PAPER

Collective noise-resistant multi-party semi-quantum secret sharing protocols

To cite this article: Jian Li *et al* 2024 *Phys. Scr.* **99** 095123

Physica Scripta

PAPER

Collective noise-resistant multi-party semi-quantum secret sharing protocols

RECEIVED
2 June 2024

REVISED
31 July 2024

ACCEPTED FOR PUBLICATION
12 August 2024

PUBLISHED
23 August 2024

Jian Li[1,2], Chong-Qiang Ye[2] and Wang Zhuo[2]

[1] School of Information Engineering, Ningxia University, Yinchuan, 750021, People's Republic of China
[2] School of Artificial Intelligence, Beijing University of Posts Telecommunications, Beijing 100876, People's Republic of China

E-mail: chongqiangye@bupt.edu.cn

Keywords: semi-quantum, quantum cryptography, data sharing, noise-resistant

Abstract

Semi-quantum secret sharing facilitates the sharing of private data between quantum users and 'classical' users with limited quantum capabilities, thereby lowering the barrier to utilizing quantum technology. However, most current semi-quantum secret sharing protocols are confined to ideal environments and two-party scenarios. In this paper, we design two collective noise-resistant multi-party semi-quantum secret sharing protocols based on decoherence-free states to address potential noise interference during transmission. These protocols use decoherence-free states as information carriers for data interaction and exhibit strong resilience to both internal and external threats. We also conduct simulation experiments using IBM Qiskit to verify the stability and feasibility of the protocols in the noisy environments. The results of these experiments underscore the robustness of the protocols, particularly in the presence of collective noise. Compared with previous related protocols, our protocols have advantages in noise resistance and applicability to multi-party scenarios. Therefore, the proposed protocols may be more in line with the secret sharing needs of actual environments.

1. Introduction

With the advancement of information technology, the demand for secure data sharing has grown significantly. Traditional encryption schemes are vulnerable to modern computationally powerful attackers. This vulnerability is especially evident in the face of emerging quantum computing attacks [1, 2]. To address these challenges, researchers have begun to focus on the application of quantum technology to information security [3, 4].

Quantum technology has opened up new possibilities for the development of information secure field. Various quantum communication and cryptography technologies have emerged to enhance the security of data sharing [5, 6]. For example, quantum key distribution technology [7–9] has been extensively researched and applied, enabling secure key establishment for users with rigorous mathematical proofs of its security. Currently, quantum key distribution is widely employed in fields such as telecommunications and power networks to safeguard sensitive data [10]. Another critical branch of quantum cryptography is quantum secret sharing [11–13], which allows multiple parties to share secret information while protecting it from any single entity's exposure. The research and development of quantum secret sharing offer devices additional options for privacy protection [14]. This is particularly valuable in scenarios requiring multi-party collaboration or data sharing.

Quantum secret sharing technology has emerged to provide strong support for ensuring data sharing in different devices. However, despite the theoretical excellence of quantum secret sharing technology, its practical application still faces a number of challenges [15]. One of these issues is that quantum devices remain relatively expensive, and ordinary users cannot afford the financial pressure of being responsible for them, resulting in their lack of popularity in practical applications [16].

In response to the problem of expensive quantum devices, semi-quantum secret sharing (SQSS) technology [17–24] has emerged as a promising solution. It offers an alternative approach to traditional quantum secret

Table 1. The characteristics of related SQSS protocols.

Protocol	Quantum resources	Channel type	Shared key type	Circuit simulation	Multi-party scenarios
[17]	GHZ states	Ideal channel	Random	No	No
[18]	Single-particle states	Ideal channel	Random	No	Yes
[19]	Bell states	Ideal channel	Specific	No	No
[20]	Single-particle states	Ideal channel	Random	No	No
[21]	d-level single-particle states	Ideal channel	Random	No	No
[22]	Bell states	Ideal channel	Specific	No	No
[23]	χ-type states	Ideal channel	Random	No	No
[24]	Multi-degree-of-freedom qubits	Ideal channel	Random	No	No

sharing, providing similar levels of security while being more cost-effective. Generally, in SQSS, there is only one participant with full quantum capabilities, commonly referred to as the 'quantum' user, while the rest of the participants are known as 'classical' users. These classical users have limited quantum abilities, enabling them to perform simpler quantum operations, including: Conducting computational basis measurements and preparations, directly reflecting quantum states, and reordering quantum states. SQSS enables secure data sharing among multiple parties, all the while reducing the reliance on complex quantum devices by most users. Therefore, it has received widespread attention from researchers.

SQSS was first proposed by Li *et al* [17] in 2010. In their protocol, quantum and classical users share secret information through maximally entangled GHZ-type states. Then in 2013, Li *et al* [18] designed a SQSS protocol based on GHZ-type states and gave a general model for analyzing the security of SQSS protocol. Subsequently, Xie *et al* [19] developed a SQSS protocol based on entangled states, effectively achieving specific secret information sharing. Then, Ye *et al* [20, 21] extended SQSS to circular transmission structures and high-dimensional scenarios. In 2021, Tian *et al* [22] presented a new SQSS protocol, which can also achieve shared deterministic secrets. Recently, Chen *et al* [23] utilized the χ-type states to design the SQSS protocol, while Tian *et al* [24] used multiple degrees of freedom quantum states to design a high channel capacity SQSS protocol. The characteristics of the above related papers are shown in table 1.

The aforementioned solutions are primarily designed to function in ideal, noise-free environments. However, in practice, the impact of noise on protocol performance cannot be underestimated. Noise has the potential to significantly reduce quantum efficiency, resulting in communication errors and compromising protocol security. Consequently, the research and development of secure, noise-resistant SQSS protocols is of utmost importance. It is worth noting that in the field of semi-quantum cryptography, research on noise resistance is primarily focused on the semi-quantum key distribution and private comparison [25–27]. To our knowledge, studies on noise-resistant SQSS protocols have not been conducted. By investigating related noise-resistant quantum protocols [26, 27], it is found that in the quantum channel on which the SQSS protocol depends, the correlation noise can be regarded as the collective noise, and the decoherence-free (DF) states can resist the collective noise. DF states are quantum states that remain unaffected by certain types of decoherence or noise within a quantum system. These states are particularly valuable in quantum communication and computation, as they help preserve quantum information by avoiding the destructive effects of environmental interactions. Inspired by this, the DF states can be utilized to design SQSS protocols that resist collective noise, which can better serve secure data sharing of devices in practical applications.

In this paper, we leverage the advantages of DF states to design the collective noise-resistant multi-party SQSS protocols for addressing collective dephasing noise and collective rotation noise. In our protocols, the shared secret information can be finally recovered only when all classical users cooperate with each other, and no individual user can recover the secret information alone. Thus, our protocols can be applied to secure data sharing between different devices in noisy environments. We also discuss the threats to the protocols from external and internal attacks, and the analysis shows that the protocols can be resistant to eavesdroppers. The main contributions of this paper are as follows:

- Two collective noise resistant semi-quantum secret sharing schemes are proposed, which are able to resist the interference of collective noise, while all the previous SQSS protocols can only be applied to the ideal environment.
- The proposed protocols are scalable and suitable for multi-party scenarios, and the shared secret information is deterministic.

Table 2. Notation.

Notation	Description
$\|\cdot\rangle$	Dirac symbol, used to represent quantum states
θ	Noise parameter fluctuating with time
$\oplus$	XOR operation
U_{dp}	The operation of collective dephasing noise on quantum states
U_r	The operation of collective rotation noise on quantum states
$\|0_d\rangle, \|1_d\rangle, \|+_d\rangle, \|-_d\rangle$	Logic qubits resistant to collective dephasing noise
$\|0_r\rangle, \|1_r\rangle, \|+_r\rangle, \|-_r\rangle$	Logic qubits resistant to collective rotation noise
Z_d-basis/ X_d-basis	Measurement basis based on $\{\|0_d\rangle, \|1_d\rangle\}$/ $\{\|+_d\rangle, \|-_d\rangle\}$
Z_r-basis/ X_r-basis	Measurement basis based on $\{\|0_r\rangle, \|1_r\rangle\}$/ $\{\|+_r\rangle, \|-_r\rangle\}$
measure	Measure the qubit in computational basis $Z_d(Z_r)$ and regenerate one in the same state
reflect	Reflect the qubit directly

- The corresponding quantum circuits are given and simulated by IBM Qiskit. The results show that our protocols are robust under collective noises and are feasible under current quantum technology.

The subsequent sections of this paper are structured as follows: In section 2, some foundational concepts and background information are presented. Section 3 provides a comprehensive description of the proposed SQSS protocols. Section 4 offers an analysis of the protocols' resilience against both external and internal attacks. Then section 5 gives the circuit simulation procedure of the protocol. Lastly, in section 6, we discuss the proposed SQSS protocols with previous protocols and give a brief conclusion.

2. Preliminaries

In this section, we introduce the DF states resistant to collective dephasing noise and collective rotation noise, as well as the quantum resources needed for the protocol designed in this paper. Moreover, the specific notations are listed in table 2.

