International Journal of Theoretical Physics (2023) 62:176
https://doi.org/10.1007/s10773-023-05403-y

RESEARCH

Quantum Secure Direct Communication Against Collective Noise Based on W States

Shiming Liu[1,2] · Yuqi Wang[1,2] · Geng Chen[1] · Yi Zhou[1] · Kun Yang[1] · Jiawei Luo[1] · Jiaji Wang[1]

Received: 10 February 2023 / Accepted: 7 June 2023 / Published online: 7 August 2023

Abstract

The three-particle W state is used as a quantum resource in this research. The sender's unitary operator works on the Bell state via the Pauli and controlled Z gates and encodes the unitary operations. Subsequently, the receiver measures the joint Bell state. Next, the receiver identifies the sender's unitary process and decodes the secret message for its retrieval. Finally, two quantum secure direct communication protocols are developed under collective noise channels. These protocols use different logical Bell states to resolve two different types of noise in the transmission channel. The protocol compensates for the weaknesses of three-particle W state quantum secure direct communication in resisting the collective noise. Moreover, the logical W state is applied to protect the quantum state, which increases its fidelity and improves the information transmission rate. In addition, the security of this study's protocols is demonstrated using a rigorous security analysis of diverse attacks.

Geng Chen, Yi Zhou, Kun Yang, Jiawei Luo and Jiaji Wang contributed equally to this work.

✉ Yuqi Wang
paiter_w@126.com

Shiming Liu
2981086926@qq.com

Geng Chen
326643681@qq.com

Yi Zhou
1159426969@qq.com

Kun Yang
1179830712@qq.com

Jiawei Luo
2305242837@qq.com

Jiaji Wang
2586590669@qq.com

[1] School of Computer Science, Minnan Normal University, Zhangzhou 363000, China

[2] Lab of Data Science and Intelligence Application, Minnan Normal University, Zhangzhou 363000, China

Keywords W state · Quantum secure direct communication · Collective noise

1 Introduction

The rapid development of quantum computing poses a severe threat to traditional cryptography; however, the advances in quantum cryptography also bring promising opportunities [1, 2]. Unlike conventional cryptography, quantum cryptography is based on the principles of quantum mechanics rather than mathematical problems. It is unconditionally secure over insecure channels; moreover, the laws of quantum mechanics, such as the Heisenberg uncertainty principle and the no-cloning theorem, ensure its security. Therefore, it has additional advantages in terms of security. Over the past three decades, quantum cryptography has evolved rapidly, resulting in several new disciplines; for example, quantum key distribution (QKD) [3, 4], quantum secure direct communication (QSDC) [5–7] and quantum secret sharing (QSS) [8, 9].

Because the first QKD scheme was proposed by Bennett and Brassard [10] in 1984, many scholars have conducted in-depth research on QKD. However, QKD only shares a key between the two communicating parties and cannot directly transmit secret information. The QSDC protocol addresses the problem of not sending secret messages directly and permits confidential communication without pre-distributed keys. In the QSDC protocol, one party can directly send a secret message to the other party without sharing a secret key beforehand. In 2002, Long and Liu proposed the first QSDC protocol [11], which sends confidential information from Alice to Bob using Bell states. Afterwards, an increasing number of QSDC protocols were presented. In 2003, Deng et al. proposed a two-step QSDC scheme based on entanglement [12]. In the same year, Deng and Long proposed a QSDC scheme [13]. This one-time pad scheme uses different polarisation directions of individual photons as carriers and specifies the conditions that must be fulfilled to ensure QSDC security. Next, Marco Lucamarini and Stefano Mancini proposed a QSDC scheme without entanglement [14]. Early studies of QSDC [15, 16] focused on using single photons and Bell states. Later, increasingly entangled states, Greenberger-Horne-Zeilinger (GHZ) states [17] and W states [18] were applied to QSDC. In 2005, Cao and Song proposed QSDC using four-qubit W states. In 2006, Wang et al. [19]. also suggested a QSDC scheme for W states, which uses two different sets of three-qubit W states for transmission.

In practice, the interaction between the environment and the particles in the quantum channel may generate noise in communication, affecting its correctness and efficiency. Even if the quantum channel is assumed to be noise-free, noise is inevitable due to the defects of the transmission medium in the quantum transmission process. In general, there are two types of noise in a quantum channel. The first category is collective dephasing noise, and the second is collective rotation noise. As a result, the transmitted quantum changes the original state; therefore, designing a QSDC protocol against collective noise holds great significance. There are many standard methods to overcome the noise of quantum channels, such as quantum error correction codes (QECCs) [20], entanglement purification [21] and decoherence-free subspaces (DFSs)[22]. A QECC requires at least five entangled quantum systems, which consume numerous quantum resources and are challenging to realise in practical applications. Entanglement purification also consumes numerous quantum resources and is unsuitable for practical applications. Although quantum error suppression consumes a few quantum resources, it is successful with probability. Therefore, an effective way to eliminate the adverse effects of collective noise is to use DFSs.

