

Three-party quantum key agreement with seven-particle entangled states against collective noise: IBM Qiskit implementation

She-Xiang Jiang(蒋社想) and Jin-Huan Li(李金欢)
Citation: Chin. Phys. B, 2026, 35 (**7**): 070307. DOI: 10.1088/1674-1056/ae53b6
http://cpb.iphy.ac.cn; http://iopscience.iop.org/cpb

What follows is a list of articles you may be interested in

Experimental demonstration of quantum optimal control via the alternating control-evolution protocol

Ruiqi Tang(汤睿琪), Yanjun Hou(侯彦君), Zhenyue Du(杜臻越), Zhuoyue Xu(徐卓越), Yuquan Chen(陈昱全), Zhaokai Li(李兆凯), and Xinhua Peng(彭新华)
Chin. Phys. B, 2026, 35 (**6**): 060302. DOI: 10.1088/1674-1056/ae56e0

Distributed quantum circuit partitioning and teleportation optimization based on a multi-dimensional evaluation strategy

Le Zhang(张乐), Zhijin Guan(管致锦), Shuo Qin(秦硕), Zheng Luo(罗政), Fei Ding(丁飞), and Xueyun Cheng(程学云)
Chin. Phys. B, 2026, 35 (**5**): 050305. DOI: 10.1088/1674-1056/ae1c30

Fault tolerant controlled quantum dialogue against collective noise

Li-Wei Chang(常利伟), Yu-Qing Zhang(张宇青), Xiao-Xiong Tian(田晓雄), Yu-Hua Qian(钱宇华), Shi-Hui Zheng(郑世慧)
Chin. Phys. B, 2020, 29 (**1**): 010304. DOI: 10.1088/1674-1056/ab5786

Faithful deterministic secure quantum communication and authentication protocol based on hyperentanglement against collective noise

Chang Yan (昌燕), Zhang Shi-Bin (张仕斌), Yan Li-Li (闫丽丽), Han Gui-Hua (韩桂华)
Chin. Phys. B, 2015, 24 (**8**): 080306. DOI: 10.1088/1674-1056/24/8/080306

Multi-user quantum key distribution with collective eavesdropping detection over collective-noise channels

Huang Wei (黄伟), Wen Qiao-Yan (温巧燕), Liu Bin (刘斌), Gao Fei (高飞)
Chin. Phys. B, 2015, 24 (**7**): 070308. DOI: 10.1088/1674-1056/24/7/070308

Three-party quantum key agreement with seven-particle entangled states against collective noise: IBM Qiskit implementation

She-Xiang Jiang(蒋社想)[1,2,†] and Jin-Huan Li(李金欢)[1,2]

[1] *State Key Laboratory of Digital Intelligent Technology for Unmanned Coal Mining, Anhui University of Science and Technology, Huainan* 232001, *China*
[2] *School of Computer Science and Engineering, Anhui University of Science and Technology, Huainan* 232001, *China*

(Received 20 January 2026; revised manuscript received 15 March 2026; accepted manuscript online 18 March 2026)

Quantum key agreement (QKA) constitutes a vital branch of quantum cryptography, referring to the collaborative establishment of a shared key among multiple participants. Among these, the three-party quantum key agreement (TPQKA) represents a specific form of QKA involving only three participants. Quantum states inevitably suffer from noise during transmission through quantum channels, which reduces the efficiency of qubits. To significantly improve the efficiency of qubits and further enhance their reliability in quantum applications, this paper proposes two TPQKA protocols based on seven-particle entangled states to provide protection against collective noise effects. In this paper, IBM Qiskit is employed to present the preparation circuit of the seven-particle entangled state, as well as the quantum circuits under two types of collective noise. In both protocols, the three parties apply a hash function to their own keys. In the particle transmission process, according to the measurement results of the particles, the three parties perform the corresponding unitary operation, and ultimately they equally negotiate the final shared key. Both protocols are robust against collective noise, and their qubit efficiency reaches 19.35%. In addition, the security analysis shows that both protocols are resistant to participant attacks and outside attacks, including intercept-resend attacks and entangle-measure attacks. This paper details the detection method of eavesdropping by eavesdroppers in collective noise through simulation, and finally presents key post-processing.

Keywords: three-party quantum key agreement, seven-particle entangled states, collective noise, simulation, key post-processing

PACS: 03.67.–a, 03.67.Dd, 03.67.Hk

DOI: 10.1088/1674-1056/ae53b6 **CSTR:** 32038.14.CPB.ae53b6

1. Introduction

Quantum cryptography is a new type of cryptographic system resulting from the combination of classical cryptographic theory and the principles of quantum mechanics. Its security is guaranteed by the theory of quantum mechanics, and is independent of the attacker's computational ability. As early as 1969, the paper "Conjugate coding"[1] used quantum effects to protect the idea of information. Unfortunately, for various reasons, this paper was not published until 1983. Since the introduction of quantum key distribution (QKD),[2–4] various quantum cryptography methods such as quantum secure direct communication (QSDC),[5,6] quantum secret sharing (QSS),[7–10] quantum private query (QPQ),[11,12] and quantum private comparison (QPC)[13–17] have been proposed. QKD has made great strides and developments, translating fundamental physics into practical applications in academia and industry.[18,19]

In 2004, Zhou *et al.*[20] introduced a QKA protocol utilizing quantum teleportation as its foundation, enabling the secure generation of private key bits between two parties through the public communication channel. Subsequently, Chong *et al.*[21] pointed out that in the Zhou *et al.* scheme, a participant may have the ability to determine the final shared key without being detected. In 2013, Shi *et al.*[22] introduced two-party and multi-party QKA protocols that relied on entanglement switching, which was the first multi-party QKA protocol. Since then, many QKA protocols[23–29] have emerged that rely on multiple qubit states and quantum entanglement switching technology. In recent years, as the application field of quantum cryptography continues to expand, multi-party quantum key agreement (MQKA) has become the focus of scholars' attention. Yang *et al.*[30] proposed an efficient one-state TPQKA protocol using maximally entangled states as quantum resources. Zhou *et al.*[31] proposed a TPQKA protocol based on seven-qubit entangled states using different encryption methods to transmit keys of the same length. Li *et al.*[32] proposed two tripartite quantum key negotiation protocols based on logic four-particle cluster states resistant to collective noise. Hwang *et al.*[33] proposed two three-party QKD protocols to safeguard the security of large-scale networks, one employing implicit user authentication and the other explicit mutual authentication. He *et al.*[34] proposed a TPQKA protocol based on four-particle cluster states. Tang *et al.*[35] proposed a three-party controlled QKA protocol with three levels of GHZ states and Bell measurements. Younes *et al.*[36] proposed a novel lightweight QKD protocol based on four-

†Corresponding author. E-mail: sxjiang@aust.edu.cn

© 2026 Chinese Physical Society and IOP Publishing Ltd. All rights, including for text and data mining, AI training, and similar technologies, are reserved.

particle cluster states, addressing several limitations of existing semi-quantum key distribution schemes relying on bidirectional or cyclic transmission methods. Xu *et al.*[37] proposed a TPQKA protocol based on GHZ entangled states. Zhu *et al.*[38] proposed a QKA protocol for semi-honest three-party mutual authentication based on GHZ-like states. However, research on three-party or multi-party QKA protocols is still at an early stage, with relatively low efficiency and limited resistance to collective noise.

Although various TPQKA protocols have been proposed, most existing schemes either focus primarily on ideal noiseless channels or suffer from relatively low qubit efficiency. In practical quantum communication scenarios, collective noise is unavoidable and can significantly degrade protocol performance. While some studies have considered noise resistance, few protocols simultaneously achieve robustness against collective noise and maintain relatively high qubit efficiency. Therefore, it remains meaningful to design TPQKA protocols that are both noise-resilient and efficient.

Motivated by this gap, we propose two TPQKA protocols based on seven-particle entangled states, which encode logical qubits into decoherence-free subspaces to resist collective noise while improving qubit efficiency. Seven-particle entangled states involve more qubits than GHZ states or five-particle entangled states,[39] making it more difficult for eavesdroppers to eavesdrop without drawing attention to themselves. Considering that the original seven-particle entangled state needs to be transformed to resist the collective noise during the execution of the protocol, this paper adds phase gates and rotating Y gates to simulate the collective noise, where the angle of rotation is randomized. In the two proposed protocols, the three parties first use hash functions to encrypt their own keys to improve their security. Subsequently, Bob and Charlie perform the corresponding unitary operations based on the measurement results of the received sequences, and finally, through the published information, the three parties jointly negotiate the final shared key. In addition, the security analysis results show that both protocols are resistant to attacks from participants and outsiders, where intercept-resend attacks and entangle-measure attacks are used to simulate the malicious behavior of eavesdroppers using IBM Qiskit.

The rest of the paper is structured as follows. Section 2 provides theoretical knowledge. Then, Section 3 describes two TPQKA protocols against collective noise. Section 4 analyzes the protocol's security. Section 5 calculates the protocol's qubit efficiency. Section 6 presents a discussion. Finally, Section 7 presents the conclusions.

2. Theoretical knowledge

This section presents some theoretical knowledge related to protocols, including some common quantum gates, seven-particle entangled states, collective noise, and more.

2.1. Quantum gates

Quantum gates are the fundamental building blocks of quantum computation and are used to manipulate and control quantum information. The basic single-qubit gates are as follows:

$$I=\begin{pmatrix}1&0\\0&1\end{pmatrix},\ X=\begin{pmatrix}0&1\\1&0\end{pmatrix},\ Y=\begin{pmatrix}0&-\mathrm{i}\\\mathrm{i}&0\end{pmatrix},$$
$$H=\frac{1}{\sqrt{2}}\begin{pmatrix}1&1\\1&-1\end{pmatrix},\ Z=\begin{pmatrix}1&0\\0&-1\end{pmatrix}. \tag{1}$$

The C-NOT gate is the most commonly used two-qubit logical gate that accepts two qubits as input and outputs two qubits. These two input qubits are often referred to as the control qubit and the target qubit. When the control qubit is $|1\rangle$, a NOT gate operation is performed on the target qubit, namely, flipping its state; while when the control qubit is $|0\rangle$, the state of the target qubit remains unchanged. The unitary matrix of the C-NOT gate is

$$\mathrm{CNOT}=\begin{bmatrix}1&0&0&0\\0&1&0&0\\0&0&0&1\\0&0&1&0\end{bmatrix}=\begin{pmatrix}I&0\\0&X\end{pmatrix}. \tag{2}$$

2.2. The Bell state and seven-particle entangled states

Four Bell states can be represented as

$$|\phi^{\pm}\rangle=\frac{1}{\sqrt{2}}(|00\rangle\pm|11\rangle), \tag{3}$$
$$|\psi^{\pm}\rangle=\frac{1}{\sqrt{2}}(|01\rangle\pm|10\rangle). \tag{4}$$

When performing the unitary operation $U_{i_1i_2}$ $(i_1i_2=0,1)$ on the second particle of the Bell state, that Bell state is transformed into another Bell state, where $U_{00}\equiv I=|0\rangle\langle0|+|1\rangle\langle1|$, $U_{01}\equiv X=|0\rangle\langle1|+|1\rangle\langle0|$, $U_{10}\equiv Z=|0\rangle\langle0|-|1\rangle\langle1|$, and $U_{11}\equiv iY=|0\rangle\langle1|-|1\rangle\langle0|$. Table 1 details the correspondence between the four Bell states and the applied unitary operation. In addition, the Z-basis and the X-basis are two sets of orthogonal bases that can be used as measurement bases. $|0\rangle$ and $|1\rangle$ can form the Z-basis, while $|+\rangle$ and $|-\rangle$ can form the X-basis, where $|\pm\rangle=\frac{1}{\sqrt{2}}(|0\rangle\pm|1\rangle)$.