In optical implementations, one of the primary sources of noise is due to fluctuations in the birefringence of the optical fiber, commonly referred to as collective noise. The most common types of collective noise in quantum protocols are collective dephasing noise and collective rotation noise. Collective dephasing noise is a type of noise that affects multiple qubits in a quantum system in a correlated manner, causing simultaneous phase shifts across all qubits [28]. Specifically, the effect of collective dephasing noise in the single qubit can be described as :

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

where θ is the noise parameter fluctuating with time. To mitigate the effects of collective dephasing noise, we employ DF states $|01\rangle$ and $|10\rangle$ as the basic information carrier. Initially, we define logical qubits $|0_d\rangle$ and $|1_d\rangle$ as:

$$|0_d\rangle = |01\rangle, \quad |1_d\rangle = |10\rangle. \tag{2}$$

It is not difficult to find that logical qubits $|0_d\rangle$ and $|1_d\rangle$ are resistant to collective dephasing noise because they have the same phase shift, i.e., $i\theta$:

$$U_{dp}|0_d\rangle = e^{i\theta}|0_d\rangle, \quad U_{dp}|1_d\rangle = e^{i\theta}|1_d\rangle. \tag{3}$$

Correspondingly, the superpositions of $|0_d\rangle$ and $|1_d\rangle$ are immune to the collective dephasing noise, i.e., $|+_d\rangle = \frac{1}{\sqrt{2}}(|0_d\rangle + |1_d\rangle), |-_d\rangle = \frac{1}{\sqrt{2}}(|0_d\rangle - |1_d\rangle)$. Note that the $\{|0_d\rangle, |1_d\rangle\}$ and $\{|+_d\rangle, |-_d\rangle\}$ form two sets of measurement bases, denoted Z_d-basis and X_d-basis, respectively.

Another type of collective noise is collective rotational noise, which affects the entire ensemble of qubits by rotating them around a common axis in the Bloch sphere. This type of noise is particularly relevant in systems where qubits are subjected to global control fields or environmental interactions that induce identical rotations on all qubits. Its effect on the quantum state can be described as:

$$U_r|0\rangle = \cos\theta|0\rangle + \sin\theta|1\rangle, \quad U_r|1\rangle = -\sin\theta|0\rangle + \cos\theta|1\rangle. \tag{4}$$

Here, we adopt the DF states $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ and $\frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$ as the logical qubits $|0_r\rangle$ and $|1_r\rangle$, respectively. Then it's easy to see that these logical qubits can be immune to the collective rotation noise [28]:

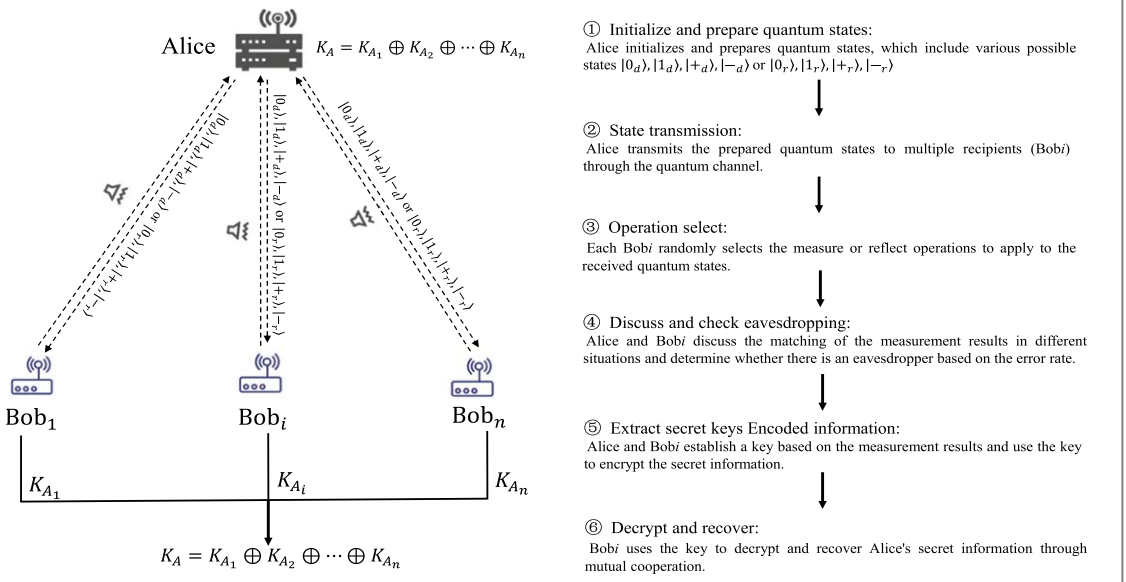


Figure 1. Schematic diagram of the SQSS protocol, where the dashed lines in the figure represent quantum channels, which are affected by collective noise, while the solid lines represent classical channels.

Table 3. The operations performed by Alice and the corresponding results.

Case	Initial basis of the particle	Bob_i's operations	Alice's operations	Usage
1)	Z_d-basis	***measure***	Z_d-basis measurement	Create secret key
2)	Z_d-basis	***reflect***	Z_d-basis measurement	Eavesdropping detection
3)	X_d-basis	***measure***	Z_d-basis measurement	Create secret key
4)	X_d-basis	***reflect***	X_d-basis measurement	Eavesdropping detection

$$U_r|0_r\rangle = |0_r\rangle, \quad U_r|1_r\rangle = |1_r\rangle. \tag{5}$$

Similarly, the superpositions of $|0_r\rangle$ and $|1_r\rangle$ are immune to the collective rotation noise, i.e., $|+_r\rangle = \frac{1}{\sqrt{2}}(|0_r\rangle + |1_r\rangle), |-_r\rangle = \frac{1}{\sqrt{2}}(|0_r\rangle - |1_r\rangle)$. Note that the $\{|0_r\rangle, |1_r\rangle\}$ and $\{|+_r\rangle, |-_r\rangle\}$ can form two sets of measurement bases, denoted Z_r-basis and X_r-basis, respectively.

In the above, we introduced two types of DF states and provided corresponding logical qubits. Building upon these logical qubits, we can construct quantum protocols that are resilient to specific noise. In the following, we utilize the DF states $\{|0_d\rangle, |1_d\rangle, |+_d\rangle, |-_d\rangle\}$ and $\{|0_r\rangle, |1_r\rangle, |+_r\rangle, |-_r\rangle\}$ as quantum resources to design the SQSS protocol.

3. SQSS protocol

Before detailing the specific steps of the protocol, let's provide an overview of the fundamental settings. In the proposed SQSS protocol, Alice is a user with full quantum capabilities, whereas Bob_1 Bob_2,..., Bob_n are the other users with restricted quantum capabilities. Their roles are primarily limited to performing ***measure*** operation and ***reflect*** operation. In more detail, ***measure*** operation means: measure the qubit in the computational basis and regenerate one in the same state; ***reflect*** operation means: reflect the qubit directly. Then, Alice wants to share her secret information $K_A = K_{A_1} \oplus K_{A_2} \oplus ,\ldots,\oplus K_{A_n}$ to Bob_1 Bob_2,..., Bob_n. However, Bob_1 Bob_2,..., Bob_n can only recover Alice's information by collaborating with each other. In addition, it should be emphasized that the quantum channel used in the entire protocol does need to be authenticated to ensure the security and reliability of quantum communication. The detailed description of the protocol steps is shown below (also see figure 1).

3.1. Protocol description for resisting collective dephasing noise

Depending on the nature of the channel noise, we need employ different logical qubits as carriers of information. Here, we first take resisting collective dephasing noise as an example to describe the protocol steps, also see algorithm 1. For a clearer description, the specific steps of the protocol are shown below:

Table 4. Cases for performing different operations.

Case	Initial basis of the particle	Bob$_i$'s operations	Alice's operations	Usage
(i)	Z_r-basis	***measure***	/	Create secret key
(ii)	Z_r-basis	***reflect***	Z_r-basis measurement	Eavesdropping detection
(iii)	X_r-basis	***measure***	/	Discard
(iv)	X_r-basis	***reflect***	X_r-basis measurement	Eavesdropping detection

Algorithm 1. Semi-quantum secret sharing against collective dephasing noise

Data: Alice's secret: $K_A = K_{A_1} \oplus K_{A_2} \oplus ,\ldots,\oplus K_{A_n}$; Dephasing noise channel
Result: Bob$_1$ Bob$_2$,..., Bob$_n$ recover Alice's secret $K_A = K_{A_1} \oplus K_{A_2} \oplus ,\ldots,\oplus K_{A_n}$
1 **Initialization:** Alice uses $\{|0_d\rangle, |1_d\rangle, |+_d\rangle, |-_d\rangle\}$ to form sequences $S_1, S_2,\ldots,S_n$ and then sends to Bob$_1$ Bob$_2$,..., Bob$_n$, respectively;
2 **Operation select:** Bob$_i$ ($i = 1, 2, \ldots, n$) randomly chooses the ***measure*** or ***reflect*** operation;
3 **Discussion:** Alice and Bob$_i$ discuss different cases for eavesdropping check and key establishment;
4 **If** Bob$_i$ performs ***measure*** operation **then**
5 Alice will measure the received particles in Z_d-basis. Alice and Bob$_i$ use these result as secret key, labeled as K_{ABi};
6 **If** Bob$_i$ performs ***reflect*** operation **then**
7 Alice will measure the received particles in Z_d-basis or X_d-basis based on their initial preparation base. These cases will use to eavesdropping check;
8 **Encoded information:** Alice uses K_{AB_i} to encrypt her secret information K_{A_i} as $C_i = K_{AB_i} \oplus K_{A_i}$, and then sends it to Bob$_i$;
9 **Decrypt and recover:** Based on C_i and K_{tAB_i}, Bob$_i$ decrypts and obtains Alice's partial secret information K_{itA_i}. All Bobs cooperate with each other and obtain Alice's secret $K_A = K_{A_1} \oplus K_{A_2} \oplus ,\ldots,\oplus K_{A_n}$;

