

Letter

Multi-party semi-quantum secret sharing protocol based on measure-flip and reflect operations

Jian Li^{1,3} and Chong-Qiang Ye^{2,*}¹ School of Information Engineering, Ningxia University, Yinchuan 750021, People's Republic of China² School of Artificial Intelligence, Beijing University of Posts Telecommunications, Beijing 100876, People's Republic of China³ Information Security Center, State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing 100876, People's Republic of ChinaE-mail: chongqiangye@bupt.edu.cn

Received 7 May 2024

Accepted for publication 13 May 2024

Published 30 May 2024

**Abstract**

Semi-quantum secret sharing (SQSS) protocols serve as fundamental frameworks in quantum secure multi-party computations, offering the advantage of not requiring all users to possess intricate quantum devices. However, current SQSS protocols mainly cater to bipartite scenarios, with few protocols suitable for multi-party scenarios. Moreover, the multi-party SQSS protocols face limitations such as low qubit efficiency and inability to share deterministic secret information. To address this gap, this paper proposes a multi-party SQSS protocol based on multi-particle GHZ states. In this protocol, the quantum user can distribute the predetermined secret information to multiple classical users with limited quantum capabilities, and only through mutual cooperation among all classical users can the correct secret information be reconstructed. By utilizing measure-flip and reflect operations, the transmitted multi-particle GHZ states can all contribute keys, thereby improving the utilization of transmitted particles. Then, security analysis shows that the protocol's resilience against prevalent external and internal threats. Additionally, employing IBM Qiskit, we conduct quantum circuit simulations to validate the protocol's accuracy and feasibility. Finally, compared to similar studies, the proposed protocol has advantages in terms of protocol scalability, qubit efficiency, and shared message types.

Keywords: semi-quantum secret sharing (SQSS), multi-party, measure-flip, efficiency

1. Introduction

Quantum cryptography, whose security is based on quantum laws, contrarily, classical cryptography usually relies on computational complexity assumptions, which is vulnerable to a computationally unbounded adversary. In recent years, many

important advances have been made in the field of quantum cryptography [1–4].

Quantum secret sharing (QSS) [5] is one of the fundamental applications in quantum cryptography. It aims to allow the sharing of secrets held by a server among multiple participants, with the capability to recover the secret when a sufficient number of participants collaborate. QSS can be regarded as the quantum counterpart of classical secret sharing protocols, designed to enhance protocol security and withstand threats from quantum adversaries. Therefore, QSS has

* Author to whom any correspondence should be addressed.

attracted considerable attention from researchers and has been continuously explored and studied. Many significant research findings have been proposed in this field [6–10]. Moreover, due to its ability to satisfy the requirements of multi-user secret sharing, QSS can be applied to scenarios of quantum secure multiparty computation. Serving as a foundational module, QSS can facilitate the construction of secure multiparty computation protocols with various functions, such as quantum sealed-bid auction [11–13] and quantum summation [14–17].

Although the aforementioned quantum protocols have advantages in terms of security, they all require users in the protocol to have complete quantum capabilities, resulting in significant quantum overhead for the protocol users. However, in the current scenario where quantum resources are insufficient, not all users can access an adequate amount of quantum resources [1]. In reality, most users are unable to afford the burden of complex quantum state preparation and measurement operations. Fortunately, Boyer *et al* [18, 19] proposed the idea of semi-quantum, which provides a solution for the high cost of quantum resources. In semi-quantum protocols, typically only one user needs to possess full quantum capabilities, while the quantum capabilities of other users are restricted to performing simple operations. These users with restricted capabilities are also referred to as ‘classical’ users. They can only carry out computational basis (i.e. $\{|0\rangle, |1\rangle\}$) state preparation and measurements, direct reflect, as well as reordering operations. Semi-quantum protocols reduce the dependency of users on quantum resources, thus attracting widespread attention from researchers. Current research in the field of semi-quantum cryptography includes semi-quantum key distribution [20–25], semi-quantum secure direct communication [26–29], semi-quantum secret sharing (SQSS) [30–39], semi-quantum secure multi-party computation [40–42], and more. Readers can refer to [43] for a detailed overview of semi-quantum cryptography.