Subsequently, many scholars began to focus on and study collective noise in quantum transmission. Various anti-collective noise protocols have been proposed for different collective noises. To date, many different types of fault-tolerant quantum communication protocols have been proposed, such as the fault-tolerant QKD protocol [23, 24], fault-tolerant DSQC protocol [25, 26] and fault-tolerant QSDC protocol. Ge and Liu (2007) proposed a QSDC protocol against collective dephasing noise channels using DFS [27]. However, the proposed protocol cannot resist the Trojan horse attack. In 2011, Yang presented a two-step QSDC protocol against collective noise [28]. In 2012, Yang proposed a QSDC protocol [29] to enhance the Ge protocol. In 2014, Chang designed the EPR pair-based QSDC protocol against collective noise [30], which combined identity authentication into QSDC against collective noise. In 2017, He et al. [31]. forwarded a collective noise-resistant tripartite QSDC protocol based on six-particle state pairs. In 2020, Gao suggested the collective noise-resistant QSDC protocol [32] in free space, which uses a single photon to encode the polarisation and spatial mode degrees of freedom, thereby creating a decoherence-free space.

This paper proposes two QSDC protocols with logical quantum states, which are immune to collective dephasing noise and rotation noise, respectively. Secret information can be transmitted by different codes and measurements in these two QSDC protocols. There is no information leakage issue, and the two protocols are naturally immune to Trojan horse and teleportation attacks due to the unidirectional transmission mode. Moreover, the two collective noise-resistant QSDC protocols are secure against other active attacks. Finally, the quantum bit efficiency of the two collective noise-resistant QSDC protocols is analysed.

The rest of this paper is organised as follows. First, Section 2 introduces W entangled states, collective noise and QSDC to describe the theory. Section 3 describes two collective noise-resistant QSDC protocols. Sections 4 discuss their security and efficiency analysis, respectively. Finally, Section 5 provides the conclusions.

2 Preliminaries

This section primarily introduces the entanglement W state of quantum resources used in the protocol, the effects of collective noise on the channel and the principle of resistance to collective noise using DFSs. It also expounds the process from the definition of noise to the anti-noise of logical quantum bits.

2.1 W State

The entangled W state is an essential resource for quantum communication and can be expressed as follows:

$$|W\rangle = \frac{1}{\sqrt{3}}(|100\rangle + |010\rangle + |001\rangle) \tag{1}$$

The most notable property of the W state is that entanglement remains between the remaining two particles even if one of the particles is lost. Unlike single particles, entangled quantum states have the critical property: measuring one of the particles in an entangled state affects the other entangled particles. Suppose a third particle is measured, and the result is $|1\rangle$. Then, the state of the other particles must be at $|00\rangle$.

2.2 Logical Qubits Resistant to Dephasing Noise

For dephasing noise, a qubit is subjected to noise in the same time window, which is defined as $U_{dp} = |0\rangle\langle 0| + e^{i\theta}|1\rangle\langle 1|$ quantum states in the channel under the influence of dephasing noise. The change of quantum state $|0\rangle$ is expressed as follows:

$$U_{dp}|0\rangle \rightarrow |0\rangle \tag{2}$$

The change of quantum state $|1\rangle$ is represented as follows:

$$U_{dp}|1\rangle \rightarrow e^{i\theta}|1\rangle \tag{3}$$

where θ is the time-varying noise parameter, $|0\rangle$ and $|1\rangle$ are the horizontal and vertical polarisation of the photon, respectively. Logical qubits are introduced to achieve the purpose of anti-dephasing noise.

$$|0\rangle_L = |10\rangle \qquad |1\rangle_L = |01\rangle \tag{4}$$

2.3 Logic Qubits Resistant to Rotational Noise

For rotational noise, qubits in the window affected by noise are defined as $U_r = \cos\theta|0\rangle\langle 0| - \sin\theta|0\rangle\langle 1| + \sin\theta|1\rangle\langle 0| + \cos\theta|1\rangle\langle 1|$, the quantum state in the channel under the influence of rotational noise. The change of quantum state $|0\rangle$ is defined as follows:

$$U_r|0\rangle \rightarrow \cos\theta|0\rangle + \sin\theta|1\rangle \tag{5}$$

The change of quantum state $|1\rangle$ is represented as follows:

$$U_r|1\rangle \rightarrow -\sin\theta|0\rangle + \cos\theta|0\rangle \tag{6}$$

The parameter θ is related to time and fluctuates with it. Bell states $|\phi^+\rangle$ and $|\psi^-\rangle$ are resistant to interference when transmitted with this type of noise; therefore, the logical qubits can be selected as follows:

$$|0\rangle_L = |\phi^+\rangle \qquad |1\rangle_L = |\psi^-\rangle \tag{7}$$

3 The Quantum Secure Direct Communication Protocol

Based on the above preparatory knowledge, this section proposes two quantum secure direct communication protocols for resisting two different types of collective noise. The protocol under collective dephasing noise and the protocol under collective rotational noise are proposed.

3.1 Quantum Secure Direct Communication Against Collective Dephasing Noise

This section proposes a secure direct communication protocol against collective dephasing noise. From the definition of logical states resistant to dephasing noise, it can be inferred that the Bell states $|\Psi^+\rangle$ and $|\Psi^-\rangle$ are resistant to noise. Here is how resistance works:

$$U_{dp}|\Psi^{\pm}\rangle = U_{dp}^{\otimes 2}\frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle) = \frac{e^{i\theta}}{\sqrt{2}}(|01\rangle \pm |10\rangle) \tag{8}$$

Alice needs to share the coding scheme with Bob before the beginning of the protocol. Several Pauli matrices must be introduced before the coding scheme can be determined. The Pauli matrices are denoted as follows:

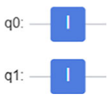
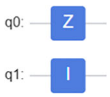
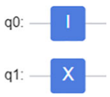
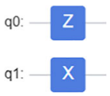
$$\begin{aligned} I &= |0\rangle\langle 0| + |1\rangle\langle 1| \\ X &= |0\rangle\langle 1| + |1\rangle\langle 0| \\ Z &= |0\rangle\langle 0| - |1\rangle\langle 1| \end{aligned} \tag{9}$$

The foundation of the implementation of this protocol is the effect of resistance towards noise via the conversion of different bell states. The unitary operation is constructed from the tensor product of the above three Pauli matrices: $U_{00} = I \otimes I$, $U_{01} = Z \otimes I$, $U_{10} = I \otimes X$ and $U_{11} = Z \otimes X$. Table 1 shows the quantum circuit diagrams of these unitary operations. These unitary operations are performed on the logical qubits. Table 2 presents the transformations of the two logical states in defining unitary operations.

The corresponding unitary operations are also defined for logical qubits $|0\rangle_L$ and $|1\rangle_L$, which can convert two logical qubits into each other without affecting their noise-resistant properties. The unitary operations of the logic quantum bit under anti-dephase noise are defined as: $U_i = I \otimes I$ and $U_z = Z \otimes Z$. These unitary operations are performed on the logic quantum bit. Table 3 presents the transformations of the two logical states under defining unitary operations.

The encoding rules shown in Table 4 can be determined by combining the operations of Tables 2 and 3. The encoding rules are a crucial step in message delivery. With Alice and

Table 1 Quantum circuit diagrams of these unitary operations

Quantum Gates	Quantum Circuits[1]	Matrix Representation[2]
U_{00}		$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$
U_{01}		$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}$
U_{10}		$\begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$
U_{11}		$\begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & -1 & 0 \end{bmatrix}$

[a] Quantum circuits generated by the HiQ quantum computing cloud platform

[b] Concrete matrix representing unitary operations

Table 2 Transitions of Bell states under defining unitary operations

	$\|\phi^+\rangle$	$\|\phi^-\rangle$	$\|\psi^+\rangle$	$\|\psi^-\rangle$
U_{00}	$\|\phi^+\rangle$	$\|\phi^-\rangle$	$\|\psi^+\rangle$	$\|\psi^-\rangle$
U_{01}	$\|\phi^-\rangle$	$\|\phi^+\rangle$	$\|\psi^-\rangle$	$\|\psi^+\rangle$
U_{10}	$\|\psi^+\rangle$	$\|\psi^-\rangle$	$\|\phi^+\rangle$	$\|\phi^-\rangle$
U_{11}	$\|\psi^-\rangle$	$\|\psi^+\rangle$	$\|\phi^-\rangle$	$\|\phi^+\rangle$

Transformation of four Bell states under four unitary operations. The leftmost column is a unitary operation, and the top row is a bell state According to the table, the results of anyone Bell state under the unitary operation

Bob agreeing on the rules in advance, the protocol can finally decode the secret message sent by Alice.

The specific steps of the protocol are presented as follows:

Step 1: Alice prepares N pairs of W states $|W\rangle_{ABC} = \frac{1}{\sqrt{3}}(|100\rangle + |010\rangle + |001\rangle)_{ABC}$. These particles are in a maximally entangled state. To remove the phase noise, the third particle in each pair of W states is extracted to create a particle set C, $C \in \{|0\rangle, |1\rangle\}$. After extracting the third particle, it is replaced by the logical state against collective dephasing, and the particle entanglement state becomes $|W\rangle = \frac{1}{\sqrt{3}}((|10\rangle + |01\rangle)|0\rangle_L + |00\rangle|1\rangle_L)_{ABC}$. After replacing the set of particles C_L, $C_L \in \{|0\rangle_L, |1\rangle_L\}$, Alice encodes the third particle to avoid affecting its ability to resist the collective dephasing noise. Encodings can only be selected from $U_i = I \otimes I$ and $U_z = Z \otimes Z$. In a random insertion of set into the logic state S_{dp1}, $S_{dp1} \in \{|0\rangle_L, |1\rangle_L, |+\rangle_L, |-\rangle_L\}$, a set C'_L is formed. C'_L is sent to Bob. Alice simultaneously sends the set of particles comprising AB to Bob and randomly inserts the decoy state S_{dp2} in the transmission sequence. The decoy state is in one of the two Bell states. The basis used is also at $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$.

Step 2: After receiving the C'_L sequence sent by Alice, Bob performs the first security detection. Next, Alice announces the location of the decoy state and the measurement basis

Table 3 Transformations of logical states under defining unitary operations

	$\|0\rangle_L$	$\|1\rangle_L$
U_i	$\|0\rangle_L$	$\|1\rangle_L$
U_z	$\|1\rangle_L$	$\|0\rangle_L$

The transformation of the logical Bell state is represented in the table, with the unitary operation in the leftmost column and the logical Bell state in the top row

Table 4 Transformations of logical states under defining unitary operations

	$U_{00}U_{10}$	$U_{01}U_{10}$	$U_{00}U_{11}$	$U_{01}U_{11}$
U_i	000	001	010	011
U_z	100	101	110	111

Suppose Alice performs U_i operation on the third particle in the first step and performs U_{00} and U_{10} operations on the remaining two particles in the subsequent step

In that case, Bob receives the quantum state and measures it, and then decodes 000 according to the coding rules of the decoy state. Bob measures the decoy state, and if the error threshold is within the trusted range, the protocol continues; otherwise, the protocol is interrupted.

