF} - |1111\rangle_{ABEF})|\Phi^{-}\rangle_{CD} + \\
&(|0001\rangle_{ABEF} - |0111\rangle_{ABEF} - |1001\rangle_{ABEF} + |1110\rangle_{ABEF})|\Psi^{+}\rangle_{CD} + \\
&(|0010\rangle_{ABEF} - |0100\rangle_{ABEF} + |1011\rangle_{ABEF} - |1101\rangle_{ABEF})|\Psi^{-}\rangle_{CD} + \\
&(|0011\rangle_{ABEF} + |0101\rangle_{ABEF} + |1010\rangle_{ABEF} + |1100\rangle_{ABEF})|\Phi^{+}\rangle_{CD}\big]
\end{aligned}
\tag{1}
$$

If Bob performs the *ZZZZ basis*$\{|0000\rangle,|0001\rangle,|0010\rangle,|0011\rangle,|0100\rangle,|0101\rangle,|0110\rangle,|0111\rangle,|1000\rangle,|1001\rangle,|1010\rangle,|1011\rangle,|1100\rangle,|1101\rangle,|1110\rangle,|1111\rangle\}$ measurement on particles A, B, E and F, and Alice carries out the Bell measurement on particles C and D, the state $|\psi\rangle_{\mathrm{ABCDEF}}$ will collapse to the states $|0000\rangle_{\mathrm{ABEF}}|\Phi^{-}\rangle_{CD}$, $|0110\rangle_{ABEF}|\Phi^{-}\rangle_{CD}$, $|1001\rangle_{ABEF}|\Phi^{-}\rangle_{CD}$, $|1111\rangle_{ABEF}|\Phi^{-}\rangle_{CD}$, $|0001\rangle_{ABEF}|\Psi^{+}\rangle_{CD}$, $|0111\rangle_{ABEF}|\Psi^{+}\rangle_{CD}$, $|1000\rangle_{ABEF}|\Psi^{+}\rangle_{CD}$, $|1110\rangle_{ABEF}|\Psi^{+}\rangle_{CD}$, $|0010\rangle_{ABEF}|\Psi^{-}\rangle_{CD}$, $|0100\rangle_{ABEF}|\Psi^{-}\rangle_{CD}$, $|1011\rangle_{ABEF}|\Psi^{-}\rangle_{CD}$, $|1011\rangle_{ABEF}|\Psi^{-}\rangle_{CD}$, $|0011\rangle_{ABEF}|\Phi^{+}\rangle_{CD}$, $|0101\rangle_{ABEF}|\Phi^{+}\rangle_{CD}$, $|1010\rangle_{ABEF}|\Phi^{+}\rangle_{CD}$ and $|1100\rangle_{ABEF}|\Phi^{+}\rangle_{CD}$ with the probability of 1/16, respectively. As we can see, Alice and Bob's measurement results have a distinct correlation.

Table 1 Unitary operations and their transformation results

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

2.2 Collective Noise

According to the literature [16], collective noise can fall into two categories: collective-dephasing noise and collective-rotation noise. Next, we use the evolution of quantum states to illustrate the effects of these two noises on the Z-basis. Qubits $|0\rangle$ and $|1\rangle$ in the first type of noise evolve as follows:

$$\begin{aligned} U_{dp} \mid 0\rangle &= \begin{pmatrix} 1 & 0 \\ 0 & e^{i\varphi_{(t)}} \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \mid 0\rangle \\ U_{dp} \mid 1\rangle &= \begin{pmatrix} 1 & 0 \\ 0 & e^{i\varphi_{(t)}} \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = e^{i\varphi_{(t)}} \mid 1\rangle \end{aligned} \tag{2}$$

where U_{dp} represents the matrix form of collective-dephasing noise, and $\varphi_{(t)}$ represents the phase noise parameter that varies with time. Similarly, qubits $|0\rangle$ and $|1\rangle$ in collective-rotation noise undergo the following evolution:

$$\begin{aligned} U_r \mid 0\rangle &= \begin{pmatrix} \cos\theta_{(t)} & \sin\theta_{(t)} \\ -\sin\theta_{(t)} & \cos\theta_{(t)} \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \cos\theta_{(t)} \mid 0\rangle + \sin\theta_{(t)} \mid 1\rangle \\ U_r \mid 1\rangle &= \begin{pmatrix} \cos\theta_{(t)} & \sin\theta_{(t)} \\ -\sin\theta_{(t)} & \cos\theta_{(t)} \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = -\sin\theta_{(t)} \mid 0\rangle + \cos\theta_{(t)} \mid 1\rangle \end{aligned} \tag{3}$$

where U_r represents the matrix form of collective-rotation noise, and $\theta_{(t)}$ represents the rotation noise parameter that varies with time.

3 The Two-Party QKA Protocols Against Collective Noise

3.1 The QKA Protocol Against Collective-Dephasing Noise

Two logical qubits, $|0_{dp}\rangle = |01\rangle$ and $|1_{dp}\rangle = |10\rangle$ [16], as well as their superposition states $|+_{dp}\rangle = 1/\sqrt{2}(|0_{dp}\rangle + |1_{dp}\rangle)$ and $|-_{dp}\rangle = 1/\sqrt{2}(|0_{dp}\rangle - |1_{dp}\rangle)$ are unaffected in the collective-dephasing noise channel.

Then exploiting this, we provide a two-party QKA protocol with logical six-particle entangled states resistant to collective-dephasing noise. The protocol works as follows.

Step 1 Each of Alice and Bob produces $4n$-bit keys at random:

$$\begin{aligned} K_A &= K_A^1 \parallel K_A^2 \parallel \cdots \parallel K_A^n \\ K_B &= K_B^1 \parallel K_B^2 \parallel \cdots \parallel K_B^n \end{aligned}$$

where $K_A^i, K_B^i \in \{0000,0001,0010,0011,0100,0101,0110,0111,1000,1001,1010,1011,1100,1101,1110,1111\}$, $i = 1, 2\ldots, n$.

Step 2 Alice is going to prepare n logical six-particle entangled states $|\psi_{dp}\rangle_{ABCDEF}$:

$$
\begin{aligned}
&|\psi_{dp}\rangle_{ABCDEF}\\
&=1/\sqrt{32}(|0_{dp}\rangle|0_{dp}\rangle|00\rangle|0_{dp}\rangle|0_{dp}\rangle+|1_{dp}\rangle|1_{dp}\rangle|11\rangle|1_{dp}\rangle|1_{dp}\rangle+\\
&|0_{dp}\rangle|0_{dp}\rangle|00\rangle|1_{dp}\rangle|1_{dp}\rangle+|1_{dp}\rangle|1_{dp}\rangle|11\rangle|0_{dp}\rangle|0_{dp}\rangle+|0_{dp}\rangle|0_{dp}\rangle|01\rangle|0_{dp}\rangle|1_{dp}\rangle+\\
&|1_{dp}\rangle|1_{dp}\rangle|10\rangle|1_{dp}\rangle|0_{dp}\rangle+|0_{dp}\rangle|0_{dp}\rangle|01\rangle|1_{dp}\rangle|0_{dp}\rangle+|1_{dp}\rangle|1_{dp}\rangle|10\rangle|0_{dp}\rangle|1_{dp}\rangle+\\
&|0_{dp}\rangle|0_{dp}\rangle|10\rangle|0_{dp}\rangle|1_{dp}\rangle+|1_{dp}\rangle|1_{dp}\rangle|01\rangle|1_{dp}\rangle|0_{dp}\rangle+|0_{dp}\rangle|0_{dp}\rangle|11\rangle|1_{dp}\rangle|1_{dp}\rangle+\\
&|1_{dp}\rangle|1_{dp}\rangle|00\rangle|0_{dp}\rangle|0_{dp}\rangle+|0_{dp}\rangle|1_{dp}\rangle|00\rangle|0_{dp}\rangle|1_{dp}\rangle+|1_{dp}\rangle|0_{dp}\rangle|11\rangle|1_{dp}\rangle|0_{dp}\rangle+\\
&|0_{dp}\rangle|1_{dp}\rangle|00\rangle|1_{dp}\rangle|0_{dp}\rangle+|1_{dp}\rangle|0_{dp}\rangle|11\rangle|0_{dp}\rangle|1_{dp}\rangle+|0_{dp}\rangle|1_{dp}\rangle|10\rangle|0_{dp}\rangle|0_{dp}\rangle+\\
&|1_{dp}\rangle|0_{dp}\rangle|01\rangle|1_{dp}\rangle|1_{dp}\rangle+|0_{dp}\rangle|1_{dp}\rangle|11\rangle|0_{dp}\rangle|1_{dp}\rangle+|1_{dp}\rangle|0_{dp}\rangle|00\rangle|1_{dp}\rangle|0_{dp}\rangle-\\
&|0_{dp}\rangle|0_{dp}\rangle|10\rangle|1_{dp}\rangle|0_{dp}\rangle-|1_{dp}\rangle|1_{dp}\rangle|01\rangle|0_{dp}\rangle|1_{dp}\rangle-|0_{dp}\rangle|1_{dp}\rangle|11\rangle|0_{dp}\rangle|0_{dp}\rangle-\\
&|1_{dp}\rangle|1_{dp}\rangle|00\rangle|1_{dp}\rangle|1_{dp}\rangle+|0_{dp}\rangle|1_{dp}\rangle|01\rangle|0_{dp}\rangle|0_{dp}\rangle+|1_{dp}\rangle|0_{dp}\rangle|10\rangle|1_{dp}\rangle|1_{dp}\rangle+\\
&|0_{dp}\rangle|1_{dp}\rangle|01\rangle|1_{dp}\rangle|1_{dp}\rangle+|1_{dp}\rangle|0_{dp}\rangle|00\rangle|0_{dp}\rangle|0_{dp}\rangle+|0_{dp}\rangle|1_{dp}\rangle|10\rangle|1_{dp}\rangle|1_{dp}\rangle+\\
&|1_{dp}\rangle|0_{dp}\rangle|01\rangle|0_{dp}\rangle|0_{dp}\rangle+|0_{dp}\rangle|1_{dp}\rangle|11\rangle|1_{dp}\rangle|0_{dp}\rangle+|1_{dp}\rangle|0_{dp}\rangle|00\rangle|0_{dp}\rangle|1_{dp}\rangle)_{ABCDEF}\\
&=\frac{1}{8}[(|0_{dp}\rangle_A|0_{dp}\rangle_B|0_{dp}\rangle_E|0_{dp}\rangle_F+|0_{dp}\rangle_A|1_{dp}\rangle_B|1_{dp}\rangle_E|0_{dp}\rangle_F-|1_{dp}\rangle_A|0_{dp}\rangle_B|0_{dp}\rangle_E|1_{dp}\rangle_F-\\
&|1_{dp}\rangle_A|1_{dp}\rangle_B|1_{dp}\rangle_E|1_{dp}\rangle_F|\Phi^-\rangle_{CD}+(|0_{dp}\rangle_A|0_{dp}\rangle_B|0_{dp}\rangle_E|1_{dp}\rangle_F-|0_{dp}\rangle_A|1_{dp}\rangle_B|1_{dp}\rangle_E|1_{dp}\rangle_F-\\
&|1_{dp}\rangle_A|0_{dp}\rangle_B|0_{dp}\rangle_E|0_{dp}\rangle_F+|1_{dp}\rangle_A|1_{dp}\rangle_B|1_{dp}\rangle_E|0_{dp}\rangle_F)|\Psi^+\rangle_{CD}+(|0_{dp}\rangle_A|0_{dp}\rangle_B|1_{dp}\rangle_E|0_{dp}\rangle_F-\\
&|0_{dp}\rangle_A|1_{dp}\rangle_B|0_{dp}\rangle_E|0_{dp}\rangle_F+|1_{dp}\rangle_A|0_{dp}\rangle_B|1_{dp}\rangle_E|1_{dp}\rangle_F-|1_{dp}\rangle_A|1_{dp}\rangle_B|0_{dp}\rangle_E|0_{dp}\rangle_E|1_{dp}\rangle_F)|\Psi^-\rangle_{CD}+\\
&(|0_{dp}\rangle_A|0_{dp}\rangle_B|1_{dp}\rangle_E|1_{dp}\rangle_F|0_{dp}\rangle_A|1_{dp}\rangle_B|0_{dp}\rangle_E|1_{dp}\rangle_F+|1_{dp}\rangle_A|0_{dp}\rangle_B|1_{dp}\rangle_E|0_{dp}\rangle_F+\\
&|1_{dp}\rangle_A|1_{dp}\rangle_B|0_{dp}\rangle_E|0_{dp}\rangle_F)|\Phi^+\rangle_{CD}]\\
&=\frac{1}{8}[(|01\rangle_{A_1A_2}|01\rangle_{B_1B_2}|01\rangle_{E_1E_2}|01\rangle_{F_1F_2}+|01\rangle_{A_1A_2}|10\rangle_{B_1B_2}|10\rangle_{E_1E_2}|01\rangle_{F_1F_2}-\\
&|10\rangle_{A_1A_2}|01\rangle_{B_1B_2}|01\rangle_{E_1E_2}|10\rangle_{F_1F_2}-|10\rangle_{A_1A_2}|10\rangle_{B_1B_2}|10\rangle_{E_1E_2}|10\rangle_{F_1F_2})|\Phi^-\rangle_{CD}+\\
&(|01\rangle_{A_1A_2}|01\rangle_{B_1B_2}|01\rangle_{E_1E_2}|01\rangle_{F_1F_2}-|01\rangle_{A_1A_2}|10\rangle_{B_1B_2}|10\rangle_{E_1E_2}|10\rangle_{F_1F_2}-\\
&|10\rangle_{A_1A_2}|01\rangle_{B_1B_2}|01\rangle_{E_1E_2}|01\rangle_{F_1F_2}+|10\rangle_{A_1A_2}|10\rangle_{B_1B_2}|10\rangle_{E_1E_2}|01\rangle_{F_1F_2})|\Psi^+\rangle_{CD}+\\
&(|01\rangle_{A_1A_2}|01\rangle_{B_1B_2}|10\rangle_{E_1E_2}|01\rangle_{F_1F_2}-|01\rangle_{A_1A_2}|10\rangle_{B_1B_2}|01\rangle_{E_1E_2}|01\rangle_{F_1F_2}+\\
&|10\rangle_{A_1A_2}|01\rangle_{B_1B_2}|10\rangle_{E_1E_2}|10\rangle_{F_1F_2}-|10\rangle_{A_1A_2}|10\rangle_{B_1B_2}|01\rangle_{E_1E_2}|10\rangle_{F_1F_2})|\Psi^-\rangle_{CD}+\\
&(|01\rangle_{A_1A_2}|01\rangle_{B_1B_2}|10\rangle_{E_1E_2}|10\rangle_{F_1F_2}+|01\rangle_{A_1A_2}|10\rangle_{B_1B_2}|01\rangle_{E_1E_2}|10\rangle_{F_1F_2}+\\
&|10\rangle_{A_1A_2}|01\rangle_{B_1B_2}|10\rangle_{E_1E_2}|01\rangle_{F_1F_2}+|10\rangle_{A_1A_2}|10\rangle_{B_1B_2}|01\rangle_{E_1E_2}|01\rangle_{F_1F_2})|\Phi^+\rangle_{CD}]
\end{aligned}
\tag{4}
$$

These logical states are separated into six ordered sequences S_A, S_B, S_C, S_D, S_E, and S_F, consisting of logical qubits A, logical qubits B, particles C, particles D, logical qubits E and logical qubits F, respectively. Among them, the logical qubits A, B, E , and F are made up of two physical qubits, namely A_1 and A_2, B_1 and B_2, E_1 and E_2, and F_1 and F_2, respectively. Alice randomly selects logical qubits from $\{|0_{dp}\rangle|1_{dp}\rangle|+_{dp}\rangle|-_{dp}\rangle\}$ as decoy states and inserts them into S_A, S_B, S_E, and S_F to obtain S'_A, S'_B, S'_E, and S'_F. Afterwards, Alice sends them to Bob and holds the sequences S_C and S_D.

Step 3 After confirming that Bob has received sequences S'_A, S'_B, S'_E, and S'_F, Alice announces the decoy logical qubits' locations and the measurement basis ($\{|0_{dp}\rangle|1_{dp}\rangle\}$ ***or*** $\{|+_{dp}\rangle|-_{dp}\rangle\}$). Bob uses the correct measurement basis to measure these decoy logical qubits

Table 2 Measurement results and corresponding values

Alice's measurement result	Bob's measurement result	M^i
$\|\Phi^-\rangle$	$\|0000\rangle$	0000
$\|\Phi^-\rangle$	$\|0110\rangle$	0110
$\|\Phi^-\rangle$	$\|1001\rangle$	1001
$\|\Phi^-\rangle$	$\|1111\rangle$	1111
$\|\Psi^+\rangle$	$\|0001\rangle$	0001
$\|\Psi^+\rangle$	$\|0111\rangle$	0111
$\|\Psi^+\rangle$	$\|1000\rangle$	1000
$\|\Psi^+\rangle$	$\|1110\rangle$	1110
$\|\Psi^-\rangle$	$\|0010\rangle$	0010
$\|\Psi^-\rangle$	$\|0100\rangle$	0100
$\|\Psi^-\rangle$	$\|1011\rangle$	1011
$\|\Psi^-\rangle$	$\|1101\rangle$	1101
$\|\Phi^+\rangle$	$\|0011\rangle$	0011
$\|\Phi^+\rangle$	$\|0101\rangle$	0101
$\|\Phi^+\rangle$	$\|1010\rangle$	1010
$\|\Phi^+\rangle$	$\|1100\rangle$	1100

and notifies Alice of the results. Thus, Alice can calculate the error rate. If the error rate is lower than predetermined threshold, go to Step 4. Otherwise, there exists eavesdropping in quantum channels. Abort the protocol and restart from Step 1.