Table 1. Relationship between unitary operations and Bell states

Bell state	$I\otimes U_{00}$	$I\otimes U_{01}$	$I\otimes U_{10}$	$I\otimes U_{11}$
$\|\phi^{\pm}\rangle$	$\|\phi^{\pm}\rangle$	$\|\psi^{\pm}\rangle$	$\|\phi^{\mp}\rangle$	$\|\psi^{\mp}\rangle$
$\|\psi^{\pm}\rangle$	$\|\psi^{\pm}\rangle$	$\|\phi^{\pm}\rangle$	$\|\psi^{\mp}\rangle$	$\|\phi^{\mp}\rangle$

The seven-particle maximally entangled state is given by Zha *et al.*[40] The seven-particle entangled state is shown below:

$$
\begin{aligned}
&|\varphi\rangle_{ABCDEFG}\\
&= \frac{1}{4\sqrt{2}}\big[(|0000000\rangle + |0000011\rangle + |0001101\rangle + |0001110\rangle\\
&\quad + |0010001\rangle - |0010010\rangle + |0011100\rangle - |0011111\rangle\\
&\quad + |0101000\rangle - |0100101\rangle - |0100110\rangle + |0101011\rangle\\
&\quad + |0110100\rangle - |0110111\rangle - |0111001\rangle + |0111010\rangle\\
&\quad + |1001001\rangle - |1000100\rangle - |1000111\rangle + |1001010\rangle\\
&\quad + |1010101\rangle - |1010110\rangle - |1011000\rangle + |1011011\rangle\\
&\quad + |1100001\rangle + |1100010\rangle + |1101100\rangle + |1101111\rangle\\
&\quad + |1110000\rangle - |1110011\rangle + |1111101\rangle\\
&\quad - |1111110\rangle)\big]_{ABCDEFG}\\
&= \frac{1}{4}\big\{|0\rangle_A \otimes \big[(|0000\rangle_{BCDE} + |1010\rangle_{BCDE})|\phi^+\rangle_{FG}\\
&\quad + (|1101\rangle_{BCDE} + |0111\rangle_{BCDE})|\phi^-\rangle_{FG}\\
&\quad + (|0011\rangle_{BCDE} + |1001\rangle_{BCDE})|\psi^+\rangle_{FG}\\
&\quad + (|0100\rangle_{BCDE} - |1110\rangle_{BCDE})|\psi^-\rangle_{FG}\big]\\
&\quad + |1\rangle_A \otimes \big[|1011\rangle_{BCDE}|\phi^+\rangle_{FG}\\
&\quad + (|0001\rangle_{BCDE} - |0110\rangle_{BCDE} + |1100\rangle_{BCDE})|\phi^-\rangle_{FG}\\
&\quad + (|0010\rangle_{BCDE} + |1001\rangle_{BCDE})|\psi^+\rangle_{FG}\\
&\quad + (|0101\rangle_{BCDE} + |1110\rangle_{BCDE})|\psi^-\rangle_{FG}\big]\big\}. \qquad (5)
\end{aligned}
$$

The corresponding quantum state circuit diagram[41] is shown in Fig. 1.

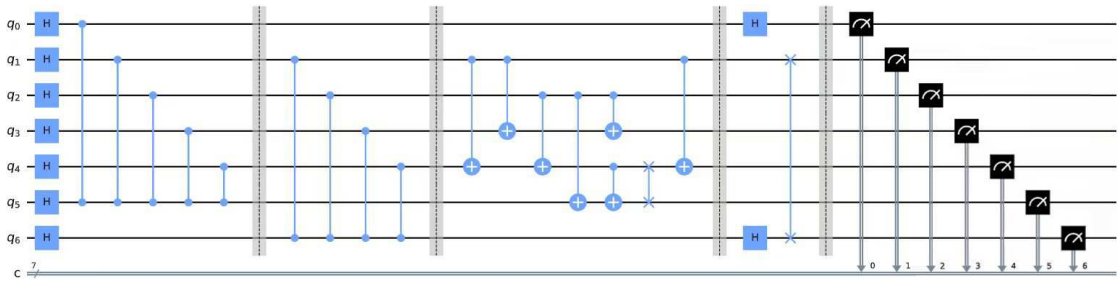


Fig. 1. Seven-particle quantum circuit.

2.3. Collective noise

Collective noise, including collective-dephasing noise and collective-rotation noise, is a significant challenge in quantum communication and quantum key distribution. These types of noise affect multiple qubits simultaneously, making them particularly problematic for quantum systems. In the following, this subsection discusses the mathematical representation of these noises, as well as the logical qubits proposed to mitigate the effects of the noise.

Collective-dephasing noise affects the phase of quantum states. For a single qubit, the state evolution under collective-dephasing noise is described by

$$|\varphi\rangle = \alpha|0\rangle + \beta|1\rangle \to |\varphi'\rangle = \alpha|0\rangle + \mathrm{e}^{\mathrm{i}\varphi_{(t)}}\beta|1\rangle, \qquad (6)$$

where $\varphi(t)$ represents the phase noise parameter that varies over time. The measurement results of single qubits in collective-dephasing noise are shown in Fig. 2, where the measurement results show 50% each of $|0\rangle$ and $|1\rangle$. The collective-dephasing noise can be represented by the following matrix:

$$U_{\mathrm{dp}} = \begin{pmatrix} 1 & 0 \\ 0 & \mathrm{e}^{\mathrm{i}\varphi_{(t)}} \end{pmatrix}. \qquad (7)$$

This matrix acts on the qubit state, introducing a phase shift in the $|1\rangle$ component. To reduce the impact of collective-dephasing noise, logical qubits are proposed. These logical qubits are encoded in a decoherence-free subspace (DFS), which is immune to collective noise. For example, $|0_{\mathrm{dp}}\rangle = |01\rangle$ and $|1_{\mathrm{dp}}\rangle = |10\rangle$.

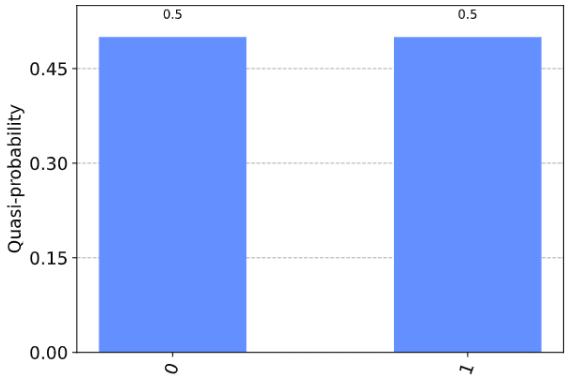


Fig. 2. Single quantum in collective-dephasing noise.

Collective-rotation noise affects the entire Bloch sphere, causing a rotation of the quantum state around a specific axis (e.g., the y-axis). For a single qubit, the state evolution under collective-rotation noise is given by

$$|\varphi\rangle = \alpha|0\rangle + \beta|1\rangle \to |\varphi'\rangle = \mathrm{e}^{\mathrm{i}\theta_{(t)}\sigma_y}\beta|\varphi\rangle. \qquad (8)$$

where $\theta_{(t)}$ represents the rotation noise parameter that varies over time, and σ_y is the Pauli-Y matrix. The measurement re-

sults of single qubits in collective-rotation noise are shown in Fig. 3. In the absence of noise, the measurement results of $|0\rangle$ and $|1\rangle$ should be 50% each. However, due to the presence of rotational noise, the distribution of the measurement results will deviate from this ideal situation. The collective-rotation noise can be represented by the following matrix:

$$U_{\mathrm{r}} = \begin{pmatrix} \cos\theta_{(t)} & -\sin\theta_{(t)} \\ \sin\theta_{(t)} & \cos\theta_{(t)} \end{pmatrix}. \tag{9}$$

When this matrix acts on a quantum state, it causes it to rotate by an angle $\theta_{(t)}$ about the y-axis on the Bloch sphere. To mitigate collective-rotation noise, logical qubits are again encoded in a DFS. For example, $|0_{\mathrm{r}}\rangle = |\phi^{+}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ and $|1_{\mathrm{r}}\rangle = |\psi^{-}\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$.

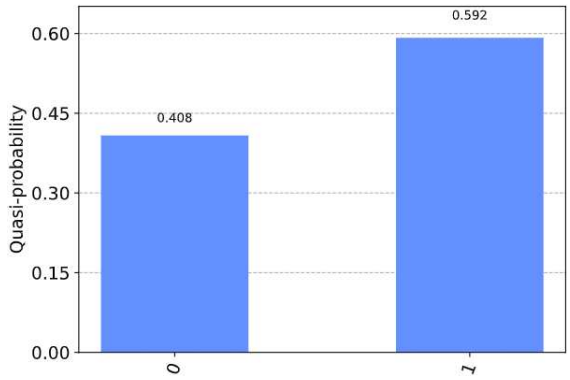


Fig. 3. Single quantum in collective-rotation noise.

3. The TPQKA protocol against collective noise

To facilitate a more intuitive understanding of the proposed protocol, Table 2 is provided to explain the specific meaning of each symbol within the protocol.

Table 2. Symbolic explanations of the protocol.

Symbol	Explanation
Alice, Bob, Charlie	Three participants in the protocol
$K_{\mathrm{A}}, K_{\mathrm{B}}, K_{\mathrm{C}}$	Raw private key
$M_A, M_{BC}, M_{DE}, M_{FG}$	Sequence measurement results
$\oplus$	XOR operation
$Q_{\mathrm{A}}, Q_{\mathrm{B}}, Q_{\mathrm{C}}$	The sequence measurement results undergo an XOR operation with the key.
$K^{*}_{\mathrm{A}}, K^{*}_{\mathrm{B}}, K^{*}_{\mathrm{C}}$	Results derived from $Q_{\mathrm{A}}, Q_{\mathrm{B}}, Q_{\mathrm{C}}$
K	Final shared key

3.1. The TPQKA protocol against collective-dephasing noise

The QKA protocol with collective-dephasing noise is shown in Fig. 4. Now, for collective-dephasing noise, this paper proposes a TPQKA protocol based on seven-particle entangled states. It includes the following steps.