The concept of SQSS was first introduced by Li *et al* [30] in 2010. In SQSS, the quantum user, Alice, possesses full quantum capabilities and aims to share secret information with ‘classical’ users, Bob and Charlie. Only through mutual cooperation between Bob and Charlie can Alice’s secret information be recovered. Subsequently, various types of SQSS protocols have been proposed [31–39]. For example, in 2015, Xie *et al* [31] introduced a novel SQSS protocol where the quantum party can share specific messages with classical parties instead of random messages. In 2023, Xing *et al* [32] achieved an SQSS protocol capable of sharing deterministic information using single photons. Later, Hu *et al* [33] utilized high-dimensional quantum states as information carriers to design SQSS protocol, extending the protocol to the high-dimensional scenarios. Recently, He *et al* [34] pointed out that the protocol based on single particle states proposed by Tian *et al* [35] in 2021 that can share certain secret information has security vulnerabilities, and gave an improved method. In 2024, Hou *et al* [36] devised an SQSS protocol combining single-particle states and GHZ states with a circular transmission mode. Most of the aforementioned protocols are applicable only to two-party scenarios, meeting the requirement

for secret sharing between two ‘classical’ users. In practical scenarios, the number of users sharing secret information is often random and more than two. Multi-party SQSS protocols, which are more in line with real-world situations, have become a research hotspot. Currently, several multi-party SQSS protocols have been proposed [37–39], which can share random secret information among multiple ‘classical’ users.

However, due to the limitations of ‘classical’ users’ capabilities in semi-quantum protocols, multi-party SQSS protocols exhibit significant efficiency disadvantages. In more detail, in previous SQSS protocols, only particles measured by ‘classical’ users could serve as the basis for establishing mutual keys, while directly reflected particles could only be utilized for eavesdropping. Moreover, to ensure the security of shared secret information, the operations performed by ‘classical’ users on received particles were random. Only when certain conditions were met among users (such as all users measuring the particles in computational basis), it could be used to construct the final secret information. As the number of users increases, satisfying these conditions becomes more stringent. For example, if there are n users, the probability of this situation occurring, where they all choose to measure operations, will be $1/2^n$. This leads to the need for more quantum states, resulting in a significant decrease in protocol efficiency. The low qubit efficiency is the main reason to limit the development of multi-party semi-quantum protocols. Therefore, effectively using the transmitted particles as the secret keys becomes particularly important.

Currently, multi-party SQSS protocols [37–39] also grapple with the challenge of low protocol efficiency, as well as the fact that the shared keys are random rather than deterministic. These issues pose difficulties in meeting the practical demand for secret sharing in real-world scenarios.

To address these issues, this work proposes a novel multi-party semi-quantum secret sharing protocol (MSQSS) based on $(n + 1)$ -qubit GHZ states. Using measure-flip and reflect operations, ‘classical’ users can encode secret information onto quantum carriers by altering or maintaining the state of the receiving particles. In the proposed protocol, the transmitted multi-particle GHZ states can all contribute to the key, thereby enhancing the utilization efficiency of the transmitted particles. In addition to GHZ states, the protocol also requires some decoy states (i.e. $\{|0\rangle, |1\rangle, |-\rangle, |+\rangle\}$) to be randomly inserted into GHZ state particles as decoy states to ensure the security of transmitted particles. Security analysis shows that the protocol can withstand typical external and internal attacks. Furthermore, to verify the feasibility of the protocol, we also conducted circuit simulations. Compared to previous protocols, our protocol has advantages in terms of qubit efficiency, protocol scalability, and types of shared messages.

The remaining organization is shown below. Section 2 introduces the basic settings of the protocol and properties of $(n + 1)$ -qubit GHZ states. Section 3 provides a detailed illustration of the proposed protocol. Subsequently, in section 4, we analyze the security of the proposed protocol. In section 5, we conduct circuit simulation and discussion. Finally, in section 6 we perform a summary of the protocol.