Step 1: Alice first prepares n particle sequences labeled as $S_1, S_2, \ldots, S_n$, where each sequence's particles are randomly selected from the set $\{|0_d\rangle, |1_d\rangle, |+_d\rangle, |-_d\rangle\}$, and each sequence contains $4l$ particles. **Step 2:** Alice then sends the sequences $S_1, S_2, \ldots, S_n$ to Bob$_1$ Bob$_2$,..., Bob$_n$, respectively. **Step 3:** For each received qubit, Bob$_i$ ($i = 1, 2, \ldots, n$) randomly chooses the ***measure*** or ***reflect*** operation. If Bob$_i$ chooses the ***measure*** operation, he will record the measurement result. After Bob$_i$'s operations, the particles will be sent to Alice. **Step 4:** After receiving all the particles, Alice will allow Bob$_i$ to disclose his operations. Then Alice performs corresponding operations based on the information disclosed by Bob$_i$. Details are shown below and also in table 3.

1. The initial basis of the particle is $\{|0_d\rangle, |1_d\rangle\}$, while Bob$_i$ selects the ***measure*** operation. In this case, Alice will select Z_d-basis, i.e., $\{|0_d\rangle, |1_d\rangle\}$ to measure the particle. Here, Alice's measurements need to be consistent with the particle's initial state and Bob's measurements; otherwise it indicates that an error has been introduced. This case will be used for key establishment between Alice and Bob$_i$.
2. The initial basis of the particle is $\{|0_d\rangle, |1_d\rangle\}$, while Bob$_i$ selects the ***reflect*** operation. This case will be used to eavesdropping detection. If there is no eavesdropping, Alice's measurements should be consistent with the particle's initial state.
3. The particle initially exists in the X_d-basis, i.e., $\{|+_d\rangle, |-_d\rangle\}$, and Bob$_i$ chooses the ***measure*** operation. Here, Alice will select Z_d-basis to measure the particle and the measurement result will be the secret key between Bob$_i$.
4. The particle initially exists in the X_d-basis, and Bob$_i$ chooses the ***reflect*** operation. In this case, Alice will use X_d-basis to measure the particle. If there is no eavesdropping, Alice's measurements should be consistent with the particle's initial state.

Alice and Bob$_i$ ($i = 1, 2, \ldots, n$) discuss the above cases. If the error rate for Cases 2) and 4) exceeds the threshold, the protocol restarts; otherwise it goes to the next step. **Step 5:** After eavesdropping check, Alice and Bob$_i$ ($i = 1, 2,\ldots, n$) utilize the measurements in cases 1 and 3 as the secret key, labeled as K_{AB_i}. Then, Alice uses K_{AB_i} to encrypt her secret information K_{A_i} as $C_i = K_{AB_i} \oplus K_{A_i}$. Next, Alice sends C_i to Bob$_i$ via a classical channel. **Step 6:** Based on C_i and K_{AB_i}, Bob$_i$ can decrypt and obtain Alice's partial secret information K_{A_i}. Finally, when all Bobs cooperate with each other, they can obtain Alice's complete secret information, i.e., $K_A = K_{A_1} \oplus K_{A_2} \oplus ,\ldots,\oplus K_{A_n}$.

3.2. Protocol description for resisting collective rotation noise

Here, we give the steps of the protocol against collective rotation noise, also see algorithm 2. The following are the specific steps:

Algorithm 2. Semi-quantum secret sharing against collective rotation noise

Data Alice's secret: $K_A = K_{A_1} \oplus K_{A_2} \oplus ,\ldots,\oplus K_{A_n}$; Rotation noise channel
Result Bob_1 Bob_2,..., Bob_n recover Alice's secret $K_A = K_{A_1} \oplus K_{A_2} \oplus ,\ldots,\oplus K_{A_n}$
1 **Initialization:** Alice uses $\{|0_r\rangle, |1_r\rangle, |+_r\rangle, |-_r\rangle\}$ to form sequences $S_1', S_2', \ldots, S_n'$ and then sends to Bob_1 Bob_2,..., Bob_n, respectively;
2 **Operation select:** Bob_i $(i = 1, 2, \ldots, n)$ randomly chooses the ***measure*** or ***reflect*** operation ;
3 **Discussion:** Alice and Bob_i discuss different cases for eavesdropping check and key establishment ;
4 **If**Alice sends $|0_r\rangle$ or $|1_r\rangle$ and Bob_i performs ***measure*** operation **then**
5 Alice and Bob_i will use these result as secret key, labeled as K^*_{ABi};
6 **If** Alice sends $|+_r\rangle$ or $|-_r\rangle$ and Bob_i performs ***measure*** operation **then**
7 This case will be discarded;
8 **If** Bob_i performs ***reflect*** operation **then**
9 Alice will measure the received particles in Z_r-basis or X_r-basis based on their initial preparation base. These cases will use to eavesdropping check;
10 **Encoded information:** Alice uses K^*_{ABi} to encrypt her secret information K_{A_i} as $C_i^* = K^*_{ABi} \oplus K_{A_i}$, and then sends it to Bob_i ;
11 **Decrypt and recover:** Based on C_i^* and K^*_{ABi}, Bob_i decrypts and obtains Alice's partial secret information K_{A_i}. All Bobs cooperate with each other and obtain Alice's secret $K_A = K_{A_1} \oplus K_{A_2} \oplus ,\ldots,\oplus K_{A_n}$;

Step 1*: Alice first prepares n particle sequences labeled as $S_1', S_2', \ldots, S_n'$, where each sequence's particles are randomly selected from the set $\{|0_r\rangle, |1_r\rangle, |+_r\rangle, |-_r\rangle\}$, and each sequence contains $4l$ particles. **Step 2*:** Alice then sends the sequences $S_1', S_2', \ldots, S_n'$ to Bob_1 Bob_2,..., Bob_n, respectively. **Step 3*:** Bob_i $(i = 1, 2, \ldots, n)$ randomly chooses the ***measure*** or ***reflect*** operation on the received qubits. If Bob_i chooses the ***measure*** operation, he will record the measurement result. **Step 4*:** After receiving all the particles, Alice will allow Bob_i to disclose his operations. Then Alice performs corresponding operations based on the information disclosed by Bob_i, as shown in table 4.

(i) The initial basis of the particle is Z_r-basis, i.e., $\{|0_r\rangle, |1_r\rangle\}$, while Bob_i selects the ***measure*** operation. This case will be used for key establishment between Alice and Bob_i. In more detail, if Bob_i's measurement results are $|00\rangle$ or $|11\rangle$, it means that Alice sent the $|0_r\rangle$ state. If the results are $|10\rangle$ or $|01\rangle$, it signifies that Alice sent the $|1_r\rangle$ state. Since Alice prepared these particles, she naturally knows their states. Hence, they can establish secret key based on these particles.

(ii) The initial basis of the particle is Z_r-basis, while Bob selects the ***reflect*** operation. This case will be used to eavesdropping detection. If there is no eavesdropping, Alice's measurements should be consistent with the particle's initial state.

(iii) The particle initially exists in the X_r-basis, i.e., $\{|+_r\rangle, |-_r\rangle\}$, and Bob_i chooses the ***measure*** operation. This case will be discarded.

(iv) The particle initially exists in the X_r-basis, and Bob_i chooses the ***reflect*** operation. This case will be used to eavesdropping detection. If there is no eavesdropping, Alice's measurements should be consistent with the particle's initial state.

After that, Alice and Bob_i $(i = 1, 2, \ldots, n)$ discuss the above cases. If the error rate for Cases (ii) and (iv) exceeds the threshold, the protocol restarts; otherwise it goes to the next step. It should be noted that since Bob_i can only work in the computational basis, he cannot prepare logical qubits $|0_r\rangle$ and $|1_r\rangle$ that can resist collective rotation noise. Therefore Alice cannot obtain useful information from Bob_i's particles after the ***measure*** operation.

Step 5*: After eavesdropping check, Alice and Bob_i $(i = 1, 2, \ldots, n)$ utilize the measurements in cases (i) as the secret key, labeled as K^*_{ABi}. Then, Alice uses K^*_{ABi} to encrypt her secret information K_{A_i} as $C_i^* = K^*_{ABi} \oplus K_{A_i}$. Next, Alice sends C_i^* to Bob_i via a classical channel. **Step 6*:** Based on C_i^* and K^*_{ABi}, Bob_i can decrypt and obtain Alice's partial secret information K_{A_i}. Finally, when all Bobs cooperate with each other, they can obtain Alice's complete secret information, i.e., $K_A = K_{A_1} \oplus K_{A_2} \oplus ,\ldots,\oplus K_{A_n}$.