Step 4 After removing the decoy logical qubits, the sequences S'_A, S'_B, S'_E, and S'_F revert to S_A, S_B, S_E, and S_F. Bob executes the CNOT operations on the logical qubits A, B, E, and F, respectively. Particles A_1, B_1, E_1, and F_1 serve as control qubits, while particles A_2, B_2, E_2, and F_2 serve as target qubits. After four CNOT operations, each logical quantum state $|\psi_{\mathrm{dp}}\rangle_{\mathrm{ABCDEF}}$ is converted to

$$
\begin{aligned}
|\Lambda_{dp}\rangle_{ABCDEF} &= U_{CNOT}^{A_1A_2} \otimes U_{CNOT}^{B_1B_2} \otimes U_{CNOT}^{E_1E_2} \otimes U_{CNOT}^{F_1F_2} \otimes |\psi_{dp}\rangle_{ABCDEF} \\
&= {}^1\!/_8 \Big[\Big(\Big| 01_{A_1A_2} \Big| 01_{B_1B_2} \Big| 01_{E_1E_2} \quad \Big| 01_{F_1F_2} + |01\rangle_{A_1A_2} |11\rangle_{B_1B_2} |11\rangle_{E_1E_2} |01\rangle_{F_1F_2} - \\
&\quad |11\rangle_{A_1A_2} |01\rangle_{B_1B_2} |01\rangle_{E_1E_2} |11\rangle_{F_1F_2} - |11\rangle_{A_1A_2} |11\rangle_{B_1B_2} |11\rangle_{E_1E_2} |11\rangle_{F_1F_2} \rangle |\Phi^-\rangle_{CD} + \\
&\quad (|01\rangle_{B_1B_2} |01\rangle_{E_1E_2} |11\rangle_{F_1F_2} - |01\rangle_{A_1A_2} |11\rangle_{B_1B_2} |11\rangle_{E_1E_2} |11\rangle_{F_1F_2} - \\
&\quad |11\rangle_{A_1A_2} |01\rangle_{B_1B_2} |01\rangle_{E_1E_2} |01\rangle_{F_1F_2} + |11\rangle_{A_1A_2} |11\rangle_{B_1B_2} |11\rangle_{E_1E_2} |01\rangle_{F_1F_2} \rangle |\Psi^+\rangle_{CD} + \\
&\quad (|01\rangle_{B_1B_2} |11\rangle_{E_1E_2} |01\rangle_{F_1F_2} - |01\rangle_{A_1A_2} |11\rangle_{B_1B_2} |01\rangle_{E_1E_2} |01\rangle_{F_1F_2} + \\
&\quad |11\rangle_{A_1A_2} |01\rangle_{B_1B_2} |11\rangle_{E_1E_2} |11\rangle_{F_1F_2} - |11\rangle_{A_1A_2} |10\rangle_{B_1B_2} |01\rangle_{E_1E_2} |11\rangle_{F_1F_2} \rangle |\Psi^-\rangle_{CD} + \\
&\quad (|01\rangle_{B_1B_2} |11\rangle_{E_1E_2} |11\rangle_{F_1F_2} + |01\rangle_{A_1A_2} |11\rangle_{B_1B_2} |01\rangle_{E_1E_2} |11\rangle_{F_1F_2} + \\
&\quad |11\rangle_{A_1A_2} |01\rangle_{B_1B_2} |11\rangle_{E_1E_2} |01\rangle_{F_1F_2} + |11\rangle_{A_1A_2} |11\rangle_{B_1B_2} |01\rangle_{E_1E_2} |01\rangle_{F_1F_2} \rangle |\Phi^+\rangle_{CD} \Big] \\
&= 1/8 [(|0000\ \rangle_{A_1B_1E_1F_1} + |0110\rangle_{A_1B_1E_1F_1} - |1001\rangle_{A_1B_1E_1F_1} - |1111\rangle_{A_1B_1E_1F_1} |\Phi^-\rangle_{CD} + \\
&\quad (|0001\rangle_{A_1B_1E_1F_1} - |0111\rangle_{A_1B_1E_1F_1} - |1000\rangle_{A_1B_1E_1F_1} + |1110\rangle_{A_1B_1E_1F_1} |\Psi^+\rangle_{CD} + \\
&\quad (|0010\rangle_{A_1B_1E_1F_1} - (|0100\rangle_{A_1B_1E_1F_1} + (|1011\rangle_{A_1B_1E_1F_1} - (|1101\rangle_{A_1B_1E_1F_1} |\Psi^-\rangle_{CD} + \\
&\quad (|0011\rangle_{A_1B_1E_1F_1} + (|0101\rangle_{A_1B_1E_1F_1} + (|1010\rangle_{A_1B_1E_1F_1} + (|1100\rangle_{A_1B_1E_1F_1} |\Phi^+\rangle_{CD}] \otimes |1111\rangle_{A_2B_2E_2F_2} \\
&= |\psi\rangle_{A_1B_1CDE_1F_1} \otimes |1111\rangle_{A_2B_2E_2F_2}
\end{aligned}
\tag{5}
$$

Later, Alice applies the Bell measurement to each pair of the corresponding particles in sequences S_C and S_D, and Bob applies the *ZZZZ basis* measurement to the corresponding particles A_1 in S_A, B_1 in S_B, E_1 in S_E, and F_1 in S_F. The encoding scheme agreed upon by Alice and Bob is

$$\begin{aligned}
&|0000\rangle \rightarrow 0000, |0001\rangle \rightarrow 0001, |0010\rangle \rightarrow 0010, |0011\rangle \rightarrow 0011,\\
&|0100\rangle \rightarrow 0100, |0101\rangle \rightarrow 0101, |0110\rangle \rightarrow 0110, |0111\rangle \rightarrow 0111,\\
&|1000\rangle \rightarrow 1000, |1001\rangle \rightarrow 1001, |1010\rangle \rightarrow 1010, |1011\rangle \rightarrow 1011,\\
&|1100\rangle \rightarrow 1100, |1101\rangle \rightarrow 1101, |1110\rangle \rightarrow 1110, |1111\rangle \rightarrow 1111
\end{aligned} \tag{6}$$

Afterwards, all the Bob's measurement results are coded as $M = M^1 \| M^2 \| \cdots \| M^n$, where M^i is the code of Bob's ith measurement result ($i = 1, 2, \cdots, n$). Table 2 displays the measurement results and corresponding values.

When Bob finally publishes the measurement results for particles A_1 and B_1, Alice and Bob will know each other's results. As a consequence, they share a classic bit string M.

Step 5 Introduce the four unitary operations U_{00}, U_{01}, U_{10} and U_{11}. According to the key K_A, Alice lets $i_1 i_2 = K^i_{A12}$ and $i_3 i_4 = K^i_{A34}$ ($i = 1, 2, \ldots, n$). Then Alice executes the unitary operation $U_{i_1 i_2}$ on the ith particle in S_D to obtain the new sequence S^*_D. By matching two particles in S_C and S^*_D, a new Bell state is generated. Alice prepares the corresponding logical Bell state $|\lambda_{dp}\rangle_{C_1C_2D_1D_2}$ in accordance with the new Bell state. Then Alice executes the unitary operation $U_{i_3 i_4}$ on the ith particle in S^*_D to obtain the new sequence $S^{*(1)}_D$. The matched two particles in S_C and $S^{*(1)}_D$ constitute a new Bell state. Similarly, Alice prepares the corresponding logical Bell state $\lambda^*_{dp\rangle_{C_1C_2D_1D_2}}$. The following are the definitions of the four logical Bell states [37]:

$$\begin{aligned}
|\Phi^+_{dp}\rangle_{C_1C_2D_1D_2} &= \frac{1}{\sqrt{2}}\left(|0_{dp}\rangle|0_{dp}\rangle + |1_{dp}\rangle|1_{dp}\rangle\right)_{C_1C_2D_1D_2}\\
&= \frac{1}{\sqrt{2}}\left(|\Phi^+\rangle|\Phi^+\rangle - |\Phi^-\rangle|\Phi^-\rangle\right)_{C_1D_1C_2D_2}\\
|\Phi^-_{dp}\rangle_{C_1C_2D_1D_2} &= \frac{1}{\sqrt{2}}\left(|0_{dp}\rangle|0_{dp}\rangle - |1_{dp}\rangle|1_{dp}\rangle\right)_{C_1C_2D_1D_2}\\
&= \frac{1}{\sqrt{2}}\left(|\Phi^-\rangle|\Phi^+\rangle - |\Phi^+\rangle|\Phi^-\rangle\right)_{C_1D_1C_2D_2}\\
|\Psi^+_{dp}\rangle_{C_1C_2D_1D_2} &= \frac{1}{\sqrt{2}}\left(|0_{dp}\rangle|1_{dp}\rangle + |1_{dp}\rangle|0_{dp}\rangle\right)_{C_1C_2D_1D_2}\\
&= \frac{1}{\sqrt{2}}\left(|\Psi^+\rangle|\Psi^+\rangle - |\Psi^-\rangle|\Psi^-\rangle\right)_{C_1D_1C_2D_2}\\
|\Psi^-_{dp}\rangle_{C_1C_2D_1D_2} &= \frac{1}{\sqrt{2}}\left(|0_{dp}\rangle|1_{dp}\rangle - |1_{dp}\rangle|0_{dp}\rangle\right)_{C_1C_2D_1D_2}\\
&= \frac{1}{\sqrt{2}}\left(|\Psi^-\rangle|\Psi^+\rangle - |\Psi^+\rangle|\Psi^-\rangle\right)_{C_1D_1C_2D_2}
\end{aligned} \tag{7}$$

Alice divides the logical Bell state $|\lambda_{dp}\rangle_{C_1C_2D_1D_2}$ into two ordered sequences $S^{(1)}_C$ and $S^{(1)}_D$, consisting of logical qubits C (two physical qubits C_1 and C_2) and logical qubits D

(two physical qubits D_1 and D_2), respectively. Likewise, the logical Bell state $|\lambda^*_{Rr}\rangle_{C_1C_2D_1D_2}$ is also divided into two ordered sequences $S_C^{(2)}$ and $S_D^{(2)}$. Then Alice performs a permutation operator $\prod_n$ on $S_C^{(1)}$ and $S_C^{(2)}$ to get two random sequences $S_C^{(1)*}$ and $S_C^{(2)*}$. Alice randomly selects the decoy logical qubits and inserts them into $S_C^{(1)*}$, $S_D^{(1)*}$, $S_C^{(2)*}$ and $S_D^{(2)}$ to generate the sequences $S_C^{(1)*\prime}$, $S_D^{(1)\prime}$, $S_C^{(2)*\prime}$ and $S_D^{(2)\prime}$, in which the decoy logical qubits are randomly taken from the set $\{|0_{dp}\rangle|1_{dp}\rangle|+_{dp}\rangle|-_{dp}\rangle\}$. Alice sends the sequences $S_C^{(1)*\prime}$, $S_D^{(1)\prime}$, $S_C^{(2)*\prime}$ and $S_D^{(2)\prime}$ to Bob.