Step 1 Alice randomly generates the $2n$-bit strings as the key $K_{\mathrm{A}} = K^{1}_{\mathrm{A}} \| K^{2}_{\mathrm{A}} \| \cdots \| K^{n}_{\mathrm{A}}$, Bob randomly generates the $2n$-bit strings as the key $K_{\mathrm{B}} = K^{1}_{\mathrm{B}} \| K^{2}_{\mathrm{B}} \| \cdots \| K^{n}_{\mathrm{B}}$, Charlie randomly generates the $2n$-bit strings as the key $K_{\mathrm{C}} = K^{1}_{\mathrm{C}} \| K^{2}_{\mathrm{C}} \| \cdots \| K^{n}_{\mathrm{C}}$, where K^{i}_{A}, K^{i}_{B}, $K^{i}_{\mathrm{C}} \in \{00, 01, 10, 11\}$, $i = 1, 2, \ldots, n$. Alice (Bob, Charlie) computes the hash value $H(K_{\mathrm{A}})(H(K_{\mathrm{B}}), H(K_{\mathrm{C}}))$ and announces the result to the other participants.

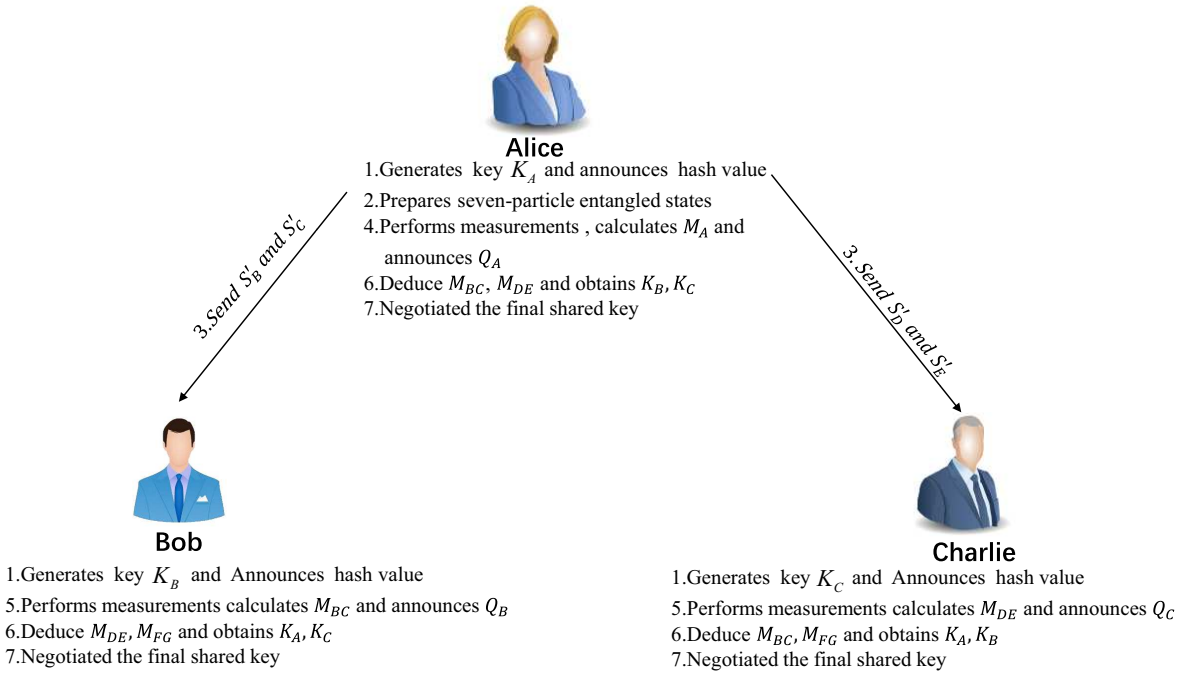


Fig. 4. Flow of the proposed TPQKA protocol.

Step 2 Alice prepares n logical seven-particle entangled states $|\psi_{\rm dp}\rangle_{ABCDEFG}$. The preparation of seven-particle entangled states in collective-dephasing is shown in Fig. 5. According to Eq. (5), the quantum state $|\psi_{\rm dp}\rangle_{ABCDEFG}$ in collective-dephasing noise is shown below:

$$
\begin{aligned}
&|\varphi_{\rm dp}\rangle_{ABCDEFG}\\
=&\frac{1}{4}\Big\{|0\rangle_A\otimes[(|01\rangle_{B_1B_2}|01\rangle_{C_1C_2}|01\rangle_{D_1D_2}|01\rangle_{E_1E_2}\\
&+|10\rangle_{B_1B_2}|01\rangle_{C_1C_2}|10\rangle_{D_1D_2}|01\rangle_{E_1E_2})|\phi^+\rangle_{FG}\\
&+(|10\rangle_{B_1B_2}|10\rangle_{C_1C_2}|01\rangle_{D_1D_2}|10\rangle_{E_1E_2}\\
&+|01\rangle_{B_1B_2}|10\rangle_{C_1C_2}|10\rangle_{D_1D_2}|10\rangle_{E_1E_2})|\phi^-\rangle_{FG}\\
&+(|01\rangle_{B_1B_2}|01\rangle_{C_1C_2}|01\rangle_{D_1D_2}|10\rangle_{E_1E_2}\\
&+|10\rangle_{B_1B_2}|01\rangle_{C_1C_2}|01\rangle_{D_1D_2}|10\rangle_{E_1E_2})|\psi^+\rangle_{FG}\\
&+(|01\rangle_{B_1B_2}|10\rangle_{C_1C_2}|01\rangle_{D_1D_2}|01\rangle_{E_1E_2}\\
&-|10\rangle_{B_1B_2}|10\rangle_{C_1C_2}|10\rangle_{D_1D_2}|01\rangle_{E_1E_2})|\psi^-\rangle_{FG}]\\
&+|1\rangle_A\otimes[|10\rangle_{B_1B_2}|01\rangle_{C_1C_2}|10\rangle_{D_1D_2}|10\rangle_{E_1E_2}|\phi^+\rangle_{FG}\\
&+(|01\rangle_{B_1B_2}|01\rangle_{C_1C_2}|01\rangle_{D_1D_2}|10\rangle_{E_1E_2}\\
&-|01\rangle_{B_1B_2}|10\rangle_{C_1C_2}|10\rangle_{D_1D_2}|01\rangle_{E_1E_2}\\
&+|10\rangle_{B_1B_2}|10\rangle_{C_1C_2}|01\rangle_{D_1D_2}|01\rangle_{E_1E_2})|\phi^-\rangle_{FG}\\
&+(|01\rangle_{B_1B_2}|01\rangle_{C_1C_2}|10\rangle_{D_1D_2}|01\rangle_{E_1E_2}\\
&+|10\rangle_{B_1B_2}|01\rangle_{C_1C_2}|01\rangle_{D_1D_2}|10\rangle_{E_1E_2})|\psi^+\rangle_{FG}\\
&+(|01\rangle_{B_1B_2}|10\rangle_{C_1C_2}|01\rangle_{D_1D_2}|10\rangle_{E_1E_2}\\
&+|10\rangle_{B_1B_2}|10\rangle_{C_1C_2}|10\rangle_{D_1D_2}|01\rangle_{E_1E_2})|\psi^-\rangle_{FG}]\Big\}. \qquad (10)
\end{aligned}
$$

Alice divides these logical states into seven sequences $S_A, S_B, S_C, S_D, S_E, S_F$, and S_G, these sequences consist of particle A, logical qubit B (where qubit B is composed of two qubits B_1B_2), logical qubit C (where qubit C is composed of two qubits C_1C_2), logical qubit D (where qubit D is composed of two qubits D_1D_2), logical qubit E (where qubit E is composed of two qubits E_1E_2), particle F, and particle G, respectively.

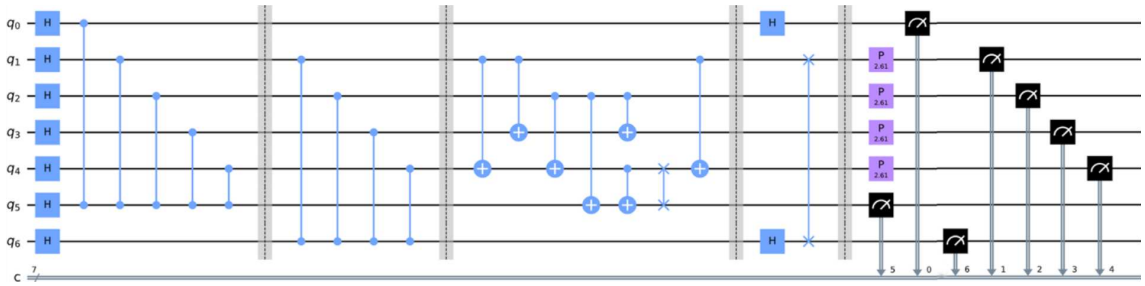


Fig. 5. Seven-particle entangled states in collective-dephasing noise, where P is the phase gate.

Step 3 Alice randomly selects enough decoy logical qubits from $\{|0_{\rm dp}\rangle, |1_{\rm dp}\rangle, |+_{\rm dp}\rangle, |-_{\rm dp}\rangle\}$ and inserts them into S_B, S_C, S_D and S_E to obtain S'_B, S'_C, S'_D and S'_E. Alice records the position and state of the inserted decoy particles, and then Alice sends sequences S'_B, S'_C to Bob and sequences S'_D, S'_E to Charlie via the quantum channel, while keeping the sequences S_A, S_F, and S_G. It should be noted that when Bob receives the sequence S'_B, S'_C, Alice sends the sequence S'_D, S'_E to Charlie. After Bob and Charlie confirm receipt of the sequence, Alice then announces the location of the decoy particles and the corresponding measurement bases.

Step 4 Using the published information, Bob and Charlie perform eavesdropping detection, and the eavesdropping detection process is shown in Fig. 6. After the eavesdropping detection, Bob and Charlie isolate and measure the decoy particles from sequences S'_B, S'_C and S'_D, S'_E, respectively, and then announce the measurement results to Alice. Alice calculates the error rate by comparing the received measurement results with the initial state of the decoy particle. If the error rate exceeds the predetermined threshold, Alice invalidates the communication. Otherwise, the protocol continues to the next step. Alice performs Z-basis measurements on sequence S_A and Bell measurements on sequences S_F and S_G, and notes the measurement results as $M_A = \{M_A^1, M_A^2, \ldots, M_A^n\}$ and $M_{FG} = \{M_{FG}^1, M_{FG}^2, \ldots, M_{FG}^n\}$, respectively. Alice calculates $Q_{\rm A} = M_{FG} \oplus K_{\rm A}$, and announces M_A and $Q_{\rm A}$ to Bob and Charlie, where $Q_{\rm A} = \{Q_{\rm A}^1, Q_{\rm A}^2, \ldots, Q_{\rm A}^n\}$.