2. Preliminary knowledge

In this part, we will introduce the basic requirements of the protocol and the quantum resources used by the protocol.

The first is an introduction to the basic settings of the proposed MSQSS protocol. In our protocol, quantum user, Alice, wants to share specific messages $K(k_1, k_2, \dots, k_L)$ with n classical Bob_{*i*} ($i = 1, 2, \dots, n$). For the secret information K shared by Alice, the correct secret information can only be recovered when all ‘classical’ users cooperate with each other. No single user can independently recover K . Here, Bob_{*i*} is limited to the following operations:

- (1) **Measure-flip**: measure the qubit in basis $\{|0\rangle, |1\rangle\}$ and regenerate one in the opposite state (e.g. $|0\rangle \rightarrow |1\rangle, |1\rangle \rightarrow |0\rangle$).
- (2) **Reflect**: reflect the qubit directly.
- (3) **Reorder**: reorder the qubit via delay lines.

Then we introduce the quantum resources used in the protocol. In our protocol, $(n+1)$ -qubit GHZ states play a crucial role as key transmission particles, facilitating the interaction of information between quantum user and classical users. According to the description in [44], it can be represented as:

$$|G_k^\pm\rangle = \frac{1}{\sqrt{2}} (|0a_1a_2\dots a_n\rangle \pm |1\bar{a}_1\bar{a}_2\dots \bar{a}_n\rangle), \quad (1)$$

where $k \in \{0, 1, \dots, 2^n - 1\}$, and $0a_1a_2\dots a_n$ is the binary representation of k in an $(n+1)$ -bit string, i.e. $k = \sum_{i=1}^n a_i \times 2^{n-i}$. Note that \bar{a}_i and a_i satisfy the relationship of $\bar{a}_i \oplus a_i = 1$, where $i = 1, 2, \dots, n$. For a single-qubit measurement on the $(n+1)$ -qubit GHZ state, we will randomly get $0a_1a_2\dots a_n$ or $1\bar{a}_1\bar{a}_2\dots \bar{a}_n$. Then the value of k can be calculated based on the measurement results. Specifically, if the measurement result of the first qubit is 0, the measurement results of the remaining qubits are equivalent to the binary expansion of k . If the measurement result of the first qubit is 1, then the measurement results of the remaining qubits, after being flipped, are equivalent to the binary sequence of k .

Furthermore, for states $|G_k^+\rangle$ and $|G_{k'}^+\rangle = \frac{1}{\sqrt{2}}(|0a'_1a'_2\dots a'_n\rangle + |1\bar{a}'_1\bar{a}'_2\dots \bar{a}'_n\rangle)$, we have

$$\langle G_k^+ | G_{k'}^+ \rangle = \delta_{k,k'}, \quad (2)$$

where $\delta_{k,k'}$ is an impulse function, and $k = \sum_{i=1}^n a_i \times 2^{n-i}$, $k' = \sum_{i=1}^n a'_i \times 2^{n-i}$. Only when k equals k' , are states $|G_k^+\rangle$ and $|G_{k'}^+\rangle$ the same. If any qubit changes, it will cause $k \neq k'$, thus it can be further concluded that states $|G_k^+\rangle$ and $|G_{k'}^+\rangle$ are different.

Let $r_i = a_i \oplus a'_i$, then the values of k and k' can be connected through r_i . As long as any two of them are known, the other can be derived. For example, if k' (i.e. $a'_1a'_2\dots a'_n$) and r_i are known, then k can be derived as follows

$$\begin{aligned} k &= (a'_1 \oplus r_1) \times 2^{n-1} + (a'_2 \oplus r_2) \times 2^{n-2} + \dots + (a'_n \oplus r_n) \times 2^0 \\ &= a_1 \times 2^{n-1} + a_2 \times 2^{n-2} + \dots + a_n \times 2^0. \end{aligned} \quad (3)$$

The protocol settings and information carriers have been introduced above. Now let us delve into the core idea of the protocol. In this paper, ‘classical’ users encode information by altering the state of the receiving particles or keeping it unchanged through the utilization of **Measure-flip** and **Reflect** operations. Furthermore, for a multi-particle GHZ state $|G_k^+\rangle$, any change in the qubits will result in a change in the value of k . Thus, ‘classical’ users can establish a relationship between the changes in k and the two different operations employed. By analyzing the operation information and the corresponding changes in k values after the quantum state changes, the initial k value, representing the secret information to be shared by the quantum user, can be deduced. Unlike previous protocols that rely on measurement outcomes as keys, this protocol establishes keys among users by utilizing operations performed by ‘classical’ users.