Step 6 After Bob receives $S_C^{(1)*\prime}$, $S_D^{(1)*\prime}$, $S_C^{(2)*\prime}$ and $S_D^{(2)\prime}$, both parties conduct precisely the same eavesdropping check as the first time.

Step 7 Bob announces the value $K'_B = K_B \oplus M = \left(K_B^1 \oplus M^1\right) \| \left(K_B^2 \oplus M^2\right) \| \cdots \| \left(K_B^n \oplus M^n\right)$. Based on the classic bit string M, Alice can deduce the key K_B. Assuming that Alice and Bob's default negotiation rule is $K_{AB} = (K_A \oplus K_B) \| (K_A \oplus K_B \oplus M)$. Then they can calculate the shared key K_{AB} of both parties.

Step 8 Alice publishes the permutation operator $\prod_n$; Bob performs its inverse permutation on the sequences $S_C^{(1)*}$ and $S_C^{(2)*}$ to obtain the sequences $S_C^{(1)}$ and $S_C^{(2)}$. Bob associates the sequence $S_C^{(1)}$ with the sequence $S_D^{(1)}$ to obtain n logical Bell states and then carries out the Bell measurements on the particles C_1, D_1 and the particles C_2, D_2, respectively. That is, Bob is aware of the logical Bell state $|\lambda_{dp}\rangle_{C_1C_2D_1D_2}$ sent by Alice and the physical Bell state corresponding to each pair of particles in S_C and S_D^*. According to the initial Bell states and the transformed Bell states, Bob is able to deduce the value K^i_{A12}. Bob combines the sequences $S_C^{(2)}$ and $S_D^{(2)}$ to obtain n logical Bell states. Then the Bell measurements are performed on the particles C_1, D_1 and the particles C_2, D_2, respectively. Thus, Bob is aware of the logical Bell state $|\lambda^*_{dp}\rangle_{C_1C_2D_1D_2}$ sent by Alice and the physical Bell state corresponding to each pair of particles in S_C and $S_D^{*(1)}$. Based on the transformation from the corresponding physical Bell state of each pair of particles in S_C and S_D^* to the corresponding physical Bell state of each pair of particles in S_C and $S_D^{*(1)}$, Bob can infer the value K^i_{A34}. Combining K^i_{A12} and K^i_{A34}, Bob is able to obtain the value K_A and produce the shared key K_{AB}.

3.2 The QKA Protocol Against Collective-Rotation Noise

In the collective-rotation noise channel, two logical qubits, $|0_r\rangle = |\phi^+\rangle = 1/\sqrt{2}(|00\rangle + |11\rangle)$ and $|1_r\rangle = |\psi^-\rangle = 1/\sqrt{2}(|01\rangle - |10\rangle)$ [16], as well as their superposition states $|+_r\rangle = 1/\sqrt{2}(|0_r\rangle + |1_r\rangle)$ and $|+_r\rangle = 1/\sqrt{2}(|0_r\rangle + |1_r\rangle)$ are not affected by the collective-rotation noise.

Now, we present a two-party QKA protocol immune to the collective-rotation noise with the logical six-particle entangled states. It consists of the following steps.

Step 1 Each of Alice and Bob generates $4n$-bit keys at random:

$$K_A = K_A^1 \| K_A^2 \| \cdots \| K_A^n$$
$$K_B = K_B^1 \| K_B^2 \| \cdots \| K_B^n$$

where $K_A^i, K_B^i \in$ {0000,0001,0010,0011,0100,0101,0110,0111,1000,1001,1010,1011,1100,1101,1110, 1111}, $i = 1, 2\ldots, n$. They adopt precisely the same rule of negotiation as the first protocol.

Step 2 Alice prepares n logical six-particle entangled states $|\psi_r\rangle_{ABCDEF}$:

$$
\begin{aligned}
&\psi_r\rangle_{ABCDEF}\\
&=\frac{1}{4\sqrt{2}}(|0_r\rangle|0_r\rangle|00\rangle|0_r\rangle|0_r\rangle+|1_r\rangle|1_r\rangle|11\rangle|1_r\rangle|1_r\rangle+\\
&|0_r\rangle|0_r\rangle|00\rangle|1_r\rangle|1_r\rangle+|1_r\rangle|1_r\rangle|11\rangle|0_r\rangle|0_r\rangle+|0_r\rangle|0_r\rangle|01\rangle|0_r\rangle|1_r\rangle+\\
&|1_r\rangle|1_r\rangle|10\rangle|1_r\rangle|0_r\rangle+|0_r\rangle|0_r\rangle|01\rangle|1_r\rangle|0_r\rangle+|1_r\rangle|1_r\rangle|10\rangle|0_r\rangle|1_r\rangle+\\
&|0_r\rangle|0_r\rangle|10\rangle|0_r\rangle|1_r\rangle+|1_r\rangle|1_r\rangle|01\rangle|1_r\rangle|0_r\rangle+|0_r\rangle|0_r\rangle|11\rangle|1_r\rangle|1_r\rangle+\\
&|1_r\rangle|1_r\rangle|00\rangle|0_r\rangle|0_r\rangle+|0_r\rangle|1_r\rangle|00\rangle|0_r\rangle|1_r\rangle+|1_r\rangle|0_r\rangle|11\rangle|1_r\rangle|0_r\rangle+\\
&|0_r\rangle|1_r\rangle|00\rangle|1_r\rangle|0_r\rangle+|1_r\rangle|0_r\rangle|11\rangle|0_r\rangle|1_r\rangle+|0_r\rangle|1_r\rangle|10\rangle|0_r\rangle|0_r\rangle+\\
&|1_r\rangle|0_r\rangle|01\rangle|1_r\rangle|1_r\rangle+|0_r\rangle|1_r\rangle|11\rangle|0_r\rangle|1_r\rangle+|1_r\rangle|0_r\rangle|00\rangle|1_r\rangle|0_r\rangle-\\
&|0_r\rangle|0_r\rangle|10\rangle|1_r\rangle|0_r\rangle-|1_r\rangle|1_r\rangle|01\rangle|0_r\rangle|1_r\rangle-|0_r\rangle|1_r\rangle|11\rangle|0_r\rangle|0_r\rangle-\\
&|1_r\rangle|1_r\rangle|00\rangle|1_r\rangle|1_r\rangle+|0_r\rangle|1_r\rangle|01\rangle|0_r\rangle|0_r\rangle+|1_r\rangle|0_r\rangle|10\rangle|1_r\rangle|1_r\rangle+\\
&|0_r\rangle|1_r\rangle|01\rangle|1_r\rangle|1_r\rangle+|1_r\rangle|0_r\rangle|00\rangle|0_r\rangle|0_r\rangle+|0_r\rangle|1_r\rangle|10\rangle|1_r\rangle|1_r\rangle+\\
&|1_r\rangle|0_r\rangle|01\rangle|0_r\rangle|0_r\rangle+|0_r\rangle|1_r\rangle|11\rangle|1_r\rangle|0_r\rangle+|1_r\rangle|0_r\rangle|00\rangle|0_r\rangle|1_r\rangle)_{ABCDEF}\\
&=\frac{1}{8}[(|0_r\rangle_A|0_r\rangle_B|0_r\rangle_E|0_r\rangle_F+|0_r\rangle_A|1_r\rangle_B|1_r\rangle_E|0_r\rangle_F-|1_r\rangle_A|0_r\rangle_B|0_r\rangle_E|1_r\rangle_F-\\
&|1_r\rangle_A|1_r\rangle_B|1_r\rangle_E|1_r\rangle_F)|\Phi^-\rangle_{CD}+(|0_r\rangle_A|0_r\rangle_B|0_r\rangle_E|1_r\rangle_F-|0_r\rangle_A|1_r\rangle_B|1_r\rangle_E|1_r\rangle_F-\\
&|1_r\rangle_A|0_r\rangle_B|0_r\rangle_E|0_r\rangle_F+|1_r\rangle_A|1_r\rangle_B|1_r\rangle_E|0_r\rangle_F)|\Psi^+\rangle_{CD}+(|0_r\rangle_A|0_r\rangle_B|1_r\rangle_E|0_r\rangle_F-\\
&|0_r\rangle_A|1_r\rangle_B|0_r\rangle_E|0_r\rangle_F+|1_r\rangle_A|0_r\rangle_B|1_r\rangle_E|1_r\rangle_F-|1_r\rangle_A|1_r\rangle_B|0_r\rangle_E|1_r\rangle_F)|\Psi^-\rangle_{CD}+\\
&(|0_r\rangle_A|0_r\rangle_B|1_r\rangle_E|1_r\rangle_F+|0_r\rangle_A|1_r\rangle_B|0_r\rangle_E|1_r\rangle_F+|1_r\rangle_A|0_r\rangle_B|1_r\rangle_E|0_r\rangle_F+\\
&|1_r\rangle_A|1_r\rangle_B|0_r\rangle_E|0_r\rangle_F)|\Phi^+\rangle_{CD}]\\
&=\frac{1}{8}[(|\Phi^+\rangle_{A_1A_2}|\Phi^+\rangle_{B_1B_2}|\Phi^+\rangle_{E_1E_2}|\Phi^+\rangle_{F_1F_2}+|\Phi^+\rangle_{A_1A_2}|\Psi^-\rangle_{B_1B_2}|\Psi^-\rangle_{E_1E_2}|\Phi^+\rangle_{F_1F_2}-\\
&|\Psi^-\rangle_{A_1A_2}|\Phi^+\rangle_{B_1B_2}|\Phi^+\rangle_{E_1E_2}|\Psi^-\rangle_{F_1F_2}-|\Psi^-\rangle_{A_1A_2}|\Psi^-\rangle_{B_1B_2}|\Psi^-\rangle_{E_1E_2}|\Psi^-\rangle_{F_1F_2})|\Phi^-\rangle_{CD}+\\
&(|\Phi^+\rangle_{A_1A_2}|\Phi^+\rangle_{B_1B_2}|\Phi^+\rangle_{E_1E_2}|\Psi^-\rangle_{F_1F_2}-|\Phi^+\rangle_{A_1A_2}|\Psi^-\rangle_{B_1B_2}|\Psi^-\rangle_{E_1E_2}|\Psi^-\rangle_{F_1F_2}-\\
&|\Psi^-\rangle_{A_1A_2}|\Phi^+\rangle_{B_1B_2}|\Phi^+\rangle_{E_1E_2}|\Phi^+\rangle_{F_1F_2}+|\Psi^-\rangle_{A_1A_2}|\Psi^-\rangle_{B_1B_2}|\Psi^-\rangle_{E_1E_2}|\Phi^+\rangle_{F_1F_2})|\Psi^+\rangle_{CD}+\\
&(|\Phi^+\rangle_{A_1A_2}|\Phi^+\rangle_{B_1B_2}|\Psi^-\rangle_{E_1E_2}|\Phi^+\rangle_{F_1F_2}-|\Phi^+\rangle_{A_1A_2}|\Psi^-\rangle_{B_1B_2}|\Phi^+\rangle_{E_1E_2}|\Phi^+\rangle_{F_1F_2}+\\
&|\Psi^-\rangle_{A_1A_2}|\Phi^+\rangle_{B_1B_2}|\Psi^-\rangle_{E_1E_2}|\Psi^-\rangle_{F_1F_2}-|\Psi^-\rangle_{A_1A_2}|\Psi^-\rangle_{B_1B_2}|\Phi^+\rangle_{E_1E_2}|\Psi^-\rangle_{F_1F_2})|\Psi^-\rangle_{CD}+\\
&(|\Phi^+\rangle_{A_1A_2}|\Phi^+\rangle_{B_1B_2}|\Psi^-\rangle_{E_1E_2}|\Psi^-\rangle_{F_1F_2}+|\Phi^+\rangle_{A_1A_2}|\Psi^-\rangle_{B_1B_2}|\Phi^+\rangle_{E_1E_2}|\Psi^-\rangle_{F_1F_2}+\\
&|\Psi^-\rangle_{A_1A_2}|\Phi^+\rangle_{B_1B_2}|\Psi^-\rangle_{E_1E_2}|\Phi^+\rangle_{F_1F_2}+|\Psi^-\rangle_{A_1A_2}|\Psi^-\rangle_{B_1B_2}|\Phi^+\rangle_{E_1E_2}|\Phi^+\rangle_{F_1F_2})|\Phi^+\rangle_{CD}]
\end{aligned}
\tag{8}
$$