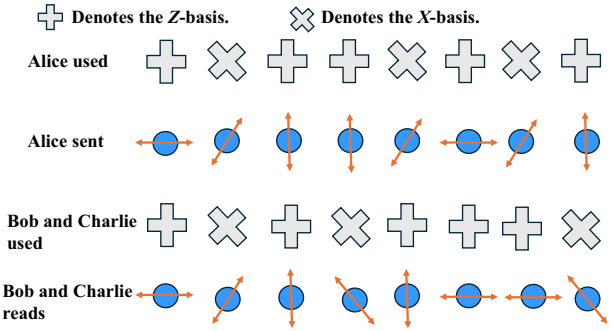


Fig. 6. Eavesdropping detection. Particles may be affected by noise during transmission, causing the state of the particle to change.

Step 5 Bob and Charlie restore the sequence to S_B, S_C and S_D, S_E after removing the decoy particles. Bob performs the ZZ-basis measurements on the sequences S_B, S_C. According to the measurement results, Bob performs the corresponding

unitary operation as shown in Table 3. Bob records the results of the unitary operation as $M_{BC} = \{M_{BC}^1, M_{BC}^2, \ldots, M_{BC}^n\}$. Bob computes $Q_{\rm B} = M_{BC} \oplus K_{\rm B}$, and announces $Q_{\rm B}$ and the unitary operations performed, where $Q_{\rm B} = \{Q_{\rm B}^1, Q_{\rm B}^2, \ldots, Q_{\rm B}^n\}$. Charlie performs the ZZ-basis measurement on the sequence S_D, S_E and performs the same unitary operation as Bob based on the measurement results. Charlie marks the results of the unitary operation as $M_{DE} = \{M_{DE}^1, M_{DE}^2, \ldots, M_{DE}^n\}$. Charlie counts $Q_{\rm C} = M_{DE} \oplus K_{\rm C}$, and announces $Q_{\rm C}$ and the unitary operations performed, where $Q_{\rm C} = \{Q_{\rm C}^1, Q_{\rm C}^2, \ldots, Q_{\rm C}^n\}$.

Table 3. Bob and Charlie perform the corresponding unitary operations.

Measurement results	Unitary operation	Record results
$\|0_{\rm dp}\rangle + \|0_{\rm dp}\rangle = \|01\rangle + \|01\rangle$ $\|0_{\rm dp}\rangle - \|0_{\rm dp}\rangle = \|01\rangle - \|01\rangle$	I	0101
$\|0_{\rm dp}\rangle + \|1_{\rm dp}\rangle = \|01\rangle + \|10\rangle$ $\|0_{\rm dp}\rangle - \|1_{\rm dp}\rangle = \|01\rangle - \|10\rangle$	X	0110
$\|1_{\rm dp}\rangle - \|0_{\rm dp}\rangle = \|10\rangle - \|01\rangle$ $-\|1_{\rm dp}\rangle - \|0_{\rm dp}\rangle = -\|10\rangle - \|01\rangle$	iY	1001
$\|1_{\rm dp}\rangle + \|1_{\rm dp}\rangle = \|10\rangle + \|10\rangle$ $\|1_{\rm dp}\rangle - \|1_{\rm dp}\rangle = \|10\rangle - \|10\rangle$	Z	1010

Step 6 Based on the information released by the three parties, Alice can deduce M_{BC} and M_{DE}, Bob can deduce M_{DE} and M_{FG}, and Charlie can deduce M_{BC} and M_{FG}. Based on M_{BC} and M_{DE}, Alice can derive $K_{\rm B}^*$ and $K_{\rm C}^*$ from $Q_{\rm B}$ and $Q_{\rm C}$, and calculate the hash values $H(K_{\rm B}^*)$ and $H(K_{\rm C}^*)$. According to M_{DE} and M_{FG}, Bob can derive $K_{\rm A}^*$ and $K_{\rm C}^*$ from $Q_{\rm A}$ and $Q_{\rm C}$, and compute the hash values $H(K_{\rm A}^*)$ and $H(K_{\rm C}^*)$. Based on M_{BC} and M_{FG}, Charlie can derive $K_{\rm A}^*$ and $K_{\rm B}^*$ from $Q_{\rm A}$ and $Q_{\rm B}$, and compute the hash values $H(K_{\rm A}^*)$ and $H(K_{\rm B}^*)$. If $H(K_{\rm A}^*) = H(K_{\rm A})$, $H(K_{\rm B}^*) = H(K_{\rm B})$, and $H(K_{\rm C}^*) = H(K_{\rm C})$, the protocol will perform the next operation; otherwise, the protocol starts from the beginning.

Step 7 The three parties have obtained each other's keys, and Alice, Bob, and Charlie negotiate the final shared key $K = K_{\rm A} \| K_{\rm B} \| K_{\rm C}$.

Step 8 Since the noise channel may cause differences in the key, this paper will introduce the key post-processing process in the security analysis, so that the three parties can negotiate the same final shared key.

3.2. The TPQKA protocol against collective-rotation noise

Like the first TPQKA protocol, this paper proposes a novel TPQKA protocol based on seven-particle entangled states against collective-rotation noise. It consists of the following steps.

Step 1 Alice randomly generates the $2n$-bit string as the key $K_{\rm A} = K_{\rm A}^1 \| K_{\rm A}^2 \| \cdots \| K_{\rm A}^n$, Bob randomly generates the $2n$-bit string as the key $K_{\rm B} = K_{\rm B}^1 \| K_{\rm B}^2 \| \cdots \| K_{\rm B}^n$, Charlie randomly generates the $2n$-bit string as the key $K_{\rm C} = K_{\rm C}^1 \| K_{\rm C}^2 \| \cdots \| K_{\rm C}^n$, where $K_{\rm A}^i, K_{\rm B}^i, K_{\rm C}^i \in \{00, 01, 10, 11\}$, $i = 1, 2, \ldots, n$. Alice (Bob, Charlie) computes the hash value $H(K_{\rm A})(H(K_{\rm B}), H(K_{\rm C}))$ and sends the result to the other participants.

Step 2 Alice prepares n logical seven-particle entangled states $|\varphi_{\rm r}\rangle_{ABCDEFG}$. The preparation of seven-particle entangled states in collective-rotation noise is shown in Fig. 7. According to Eq. (5), the quantum state $|\varphi_{\rm r}\rangle_{ABCDEFG}$ in collective-rotation noise is shown below:

$$
\begin{aligned}
&|\varphi_{\rm r}\rangle_{ABCDEFG} \\
&= \frac{1}{4}\Big\{ |0\rangle_A \otimes [(|\phi^-\rangle_{B_1B_2}|\phi^-\rangle_{C_1C_2}|\phi^-\rangle_{D_1D_2}|\phi^-\rangle_{E_1E_2} \\
&+|\psi^-\rangle_{B_1B_2}|\phi^-\rangle_{C_1C_2}|\psi^-\rangle_{D_1D_2}|\phi^-\rangle_{E_1E_2})|\phi^+\rangle_{FG} \\
&+(|\psi^-\rangle_{B_1B_2}|\psi^-\rangle_{C_1C_2}|\phi^-\rangle_{D_1D_2}|\psi^-\rangle_{E_1E_2} \\
&+|\phi^-\rangle_{B_1B_2}|\psi^-\rangle_{C_1C_2}|\psi^-\rangle_{D_1D_2}|\psi^-\rangle_{E_1E_2})|\phi^-\rangle_{FG} \\
&+(|\phi^-\rangle_{B_1B_2}|\phi^-\rangle_{C_1C_2}|\psi^-\rangle_{D_1D_2}|\psi^-\rangle_{E_1E_2} \\
&+|\psi^-\rangle_{B_1B_2}|\phi^-\rangle_{C_1C_2}|\phi^-\rangle_{D_1D_2}|\psi^-\rangle_{E_1E_2})|\psi^+\rangle_{FG} \\
&+(|\phi^-\rangle_{B_1B_2}|\psi^-\rangle_{C_1C_2}|\phi^-\rangle_{D_1D_2}|\phi^-\rangle_{E_1E_2} \\
&-|\psi^-\rangle_{B_1B_2}|\psi^-\rangle_{C_1C_2}|\psi^-\rangle_{D_1D_2}|\phi^-\rangle_{E_1E_2})|\psi^-\rangle_{FG}] \\
&+|1\rangle_A \otimes [|\psi^-\rangle_{B_1B_2}|\phi^-\rangle_{C_1C_2}|\psi^-\rangle_{D_1D_2}|\psi^-\rangle_{E_1E_2}|\phi^+\rangle_{FG} \\
&+(|\phi^-\rangle_{B_1B_2}|\phi^-\rangle_{C_1C_2}|\phi^-\rangle_{D_1D_2}|\psi^-\rangle_{E_1E_2} \\
&-|\phi^-\rangle_{B_1B_2}|\psi^-\rangle_{C_1C_2}|\psi^-\rangle_{D_1D_2}|\phi^-\rangle_{E_1E_2} \\
&+|\psi^-\rangle_{B_1B_2}|\psi^-\rangle_{C_1C_2}|\phi^-\rangle_{D_1D_2}|\phi^-\rangle_{E_1E_2})|\phi^-\rangle_{FG} \\
&+(|\phi^-\rangle_{B_1B_2}|\phi^-\rangle_{C_1C_2}|\psi^-\rangle_{D_1D_2}|\phi^-\rangle_{E_1E_2} \\
&+|\psi^-\rangle_{B_1B_2}|\phi^-\rangle_{C_1C_2}|\phi^-\rangle_{D_1D_2}|\psi^-\rangle_{E_1E_2})|\psi^+\rangle_{FG} \\
&+(|\phi^-\rangle_{B_1B_2}|\psi^-\rangle_{C_1C_2}|\phi^-\rangle_{D_1D_2}|\psi^-\rangle_{E_1E_2} \\
&+|\psi^-\rangle_{B_1B_2}|\psi^-\rangle_{C_1C_2}|\psi^-\rangle_{D_1D_2}|\phi^-\rangle_{E_1E_2})|\psi^-\rangle_{FG}]\Big\}. \quad (11)
\end{aligned}
$$

Alice divides these logical states into seven sequences $S_A, S_B, S_C, S_D, S_E, S_F$, and S_G. These sequences consist of particle A, logical qubit B (where qubit B consists of two qubits B_1B_2), logical qubit C (where qubit C consists of two qubits C_1C_2), logical qubit D (where qubit D consists of two qubits D_1D_2), logical qubit E (where qubit E consists of two qubits E_1E_2), particle F, and particle G, respectively.