4. Security analysis

In this part, we will analyze the security of the designed protocol, showing that it is resilient to external attacks and internal attacks. It's important to note that throughout the entire security analysis process, we are focusing on the security analysis of the protocol against collective dephasing noise. The security analysis for the protocol against collective rotation noise is similar and is omitted here to avoid repetition.

4.1. External attack

In external attacks, it is usually assumed that the adversary is Eve, who seeks to acquire the user's confidential information within the SQSS protocol through various means. Here, we will analyze the security of the SQSS protocol against typical external attacks, including intercept-resend attack, measure-resend attack, collective attack, and Trojan Horse attack.

4.1.1. Intercept-resend attack

Intercept-resend attack is a common form of external attack. In such attacks, Eve intercepts the quantum states within the channel and substitutes them with fabricated particles of her own, which are then transmitted to the target user. Let's analyze why such attacks cannot succeed when considering the specific steps of our protocol. Specifically, Eve may intercept all the particles that Alice sends to Bob_i, then Eve generates fake particles in Z_d-basis and sends them to Bob_i. During this attack, when Bob_i performs the ***measure*** operation on the received particles, Eve's interference does not introduce errors. However, if Bob_i opts for ***reflect*** operations, Eve's attack will invariably introduce errors. This occurs because Eve lacks knowledge about the exact state of the particles sent by Alice, and the particles she prepares are all in Z_d-basis. In the scenario where Alice sends X_d-based particles and Bob_i chooses to ***reflect***, Eve's attack will be detected by Alice. If Eve launches the attack on a single particle, the probability that Eve will be detected is $1/8 = \frac{1}{2} \times \frac{1}{2} \times \frac{1}{2}$. When she conducts such attacks on l particles, her overall detection probability becomes $1 - (7/8)^l$. As l becomes sufficiently large, the probability of her detection tends toward 1. Therefore, Eve's Intercept-resend attack cannot succeed in our protocol.

4.1.2. Measure-resend attack

The Measure-resend attack is one of Eve's common tactics. In this type of attack, Eve intercepts transmitted particles, performs measurements on them, and then forwards the measured quantum states to the target user. Our protocol is also resilient against this form of attack. Specifically, if Eve conducts Z_d-basis measurements on the particles transmitted between Alice and Bob_i, and then forwards them to the target user, her attack does not introduce errors for particles in the Z_d-basis within the channel. However, for particles in the X_d-basis, Eve's measurements will inevitably disrupt the original state. If Eve carries out the attack on a single particle, the probability of her detection is $1/8$. When she executes such attacks on l particles, her overall probability of being detected increases to $1 - (7/8)^l$. As l grows larger, the probability of her discovery approaches 1. Consequently, it is virtually certain that Eve will be detected by Alice.

4.1.3. Collective attack

Collective attacks involve the use of entangled ancillary particles with the target particles, allowing Eve to obtain the state of the target particles by observing her ancillary particles. Compared to individual attacks on transmitted particles, collective attacks often yield a higher rate of success [29]. In this part, we will demonstrate the robustness of our protocol against collective attacks and provide a simplified evaluation using the key rate as a function of distance.

Since SQSS is a two-way communication protocol, the entire attack model can be expressed as two unitary operations U_E and U_F according to the analysis method in Reference [18]. Here, U_E and U_F are the attack operators applied to the particle sent between Alice and Bob_i, respectively. Eve entangles the auxiliary particles $|\vartheta\rangle$ on the target particles through U_E and U_F to obtain some useful information. Detailed analysis is shown below.

First consider the case where Eve uses U_E to attack the particles Alice sends to Bob_i. The effect of U_E on the particles $|0_d\rangle$, $|1_d\rangle$, $|+_d\rangle$, and $|-_d\rangle$ can be expressed as [26, 29]:

$$\begin{aligned} U_E|0_d\rangle|\vartheta\rangle &= \alpha_{00}|00\rangle|\vartheta_{00}\rangle + \alpha_{01}|01\rangle|\vartheta_{01}\rangle + \alpha_{10}|10\rangle|\vartheta_{10}\rangle + \alpha_{11}|11\rangle|\vartheta_{11}\rangle, \\ &= \sum_{k,j=0}^{1} \alpha_{k,j}|k,j\rangle|\vartheta_{k,j}\rangle \\ U_E|1_d\rangle|\vartheta\rangle &= \beta_{00}|00\rangle|\vartheta'_{00}\rangle + \beta_{01}|01\rangle|\vartheta'_{01}\rangle + \beta_{10}|10\rangle|\vartheta'_{10}\rangle + \beta_{11}|11\rangle|\vartheta'_{11}\rangle \\ &= \sum_{k,j=0}^{1} \beta_{k,j}|k,j\rangle|\vartheta'_{k,j}\rangle, \end{aligned} \tag{6}$$

and

$$\begin{aligned} U_E|+_d\rangle|\vartheta\rangle &= \frac{1}{\sqrt{2}}(U_E|0_d\rangle|\vartheta\rangle + U_E|1_d\rangle|\vartheta\rangle), \\ &= \frac{1}{\sqrt{2}}\left(\sum_{k,j=0}^{1}\alpha_{k,j}|k,j\rangle|\vartheta_{k,j}\rangle + \sum_{k,j=0}^{1}\beta_{k,j}|k,j\rangle|\vartheta'_{k,j}\rangle\right), \\ U_E|-_d\rangle|\vartheta\rangle &= \frac{1}{\sqrt{2}}(U_E|0_d\rangle|\vartheta\rangle - U_E|1_d\rangle|\vartheta\rangle) \\ &= \frac{1}{\sqrt{2}}\left(\sum_{k,j=0}^{1}\alpha_{k,j}|k,j\rangle|\vartheta_{k,j}\rangle - \sum_{k,j=0}^{1}\beta_{k,j}|k,j\rangle|\vartheta'_{k,j}\rangle\right), \end{aligned} \tag{7}$$

where $\sum_{k,j=0}^{1}\alpha_{k,j}^2 = 1, \sum_{k,j=0}^{1}\beta_{k,j}^2 = 1, \alpha_{k,j}$ and $\beta_{k,j}$ are normalization parameters that depend on U_E. After Bob_i received the particles, he will randomly choose ***measure*** or ***reflect*** operations.

We here first focus on the case where Bob_i chooses to ***measure*** operations on the Z_d-basis particles. In this case, Bob_i's measurements should be consistent with the initial particles sent by Alice. If Eve wants to pass the detection, the equation (6) must be satisfied that $\alpha_{00} = \alpha_{10} = \alpha_{11} = 0$ and $\beta_{00} = \beta_{01} = \beta_{11} = 0$. Thus, equation (6) and equation (7) can be rewritten as:

$$\begin{aligned} U_E|0_d\rangle|\vartheta\rangle &= |01\rangle|\vartheta_{0,1}\rangle = |0_d\rangle|\vartheta_{0,1}\rangle, \\ U_E|1_d\rangle|\vartheta\rangle &= |10\rangle|\vartheta'_{1,0}\rangle = |1_d\rangle|\vartheta'_{1,0}\rangle, \end{aligned} \tag{8}$$

and

$$\begin{aligned} U_E|+_d\rangle|\vartheta\rangle &= \frac{1}{\sqrt{2}}(|01\rangle|\vartheta_{0,1}\rangle + |10\rangle|\vartheta'_{1,0}\rangle), \\ U_E|-_d\rangle|\vartheta\rangle &= \frac{1}{\sqrt{2}}(|01\rangle|\vartheta_{0,1}\rangle - |10\rangle|\vartheta'_{1,0}\rangle). \end{aligned} \tag{9}$$

After that, Eve launches the second attack U_F on the particles sent by Bob_i. The effect of U_F can be expressed as [26, 29]:

$$\begin{aligned} U_F|0_d\rangle|\vartheta_{0,1}\rangle &= \sum_{g,h=0}^{1}\gamma_{g,h}|g,h\rangle|\vartheta_{g,h,0,1}\rangle, \\ U_F|1_d\rangle|\vartheta'_{1,0}\rangle &= \sum_{g,h=0}^{1}\zeta_{g,h}|g,h\rangle|\vartheta'_{g,h,1,0}\rangle, \end{aligned} \tag{10}$$

where $\sum_{g,h=0}^{1}\gamma_{g,h}^2 = 1, \sum_{g,h=0}^{1}\zeta_{g,h}^2 = 1, \gamma_{g,h}$ and $\zeta_{g,h}$ are normalization parameters that depend on U_F.