These logical states are broken up into six ordered sequences, S_A, S_B, S_C, S_D, S_E, and S_F, consisting of logical qubits A, logical qubits B, particles C, particles D, logical qubits E and logical qubits F, respectively. Among them, logical qubits A, B, E , and F are made up of two physical qubits, namely A_1 and A_2, B_1 and B_2, E_1 and E_2, and F_1 and F_2. Alice randomly selects logical qubits from $\{|0_r\rangle, |1_r\rangle, |+_r\rangle, |-_r\rangle\}$ as decoy states and inserts them into S_A, S_B, S_E, and S_F to obtain S'_A, S'_B, S'_E, and S'_F. Later, Alice sends them to Bob and saves the sequences S_C and S_D.

Step 3 After Bob has received the sequences S'_A, S'_B, S'_E, and S'_F, Alice announces the locations and the measurement basis ($\{|0_r\rangle, |1_r\rangle\}$ or $\{|+_r\rangle, |-_r\rangle\}$) of the decoy logical qubits. Bob uses the correct measurement basis to measure the corresponding decoy logical

Table 3 Measurement results and corresponding values

Alice's measurement result	Bob's measurement result	M^i
$\|\Phi^-\rangle$	$\|\Phi^+\rangle_{A_1A_2}\|\Phi^+\rangle_{B_1B_2}\|\Phi^+\rangle_{E_1E_2}\|\Phi^+\rangle_{F_1F_2}$	0000
$\|\Phi^-\rangle$	$\|\Phi^+\rangle_{A_1A_2}\|\Psi^-\rangle_{B_1B_2}\|\Psi^-\rangle_{E_1E_2}\|\Phi^+\rangle_{F_1F_2}$	0110
$\|\Phi^-\rangle$	$\|\Psi^-\rangle_{A_1A_2}\|\Phi^+\rangle_{B_1B_2}\|\Phi^+\rangle_{E_1E_2}\|\Psi^-\rangle_{F_1F_2}$	1001
$\|\Phi^-\rangle$	$\|\Psi^-\rangle_{A_1A_2}\|\Psi^-\rangle_{B_1B_2}\|\Psi^-\rangle_{E_1E_2}\|\Psi^-\rangle_{F_1F_2}$	1111
$\|\Psi^+\rangle$	$\|\Phi^+\rangle_{A_1A_2}\|\Phi^+\rangle_{B_1B_2}\|\Phi^+\rangle_{E_1E_2}\|\Psi^-\rangle_{F_1F_2}$	0001
$\|\Psi^+\rangle$	$\|\Phi^+\rangle_{A_1A_2}\|\Psi^-\rangle_{B_1B_2}\|\Psi^-\rangle_{E_1E_2}\|\Psi^-\rangle_{F_1F_2}$	0111
$\|\Psi^+\rangle$	$\|\Psi^-\rangle_{A_1A_2}\|\Phi^+\rangle_{B_1B_2}\|\Phi^+\rangle_{E_1E_2}\|\Phi^+\rangle_{F_1F_2}$	1000
$\|\Psi^+\rangle$	$\|\Psi^-\rangle_{A_1A_2}\|\Psi^-\rangle_{B_1B_2}\|\Psi^-\rangle_{E_1E_2}\|\Phi^+\rangle_{F_1F_2}$	1110
$\|\Psi^-\rangle$	$\|\Phi^+\rangle_{A_1A_2}\|\Phi^+\rangle_{B_1B_2}\|\Psi^-\rangle_{E_1E_2}\|\Phi^+\rangle_{F_1F_2}$	0010
$\|\Psi^-\rangle$	$\|\Phi^+\rangle_{A_1A_2}\|\Psi^-\rangle_{B_1B_2}\|\Phi^+\rangle_{E_1E_2}\|\Phi^+\rangle_{F_1F_2}$	0100
$\|\Psi^-\rangle$	$\|\Psi^-\rangle_{A_1A_2}\|\Phi^+\rangle_{B_1B_2}\|\Psi^-\rangle_{E_1E_2}\|\Psi^-\rangle_{F_1F_2}$	1011
$\|\Psi^-\rangle$	$\|\Psi^-\rangle_{A_1A_2}\|\Psi^-\rangle_{B_1B_2}\|\Phi^+\rangle_{E_1E_2}\|\Psi^-\rangle_{F_1F_2}$	1101
$\|\Phi^+\rangle$	$\|\Phi^+\rangle_{A_1A_2}\|\Phi^+\rangle_{B_1B_2}\|\Psi^-\rangle_{E_1E_2}\|\Psi^-\rangle_{F_1F_2}$	0011
$\|\Phi^+\rangle$	$\|\Phi^+\rangle_{A_1A_2}\|\Psi^-\rangle_{B_1B_2}\|\Phi^+\rangle_{E_1E_2}\|\Psi^-\rangle_{F_1F_2}$	0101
$\|\Phi^+\rangle$	$\|\Psi^-\rangle_{A_1A_2}\|\Phi^+\rangle_{B_1B_2}\|\Psi^-\rangle_{E_1E_2}\|\Phi^+\rangle_{F_1F_2}$	1010
$\|\Phi^+\rangle$	$\|\Psi^-\rangle_{A_1A_2}\|\Psi^-\rangle_{B_1B_2}\|\Phi^+\rangle_{E_1E_2}\|\Phi^+\rangle_{F_1F_2}$	1100

qubits and then notifies Alice of the results. In this way, Alice can calculate the error rate. If the error rate is lower than predetermined threshold, go to Step 4. Otherwise, quantum channels are bugged. Abort the protocol and restart from Step 1.