Step 3 Alice randomly chooses enough decoy logical qubits from the set $\{|0_{\rm r}\rangle, |1_{\rm r}\rangle, |+_{\rm r}\rangle, |-_{\rm r}\rangle\}$ and inserts them into sequences S_B, S_C, S_D, and S_E to obtain S_B', S_C', S_D', and S_E'. Afterward, Alice sends sequences S_B', S_C' to Bob and sequences S_D', S_E' to Charlie through the quantum channel, preserving the sequence S_A, S_F, and S_G. Noted that when Bob receives sequence S_B', S_C', Alice sends sequence S_D', S_E' to Charlie. After Bob and Charlie confirm receipt of the sent sequence, Alice announces the position of the decoy particles and the corresponding measurement bases.

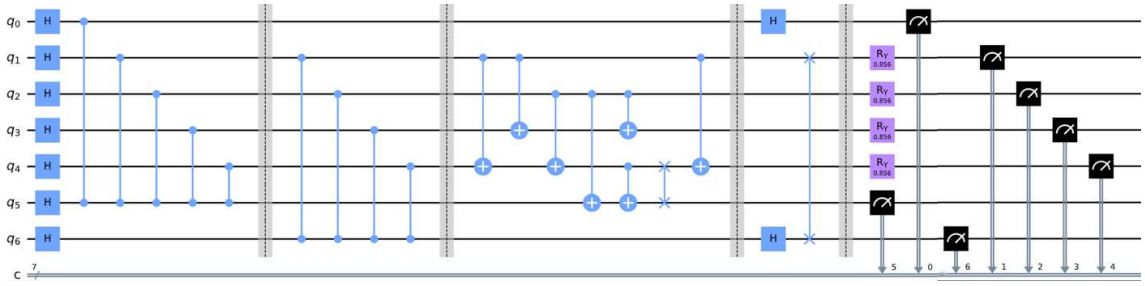


Fig. 7. Seven-particle entangled states in collective-rotation noise, where R is the rotation Y gate.

Step 4 Bob and Charlie use the released information for eavesdropping detection. After the eavesdropping detection, Bob and Charlie isolate and measure the decoy particles from sequences S'_B, S'_C and S'_D, S'_E, respectively, and then release the measurement results to Alice. Alice calculates the error rate by comparing the received measurement results with the initial state of the decoy particle. If the error rate exceeds the predetermined threshold, Alice invalidates the communication. Otherwise, the protocol continues to the next step. Alice performs the Z-basis measurements on sequence S_A and the ZZ-basis measurements on sequences S_F and S_G, notating the measurement results as $M_A = \{M_A^1, M_A^2, \ldots, M_A^n\}$ and $M_{FG} = \{M_{FG}^1, M_{FG}^2, \ldots, M_{FG}^n\}$, respectively. Alice calculates $Q_{\mathrm{A}} = M_{FG} \oplus K_{\mathrm{A}}$, and announces M_A and Q_{A} to Bob and Charlie, where $Q_{\mathrm{A}} = \{Q_{\mathrm{A}}^1, Q_{\mathrm{A}}^2, \ldots, Q_{\mathrm{A}}^n\}$.

Step 5 Bob and Charlie restore the sequence to S_B, S_C and S_D, S_E after removing the decoy particles. Bob performs the Bell measurements on the sequences S_B, S_C. According to the measurement results, Bob performs the corresponding unitary operation as shown in Table 4. Bob records the results of the unitary operation as $M_{BC} = \{M_{BC}^1, M_{BC}^2, \ldots, M_{BC}^n\}$. Bob computes $Q_{\mathrm{B}} = M_{BC} \oplus K_{\mathrm{B}}$, and announces Q_{B} and the unitary operations performed, where $Q_{\mathrm{B}} = \{Q_{\mathrm{B}}^1, Q_{\mathrm{B}}^2, \ldots, Q_{\mathrm{B}}^n\}$. Charlie performs the Bell measurements on the sequences S_D, S_E, and marks the measurement results as $M_{DE} = \{M_{DE}^1, M_{DE}^2, \ldots, M_{DE}^n\}$. Charlie counts $Q_{\mathrm{C}} = M_{DE} \oplus K_{\mathrm{C}}$, and announces Q_{C} and the unitary operations performed, where $Q_{\mathrm{C}} = \{Q_{\mathrm{C}}^1, Q_{\mathrm{C}}^2, \ldots, Q_{\mathrm{C}}^n\}$.

Table 4. Bob and Charlie perform the corresponding unitary operations.

Measurement results	Unitary operation	Record results
$\|0_{\mathrm{r}}\rangle + \|0_{\mathrm{r}}\rangle = \|\phi^+\rangle + \|\phi^+\rangle$ $\|0_{\mathrm{r}}\rangle - \|0_{\mathrm{r}}\rangle = \|\phi^+\rangle - \|\phi^+\rangle$	I	0101
$\|0_{\mathrm{r}}\rangle + \|1_{\mathrm{r}}\rangle = \|\phi^+\rangle + \|\psi^-\rangle$ $\|0_{\mathrm{r}}\rangle - \|1_{\mathrm{r}}\rangle = \|\phi^+\rangle - \|\psi^-\rangle$	X	0110
$\|1_{\mathrm{r}}\rangle - \|0_{\mathrm{r}}\rangle = \|\psi^-\rangle - \|\phi^+\rangle$ $-\|1_{\mathrm{r}}\rangle - \|0_{\mathrm{r}}\rangle = -\|\psi^-\rangle - \|\phi^+\rangle$	$\mathrm{i}Y$	1001
$\|1_{\mathrm{r}}\rangle + \|1_{\mathrm{r}}\rangle = \|\psi^-\rangle + \|\psi^-\rangle$ $\|1_{\mathrm{r}}\rangle - \|1_{\mathrm{r}}\rangle = \|\psi^-\rangle - \|\psi^-\rangle$	Z	1010

Step 6 Based on the information released by the three parties, Alice can deduce M_{BC} and M_{DE}, Bob can deduce M_{DE} and M_{FG}, and Charlie can deduce M_{BC} and M_{FG}. Based on M_{BC} and M_{DE}, Alice can derive K_{B}^* and K_{C}^* from Q_{B} and Q_{C}, and calculate the hash values $H(K_{\mathrm{B}}^*)$ and $H(K_{\mathrm{C}}^*)$. According to M_{DE} and M_{FG}, Bob can derive K_{A}^* and K_{C}^* from Q_{A} and Q_{C}, and compute the hash values $H(K_{\mathrm{A}}^*)$ and $H(K_{\mathrm{C}}^*)$. Based on M_{BC} and M_{FG}, Charlie can derive K_{A}^* and K_{B}^* from Q_{A} and Q_{B}, and compute the hash values $H(K_{\mathrm{A}}^*)$ and $H(K_{\mathrm{B}}^*)$. If $H(K_{\mathrm{A}}^*) = H(K_{\mathrm{A}})$, $H(K_{\mathrm{B}}^*) = H(K_{\mathrm{B}})$, and $H(K_{\mathrm{C}}^*) = H(K_{\mathrm{C}})$, the protocol performs the next step, otherwise, the protocol starts over.

Step 7 The three parties have obtained each other's keys, and Alice, Bob, and Charlie negotiate the final shared key $K = K_{\mathrm{A}} \| K_{\mathrm{B}} \| K_{\mathrm{C}}$.

Step 8 Since the noise channel may cause differences in the key, this paper will introduce the key post-processing process in the security analysis, so that the three parties can negotiate the same final shared key.

4. Security analyses

Between the two TPQKA protocols mentioned above, the two protocols are robust in collective noisy channels. In this section, the proposed TPQKA protocol will be shown to be secure against the common attacks in the communication process. The two TPQKA protocols face two main types of attacks: inside and outside attacks, where inside attacks refer to participant attacks, and outside attacks are classified as Trojan horse attacks, Intercept-resend attacks, entangle-measure attacks, and man-in-the-middle attacks. So, this paper will be centered on these two attacks. Finally, the keys of the two protocols in this paper are post-processed.

4.1. Inside attacks

Participant attacks are a specific type of cybersecurity threat from participants within a protocol or system. These participants, because of their roles and privileges in the execution of the protocol or the operation of the system, can launch attacks against other participants or the system as a whole. A collusion attack is when two or more dishonest participants in a protocol conspire and attempt to steal the final key ahead of time, and then decide on the final shared key alone and without

revealing their attack.[42]

Suppose Alice and Bob are dishonest participants in the protocol who want to steal Charlie's key information using a collusion attack. In Step 3 of the protocol, Alice sends the sequences S'_D and S'_E to Charlie, while simultaneously sending the sequences S_A, S'_B, S'_C, S_F and S_G to the collusion attacker Bob. After Charlie and Bob remove the decoy logical qubits from the received sequences, Charlie uses the measurement bases to measure the sequences S_D and S_E. Then Charlie performs the unitary operation based on the measurement results and publishes Q_C. At this point, Bob can reduce all sequences to seven-particle entangled states based on the published information. Under normal circumstances, Bob can use the seven-particle basis to measure the seven-particle entangled state and obtain Charlie's key information. However, because of the delayed measurement technique,[43] not only is Bob unable to obtain Charlie's key information in advance, but the shared key they ultimately negotiate may not be consistent due to noise interference. Therefore, Alice and Bob cannot steal Charlie's private key information. The two protocols are resistant to participant attacks.

4.2. Outside attacks

Suppose Eve is an attacker outside the participants attempting to steal or compromise the key information during the protocol. These outside attacks exploit certain properties of quantum mechanics or vulnerabilities in protocol implementations. Both protocols may also be subject to Trojan horse attacks, intercept-resend attacks, entangle-measure attacks, and man-in-the-middle attacks.

Trojan horse attacks In both anti-noise protocols, both protocols are immune to Trojan horse attacks because the same particles are transmitted only once. However, if the same particle is transmitted multiple times, to avoid Trojan horse attacks, three parties can use a wavelength filter and photon separator (PNS:50/50).[44] They can use the photon separator to split each signal into two parts. An attack can be detected if an abnormal multi-photon rate is observed. Therefore, neither protocol is threatened by Trojan horse attacks.

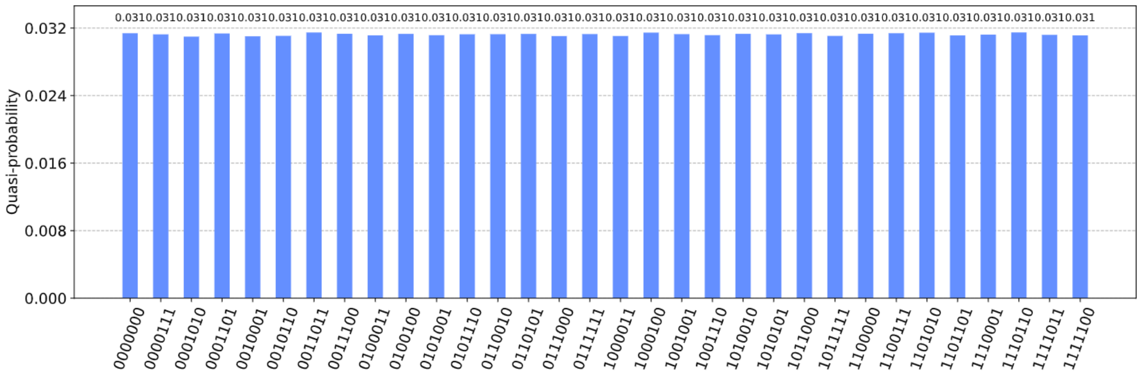


Fig. 8. Collective dephasing noise probability.