Step 3: Alice will be in the hands of the remaining two groups of particles $|00\rangle_{AB}$ and $(|10\rangle + |01\rangle)_{AB}$, where $\frac{1}{\sqrt{2}}(|\phi^+\rangle + |\phi^-\rangle)_{AB}$ is available to replace $|00\rangle_{AB}$. The Bell state comprising the first particle and the second particle can be regarded as a logical Bell state, namely, $(|\phi^+\rangle + |\phi^-\rangle)_{AB}$ and $|\phi^-\rangle_{AB}$. These two groups of Bell state particles are resistant to collective dephasing phase noise. Following a unitary operation, they are transformed into noise-resistant Bell state, that is, $|\phi^+\rangle$ and $|\phi^-\rangle$. For $|\phi^-\rangle_{AB}$, only unitary operations U_{00} and U_{01} can be performed. For the other pair of Bell states $\frac{1}{\sqrt{2}}(|\phi^+\rangle + |\phi^-\rangle)_{AB}$, only the unitary operations U_{10} and U_{11} can be performed. Alice sends a set of particles comprising AB to Bob simultaneously and randomly inserts the decoy state $S_{dp2} \in \left\{|\phi^+\rangle, |\psi^-\rangle\right\}$ in the transmission sequence. The decoy state is in one of the two Bell states. The basis used is also $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$.

Step 4: Bob receives the logical Bell state transmitted by Alice and performs the second security detection. Alice announces the position of the decoy Bell state and the measurement basis. Bob performs Bell measurement on the decoy state, and the protocol is interrupted if the error rate exceeds the threshold. If the error rate is lower than the threshold, the protocol can continue; otherwise, the protocol is aborted.

Step 5: After receiving the logical quantum state and the logical Bell state, Bob reads out the corresponding secret message according to the encoding rules Alice agreed to in advance. A quantum direct communication protocol against collective dephasing noise is completed. Table 4 shows the encoding rules.

3.2 Quantum Secure Direct Communication Against Collective Rotational Noise

The procedure of anti-collective rotation noise is similar to the previous protocol, and only the W state and unitary operation underwent some changes. Table 5 presents the representations of the new quantum circuits.

The corresponding unitary operations are also defined for logical qubits $|0\rangle_L$ and $|1\rangle_L$, which can convert two logical qubits into each other without affecting their noise resistance properties. The unitary operations on a logical qubit under noise conditions are defined as $U_i = I \otimes I$ and $U_z = Z \otimes I$. These unitary operations are performed on logical qubits. Table 6 presents the transformation of two logical states defined by unitary operations.

The specific steps of the protocol are as follows:

Step 1: Alice prepares N pairs of W states $|W\rangle_{ABC} = \frac{1}{\sqrt{3}}(|-+0\rangle + |+-0\rangle + |++1\rangle)_{ABC}$. Similar to the anti-collective dephasing noise step, the third particle in each pair of W states is extracted to form particle set C, $C_L \in \{|0\rangle_L, |1\rangle_L\}$ to immunise collective rotation noise. After extracting the third particle, it is replaced by the logical state against collective rotation, and the particle entanglement state becomes $|W\rangle_{ABC} = \frac{1}{\sqrt{3}}((|-+\rangle + |+-\rangle)|0\rangle_L + |++\rangle|1\rangle_L)_{ABC}$. Alice encodes the third particle to preserve its ability to resist the collective rotation noise. Encodings can only be selected from $U_i = I \otimes I$ and $U_y = Z \otimes I$. In the unitary operation, the transformation of the two logical Bell states against collective rotation is the same as in the dephasing noise protocol. Next, Alice randomly inserts logical Bell states as decoys. The decoy particles are selected from set S_{r1}, $S_{r1} \in \{|0\rangle_L, |1\rangle_L, |+\rangle_L, |-\rangle_L\}$ to create a set C', which is then sent to Bob.

Step 2: After receiving the C' sequence sent by Alice, Bob performs the first security detection. Next, Alice announces the location of the decoy state and the measurement basis

Table 5 Quantum circuit diagrams of these unitary operations

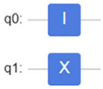
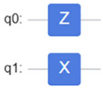
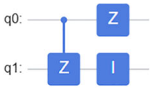
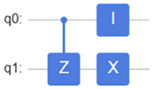
Quantum Gates	Quantum Circuits	Matrix Representation
U_{00}		$\begin{bmatrix}0&1&0&0\\1&0&0&0\\0&0&0&1\\0&0&1&0\end{bmatrix}$
U_{01}		$\begin{bmatrix}0&1&0&0\\1&0&0&0\\0&0&0&-1\\0&0&-1&0\end{bmatrix}$
U_{10}		$\begin{bmatrix}1&0&0&0\\0&1&0&0\\0&0&-1&0\\0&0&0&1\end{bmatrix}$
U_{11}		$\begin{bmatrix}0&1&0&0\\1&0&0&0\\0&0&0&-1\\0&0&1&0\end{bmatrix}$