Step 4 After removing the decoy logical qubits, the sequences S'_A, S'_B, S'_E, and S'_F are restored to S_A, S_B, S_E and S_F. Alice carries out the Bell measurement on each pair of the corresponding particles in sequences S_C and S_D, and Bob carries out the Bell measurements on particles A_1 and A_2 in S_A, B_1 and B_2 in S_B, E_1 and E_2 in S_E, F_1 and F_2 in S_F. The encoding scheme agreed upon by Alice and Bob is

$$\begin{aligned}
&|\Phi^+\rangle_{A_1A_2}|\Phi^+\rangle_{B_1B_2}|\Phi^+\rangle_{E_1E_2}|\Phi^+\rangle_{F_1F_2}\rightarrow 0000, |\Phi^+\rangle_{A_1A_2}|\Phi^+\rangle_{B_1B_2}|\Phi^+\rangle_{E_1E_2}|\Psi^-\rangle_{F_1F_2}\rightarrow 0001,\\
&|\Phi^+\rangle_{A_1A_2}|\Phi^+\rangle_{B_1B_2}|\Psi^-\rangle_{E_1E_2}|\Phi^+\rangle_{F_1F_2}\rightarrow 0010, |\Phi^+\rangle_{A_1A_2}|\Phi^+\rangle_{B_1B_2}|\Psi^-\rangle_{E_1E_2}|\Psi^-\rangle_{F_1F_2}\rightarrow 0011,\\
&|\Phi^+\rangle_{A_1A_2}|\Psi^-\rangle_{B_1B_2}|\Phi^+\rangle_{E_1E_2}|\Phi^+\rangle_{F_1F_2}\rightarrow 0100, |\Phi^+\rangle_{A_1A_2}|\Psi^-\rangle_{B_1B_2}|\Phi^+\rangle_{E_1E_2}|\Psi^-\rangle_{F_1F_2}\rightarrow 0101,\\
&|\Phi^+\rangle_{A_1A_2}|\Psi^-\rangle_{B_1B_2}|\Psi^-\rangle_{E_1E_2}|\Phi^+\rangle_{F_1F_2}\rightarrow 0110, |\Phi^+\rangle_{A_1A_2}|\Psi^-\rangle_{B_1B_2}|\Psi^-\rangle_{E_1E_2}|\Psi^-\rangle_{F_1F_2}\rightarrow 0111,\\
&|\Psi^-\rangle_{A_1A_2}|\Phi^+\rangle_{B_1B_2}|\Phi^+\rangle_{E_1E_2}|\Phi^+\rangle_{F_1F_2}\rightarrow 1000, |\Psi^-\rangle_{A_1A_2}|\Phi^+\rangle_{B_1B_2}|\Phi^+\rangle_{E_1E_2}|\Psi^-\rangle_{F_1F_2}\rightarrow 1001,\\
&|\Psi^-\rangle_{A_1A_2}|\Phi^+\rangle_{B_1B_2}|\Psi^-\rangle_{E_1E_2}|\Phi^+\rangle_{F_1F_2}\rightarrow 1010, |\Psi^-\rangle_{A_1A_2}|\Phi^+\rangle_{B_1B_2}|\Psi^-\rangle_{E_1E_2}|\Psi^-\rangle_{F_1F_2}\rightarrow 1011,\\
&|\Psi^-\rangle_{A_1A_2}|\Psi^-\rangle_{B_1B_2}|\Phi^+\rangle_{E_1E_2}|\Phi^+\rangle_{F_1F_2}\rightarrow 1100, |\Psi^-\rangle_{A_1A_2}|\Psi^-\rangle_{B_1B_2}|\Phi^+\rangle_{E_1E_2}|\Psi^-\rangle_{F_1F_2}\rightarrow 1101,\\
&|\Psi^-\rangle_{A_1A_2}|\Psi^-\rangle_{B_1B_2}|\Psi^-\rangle_{E_1E_2}|\Phi^+\rangle_{F_1F_2}\rightarrow 1110, |\Psi^-\rangle_{A_1A_2}|\Psi^-\rangle_{B_1B_2}|\Psi^-\rangle_{E_1E_2}|\Psi^-\rangle_{F_1F_2}\rightarrow 1111
\end{aligned} \tag{9}$$

Like the first protocol, all the Bob's measurement results are coded as $M = M^1 \| M^2 \| \cdots \| M^n$, where M^i is the code of Bob's ith measurement result ($i = 1, 2, \cdots, n$). Table 3 shows the measurement results and corresponding values.

When Bob finally publishes the Bell measurement results for A_1 and A_2 in S_A, B_1 and B_2 in S_B, Alice and Bob can deduce each other's results. That is, they share a classic bit string M.

Step 5 According to the key K_A, Alice lets $i_1 i_2 = K^i_{A12}$ and $i_3 i_4 = K^i_{A34}$(i = 1, 2, … , n). Then Alice performs the unitary operation $U_{i_1 i_2}$ on the ith particle in S_D to obtain the new sequence S^*_D. By matching two particles in S_C and S^*_D, a new Bell state is produced in this manner. In accordance with the new Bell state, Alice prepares the relevant logical Bell state $\lambda_r\rangle_{C_1C_2D_1D_2}$. Then Alice performs the unitary operation $U_{i_3 i_4}$ on the ith particle in S^*_D to obtain the new sequence $S^{*(1)}_D$. The corresponding two particles in S_C and $S^{*(1)}_D$ constitute a new Bell state. Similarly, Alice prepares the corresponding logical Bell state $|\lambda^*{}_r\rangle_{C_1,C_2,D_1,D_2}$. The four logical Bell states [37] are described as follows:

$$
\begin{aligned}
|\boldsymbol{\Phi}^+_r\rangle_{C_1C_2D_1D_2} &= \frac{1}{\sqrt{2}}\left(|0_r\rangle|0_r\rangle + |1_r\rangle|1_r\rangle\right)_{C_1C_2D_1D_2} \\
&= \frac{1}{\sqrt{2}}\left(|\boldsymbol{\Phi}^+\rangle|\boldsymbol{\Phi}^+\rangle + |\boldsymbol{\Psi}^-\rangle|\boldsymbol{\Psi}^-\rangle\right)_{C_1D_1C_2D_2} \\
|\boldsymbol{\Phi}^-_r\rangle_{C_1C_2D_1D_2} &= \frac{1}{\sqrt{2}}\left(|0_r\rangle|0_r\rangle - |1_r\rangle|1_r\rangle\right)_{C_1C_2D_1D_2} \\
&= \frac{1}{\sqrt{2}}\left(|\boldsymbol{\Phi}^-\rangle|\boldsymbol{\Phi}^-\rangle + |\boldsymbol{\Psi}^+\rangle|\boldsymbol{\Psi}^+\rangle\right)_{C_1D_1C_2D_2} \\
|\boldsymbol{\Psi}^+_r\rangle_{C_1C_2D_1D_2} &= \frac{1}{\sqrt{2}}\left(|0_r\rangle|1_r\rangle + |1_r\rangle|0_r\rangle\right)_{C_1C_2D_1D_2} \\
&= \frac{1}{\sqrt{2}}\left(|\boldsymbol{\Phi}^-\rangle|\boldsymbol{\Psi}^+\rangle - |\boldsymbol{\Psi}^+\rangle|\boldsymbol{\Phi}^-\rangle\right)_{C_1D_1C_2D_2} \\
|\boldsymbol{\Psi}^-_{dp}\rangle_{C_1C_2D_1D_2} &= \frac{1}{\sqrt{2}}\left(|0_r\rangle|1_r\rangle - |1_r\rangle|0_r\rangle\right)_{C_1C_2D_1D_2} \\
&= \frac{1}{\sqrt{2}}\left(|\boldsymbol{\Phi}^+\rangle|\boldsymbol{\Psi}^-\rangle - |\boldsymbol{\Psi}^-\rangle|\boldsymbol{\Phi}^+\rangle\right)_{C_1D_1C_2D_2}
\end{aligned}
\tag{10}
$$

Alice divides the logical Bell state $|\lambda_r\rangle_{C_1C_2D_1D_2}$ into two ordered sequences $S^{(1)}_D$ and $S^{(1)}_D$, consisting of logical qubits C (two physical qubits C_1 and C_2) and logical qubits D (two physical qubits D_1 and D_2), respectively. Likewise, the logical Bell state $|\lambda^*{}_r\rangle_{C_1C_2D_1D_2}$ is also divided into two ordered sequences $S^{(2)}_C$ and $S^{(2)}_D$. Then Alice performs a permutation operator $\prod_n$ on $S^{(1)}_C$ and $S^{(2)}_C$ to get two random sequences $S^{(1)*}_C$ and $S^{(2)*}_C$. Alice randomly selects the decoy logical qubits and inserts them into $S^{(1)*}_C$, $S^{(1)}_D$, $S^{(2)*}_C$ and $S^{(2)}_D$ to generate the sequences $S^{(1)*\prime}_C$, $S^{(1)\prime}_D$, $S^{(2)*\prime}_C$ and $S^{(2)\prime}_D$, in which the decoy logical qubits are randomly taken from the set $\{|0_r\rangle, |1_r\rangle, |+_r\rangle, |-_r\rangle\}$. Alice sends the sequences $S^{(1)*\prime}_C$, $S^{(1)\prime}_D$, $S^{(2)*\prime}_C$ and $S^{(2)\prime}_D$ to Bob.

Step 6 These steps resemble steps 6-8 of the protocol against collective-dephasing noise.