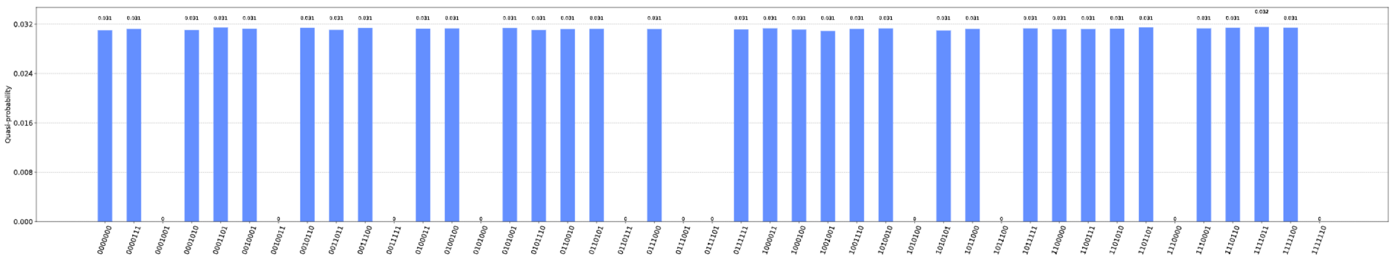


Fig. 9. Collective-rotation noise probability.

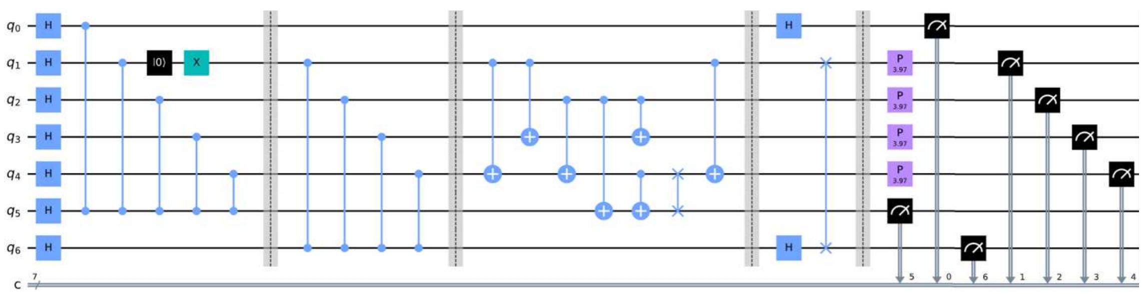


Fig. 10. Quantum circuits after an eavesdropping attack.

Intercept–resend attacks When Eve performs an intercept–resend attack[45] on a triad, she must first intercept sequences S'_B, S'_C and S'_D, S'_E in Step 3. Eve measures the intercepted sequence, forges two sequences based on the measurement results, and sends the forged sequences to Bob and Charlie, respectively. However, Eve does not know the exact location of the decoy logic qubit and the corresponding measurement bases until the protocol performs the eavesdropping detection in Step 4. Therefore, the probability of detecting intercept–resend attacks when performing the wiretap check in Step 4 is $1-\left(\frac{1}{4}\right)^n$, where n represents the number of decoy logical qubits used. This means that when n reaches a sufficiently large value, participants are able to easily recognize the presence of an eavesdropper. Due to the special nature of quantum mechanics and the collapse caused by measurements, Eve's behavior would normally be detected.

When the seven-particle entangled state is in collective-dephasing noise, its probability can be obtained according to Fig. 5, as shown in Fig. 8. The figure shows that the probability of each measurement result is about 3.1%. When the seven-particle entangled state is in collective rotation noise, its probability is shown in Fig. 9. (Since the angle of the rotational noise is random, it can lead to the generation of spurious states, tested to produce up to 2^7 measurement results). For ease of description, in this paper, collective-dephasing noise is used as an example to simulate the intercept-resend attacks. When the simulation measurement does not exceed 32 results, it shows that there is eavesdropping behavior in the communication process. In the intercept-resend attacks, the eavesdropper Eve intercepts a quantum state of the sender and measures it, and then sends the forged quantum state to the receiver. Due to the quantum no-cloning theorem and the measurement collapse theory, the quantum state changes after the measurement. The subsequent quantum circuit is shown in Fig. 10, and the corresponding probability distribution is shown in Fig. 11. It can be seen from the probability distribution diagram that only 16 results appear after the measurement, and the probability of each measurement result is about 6.3%. In summary, this paper can judge whether there is eavesdropping behavior in the intercept-resend attacks according to the simulation output results.

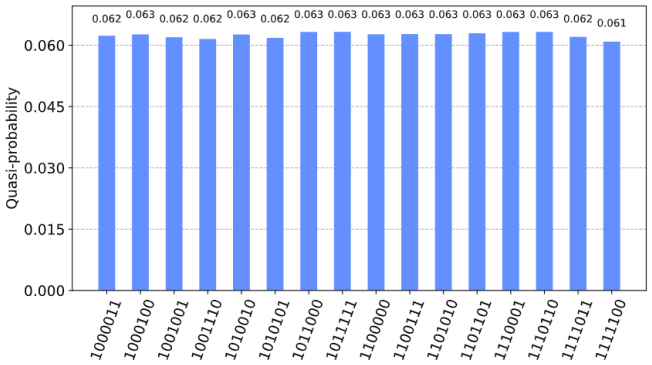


Fig. 11. Simulation results with eavesdropping behavior.

Entangle-measure attacks If Eve engages in an entangle-measure attack,[46] Eve intercepts the logical qubits sent by Alice and entangles them with her own auxiliary qubits $|E\rangle$ through the CNOT operation, and finally Eve sends them to the receiver based on the measurement results. This attack takes the TPQKA protocol against collective-dephasing noise as an example. Assuming that $|e_0e_0\rangle, |e_0e_1\rangle, |e_1e_0\rangle, |e_1e_1\rangle, |e'_0e'_0\rangle, |e'_0e'_1\rangle, |e'_1e'_0\rangle, |e'_1e'_1\rangle$ are the probe state, the simulation process of the eavesdropper's entangle-measure attacks is shown in Fig. 12, and the evolution of the quantum system is as follows:

$$U(|0_{\rm dp}\rangle|E\rangle) = a_{00}|00\rangle|e_0e_0\rangle + a_{01}|01\rangle|e_0e_1\rangle + a_{10}|10\rangle|e_1e_0\rangle + a_{11}|11\rangle|e_1e_1\rangle, \tag{12}$$

$$U(|1_{\rm dp}\rangle|E\rangle) = b_{00}|00\rangle|e'_0e'_0\rangle + b_{01}|01\rangle|e'_0e'_1\rangle + b_{10}|10\rangle|e'_1e'_0\rangle + b_{11}|11\rangle|e'_1e'_1\rangle, \tag{13}$$

$$\begin{aligned} U(|+_{\rm dp}\rangle|E\rangle) &= \frac{1}{\sqrt{2}}[U(|0_{\rm dp}\rangle|E\rangle) + U(|1_{\rm dp}\rangle|E\rangle)] \\ = \ & \frac{1}{2}[|\phi^+\rangle(a_{00}|e_0e_0\rangle + a_{11}|e_1e_1\rangle + b_{00}|e'_0e'_0\rangle + b_{11}|e'_1e'_1\rangle) + |\phi^-\rangle(a_{00}|e_0e_0\rangle - a_{11}|e_1e_1\rangle - b_{00}|e'_0e'_0\rangle + b_{11}|e'_1e'_1\rangle) \\ & + |\psi^+\rangle(a_{01}|e_0e_1\rangle + a_{10}|e_1e_0 - b_{01}|e'_0e'_1\rangle - b_{10}|e'_1e'_0\rangle) + |\psi^-\rangle(a_{01}|e_0e_1\rangle - a_{10}|e_1e_0\rangle - b_{01}|e'_0e'_1\rangle + b_{10}|e'_1e'_0\rangle), \end{aligned} \tag{14}$$

$$\begin{aligned} U(|-_{\rm dp}\rangle|E\rangle) &= \frac{1}{\sqrt{2}}[U(|0_{\rm dp}\rangle|E\rangle) - U(|1_{\rm dp}\rangle|E\rangle)] \\ = \ & \frac{1}{2}[|\phi^+\rangle(a_{00}|e_0e_0\rangle + a_{11}|e_1e_1\rangle - b_{00}|e'_0e'_0\rangle - b_{11}|e'_1e'_1\rangle) + |\phi^-\rangle(a_{00}|e_0e_0\rangle - a_{11}|e_1e_1\rangle - b_{00}|e'_0e'_0\rangle + b_{11}|e'_1e'_1\rangle) \\ & + |\psi^+\rangle(a_{01}|e_0e_1\rangle + a_{10}|e_1e_0\rangle - b_{01}|e'_0e'_1\rangle - b_{10}|e'_1e'_0\rangle) + |\psi^-\rangle(a_{01}|e_0e_1\rangle - a_{10}|e_1e_0\rangle - b_{01}|e'_0e'_1\rangle + b_{10}|e'_1e'_0\rangle), \end{aligned} \tag{15}$$

where $|a_{00}|^2+|a_{01}|^2+|a_{10}|^2+|a_{11}|^2=1$ and $|b_{00}|^2+|b_{01}|^2+|b_{10}|^2+|b_{11}|^2=1$. If Eve does not want to be detected by eavesdropping checks, then U must meet these conditions: $a_{01}=b_{01}=1, a_{00}=a_{10}=a_{11}=0, b_{00}=b_{10}=b_{11}=0$ and $a_{01}|e_0e_1\rangle = b_{10}|e'_1e'_0\rangle$. Then the measurement results of Fig. 12 are shown in Fig. 13, and the Eqs. (12)–(15) become

the following equation:

$$U(|0_{\rm dp}\rangle|E\rangle) = |01\rangle|e_0e_1\rangle, \tag{16}$$

$$U(|1_{\rm dp}\rangle|E\rangle) = |01\rangle|e_0'e_1'\rangle, \tag{17}$$

$$\begin{aligned} U(|+_{\rm dp}\rangle|E\rangle) &= \frac{1}{\sqrt{2}}[U(|0\rangle|E\rangle)+U(|1\rangle|E\rangle)] \\ &= \frac{1}{\sqrt{2}}(|01\rangle|e_0e_1\rangle - |01\rangle|e_0'e_1'\rangle), \end{aligned} \tag{18}$$

$$\begin{aligned} U(|-_{\rm dp}\rangle|E\rangle) &= \frac{1}{\sqrt{2}}[U(|0\rangle|E\rangle)-U(|1\rangle|E\rangle)] \\ &= \frac{1}{\sqrt{2}}(|01\rangle|e_0e_1\rangle - |01\rangle|e_0'e_1'\rangle). \end{aligned} \tag{19}$$

Based on the entangle-measure attack probability figure and the newly generated equation, she cannot distinguish between auxiliary photons $a_{01}|e_0e_1\rangle$ and $b_{10}|e_1'e_0'$, so she cannot obtain information about $K_{\rm A}, K_{\rm B}$ and $K_{\rm C}$ by observing her auxiliary particles. Therefore, both protocols can resist Eve's entangle-measure attack.