Above, we analyzed the situation where Bob_i chooses the ***measure*** operation; next, we consider the situation of ***reflect***, i.e., Cases 2 and 4. In these cases, Alice's measurement of the particle should be the same as the particle's initial state. Hence, to avoid introducing errors in U_F attack, the effect of U_F should satisfy: $\gamma_{00} = \gamma_{10} = \gamma_{11} = 0, \zeta_{00} = \zeta_{01} = \zeta_{11} = 0$ and $|\vartheta_{0,1,0,1}\rangle = |\vartheta'_{1,0,1,0}\rangle = |\hat{\vartheta}\rangle$. Combining equations (8), (9)and (10) we have

$$\begin{aligned} U_F U_E|0_d\rangle|\vartheta\rangle &= U_F|0,1\rangle|\vartheta_{0,1}\rangle = |01\rangle|\vartheta_{0,1,0,1}\rangle = |0_d\rangle|\hat{\vartheta}\rangle \\ U_F U_E|1_d\rangle|\vartheta\rangle &= U_F|1,0\rangle|\vartheta'_{1,0}\rangle = |10\rangle|\vartheta'_{1,0,1,0}\rangle = |1_d\rangle|\hat{\vartheta}\rangle, \end{aligned} \tag{11}$$

and

$$\begin{aligned} U_F U_E|+_d\rangle|\vartheta\rangle &= \frac{1}{\sqrt{2}}(|01\rangle|\vartheta_{0,1,0,1}\rangle + |10\rangle|\vartheta'_{1,0,1,0}\rangle), \\ &= \frac{1}{\sqrt{2}}(|0_d\rangle + |1_d\rangle)|\hat{\vartheta}\rangle = |+_d\rangle|\hat{\vartheta}\rangle, \\ U_F U_E|-_d\rangle|\vartheta\rangle &= \frac{1}{\sqrt{2}}(|01\rangle|\vartheta_{0,1,0,1}\rangle - |10\rangle|\vartheta'_{1,0,1,0}\rangle) \\ &= \frac{1}{\sqrt{2}}(|0_d\rangle - |1_d\rangle)|\hat{\vartheta}\rangle = |-_d\rangle|\hat{\vartheta}\rangle. \end{aligned} \tag{12}$$

From equations (11) and (12) it can be easily obtained that, regardless of whether the target particle is the Z_d-based or X_d-based particle, Eve's auxiliary particle is always $|\hat{\vartheta}\rangle$ after the attack of U_E and U_F, which means that Eve cannot get any information about the target particle from her auxiliary particle. Therefore, Eve's collective attack is ineffective against our protocol.

The above has analyzed the robustness of the protocol against collective attacks. Next, we will briefly discuss the protocol key rate. The key rate as a function of distance is an effective security analysis method derived from quantum key distribution (QKD) [30–32]. In our protocol, quantum user and 'classical' users interact using two sets of non-orthogonal states as information carriers, similar to the transmission mode of typical QKD protocols. Therefore, we attempt to employ the key rate versus distance function to provide a basic analytical evaluation of our protocol.

The key rate r in QKD can be determined using the Devetak-Winter bound, which provides a lower bound on the rate at which secret key bits can be distilled from shared quantum states. Similar to the analytical approach for QKD, in our protocol, for collective attacks, the key rate can be expressed as:

$$r \geqslant \max\{0,\, I(A\colon B) - \chi(B\colon E)\}, \tag{13}$$

where $I(A\colon B)$ is the mutual information between the legitimate parties Alice (A) and Bob$_i$ (B), $\chi(B\colon E)$ is the Holevo quantity, representing the upper bound on the information that the eavesdropper Eve (E) can obtain about Bob$_i$'s key. According to the semi-quantum cryptographic protocol based on two sets of non-orthogonal states as transmission particles, the key rate between quantum user and classical user can be derived as a function of the quantum bit error rate (QBER, denoted by Q) [33]. More specifically, the functional relationship between r and Q can be expressed as (considering the same error rate of X-basis and Z-basis):

$$r \geqslant (1 - Q)^2[1 - h(\lambda_1)] + 2Q(1 - Q) + Q^2, \tag{14}$$

where $\lambda_1 = \frac{1}{2} + \frac{Q^2 - 4Q + 1}{2(1-Q)^2}$, and $h(\lambda_1) = -\lambda_1 \log \lambda_1 - (1 - \lambda_1)\log(1 - \lambda_1)$.

As for QBER, it is a crucial parameter that depends on both the distance and the noise in the quantum channel [32]. Here, we simply assume that QBER can be modeled as :

$$Q = \frac{p_d}{p_{signal} + p_d - p_{signal}p_d}, \tag{15}$$

where p_d is the dark count rate, p_{signal} denotes the signal detection rate, and can be approximated by

$$p_{signal} = \mu t \eta, \tag{16}$$

where μ, t, and η indicate the quantum efficiency of the detector, transmitivity and the average number of emitted photons per pulse, respectively. The transmitivity of the fiber link is given by

$$t = 10^{\frac{-\alpha L}{10}}, \tag{17}$$

where L denotes the distance in km, α is the attenuation parameter. Using equations (14) to (17) a functional relationship between the key rate and distance can be established. Below, a calculation will be performed based on a simple parameter assumption. The relevant parameter settings refer to references [32, 34], and their values are assumed to be $p_d = 10^{-5}$, $\eta = 0.1$, $\alpha = 0.2$, $\mu = 0.3$. Therefore, the relationship between the key rate and the distance can be obtained, as shown in figure 2.

From figure 2, it can be observed that the maximum distance for establishing a key between the quantum user and the classical user is 130 km. Notably, due to the bidirectional communication of the SQSS protocol, the maximum channel distance between Alice and Bob$_i$ is 65 km. It should be noted that the method used here for calculating the key rate and transmission distance is relatively simple and still lags behind the well-established calculation frameworks of QKD protocols.

4.1.4. Trojan Horse attack

Since SQSS is a two-way protocol, it is vulnerable to Trojan Horse attacks. Eve may employ the Trojan horse attack to intercept private information. Therefore it is necessary to analyze this attack. Delay-photon attacks and invisible photon attacks are the two types of Trojan horse attacks. In order to resist these two attacks, it is necessary for the user to be equipped with the wavelength quantum filter and photon number discriminator. These two devices have been shown to be very resistant to Trojan attacks [35, 36].

4.2. Internal attack

Internal attacks pose a significant threat to the security of the SQSS protocol. In the context of the SQSS protocol, internal attacks refer to dishonest users attempting to recover Alice's key independently, without the assistance of other users.

Without loss of generality, here, we assume that Bob$_i$ is a dishonest user who wants to obtain Alice's secret information through attack methods. To obtain Alice's secret information, Bob$_i$ needs to gain access to the portion of Alice's secret information obtained by other users, which means Bob$_i$ needs to acquire the key, $K_{A_j}(i \neq j)$. Thus, Bob$_i$ may attempt to launch attacks on the particles transmitted between Alice and Bob$_j$. It's important to note that in our protocol, no particles are transmitted between Bob$_i$ and Bob$_j$. It's evident that Bob$_j$ is entirely independent of Bob$_i$, and, as a result, Bob$_i$ essentially functions as an external eavesdropper when

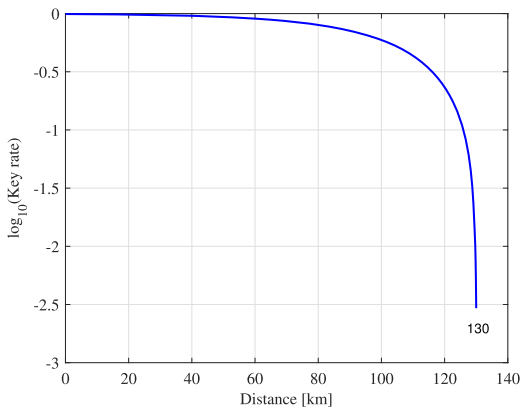


Figure 2. The relationship between key rate and distance of the SQSS protocol.

targeting the particles transmitted between Alice and Bob$_j$. Building on the analysis of external attacks presented above, Alice has a non-zero probability of detecting Bob$_i$'s attacks. Hence, our protocol is resilient against dishonest user's attacks.

5. Simulation

In this section, we use IBM's Qiskit to conduct circuit simulations of the proposed SQSS protocol to verify the correctness and feasibility of the protocol. For the sake of simplicity, we omit the considerations of eavesdropping or attacks in the following procedures. This is a typical assumption in the simulation phase of semi-quantum cryptographic protocols. In the subsequent simulation stage, we will use the operational process between Alice and Bob$_i$ as an illustrative example. Furthermore, in the simulation result graphs below, the horizontal axis represents the measurement outcomes in the Z-basis, while the vertical axis indicates the frequency of each measurement outcome. Each experiment was simulated 1024 times.