Table 6 Transitions of Bell states under defining unitary operations

	$\vert\phi^+\rangle$	$\vert\phi^-\rangle$	$\vert\psi^+\rangle$	$\vert\psi^-\rangle$
U_{00}	$\vert\psi^+\rangle$	$\vert\psi^-\rangle$	$\vert\phi^+\rangle$	$\vert\phi^-\rangle$
U_{01}	$\vert\psi^-\rangle$	$\vert\psi^+\rangle$	$\vert\phi^-\rangle$	$\vert\phi^+\rangle$
U_{10}	$\vert\phi^+\rangle$	$\vert\phi^-\rangle$	$\vert\psi^-\rangle$	$\vert\psi^+\rangle$
U_{11}	$\vert\psi^-\rangle$	$\vert\psi^+\rangle$	$\vert\psi^+\rangle$	$\vert\psi^-\rangle$

The transformation of four Bell states under four unitary operations. The left column is a unitary operation, and the top row is a bell state. According to the table, the results of any single Bell state under the unitary process

of the decoy state. Bob measures the deception state, and the protocol continues if the error threshold is within the trusted range; otherwise, the protocol is interrupted.

Step 3: Alice will be in the hands of the remaining two groups of particles $|++\rangle_{AB}$ and $(|-+\rangle+|+-\rangle)_{AB}$. As the ant-collective dephasing noise protocol, $|++\rangle_{AB}$ is replaced with $\frac{1}{\sqrt{2}}(|\phi^+\rangle+|\psi^+\rangle)_{AB}$. The Bell state consisting the first particle and the second particle can be regarded as a logical Bell state, namely, $(|\phi^+\rangle+|\psi^+\rangle)_{AB}$ and $|\phi^-\rangle_{AB}$, respectively. These two groups of Bell state particles are resistant to collective rotational noise. After a unitary operation, they are transformed into noise-resistant Bell states, namely, $|\phi^+\rangle$ and $|\psi^-\rangle$. For $|\psi^-\rangle_{AB}$, only unitary operations U_{00} and U_{01} can be performed. For the other pair of Bell states $\frac{1}{\sqrt{2}}(|\phi^+\rangle+|\psi^+\rangle)_{AB}$, only unitary operations U_{10} and U_{11} can be performed. Alice sends the set of particles comprising AB to Bob simultaneously, and randomly inserts the decoy state S_{r2}, $S_{r2}\in[|\phi^+\rangle, |\psi^-\rangle]$, into the transmission sequence. The decoy state is in one of the two Bell states. The basis used is also $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$.

Step 4: Bob receives the logical Bell state transmitted by Alice and performs the second security detection. Alice announces the position of the decoy Bell state and the measurement basis. Bob performs Bell measurement on the decoy state, and the protocol is interrupted if the error rate exceeds the threshold. If the error rate is lower than the threshold, the protocol can continue; otherwise, the protocol is aborted.

Step 5: After receiving the logical quantum state and the logical Bell state, Bob reads out the corresponding secret message according to the encoding rules Alice agreed to in advance. A quantum direct communication protocol against collective rotational noise is completed. Table 3 shows the encoding rules.

3.3 Example of Protocol

This subsection gives a specific example of the protocol in operation, focusing on the first and third steps since the key steps of the protocol are in these two parts. The first step of the protocol is shown in Fig. 1. The third step of the protocol is shown in Fig. 2. These figures depict the data transfer using particles, where information is sent from Alice to Bob after the particles have been operated on and measured by both communicating parties. The final step of Bob's decoding of the message is also shown in Fig. 3.

The basic flow of both protocols can follow these flowcharts, the biggest difference between the two protocols is that the initial W-state and the defined unitary operations are different.

These diagrams contain only the important steps of the protocol, and the transmission and security check steps of the particles on the channel are streamlined in order to show the data transmission flow. In Fig. 1, Alice generates the W-state and separates the third particle to operate mainly on the third particle, and sends the particle to Bob after the operation. Figure 2 mainly depicts Alice's operation on the remaining particles and sends them to Bob. Figure 3 depicts Bob's measurement and decoding process.