Man-in-the-middle attack[47] is an important security issue in the field of quantum secure communication, which refers to an eavesdropper Eve in the middle of the three parties' communication line pretending to be a legitimate user of the communication as a way to extract the keys of the three parties of the communication. Suppose Eve first intercepts the sequences S_B', S_C' sent by Alice to Bob and the sequences S_D', S_E' from Charlie and subsequently performs the first eavesdropping detection. Since Eve does not know the corresponding measurement bases of the decoy logical qubit and its position in the sequence, the measurement results obtained by Eve will be different from those announced by Alice. Eve's eavesdropping methods cannot be invisible in quantum communication and her eavesdropping will be detected in the eavesdropping detection. Thus, both protocols are resistant to Eve's man-in-the-middle attacks.

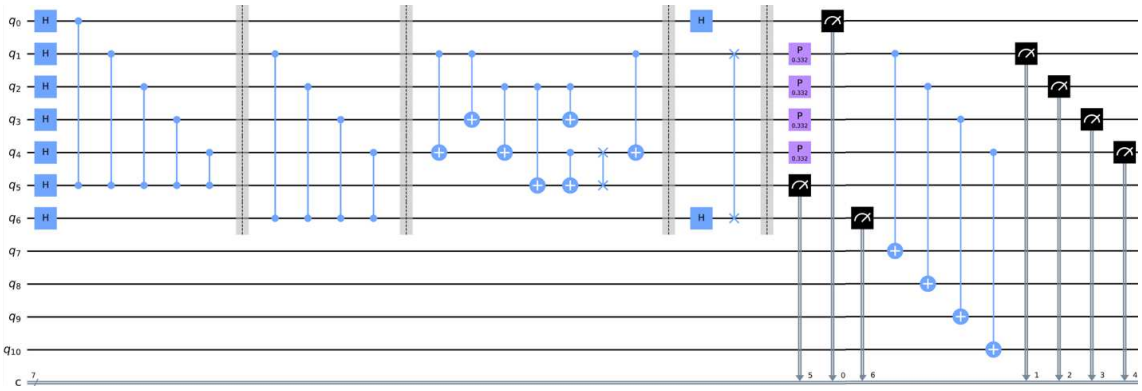


Fig. 12. Simulation of entangle-measure attacks.

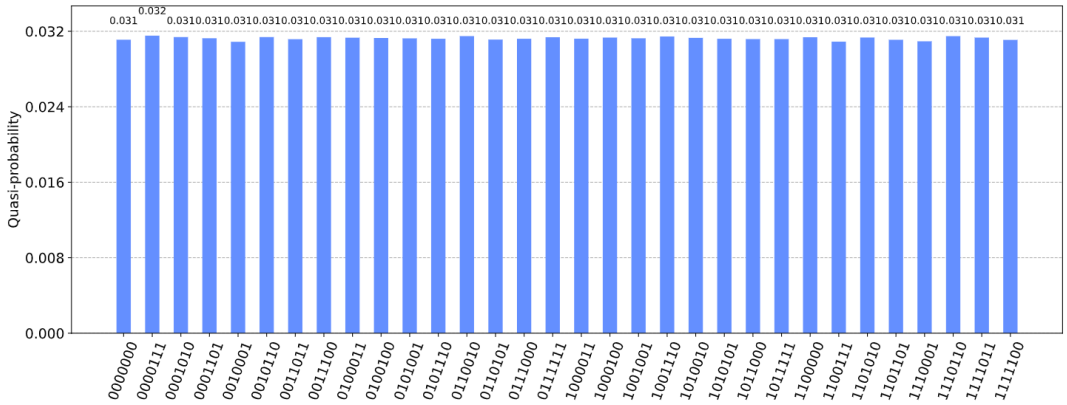


Fig. 13. Probability distribution of entangle-measure attacks.

4.3. Shared key post-processing

Since the noise channel may cause differences in the key, this article will perform information reconciliation and privacy amplification in this section to enable the three parties to negotiate the same final shared key. Information reconciliation is an important step in the process of quantum key distribution.[48,49] Its purpose is to change two different bit strings into the same bit string by exchanging information through a publicly verifiable channel. In the noise channel, the transmitted sequence may cause bit errors. After Alice calculates the error rate, the corresponding positions of the sequences after Alice, Bob, and Charlie's measurements may be inconsistent. The three parties can exchange redundant information in the open channel, and use error correction tech-

nology to correct bit errors. The dichotomy[50] method is an efficient protocol for information reconciliation. To make the error bits evenly distributed, Bob and Charlie rearrange the positions in the sequence. Bob and Charlie divide the sequence into groups of length k ($k < n$), such that the number of errors in each group is not more than 1. Bob and Charlie respectively detect the parity of each group of data, which is represented by the parity bits 0 and 1, and compare the parity bits through the open channel. If the corresponding arrays are different from each other, it means that the group must have errors. If the number of errors is odd, divide the array into two, and then perform parity detection and comparison until it reaches the last data, which is the wrong data. To prevent eavesdropper Eve from eavesdropping on information, the last digit of the array is discarded every time the check bits of the array are publicly disclosed, and the wrong data found is also discarded. After the last round of error correction, although the parity of each array is the same, there may still be an even number of errors. It is necessary to repeat the above three steps for a new round of error correction. The length of the new round of arrays should generally be longer than that of the previous round until Bob and Charlie get the same sequence.

In the process of quantum key distribution, the keys may be inconsistent due to noise and other reasons, and the keys may be eavesdropped on in the noise channel, resulting in information leakage. Although the information reconciliation process has achieved the goal of 100% key consistency between the three parties, there is information leakage in this process. Due to information leakage, Eve can derive the final key through a huge amount of calculations, so this article needs to generate an absolutely secure shared key through privacy amplification,[51,52] as shown in Fig. 14.

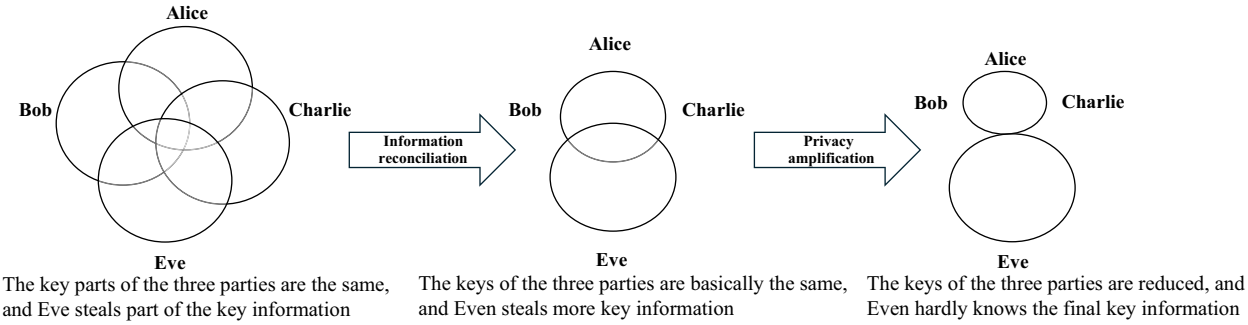


Fig. 14. Key post-processing.

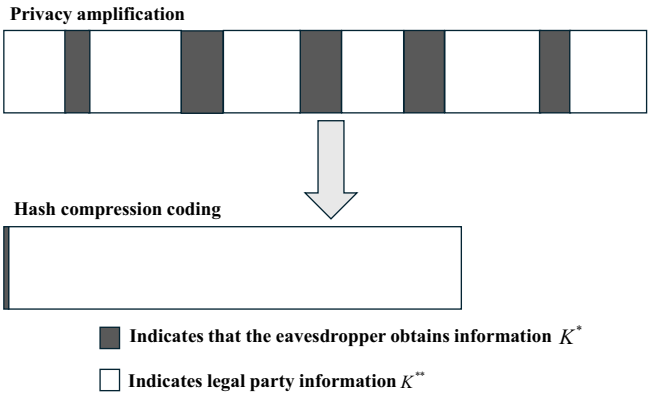


Fig. 15. Hash compression coding for privacy amplification.

The essence of privacy amplification is to sacrifice the length of the key in exchange for security, and compress the information that Eve has stolen as much as possible so that the uncertainty of the stolen key becomes larger. The goal of this is to XOR the data bits determined by Eve with the uncertain data bits, so that they become data that Eve does not know, effectively eliminating it. In privacy amplification applications, the choice of compression function is usually a hash function. As shown in Fig. 15, the key information obtained by the eavesdropper Eve is K^*, and the key information of the legitimate party is K^{**}. Three parties compress the information by an XOR operation to transform K^* into K, that is $K = K^* \oplus K^{**}$. The eavesdropper Eve cannot obtain K.

5. Efficiency analysis

The qubit efficiency of the TPQKA protocol defined in Cabello[53] is expressed as $\eta = \frac{c}{q+b}$, where c is the length of the final negotiation key, q is the number of qubits used, and b is the number of classical bits exchanged for decoding. In the two TPQKA protocols, the final negotiated key length is $6n$, namely, $c = 6n$. Alice prepares n seven-particle entangled states in Step 2, where particles B, C, D, and E are logic qubits (containing two particles); Alice uses $4n$ decoy logic qubits (containing two particles) in Step 2. Thus $q = 7n + 4n + 8n$.

Table 5. Comparison of our protocols with other quantum key protocols.

QKA protocol	Quantum resource	Number of participants	Efficiency (%)
Hwang's[33]	Single photons	Three	7.14
He's[34]	Four-qubit cluster states	Three	7.41
Tang's[35]	GHZ state	Three	11.11
Younes's[36]	Four-particle cluster state	Three	12.5
Xu's[37]	GHZ state	Three	16.67
Ours	Seven-particle entangled states	Three	19.35

In Step 6, the three parties need to derive the key values for the other two participants, so $b = 12n$. Thus, the qubit efficiency of the protocol is $\eta = \frac{6n}{7n+4n+8n+12n} \approx 19.35\%$. The comparison of our protocol with other QKA protocols is shown in Table 5, which shows that our protocol has higher qubit efficiency.