5.1. Simulation for the SQSS against collective dephasing noises

Before starting the simulation experiment, it is essential to provide an introduction to the fundamental settings, which encompass the preparation and measurement of initial logic qubits, simulation of channel noise, and so on. The preparation and measurement of DF states $\{|0_d\rangle, |1_d\rangle, |+_d\rangle, |-_d\rangle\}$ are shown below (also see figure 3). Here, we all start from the initial state $|00\rangle$ to prepare the corresponding quantum state:

$$\begin{aligned} &|00\rangle_{12} \xrightarrow{I_1\otimes X_2} |0_d\rangle, \quad |00\rangle_{12} \xrightarrow{X_1\otimes I_2} |1_d\rangle, \\ &|00\rangle_{12} \xrightarrow{H_1\otimes X_2\otimes CNOT_{12}} |+_d\rangle, \quad |00\rangle_{12} \xrightarrow{X_1\otimes X_2\otimes H_1\otimes CNOT_{12}} |-_d\rangle, \end{aligned} \tag{18}$$

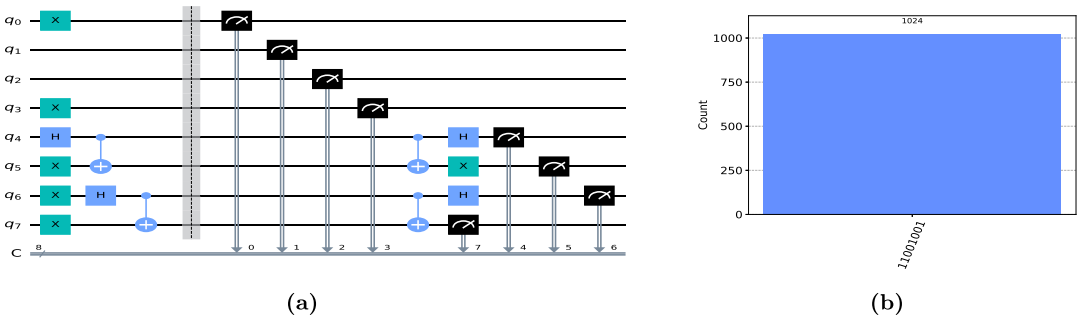
where the subscript 1 and 2 denote the position of the particles, I, H and $CNOT$ represent the I-gate, Hadamard-gate and Control-Not-gate, respectively. Then, in order to better distinguish these quantum states during circuit simulation, we also made corresponding adjustments during Alice's measurement so that each quantum state corresponds to a certain measurement result. The details are as follows:

$$\begin{aligned} &|0_d\rangle \rightarrow |01\rangle, \quad |1_d\rangle \rightarrow |10\rangle, \\ &|+_d\rangle \xrightarrow{CNOT_{12}\otimes X_2\otimes H_1} |00\rangle, \quad |-_d\rangle \xrightarrow{CNOT_{12}\otimes H_1} |11\rangle. \end{aligned} \tag{19}$$

In addition, according to literature [26], collective dephasing noise can be simulated by RZ operation. For convenience, we assume that the channel noise between Alice and Bob is $RZ(\pi/3)$, that is, the phase remains unchanged when $|0\rangle$ passes through the channel, and when $|1\rangle$ passes through the channel, the phase will change $e^{i\pi/3}$.

In the following, we validate the simulation by incorporating the specific steps of the protocol. Assuming that the Z_d-based particles and X_d-based particles prepared by Alice correspond to $|0_d\rangle$ and $|+_d\rangle$, respectively. Then the quantum circuits according to the steps of the protocol are depicted in figure 4. In this circuit, Alice prepares $|0_d\rangle, |+_d\rangle, |0_d\rangle, |+_d\rangle$ and sends them to Bob$_i$. Then, Bob$_i$ respectively performs ***measure*** and ***reflect*** operations on these particles. Eventually, Alice performs measurements on different bases depending on Bob$_i$'s operations.

To demonstrate the circuit's correctness, the circuit was simulated 1024 times, and the results are shown in figure 5. From the figure 5, we can see that Bob$_i$'s measurement results are distributed between 0101 and 1001,



(a) (b)

Figure 3. Quantum circuit diagrams for preparation and measurement of quantum states resistant to collective dephasing noise. Registers (q_0, q_1), (q_2, q_3), (q_4, q_5) and (q_6, q_7) are used to prepare $|0_d\rangle$, $|1_d\rangle$, $|+_d\rangle$ and $|-_d\rangle$ respectively. From the measurement results, it can be seen that $|0_d\rangle$, $|1_d\rangle$, $|+_d\rangle$ and $|-_d\rangle$ correspond to 01, 10, 00 and 11, respectively.

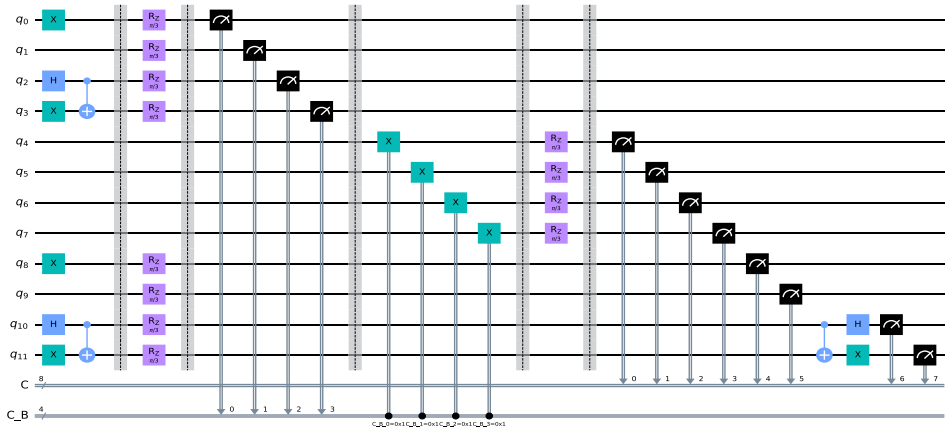


Figure 4. Schematic diagram of the resistant collective dephasing noise protocol quantum circuit, where registers (q_0, q_1, q_2, q_3) and $(q_8, q_9, q_{10}, q_{11})$ are in Alice's hands for the preparation of the initial quantum states $|0_d\rangle$, $|+_d\rangle$, $|0_d\rangle$, $|+_d\rangle$; and registers (q_4, q_5, q_6, q_7) are in Bob$_i$'s hands for the preparation of the particles that are sent to Alice after ***measure*** operation. In this circuit, Bob$_i$ performs ***measure*** operation on the (q_0, q_1, q_2, q_3).

where the leftmost two bits record the results of Bob$_i$'s Z_d-based measurements on the $|+_d\rangle$, while the next 2 bits record the results of Bob$_i$'s Z_d-based measurements on the $|0_d\rangle$. From the simulation results, the measurements are consistent with the setup of the protocol steps. Then for the Alice's measurements, her results are distributed between 00 010 101 and 00 011 001. These 8 bits respectively record the measurement results of the particles corresponding to $q_{11}, q_{10}, q_9, \ldots, q_4$. For example, with respect to registers q_{11} and q_{10}, they are used to prepare qubit $|+_d\rangle$. In the circuit shown in figure 4, Bob$_i$ performed a ***reflect*** operation on them, and accordingly, Alice's measurement results are 00, which aligns with the simulated results. Therefore, the simulation results meet the protocol requirements, demonstrating that the channel noise does not affect the final results.

5.2. Simulation for the SQSS against collective rotation noises

Similar to the analysis in section 5.1, here we first explain the preparation and measurement of basic quantum carriers, i.e., $|0_r\rangle$, $|1_r\rangle$, $|+_r\rangle$, $|-_r\rangle$ and noise simulation. We also start from the initial state $|00\rangle$ to prepare the corresponding quantum states (the detailed circuits are shown in figure 6):

$$\begin{aligned}
|00\rangle_{12} &\xrightarrow{H_1\otimes I_2\otimes CNOT_{12}} |0_r\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle),\\
|00\rangle_{12} &\xrightarrow{X_1\otimes X_2\otimes H_1\otimes CNOT_{12}} |1_r\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle),\\
|00\rangle_{12} &\xrightarrow{H_1\otimes X_2\otimes CNOT_{12}\otimes H_1} |+_r\rangle,\\
|00\rangle_{12} &\xrightarrow{X_1\otimes H_1\otimes CNOT_{12}\otimes H_1} |-_r\rangle.
\end{aligned} \tag{20}$$

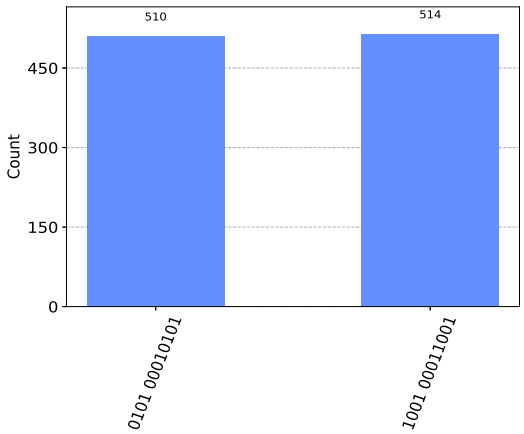


Figure 5. Simulation results of the protocol circuit. The first 4 bits of the measurement result represent Bob$_i$'s measurement result , while the last 8 bits represent Alice's measurement result.

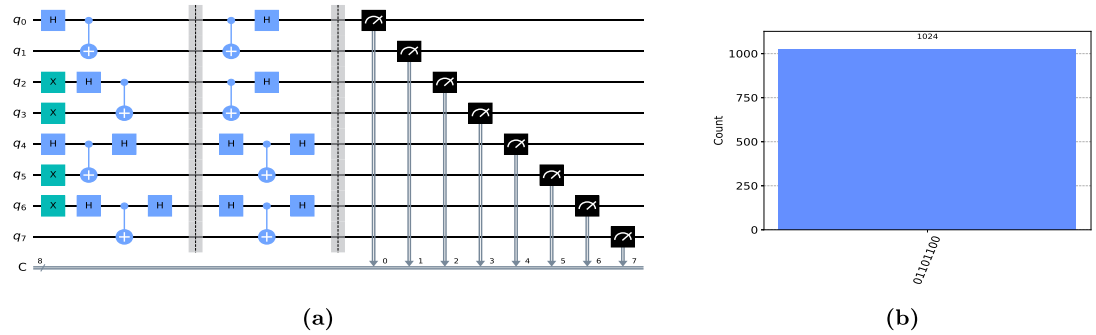


Figure 6. Quantum circuit diagrams for preparation and measurement of qubits resistant to collective rotation noise. Registers (q_0, q_1), (q_2, q_3), (q_4, q_5) and (q_6, q_7) are used to prepare $|0_r\rangle$, $|1_r\rangle$, $|+_r\rangle$ and $|-_r\rangle$ respectively. From the measurement results, it can be seen that $|0_r\rangle$, $|1_r\rangle$, $|+_r\rangle$ and $|-_r\rangle$ correspond to 00, 11, 10 and 01, respectively.