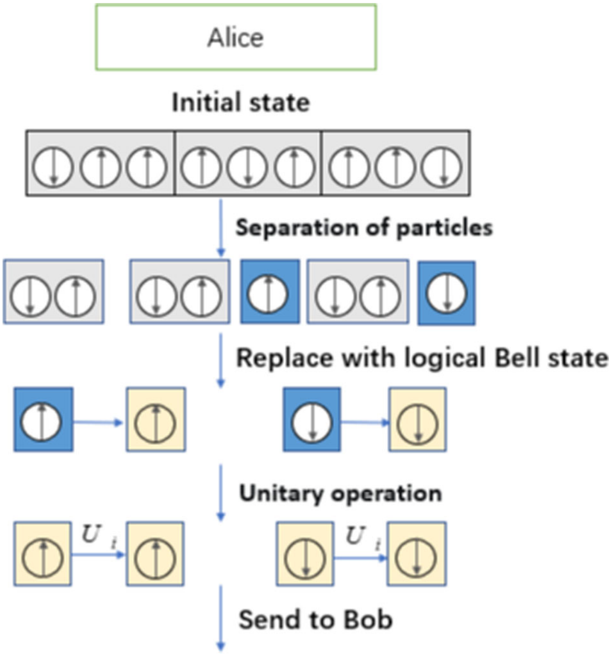


Fig. 1 First step of the protocol

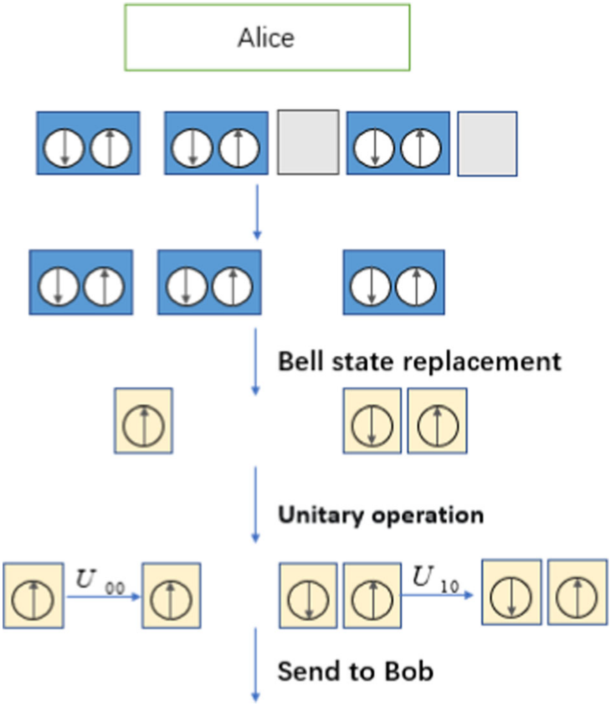


Fig. 2 Third step of the protocol

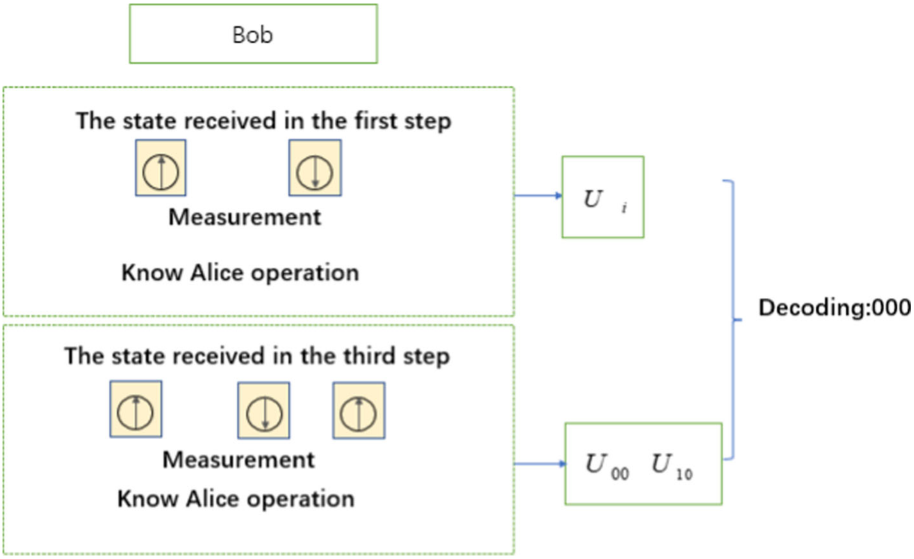


Fig. 3 Decoding

The flow chart of the implementation of the two anti-noise protocols proposed in this paper is shown in Fig. 4.

4 Protocol Analysis

The security of QSDC protocols is divided into several aspects. This paper first analyses the security of Eve with an eavesdropper. Then, it analyses the communication protocol against the Trojan horse attack. Finally, it investigates the information leakage problem.

1) Eavesdropping attack In both protocols, the qubits transmitted in the quantum channel are logical qubits unaffected by collective dephasing or rotation noise. Moreover, the qubits sent by Alice to Bob are high-fidelity. Therefore, Eve has no eavesdropping method that could possibly hide herself under noise, even if some particles are eavesdropped upon by Eve. Because the decoy states are randomly inserted in the communication process, Eve's eavesdropping inevitably impacts the decoy states. Bob can detect eavesdropping in the communication process and interrupt communication in time by calculating the error threshold.
2) Trojan Horse attack In both proposed protocols, the qubit is transmitted from Alice to Bob. Bob infers Alice's unitary operation via the measurement results to read the information in a preagreed encoding. The process is transferred only once in the quantum channel, which is a one-way transmission. A Trojan horse attack requires communication