6. Discussion

To evaluate the feasibility of the proposed protocol under realistic transmission conditions, we analyze the effect of fiber losses over long-distance optical fiber channels. In optical fiber communication systems, the total transmission efficiency[54] can be

$$T = T_1 \cdot 10^{-\alpha L/10}, \tag{20}$$

where T_1 is the fiber-coupling efficiency, α is the fiber attenuation coefficient, and L is the transmission distance. The coupling efficiency T_1 is expressed as the ratio between the output optical power and the input optical power, i.e.,

$$T_1 = \frac{P_{\text{out}}}{P_{\text{in}}}, \tag{21}$$

where P_{in} and P_{out} denote the optical powers before and after the fiber coupling, respectively. According to previously reported experimental results, the fiber-coupling efficiency T_1 typically ranges from 80% to 90%.[55–57] For standard telecommunication fibers at 1550 nm, the attenuation coefficient is typically $\alpha \approx 0.2$ dB/km, and this value is widely adopted in realistic fiber-based quantum communication systems. When the fiber-coupling efficiency is $T_1 = 88\%$, the transmission efficiency over a distance of $L = 20$ km can be estimated. The transmission loss is $\alpha L = 4$ dB, and the corresponding linear transmission coefficient is $10^{-4/10} \approx 39.8\%$. Therefore, the total transmission efficiency of the single-fiber link is $T \approx 88\% \times 39.8\% \approx 35\%$. This indicates that approximately 35% of the optical signal remains after a 20 km transmission.

In a three-party QKD protocol, Alice independently sends optical signals to Bob and Charlie (Alice $\rightarrow$ Bob and Alice $\rightarrow$ Charlie). Under the condition of passing through the BB84 protocol and ensuring no eavesdropping, each transmission has the same channel loss, so the transmission efficiency is $T_{\text{AB}} \approx T_{\text{AC}} \approx 35\%$. Since the successful implementation of the protocol requires both Bob and Charlie to receive their respective signals, the probability that both signals arrive simultaneously is $T_{\text{eff}} = T_{\text{AB}} \times T_{\text{AC}} = 35\% \times 35\% \approx 12.25\%$. In practical optical fiber channels, additional noise sources, such as guided acoustic wave Brillouin scattering (GAWBS), may further influence the effective transmission performance due to the interaction between acoustic phonons and optical fields in the fiber.[58,59] These effects can introduce extra noise and potentially reduce the effective transmission efficiency in realistic environments. Consequently, over a transmission distance of 20 km and considering actual fiber-optic loss, the effective success probability of the three-party QKD protocol is approximately 12.25%.

Our QKA protocol achieves an efficiency of approximately 19.35%. Under realistic fiber-loss conditions over a transmission distance of 20 km, this efficiency is higher than that of the conventional three-party QKD protocol.

7. Conclusion

In summary, this paper proposes two seven-particle entangled-state TPQKA protocols against collective noise. It is shown that both protocols have better resistance to collective-dephasing noise and collective-rotational noise. In both protocols, the three parties apply a hash function to their own keys. During the particle transmission process, they perform the corresponding unitary operations according to the measurement results, publicly announce the operations performed, and ultimately equally negotiate to obtain the final shared key. The security analysis results demonstrate that the proposed TPQKA protocol defends against both participant attacks and outside attacks. Additionally, eavesdropping behavior in the intercept-resend attacks and entangle-measure attacks has been simulated using IBM Qiskit, ultimately leading to the extraction of a secure shared key during the key post-processing phase. Finally, this paper calculates the qubit efficiency of both protocols. The analysis shows that both protocols demonstrate higher efficiency than several existing QKA protocols. Although the TPQKA protocol has many advantages, its technical realization still faces many challenges, such as the preparation and measurement of quantum entangled states, quantum channels involving multiple noise and loss, etc., all of which need to be further researched and resolved.

Acknowledgments

Project supported by the Coal-Major Project (Grant No. 2025ZD1700704), the Talent Introduction Fund of the Anhui University of Science and Technology (Grant No. 2021yjrc34), and the Scientific Research Fund of the Anhui Provincial Education Department (Grant No. KJ2020A0301).

References

[1] Wiesner S 1983 *ACM SIGACT News* **15** 78
[2] Bennett C H and Brassard G 2014 *Theor. Comput. Sci.* **560** 7
[3] Zhou S, Xie Q M and Zhou N R 2024 *Laser Phys. Lett.* **21** 065207
[4] Zhou C, Wang H T, Lu Y F, *et al.* 2024 *Chin. Phys. B* **33** 100302
[5] Chen S S, Zhou L and Zhong W 2018 *Sci. China Phys. Mech. Astron.* **61** 90312
[6] Dutta A and Pathak A 2022 *Quantum Inf. Process.* **22** 13
[7] Hu W W, Zhou R G and Li X 2023 *Chin. Phys. B* **32** 080303
[8] Hu W W, Zhou R G and Li X 2021 *Quantum Inf. Process.* **20** 1
[9] Bai C M, Liu L and Zhang S 2024 *Chin. Phys. B* **33** 070302
[10] Xiang Y, Tang L and Bai M Q 2021 *Mod. Phys. Lett. B* **35** 2150436

[11] Gao F, Qin S J and Huang W 2019 *Sci. China Phys. Mech. Astron.* **62** 070301
[12] Yang H and Xiao M 2020 *Quantum Inf. Process.* **19** 253
[13] Zhou N R, Chen Z Y, Liu Y Y, *et al.* 2025 *Adv. Quantum Technol.* **8** 2400530
[14] Huang J H, Li M L, Liu Y Y, *et al.* 2026 *Chin. Phys. B* **35** 080304
[15] Zhou Y Y, Wang Y P, Dai J Y, *et al.* 2025 *Adv. Quantum Technol.* **8** e00439
[16] Hu Y F, Gong L H and Zeng Q W 2025 *Quantum Inf. Process.* **24** 216
[17] Gong L H, Liu Y Y, Huang J H, *et al.* 2025 *Chin. J. Phys.* **94** 471
[18] Pirandola S, Andersen U L and Banchi L 2020 *Adv. Opt. Photonics* **12** 1012
[19] Okuła R and Mironowicz P 2025 *Quantum Inf. Process.* **24** 50
[20] Zhou N, Zeng G and Xiong J 2004 *Electron. Lett.* **40** 1149
[21] Chong S K, Tsai C W and Hwang T 2011 *Int. J. Theor. Phys.* **50** 1793
[22] Shi R H and Zhong H 2013 *Quantum Inf. Process.* **12** 921
[23] Shukla C, Alam N and Pathak A 2014 *Quantum Inf. Process.* **13** 2391
[24] Shu Y X, Bai C M and Zhang S 2025 *EPJ Quantum Technol.* **12** 48
[25] Zhou Y H, Wang M F and Shi W M 2020 *Quantum Inf. Process.* **19** 100
[26] Jiang S X, Fang L and Fang X J 2023 *Int. J. Theor. Phys.* **62** 235
[27] Tang J, Shi L and Wei J H 2020 *Laser Optoelectron. Prog.* **57** 172703
[28] Wang W, Zhou B M and Zhang L 2020 *Int. J. Theor. Phys.* **59** 1944
[29] Guo J, Yang Z and Bai M Q 2022 *Int. J. Theor. Phys.* **61** 63
[30] Yang H, Lu S and Zhou Q 2024 *Quantum Inf. Process.* **23** 150
[31] Zhou N R, Min S Q and Chen H Y 2018 *Int. J. Theor. Phys.* **57** 3505
[32] Li L, Zhou R G and Zhang X X 2023 *Quantum Inf. Process.* **22** 453
[33] Hwang T, Lee K C and Li C M 2007 *IEEE Trans. Dependable Secure Comput.* **4** 71
[34] He Y F and Ma W P 2015 *Quantum Inf. Process.* **14** 3483
[35] Tang J, Shi L and Wei J 2020 *Mod. Phys. Lett. B* **34** 2050201
[36] Younes M A, Zebboudj S and Gharbi A 2025 arXiv:2507.11188 [quant-ph]
[37] Xu Y, Wang C and Cheng K 2022 *Int. J. Theor. Phys.* **61** 245
[38] Zhu H, Wang C and Li Z 2021 *Int. J. Theor. Phys.* **60** 293
[39] Zhu H, Zhang Y and Chen L 2021 *Int. J. Theor. Phys.* **60** 2753
[40] Duan Y J, Zha X W and Sun X M 2014 *Sci. Sin. Phys. Mech. Astron.* **44** 581
[41] Jiang S X, Li J H and Li S S 2025 *Phys. Scr.* **100** 045109
[42] Hong L J 2023 *Design and Analysis of a Multi-Party Quantum Key Agreement Protocol Against Collusion Attacks* (Fujian Normal University)
[43] Deng F G, Gui L L and Yan W 2004 *Chin. Phys. Lett.* **21** 2097
[44] Deng F G, Li X H and Li C Y 2005 *Phys. Rev. A* **72** 044301
[45] Hegazy S F, Obayya S S A and Saleh B E 2022 *J. Lightwave Technol.* **40** 6995
[46] Ji Z, Fan P and Zhang H 2020 arXiv:2012.14275 [quant-ph]
[47] Desurvire E 2009 *Classical and Quantum Information Theory: An Introduction for the Telecom Scientist* (Cambridge University Press)
[48] Yuan Z H 2016 *Technol. Innov. Appl.* **8** 37
[49] Bao X M 2010 *Commun. Technol.* **43** 30
[50] Gander M J and Maurer U M 1994 *International Symposium on Information Theory*. 351
[51] Huang J 2023 *Research on Information Reconciliation and Privacy Amplification Technology in Physical Layer of Optical Communication* (Beijing University of Posts and Telecommunications)
[52] Chen L, Chen X M and Yan Y L 2024 *Sci. Rep.* **14** 25326
[53] Cabello A 2000 *Phys. Rev. Lett.* **85** 5635
[54] Pedrotti F L, Pedrotti L M and Pedrotti L S 2017 *Introduction to Optics* 3rd ed. (Cambridge University Press)
[55] Zhao H 2022 *Preparation of Quantum Entangled Optical Fields in Telecom Bands and Their Applications in Fiber-Optic Quantum Communication* (Shanxi University)
[56] Feng J, Wan Z, Li Y, *et al.* 2017 *Opt. Lett.* **42** 3399
[57] Zhao H, Feng J, Sun J, *et al.* 2022 *Opt. Express* **30** 3770
[58] Shelby R M, Levenson M D and Bayer P W 1985 *Phys. Rev. Lett.* **54** 939
[59] Cheng L, Feng J X, Li Y J, *et al.* 2024 *J. Quantum Opt.* 1