We also made corresponding adjustments during Alice's measurement so that each quantum state corresponds to a certain measurement result. The details are as follows:

$$\begin{aligned} &|0_r\rangle \xrightarrow{CNOT_{12}\otimes H_1} |00\rangle, \quad |1_r\rangle \xrightarrow{CNOT_{12}\otimes H_1} |11\rangle, \\ &|+_r\rangle \xrightarrow{H_1\otimes CNOT_{12}\otimes H_1} |10\rangle, \quad |-_r\rangle \xrightarrow{H_1\otimes CNOT_{12}\otimes H_1} |01\rangle. \end{aligned} \tag{21}$$

Therefore, the computational basis measurement of the above four states (i.e., $|0_r\rangle$, $|1_r\rangle$, $|+_r\rangle$, $|-_r\rangle$) can correspond to four distinct measurement outcomes, allowing for clearer differentiation.

Moreover, the collective rotation noise can be simulated by RY operation [26]. For convenience, we assume that the channel noise between Alice and Bob is $RY(\pi/3)$. That is, after $|0\rangle$ passes through the collective rotation channel, its status will become $\cos(\pi/3)|0\rangle + \sin(\pi/3)|1\rangle$, while $|1\rangle$ passes through the channel, the state will become $-\sin(\pi/3)|0\rangle + \cos(\pi/3)|1\rangle$.

A specific quantum circuit is given below to verify the correctness of the protocol. Suppose Alice prepares $|0_r\rangle$, $|1_r\rangle$, $|0_r\rangle$, $|+_r\rangle$ and then sends them to Bob$_i$. For the received qubits, Bob$_i$ respectively performs ***measure***, ***measure***, ***reflect***, ***reflect*** operations. Then, Alice performs the corresponding measurements based on Bob$_i$'s operations. The detailed quantum circuit is shown in figure 7.

To confirm the validity of the protocol circuit, we also conducted 1024 simulations, and the results are shown in figure 8. Based on the experimental outcomes, Alice's measurements for the particles (i.e., $|0_r\rangle$ and $+_r\rangle$) directly reflect by Bob$_i$, are always 00 and 10, respectively. This aligns with the conditions outlined in equation (21) and meets the requirements of the protocol. It is evident that the first two bits of Bob$_i$'s measurement results record his measurements on the register (q_3, q_2), i.e., $|1_r\rangle$, while the next two bits record his measurements on the register (q_1, q_0), i.e., $|0_r\rangle$. Furthermore, the distribution of Bob$_i$'s first two bits is 01 and 10, and the distribution of the last two bits is 00 and 11. Based on the above measurement results, Bob$_i$ can infer that the particles sent by Alice are $|0_r\rangle$ and $1_r\rangle$, which is consistent with the configuration of the protocol. Therefore,

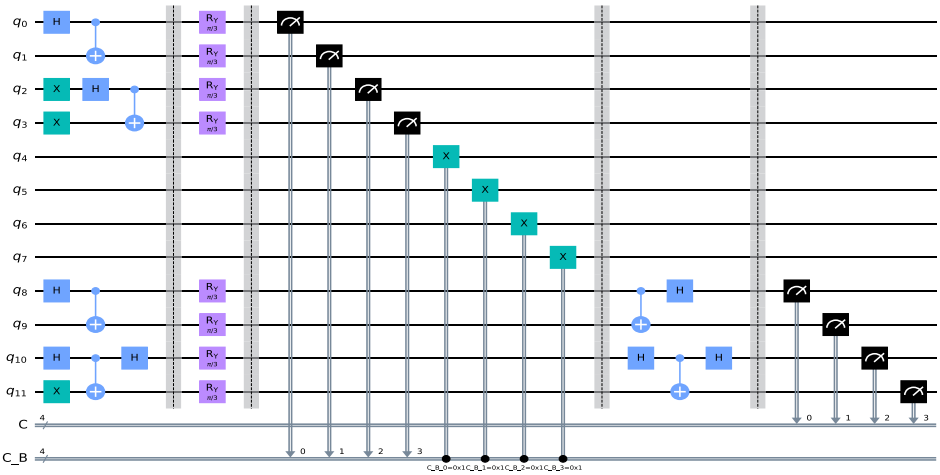


Figure 7. Schematic diagram of the resistant collective rotation noise protocol quantum circuit, where registers (q_0, q_1, q_2, q_3) and (q_8, q_9, q_{10}, q_{11}) are in Alice's hands for the preparation of the initial quantum states $|0_r\rangle$, $|1_r\rangle$, $|0_r\rangle$, $|+_r\rangle$; and registers (q_4, q_5, q_6, q_7) are in Bob$_i$'s hands for the preparation of the particles that are sent to Alice after ***measure*** operation. In this circuit, Bob$_i$ performs ***measure*** operation on the (q_0, q_1, q_2, q_3).

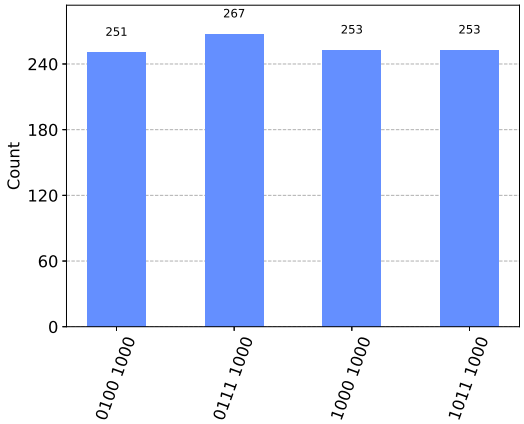


Figure 8. Simulation results of the protocol circuit. The first 4 bits of the measurement result represent Bob$_i$'s measurement result (i.e., the outcomes of the register q_3, q_2, q_1, q_0), while the last 4 bits represent Alice's measurement result (i.e., the outcomes of the register q_{11}, q_{10}, q_9, q_8).

the simulation results meet the protocol requirements, demonstrating that the channel noise does not affect the final results.

In summary, the circuit simulation results show that our protocol is resistant to collective dephasing noise and collective rotation noise and is feasible under current technology.

6. Discussion and conclusion

In this section, we discuss and summarize the work in this paper. We first discuss our proposed protocols with related existing work, including both quantum cryptography [17–24] and non-quantum cryptography solutions [37–39].

Compared to the secret sharing schemes based on classical encryption [37–39], our protocols have the property of resisting quantum attacks. Its security remains uncompromised even as attackers enhance their computational power, ensuring the security of the sharing protocol. In other words, secret sharing schemes with traditional cryptographic regimes fail to address the long-term security concerns, while quantum-cryptographic-based schemes offer prolonged security protection.

In comparison to sharing schemes based on semi-quantum cryptography [17–24], our protocols exhibit advantages in noise resistance, sharing specific information, and scalability, as illustrated in figure 9. Specifically,

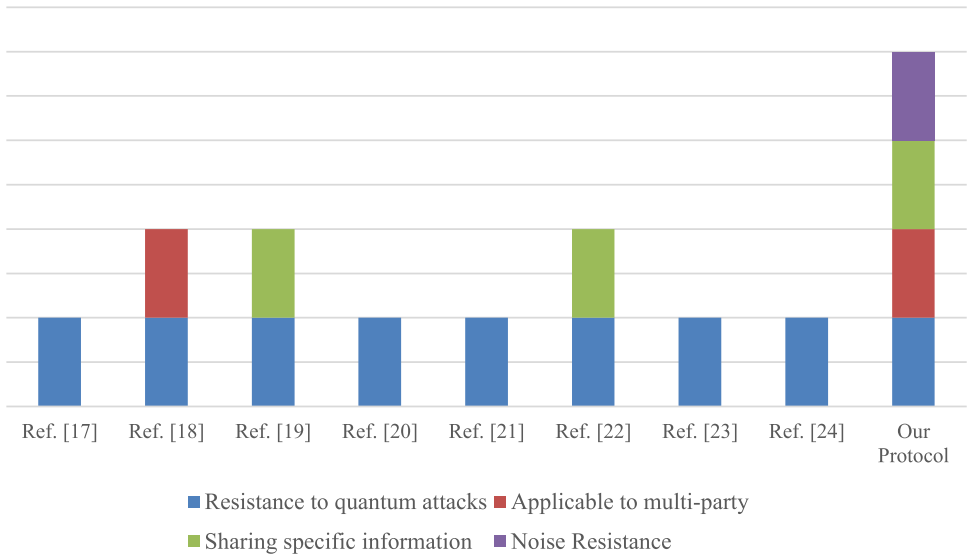


Figure 9. Comparison chart with related SQSS protocols. From the graph, it is evident that our protocols have advantages in terms of noise resistance, sharing specific information, and suitability for multi-party scenarios. It is applicable to multi-party secret sharing in noisy environments, unlike previous protocols that were limited to ideal conditions and two-party scenarios.

in terms of noise resistance, previous similar protocols, have only considered the ideal environment, i.e., the required quantum channel is free of noise interference. In reality, however, there is bound to be noise in the channel, and the noise interferes with the correctness and feasibility of the protocol. Our approach, grounded in the decoherence-free states, effectively counteracts the impact of collective dephasing noise and collective rotation noise on protocol performance. Compared to previous protocols our protocols are more suitable for practical situations.