3. The proposed MSQSS protocol

In this section, we will give the specific steps of the protocol and analyze the correctness of the protocol.

3.1. Protocol description

Step 1: According to the secret $K(k_1, k_2, \dots, k_L)$, Alice prepares L $(n+1)$ -qubit GHZ states, and the j th GHZ state is

$$|G_{k_j}^+\rangle = |G(g_0^j, g_1^j, \dots, g_n^j)\rangle = \frac{1}{\sqrt{2}} (|0a_1^j a_2^j \dots a_n^j\rangle + |1\bar{a}_1^j \bar{a}_2^j \dots \bar{a}_n^j\rangle), \quad (4)$$

where $g_0^j, g_1^j, \dots, g_n^j$ represent the qubits in $|G_{k_j}^+\rangle$, $j \in (1, 2, \dots, L)$ and $k_j = \sum_{i=1}^n a_i^j \times 2^{n-i}$. Then, Alice picks out all the qubits to construct $n+1$ sequences S_0, S_1, \dots, S_n , which can be denoted as follows

$$\begin{aligned} S_0 &: g_0^1, g_0^2, \dots, g_0^L, \\ &\vdots \\ S_i &: g_i^1, g_i^2, \dots, g_i^L, \\ &\vdots \\ S_n &: g_n^1, g_n^2, \dots, g_n^L. \end{aligned} \quad (5)$$

Step 2: Alice generates n groups of decoy photons D_1, D_2, \dots, D_n , where each group has L particles, and each is randomly taken from the set $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$. After that, D_i is inserted by Alice into S_i to produce a new sequence S_i^* . Subsequently, Alice keeps S_0 in her hands and sends $S_1^*, S_2^*, \dots, S_n^*$ to Bob₁, Bob₂, \dots , Bob_{*n*}, respectively.

Step 3: For each received qubit, Bob_{*i*} first randomly chooses the **Measure-flip** or **Reflect** operations. After that, he

Table 1. Eavesdropping check of the decoy photons.

Initial state	Bob's operations	Measurement results of Bob	Alice's operations	Measurement results of Alice
$ 0\rangle$	Measure-flip	$ 0\rangle$	M_Z	$ 1\rangle$
$ 0\rangle$	Reflect	$/$	M_Z	$ 0\rangle$
$ 1\rangle$	Measure-flip	$ 1\rangle$	M_Z	$ 0\rangle$
$ 1\rangle$	Reflect	$/$	M_Z	$ 1\rangle$
$ +\rangle$	Measure-flip	$ 0\rangle$ or $ 1\rangle$	M_Z	$ 1\rangle$ or $ 0\rangle$
$ +\rangle$	Reflect	$/$	M_X	$ +\rangle$
$ -\rangle$	Measure-flip	$ 0\rangle$ or $ 1\rangle$	M_Z	$ 1\rangle$ or $ 0\rangle$
$ -\rangle$	Reflect	$/$	M_X	$ -\rangle$

 M_Z : Measure the qubits with basis $\{|0\rangle, |1\rangle\}$; M_X : Measure the qubits with basis $\{|+\rangle, |-\rangle\}$.

performs **Reorder** operations on these qubits and sends them back to Alice. For convenience, the rearranged sequence is labeled as S'_i . Note that, in this step, Bob_{*i*} creates a $2L$ bits string $R_i(r_i^1, r_i^2, \dots, r_i^{2L})$ to record his operations. If he chooses the **Reflect** operation on the h th qubit, he sets $r_i^h = 0$. Otherwise, he sets $r_i^h = 1$. Here, $h = 1, 2, \dots, 2L$.