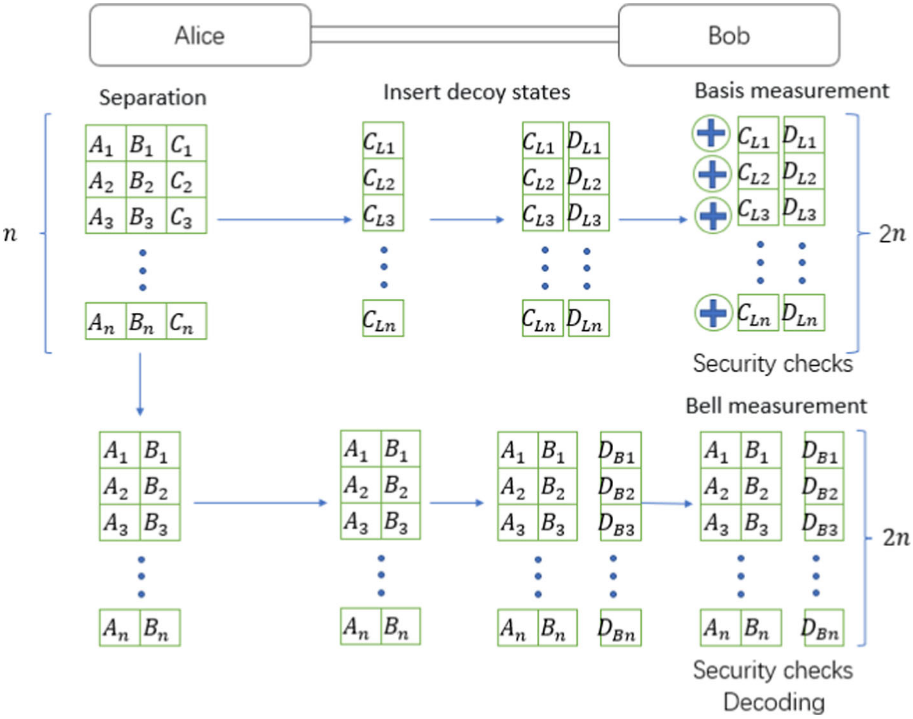


Fig. 4 Protocol execution flow chart

to be transmitted back and forth in the channel; as a result, the proposed protocol can successfully avoid Trojan horse attacks.

3) Intercept-resend attacks To steal the secret information of Alice and Bob, Eve can implement the intercept the resend attack during Alice's transmission of the W state. In this attack, Eve intercepts all transmitted qubits, replaces them with some new qubits prepared by herself and sends them to the receiver. It is clear that Eve's attack will fail. Because Eve cannot distinguish between checking qubits and decoy states prepared by Alice, Eve's attack will be discovered with high probability when the first security check between Alice and Bob is discussed publicly. The formula $P_d = 1 - (\frac{3}{4})^n$ can be used, where n is the number of qubits to be checked and P_d denotes the probability that eve is detected. For a large enough value of n, the probability will be arbitrarily close to 1. Therefore, if Eve tries to launch an intercept-resend attack, the detection qubits will be scrambled, and she will be detected eventually.

To evaluate the QSDC protocol efficiency, the qubit efficiency formula is defined as $\eta = \frac{c}{q+b}$ [33], where c, q and b are the number of secret message bits, the number of qubits used and the number of classical bits exchanged, respectively. In the proposed protocol, a total of $3n$ information particles and $3m$ decoy state particles are used to transmit a secret message of length $3n$. The proposed protocol does not require additional classical information bits because decoding the information only requires Bob to make measurements. For simplicity, it is assumed that the same number of decoy state particles and information particles is used as $m = n$. First, the quantum bit efficiency of the QSDC protocol in the ideal case is analysed. If the user Alice wants to send a secret message of n bits, then N pairs of W states must be prepared and n bits of classical information are announced. Thus, the quantum bit efficiency of the QSDC protocol is $\eta = \frac{3n}{3n+3n}$ in the ideal case. Because logical qubits are added in the noisy case, two qubits should create one logical bit during the calculation. Therefore, the two QSDC protocols resist collective noise quantum bit efficiency. They both have a quantum bit efficiency of $\eta = \frac{3n}{4n+4n} = 37.5\%$. The protocol proposed in this paper uses W states and suitable unitary operations. Each quantum state is fully utilised in the protocol process; therefore, it has certain advantages in terms of efficiency.

5 Conclusions

This paper proposes two anti-noise QSDC schemes for collective dephasing and rotation noise. Based on different unitary operation methods, the constructed QSDC protocol can resist collective noise and Trojan horse attacks, and detect intercept-resend attacks. The proposed protocol does not have the problem of information leakage. The protocol can be extended further to the quantum dialogue and multiparty QSDC protocols.

Acknowledgements We acknowledge financial support from the Natural Science Foundation of Fujian Province, China (Grant No. 2020J01812).

References

1. Gisin, N., Ribordy, G., Tittel, W., Zbinden, H.: Quantum cryptography. Rev. Mod. Phys. **74**(1), 145 (2002)
2. Pirandola, S., Andersen, U.L., Banchi, L., Berta, M., Bunandar, D., Colbeck, R., Englund, D., Gehring, T., Lupo, C., Ottaviani, C., et al.: Advances in quantum cryptography. Adv. Opt. Photon. **12**(4), 1012–1236 (2020)