3.3 Correctness Analysis of Two Protocols

Reference [38] proved that logical states $|0_{dp}\rangle$ and $|1_{dp}\rangle$ can resist collective-dephasing noise, while logical states $|0_r\rangle$ and $|1_r\rangle$ can resist collective-rotation noise. Afterwards, Kwiat et al. [39] verified the noise resistance of logical qubits in DFS through experiments. Walton et al [16] first proposed the use of logical qubits to implement quantum key distribution under collective noise.

Take the first protocol as an example, we replace the qubits to be transmitted with the corresponding logical states, that is

$$|0\rangle \rightarrow |0_{dp}\rangle, |1\rangle \rightarrow |1_{dp}\rangle \tag{11}$$

Therefore, the quantum source, decoy states, and Bell states undergo the following transformation in the protocol:

$$\begin{gathered} |\psi\rangle_{ABCDEF} \rightarrow |\psi_{dp}\rangle_{ABCDEF} \\ \{|0\rangle, |1\rangle, |+\rangle, |-\rangle\} \rightarrow \{|0_{dp}\rangle, |1_{dp}\rangle, |+_{dp}\rangle, |-_{dp}\rangle\} \\ |\Phi^+\rangle \rightarrow |\Phi^+_{dp}\rangle \; |\Phi^-\rangle \rightarrow |\Phi^-_{dp}\rangle \; |\Psi^+\rangle \rightarrow |\Psi^+_{dp}\rangle \; |\Psi^-\rangle \rightarrow |\Psi^-_{dp}\rangle \end{gathered} \tag{12}$$

These transformed quantum states are unaffected in noisy channels. Among them, the logical six-particle entangled states and the logical Bell states can transmit information through entanglement swapping, and the logical decoy states can be used as eavesdropping checks. Consequently, our protocols are working.

4 Security Analysis

Since all the transmitted particles are logical states, the above protocols can resist collective-dephasing noise and collective-rotation noise, respectively. Next, we analyze the impact of malicious attacks on protocols. QKA protocols are mainly involved in two types of attacks: internal and external attacks. In order to demonstrate the security of the protocols, we will discuss both types of attacks separately.

4.1 Internal Attack

Because of delayed measurement technology, Bob can only infer K_A after announcing $K'_B = K_B \oplus M$. As a result, he is unable to use the key K_A to manipulate the key K_B, which prevents him from carrying out the internal attack. Before sending the encoded message qubits, Alice is unaware of the key K_B; therefore, she would not alter K_A depending on it. So Alice's internal attack is invalid.

4.2 External Attack

External attack can be subdivided into the Trojan horse attacks, the intercept-resend attack, and the entangle-measure attack. Supposing Eve is an external attacker, she must eavesdrop on the values of M and K_A to acquire the shared key. The following is a detailed analysis of three primary attack strategies.

Trojan horse attacks Since these two protocols are unidirectional QKA protocols, all particle sequences are transmitted just once in quantum channels. No opportunity exists for Eve to retrieve spy photons from particle sequences. In other words, the two protocols can immunize Trojan horse attacks without using any specific detection device.

Intercept-resend attack Eve intends to execute an intercept-resend attack on the sequences S'_A, S'_B, S'_E, and S'_F transmitted in quantum channels. She has to intercept these sequences and send pseudo-random sequences to Bob. Nonetheless, Eve is uninformed

of the decoy logical qubit's position and matched measurement basis before the eavesdropping check. Therefore Eve has only a 25% probability of successfully measuring the value of the decoy logical qubit. Assuming that the number of decoy logical qubits prepared for each sequence is λ, the probability of detecting eavesdropping is $1-(3/4)^{\lambda}$, which shows that the participant can easily detect the eavesdropper' presence when λ is large enough. Once the eavesdropper is detected, this protocol is terminated and restarted. As a result, it is almost impossible for Eve to get the final key via the intercept-resend attack.

Entangle-measure attack Assuming Eve is motivated to make an entangle-measure attack on the two QKA protocols with her prepared auxiliary photon $|p\rangle$, she is likely to perform the unitary operation U on the intercepted qubit to entangle it with the auxiliary photon. Taking the QKA protocol immune to collective-dephasing noise as an example, the evolution process of the quantum system is as follows:

$$
\begin{aligned}
&U|0_{dp}\rangle|p\rangle = a_{00}|00\rangle|p_{00}\rangle + a_{01}|01\rangle|p_{01}\rangle + a_{10}|10\rangle|p_{10}\rangle + a_{11}|11\rangle|p_{11}\rangle,\\
&U|1_{dp}\rangle|p\rangle = b_{00}|00\rangle|p^{'}_{00}\rangle + b_{01}|01\rangle|p^{'}_{01}\rangle + b_{10}|10\rangle|p^{'}_{10}\rangle + b_{11}|11\rangle|p^{'}_{11}\rangle,\\
&U|+_{dp}\rangle|p\rangle = 1/\sqrt{2}(U|0_{dp}\rangle|p\rangle + U|1_{dp}\rangle|p\rangle)\\
&\qquad =1/2[|\Phi^{+}\rangle(a_{00}|p_{00}\rangle + a_{11}|p_{11}\rangle + b_{00}|p^{'}_{00}\rangle + b_{11}|p^{'}_{11}\rangle)+\\
&\qquad\ |\Phi^{-}\rangle(_{a_{00}} - a_{11}|p_{11}\rangle + b_{00}|p^{'}_{00}\rangle - b_{11}|p^{'}_{11}\rangle)+\\
&\qquad\ |\Psi^{+}\rangle(a_{01}|p_{01}\rangle + a_{10}|p_{10}\rangle + b_{01}|p^{'}_{01}\rangle + b_{10}|p^{'}_{10}\rangle)+\\
&\qquad\ |\Psi^{-}\rangle(a_{01}|p_{01}\rangle - a_{10}|p_{10}\rangle + b_{01}|p^{'}_{01}\rangle - b_{10}|p^{'}_{10}\rangle)]\\
&U|-_{dp}\rangle|p\rangle = 1/\sqrt{2}(U|0_{dp}\rangle|p\rangle - U|1_{dp}\rangle|p\rangle)\\
&\qquad =1/2[|\Phi^{+}\rangle(a_{00}|p_{00}\rangle + a_{11}|p_{11}\rangle - b_{00}|p^{'}_{00}\rangle - b_{11}|p^{'}_{11}\rangle)+\\
&\qquad\ |\Phi^{-}\rangle(a_{00}|p_{00}\rangle - a_{11}|p_{11}\rangle - b_{00}|p^{'}_{00}\rangle + b_{11}|p^{'}_{11}\rangle)+\\
&\qquad\ |\Psi^{+}\rangle(a_{01}|p_{01}\rangle + a_{10}|p_{10}\rangle - b_{01}|p^{'}_{01}\rangle - b_{10}|p^{'}_{10}\rangle)+\\
&\qquad\ |\Psi^{-}\rangle(a_{01}|p_{01}\rangle - a_{10}|p_{10}\rangle - b_{01}|p^{'}_{01}\rangle + b_{10}|p^{'}_{10}\rangle)]
\end{aligned}
\tag{13}
$$

where $|a_{00}|^2+|a_{01}|^2+|a_{10}|^2+|a_{11}|^2=|b_{00}|^2+|b_{01}|^2+|b_{10}|^2+|b_{11}|^2=1$, a_{00},a_{01},a_{10},a_{11},b_{00},b_{01}, b_{10} and b_{11} denote the vector parameters of U, $|p_{00}\rangle$,$|p_{01}\rangle$,$|p_{10}\rangle$,$|p_{11}\rangle$,$|\ p'_{00}\rangle$,$|\ p'_{01}\rangle$,$|\ p'_{10}\rangle$ and $|\ p'_{11}\rangle$ denote the states of the probe space. For the eavesdropping to go undetected, Eve's operation U must meet three conditions:$a_{00}=a_{10}=a_{11}=0$, $b_{00}=b_{01}=b_{11}=0$, and $a_{01}\ |\ p_{01}\rangle = b_{10}\ |\ p'_{10}\rangle$. Clearly, Eve introduces no error only when the auxiliary photon and the target particle are product states. That is, she just gets meaningless information on K_A and K_B. These two protocols are resistant to external attacks.

5 Efficiency Analysis

Efficiency is an important factor limiting the large-scale application of QKA protocols. In the literature [40], Cabello defines qubit efficiency as $\eta = \frac{n_k}{n_q+n_c}$, where n_k, n_q, and n_c denote the length of the final generated key, the number of qubits used, and the number of classical bits used, respectively. In our two protocols, it is assumed that n is the number of

Table 4 Comparison with other similar protocols

QKA protocol	Quantum resource	Measurement basis	Efficiency(%)
Huang's [20]	EPR pairs	Z-basis and X-basis	16.67
He's [21]	Logical χ *states*	ZZ-basis and Bell basis	21.05
Yang's[23]	Logical Bell states	Bell basis	21.05
Zhou's [25]	Logical GHZ states	ZZ-basis and Bell basis	21.05
Ours	logical six-particle entangled states	ZZZZ-basis and Bell basis	22.22

logical six-particle entangled states and m is the number of decoy logical qubits inserted in each transmitted quantum sequence.