On the other hand, regarding shared information, our SQSS protocols have the capability to share deterministic information. Multiple classical users, through collaborative efforts, can reconstruct specific secret information. In contrast, the majority of previous SQSS protocols shared random information, lacking the ability to determine the information beforehand. This imposes certain limitations in practical applications, such as in healthcare or finance, where the information to be shared is typically deterministic rather than random. Thus, our protocols hold advantages in terms of sharing specific information.

Finally, our protocols can be applied to multi-party scenarios, unlike previous protocols that are mostly limited to two-party scenarios, which limits the scope of the protocol. We also perform circuit simulations of the protocol using IBM Qiskit, and the simulation results show that our protocols are correct and feasible under current quantum technology. Therefore, compared to previous SQSS protocols, our protocol may have better results in practical applications, especially in environments where privacy protection and resistance to noise interference are required.

In conclusion, we offer a concise overview of this paper. In this work, we give an approach to achieve collective noise-resistant semi-quantum secret sharing to ensure secure data sharing among different users in noisy environments. By utilizing DF states as information carriers, the proposed protocols can resist collective dephasing noise and collective rotation noise, respectively. In comparison to previous secret sharing schemes relying on classical encryption, our protocols demonstrate the ability to withstand long-term security threats, mitigating vulnerabilities posed by advancements in computational power. In terms of existing SQSS protocols, our protocols have advantages in resisting noise interference and being suitable for multi-party scenarios. Security analysis and circuit simulations indicate that the proposed protocol is feasible under current technological conditions. Importantly, our protocol eliminates the necessity for all devices to possess full quantum capabilities, thereby significantly reducing dependence on complex quantum resources. This distinctive feature may contribute to the broader adoption of quantum technologies in information interaction systems.

Furthermore, there are many intriguing issues regarding semi-quantum secret sharing schemes that need further exploration. For instance, simulating the impact of attack methods, attack frequencies, and durations during the quantum simulation phase remains a significant challenge. Additionally, the analysis of the secret key rate for SQSS protocols requires more research. Currently, it falls short of the detailed and rigorous parameter setting and analysis seen in QKD protocols. Investigating these issues will provide a more in-depth understanding of the protocol's performance.

Acknowledgments

This work was supported in part by the Key Research and Development Program of Ningxia Hui Autonomous Region, grant number '2021BEG02007' and the Open Research Fund of Key Laboratory of Cryptography of Zhejiang Province, grant number 'No. ZCL21006'.

Data availability statement

The data cannot be made publicly available upon publication because no suitable repository exists for hosting data in this field of study. The data that support the findings of this study are available upon reasonable request from the authors.

Conflict of interest

The authors have no relevant financial or non-financial interests to disclose.

ORCID iDs

Chong-Qiang Ye https://orcid.org/0000-0003-0282-1155
Wang Zhuo https://orcid.org/0000-0003-4852-5757

References

[1] Hu X M *et al* 2023 Progress in quantum teleportation *Nature Reviews Physics* **5** 339–53
[2] Pirandola S *et al* 2020 Advances in quantum cryptography *Advances in Optics and Photonics* **12** 1012–236
[3] Feng Y *et al* 2022 SKC-CCCO: an encryption algorithm for quantum group signature *Quantum Inf. Process.* **21** 328
[4] Ye C Q *et al* 2023 Measurement-based quantum sealed-bid auction *IEEE Transactions on Circuits and Systems I: Regular Papers* **70** 5352–65
[5] Shi J *et al* 2023 Chaotic image encryption based on boson sampling *Advanced Quantum Technologies* **6** 2200104
[6] Feng Y *et al* 2019 Arbitrated quantum signature scheme with quantum walk-based teleportation *Quantum Inf. Process.* **18** 1–21
[7] Ye T Y *et al* 2022 Efficient semiquantum key distribution based on single photons in both polarization and spatial-mode degrees of freedom *Quantum Inf. Process.* **21** 123
[8] Xu F *et al* 2020 Secure quantum key distribution with realistic devices *Rev. Mod. Phys.* **92** 025002
[9] Cao Y *et al* 2022 The evolution of quantum key distribution networks: On the road to the qinternet *IEEE Communications Surveys & Tutorials* **24** 839–94
[10] Nikmehr N, Zhang P and Bragin M A 2022 Quantum distributed unit commitment: an application in microgrids *IEEE Trans. Power Syst.* **37** 3592–603
[11] Liao Q *et al* 2021 Quantum secret sharing using discretely modulated coherent states *Phys. Rev.* A **103** 032410
[12] Gu J *et al* 2021 Differential phase shift quantum secret sharing using a twin field *Opt. Express* **29** 9165–73
[13] Shen A *et al* 2023 Experimental quantum secret sharing based on phase encoding of coherent states *Science China Physics, Mechanics & Astronomy* **66** 260311
[14] Cheng C *et al* 2017 Securing the Internet of Things in a quantum world *IEEE Commun. Mag.* **55** 116–20
[15] Córcoles A D *et al* 2019 Challenges and opportunities of near-term quantum computing systems *Proc. IEEE* **108** 1338–52
[16] Iqbal H and Krawec W O 2020 Semi-quantum cryptography *Quantum Inf. Process.* **19** 1–52
[17] Li Q, Chan W H and Long D Y 2010 Semiquantum secret sharing using entangled states *Phys. Rev.* A **82** 022303
[18] Li L, Qiu D and Mateus P 2013 Quantum secret sharing with classical Bobs *J. Phys. A: Math. Theor.* **46** 045304
[19] Xie C, Li L and Qiu D 2015 A novel semi-quantum secret sharing scheme of specific bits *Int. J. Theor. Phys.* **54** 3819–24
[20] Ye C Q and Ye T Y 2018 Circular semi-quantum secret sharing using single particles *Commun. Theor. Phys.* **70** 661
[21] Ye C Q *et al* 2019 Multiparty semi-quantum secret sharing with d-level single-particle states *Int. J. Theor. Phys.* **58** 3797–814
[22] Tian Y *et al* 2021 An efficient semi-quantum secret sharing protocol of specific bits *Quantum Inf. Process.* **20** 217
[23] Chen Y and Ye T Y 2022 Semiquantum secret sharing by using χ-type states *The European Physical Journal Plus* **137** 1331
[24] Tian Y *et al* 2023 A semi-quantum secret-sharing protocol with a high channel capacity *Entropy* **25** 742
[25] Amer O and Krawec W O 2019 Semiquantum key distribution with high quantum noise tolerance *Phys. Rev.* A **100** 022319
[26] Gong L H *et al* 2023 Robust multi-party semi-quantum private comparison protocols with decoherence-free states against collective noises *Advanced Quantum Technologies* **6** 2300097
[27] Tang Y H *et al* 2022 Robust semi-quantum private comparison protocols against collective noises with decoherence-free states *Quantum Inf. Process.* **21** 97
[28] Li X H, Deng F G and Zhou H Y 2008 Efficient quantum key distribution over a collective noise channel *Phys. Rev.* A **78** 022321
[29] Ye C Q *et al* 2023 A feasible semi-quantum private comparison based on entanglement swapping of Bell states *Physica* A **625** 129023
[30] Scarani V *et al* 2009 The security of practical quantum key distribution *Rev. Mod. Phys.* **81** 1301–50
[31] Xu F *et al* 2020 Secure quantum key distribution with realistic devices *Rev. Mod. Phys.* **92** 025002
[32] Martinez-Mateo J, Elkouss D and Martin V 2013 Key reconciliation for high performance quantum key distribution *Sci. Rep.* **3** 1576
[33] Iqbal H and Krawec W O 2020 Semi-quantum cryptography *Quantum Inf. Process.* **19** 97
[34] Anisimova E *et al* 2021 A low-noise single-photon detector for long-distance free-space quantum communication *EPJ Quantum Technology* **8** 23
[35] Deng F G *et al* 2005 Improving the security of multiparty quantum secret sharing against Trojan horse attack *Phys. Rev.* A **72** 044302

[36] Lucamarini M et al 2015 Practical security bounds against the trojan-horse attack in quantum key distribution *Phys. Rev.* X **5** 031030
[37] Tang Z 2021 Secret sharing-based IoT text data outsourcing: A secure and efficient scheme *IEEE Access* **9** 76908–20
[38] Yuan B et al 2020 Secure data transportation with software-defined networking and kn secret sharing for high-confidence IoT services *IEEE Internet of Things Journal* **7** 7967–81
[39] Shivhare A et al 2022 A secret sharing-based scheme for secure and energy efficient data transfer in sensor-based IoT *The Journal of Supercomputing* **78** 17132–49