3. Chang, C.-H., Yang, C.-W., Hwang, T.: Trojan horse attack free faulttolerant quantum key distribution protocols using ghz states. Int. J. Theor. Phys. **55**(9), 3993–4004 (2016)
4. Zhu, K.-N., Zhou, N.-R., Wang, Y.-Q., Wen, X.-J.: Semi-quantum key distribution protocols with ghz states. Int. J. Theor. Phys. **57**(12), 3621–3631 (2018)
5. Chen, S.-S., Zhou, L., Zhong, W., Sheng, Y.-B.: Three-step three-party quantum secure direct communication. Sci. China Phys. Mech. Astron. **61**(9), 1–5 (2018)
6. Liu, X., Li, Z., Luo, D., Huang, C., Ma, D., Geng, M., Wang, J., Zhang, Z., Wei, K.: Practical decoy-state quantum secure direct communication. Sci. China Phys. Mech. Astron. **64**(12), 1–8 (2021)
7. Yang, Y.-F., Duan, L.-Z., Qiu, T.-R., Xie, X.-M., Duan, W.-Y.: Multiparty semi-quantum secure direct communication using greenberger-horne-zeilinger states. Quantum Inf. Process. **21**(9), 1–20 (2022)
8. Tsai, C.-W., Yang, C.-W., Lee, N.-Y.: Semi-quantum secret sharing protocol using w-state. Mod. Phys. Lett. A **34**(27), 1950213 (2019)
9. Zhou, R.-G., Huo, M., Hu, W., Zhao, Y.: Dynamic multiparty quantum secret sharing with a trusted party based on generalized ghz state. IEEE Access **9**, 22986–22995 (2021)
10. Bennett, C.H., Brassard, G.: Quantum cryptography: Public key distribution and coin tossing, India, p. 175 (1984)
11. Long, G.-L., Liu, X.S.: Theoretically efficient high-capacity quantum-keydistribution scheme. Phys. Rev. A **65**, 032302 (2002)
12. Deng, F.-G., Long, G.L., Liu, X.-S.: Two-step quantum direct communication protocol using the einstein-podolsky-rosen pair block. Phys. Rev. A **68**, 042317 (2003). https://doi.org/10.1103/PhysRevA.68.042317
13. Deng, F.-G., Long, G.L.: Secure direct communication with a quantum one-time pad. Phys. Rev. A **69**, 052319 (2004). https://doi.org/10.1103/PhysRevA.69.052319
14. Lucamarini, M., Mancini, S.: Secure deterministic communication without entanglement. Phys. Rev. Lett. **94**, 140501 (2005). https://doi.org/10.1103/PhysRevLett.94.140501
15. Beige, A., Englert, B.-G., Kurtsiefer, C., Weinfurter, H.: Secure communication with single-photon two-qubit states. J. Phys. A Math. Gen. **35**(28), 407 (2002)
16. Boström, K., Felbinger, T.: Deterministic secure direct communication using entanglement. Phys. Rev. Lett. **89**, 187902 (2002). https://doi.org/10.1103/PhysRevLett.89.187902
17. Greenberger, D.M.: In: Greenberger, D., Hentschel, K., Weinert, F. (eds.) GHZ (Greenberger–Horne–Zeilinger) Theorem and GHZ States, pp. 258–263. Springer, Berlin, Heidelberg (2009). https://doi.org/10.1007/978-3-540-70626-7 <error l="297" c="Invalid <error l="297" c="Invalid <error l="298" c="Invalid command: paragraph not started." /> command: paragraph not started." /> command: paragraph not started." /> _78
18. Jian, W., Quan, Z., Chao-Jing, T.: Quantum secure communication scheme with w state. Commun. Theor. Phys. **48**(4), 637 (2007). https://doi.org/10.1088/0253-6102/48/4/013
19. Hai-Jing, C., He-Shan, S.: Quantum secure direct communication with w state. Chin. Phys. Lett. **23**(2), 290 (2006)
20. Devitt, S.J., Munro, W.J., Nemoto, K.: Quantum error correction for beginners. Rep. Prog. Phys. **76**(7), 076001 (2013)
21. Bennett, C.H., Brassard, G., Popescu, S., Schumacher, B., Smolin, J.A., Wootters, W.K.: Purification of noisy entanglement and faithful teleportation via noisy channels. Phys. Rev. Lett. **76**(5), 722 (1996)
22. Walton, Z.D., Abouraddy, A.F., Sergienko, A.V., Saleh, B.E., Teich, M.C.: Decoherence-free subspaces in quantum key distribution. Phys. Rev. Lett. **91**(8), 087901 (2003)
23. Li, X.-H., Deng, F.-G., Zhou, H.-Y.: Efficient quantum key distribution over a collective noise channel. Phys. Rev. A **78**(2), 022321 (2008)
24. Yang, C.-W., Hwang, T.: Fault tolerant quantum key distributions using entanglement swapping of ghz states over collective-noise channels. Quantum Inf. Process. **12**(10), 3207–3222 (2013)
25. Dong, L., Xiu, X.-M., Gao, Y.-J., Chi, F.: Deterministic secure quantum communication against collective-dephasing noise by using epr pairs and auxiliary photons. Opt. Commun. **282**(8), 1688–1690 (2009)
26. Wang, P., Chen, X., Sun, Z.: Deterministic secure quantum communication against collective noise. Phys. Lett. A **446**, 128291 (2022)
27. Hua, G., Wen-Yu, L.: A new quantum secure direct communication protocol using decoherence-free subspace. Chinese Phys. Lett. **24**(10), 2727 (2007)
28. Yang, C.-W., Tsai, C., Hwang, T.: Fault tolerant two-step quantum secure direct communication protocol against collective noises. Sci. China Phys. Mech. Astron. **54**(3), 496–501 (2011)
29. Yang, C.-W., Hwang, T.: Improved qsdc protocol over a collectivedephasing noise channel. Int. J. Theor. Phys. **51** (2012). https://doi.org/10.1007/s10773-012-1286-4
30. Chang, Y., Zhang, S., Li, J., Yan, L.: Robust epr-pairs-based quantum secure communication with authentication resisting collective noise. Sci. China Phys. Mech. Astron. **57**(10), 1907–1912 (2014)

31. He, Y.-F., Ma, W.-P.: Three-party quantum secure direct communication against collective noise. Quantum Inf. Process. **16**(10), 1–21 (2017)
32. Gao, Z., Ma, M., Liu, T., Long, J., Li, T., Li, Z.: Free-space quantum secure direct communication based on decoherence-free space. JOSA B **37**(10), 3028–3033 (2020)
33. Cabello, A.: Quantum key distribution in the holevo limit. Phys. Rev. Lett. **85**, 5635–5638 (2000). https://doi.org/10.1103/PhysRevLett.85.5635