Take the protocol immune to collective-dephasing noise as an example. According to Eq. (5), each logical quantum state $|\psi_{\mathrm{dp}}\rangle_{ABCDEF}$ is transformed into $|\psi\rangle_{A_1B_1CDE_1F_1} \otimes |1111\rangle_{A_2B_2E_2F_2}$, ultimately only six particles, A_1, B_1, C, D, E_1, and F_1, are used, totaling $6n$ qubits. In Step 5, Alice uses n logical Bell states $|\lambda_{dp}\rangle_{C_1C_2D_1D_2}$ and n logical Bell states $|\lambda^*{}_{dp}\rangle_{C_1C_2D_1D_2}$, totaling $(4n+4n)$ qubits. For the eavesdropping checks, Alice inserts m decoy logical states into each of the four sequences in Step 2, and the same applies in Step 5. Each decoy logical state consists of two particles, totaling $(8m+8m)$ qubits. So the number of qubits used is $n_q=(6n+4n+4n)+(8m+8m)$. In Step 4 and Step 7, Bob publishes the measurement result for particles $A_1$and B_1, as well as the result for $K'_B = K_B \oplus M = \left(K_B^1 \oplus M^1\right) \| \left(K_B^2 \oplus M^2\right) \| \cdots \| \left(K_B^n \oplus M^n\right)$, respectively. Therefore, the number of classical bits used is $n_c=(2n+4n)$.

Thus, the qubit efficiency of the protocols is $\eta = \frac{8n}{(6n+4n+4n+8m+8m+2n+4n)}$. Let $m = n$, we have $\eta=22.22\%$.

Table 4 compares our protocols with the current representative two-party protocols for immunity to collective noise, indicating that our protocols have higher qubit efficiency.

6 Conclusion

On the basis of logical six-particle entangled states, this study presents two QKA protocols against different types of collective noise. At first, a significant advantage of proposed protocols is that only Bell or ZZZZ-basis measurements are required for quantum states. The equipment used in these two measurement methods is relatively simple and easy to realize under current conditions. In addition, security analysis demonstrates that the two protocols can also resist internal and external attacks. Lastly, we compute both protocols' qubit efficiency, and the results are relatively high.

Acknowledgements This work is supported by the Open Fund of Anhui Key Laboratory of Mine Intelligent Equipment and Technology (Grant No. ZKSYS202204), the Talent Introduction Fund of Anhui University of Science and Technology (Grant No. 2021yjrc34), and the Scientific Research Fund of Anhui Provincial Education Department (Grant No. KJ2020A0301).

Data availability Not applicable.

Code availability Not applicable.

Declarations

Conflict of interest The authors declare there is no conflict of interest.

Ethics approval Not applicable.

References

1. Shor, P.W.: Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. Siam. Rev. **41**(2), 303–332 (1999)
2. Gordon, J.: Strong RSA keys. Electron. Lett. **20**(12), 514–516 (1984)
3. Lancien, C., Majenz, C.: Weak approximate unitary designs and applications to quantum encryption. Quantum. **4**, 313 (2020)
4. Kuang, R., Perepechaenko, M.: Quantum encryption with quantum permutation pad in IBMQ systems. Epj. Quantum. Technol. **9**(1), 26 (2022)
5. Jennewein, T., Achleitner, U., Weihs, G., Weinfurter, H., Zeilinger, A.: A fast and compact quantum random number generator. Rev. Sci. Instrum. **71**(4), 1675–1680 (2000)
6. Gisin, N., Ribordy, G., Tittel, W., Zbinden, H.: Quantum cryptography. Rev. Mod. Phys. **74**(1), 145–190 (2002)
7. Bennett, C.H., Brassard, G.: Quantum cryptography: public-key distribution and coin tossing. In: Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, pp. 175–179. IEEE, New York (1984)
8. Ekert, A.K.: Quantum Cryptography and Bell's Theorem. In: Quantum Measurements in Optics, pp. 413–418. Springer, Boston, MA (1992)
9. Bennett, C.H.: Quantum cryptography using any two nonorthogonal states. Phys. Rev. Lett. **68**, 3121–3124 (1992)
10. Gao, F., Guo, F.Z., Wen, Q.Y., Zhu, F.C.: Quantum key distribution without alternative measurements and rotations. Phys. Lett. A. **349**(1-4), 53–58 (2006)
11. Zhou, N., Zeng, G., Xiong, J.: Quantum key agreement protocol. Electron. Lett. **40**, 1149–1150 (2004)
12. Chong, S.K., Hwang, T.: Quantum key agreement protocol based on BB84. Opt. Commun. **283**(6), 1192–1195 (2010)
13. Shukla, C., Alam, N., Pathak, A.: Protocols of quantum key agreement solely using Bell states and Bell measurement. Quantum Inf. Process. **13**, 2391–2405 (2014)
14. Chong, S.K., Tsai, C.W., Hwang, T.: Improvement on quantum key agreement protocol with maximally entangled states. Int. J. Theor. Phys. **50**, 1793–1802 (2011)
15. 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)
16. Walton, Z.D., Abouraddy, A.F., Sergienko, A.V., et al.: Decoherence-free subspaces in quantum key distribution. Phys. Rev. Lett. **91**, 087901 (2003)
17. Huang, W., Su, Q., Wu, X., Li, Y.B., Sun, Y.: Quantum key agreement against collective decoherence. Int. J. Theor. Phys. **53**, 2891 (2014)
18. 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)
19. He, Y.F., Ma, W.P.: Two-party quantum key agreement against collective noise. Quantum Inf. Process. **15**, 5023–5035 (2016)
20. Gao, H., Chen, X.G., Qian, S.R.: Two-party quantum key agreement protocols under collective noise channel. Quantum Inf. Process. **17**, 140 (2018)
21. Yang, Y.G., Gao, S., Li, D., Zhou, Y.H., Shi, W.M.: Quantum Inf. Process. **18**(3), 1–17 (2019)
22. Wang, S.S., Jiang, D.H., Xu, G.B., Zhang, Y.H., Liang, X.Q.: Quantum key agreement with Bell states and Cluster states under collective noise channels. Quantum Inf. Process. **18**(6), 1–14 (2019)
23. Zhou, Y.H., Wang, M.F., Shi, W.M., Yang, Y.G., Zhang, J.: Two-party quantum key agreement against collective noisy channel. Quantum Inf. Process. **19**(3), 1–15 (2020)
24. Guo, J.H., Yang, Z., Bai, M.Q., Mo, Z.W.: Quantum Key Agreement Protocols with GHZ States Under Collective Noise Channels. Int. J. Theor. Phys. **61**(3), 1–12 (2022)
25. Wang, W., Zhou, B.M., Zhang, L.: The three-party quantum key agreement protocol with quantum Fourier transform. Int. J. Theor. Phys. **59**, 1944–1955 (2020)
26. Yang, H., Lu, S., Zhu, J., Wu, J., Zhou, Q., Li, T.: A Tree-type Multiparty Quantum Key Agreement Protocol Against Collusive Attacks. Int. J. Theor. Phys. **62**(1), 7 (2022)
27. Zhao, W., Jiang, M.: Multi-party quantum key agreement with parameter-independent channels. Pramana. **97**(2), 65 (2023)

28. Deng, F.G., Long, G.L., Wang, Y., Xiao, L.: Increasing the efficiencies of random-choice-based quantum communication protocols with delayed measurement. Chin. Phys. Lett. **21**, 2097 (2004)
29. 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)
30. 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)
31. Tang, J., Shi, L., Wei, J.: Controlled quantum key agreement based on maximally three-qubit entangled states. Mod. Phys. Lett. B. **34**(18), 2050201 (2020)
32. Karim, F., Abulkasim, H., Alabdulkreem, E., Ahmed, N., Jamjoom, M., Abbas, S.: Improvements on new quantum key agreement protocol with five-qubit Brown states. Mod. Phys. Lett. A. **37**(20), 2250128 (2022)
33. Deng, F.G., Li, X.H., Zhou, H.Y., Zhang, Z.J.: Improving the security of multiparty quantum secret sharing against Trojan horse attack. Phys. Rev. A. **72**, 044302 (2005)
34. Cai, Q.Y.: Eavesdropping on the two-way quantum communication protocols with invisible photons. Phys. Lett. A. **351**, 23–25 (2006)
35. Liu, F., Su, Q., Wen, Q.Y.: Eavesdropping on multiparty quantum secret sharing scheme based on the phase shift operations. Int. J. Theor. Phys. **53**, 1730–1737 (2014)
36. Borras, A., Plastino, A.R., Batle, J., Zander, C., Casas, M., Plastino, A.: Multiqubit systems: highly entangled states and entanglement distribution. J. Phys. A-Math. Theor. **40**(44), 13407 (2007)
37. Ye, T.Y.: Robust quantum dialogue based on the entanglement swapping between any two logical Bell states and the shared auxiliary logical Bell state. Quantum Inf. Process. **14**, 1469–1486 (2015)
38. Palma, G.M., Suominen, K.A., Ekert, A.K.: Quantum computers and dissipation. Proc. R. Soc. London A. **452**(1946), 567–584 (1996)
39. Kwiat, P.G., Berglund, A.J., Altepeter, J.B., White, A.G.: Experimental verification of decoherence-free subspaces. Science. **290**(5491), 498–501 (2000)
40. Cabello, A.: Quantum key distribution in the Holevo limit. Phys. Rev. Lett. **85**, 5635–5638 (2000)

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

Springer Nature or its licensor (e.g. a society or other partner) holds exclusive rights to this article under a publishing agreement with the author(s) or other rightsholder(s); author self-archiving of the accepted manuscript version of this article is solely governed by the terms of such publishing agreement and applicable law.