Step 4: After Alice stores all the received qubits, Bob_{*i*} announces the order of sequence S'_i . Then, Alice recovers the original order of the sequence and picks out all the decoy photons. Alice informs Bob_{*i*} to announce his operations on the decoy photons. According to Bob_{*i*}'s operations, Alice measures the decoy photons and discusses the correctness of the measurement results with Bob_{*i*}. Table 1 lists all 8 possible situations. For example, when Bob_{*i*} chooses the **Reflect** operation, Alice's measurement results should be identical to her initial states. If the error rate for the above cases exceeds the threshold, the protocol will be terminated and restarted.

Step 5: Alice (Bob_{*i*}) discards the qubits (bits) used to eavesdropping check. After removing decoy photons, the sequence S'_i is denoted as S''_i . Each Bob_{*i*} uses the remaining bits of R_i as his secret, which is labeled as $R'_i(r_i'^1, r_i'^2, \dots, r_i'^L)$. Then Alice performs single-particle measurement on the qubits from S_0 and $S''_1, S''_2, \dots, S''_n$. The measurement results are denoted as follows

$$\begin{aligned}
 &M_0(m_0^1, m_0^2, \dots, m_0^L), \\
 &\vdots \\
 &M_i(m_i^1, m_i^2, \dots, m_i^L), \\
 &\vdots \\
 &M_n(m_n^1, m_n^2, \dots, m_n^L),
 \end{aligned} \quad (6)$$

where m_i^j is the measurement result of qubit g_i^j after Bob_{*i*}'s operation. Note that $m_0^1, m_0^2, \dots, m_0^L$ are the measurement results of qubits $g_0^1, g_0^2, \dots, g_0^L$. According to the value of m_0^j , Alice decides whether to flip the values of $m_1^j, m_2^j, \dots, m_n^j$ or not. After Alice's operations, the values of $m_1^j, m_2^j, \dots, m_n^j$ are denoted as $m_1^{ij}, m_2^{ij}, \dots, m_n^{ij}$ (in fact, m_i^{ij} is equal to $a_i^j \oplus r_i^{ij}$, which will be shown in section 3.2),

$$m_i^{ij} = m_i^j \oplus m_0^j = \begin{cases} m_i^j \oplus 0, & \text{if } m_0^j = 0 \\ m_i^j \oplus 1, & \text{if } m_0^j = 1 \end{cases}. \quad (7)$$

After that, Alice publishes m_i^{ij} to Bob₁, Bob₂, ..., Bob_{*n*}.

Step 6: According to the values of m_i^{ij} and r_i^{ij} , Bob₁, Bob₂, ..., Bob_{*n*} work together to calculate k_1, k_2, \dots, k_L

$$\begin{aligned}
 k_1 &= \sum_{i=1}^n (m_i'^1 \oplus r_i'^1) \times 2^{n-i} = \sum_{i=1}^n a_i^1 \times 2^{n-i}, \\
 k_2 &= \sum_{i=1}^n (m_i'^2 \oplus r_i'^2) \times 2^{n-i} = \sum_{i=1}^n a_i^2 \times 2^{n-i}, \\
 &\vdots \\
 k_L &= \sum_{i=1}^n (m_i'^L \oplus r_i'^L) \times 2^{n-i} = \sum_{i=1}^n a_i^L \times 2^{n-i}.
 \end{aligned} \quad (8)$$

Note that only when Bob₁, Bob₂, ..., Bob_{*n*} cooperate can they obtain Alice's secret $K(k_1, k_2, \dots, k_L)$.

3.2. Correctness of protocol

Without considering the decoy photons and eavesdropping check, we take the state $|G_{kj}^+\rangle$ as an example to prove the correctness of our protocol.

Firstly, suppose Alice keeps $|0\rangle$ (i.e. $m_0^j = 0$) in her hand and sends $|a_1^j\rangle, |a_2^j\rangle, \dots, |a_n^j\rangle$ to Bob₁, Bob₂, ..., Bob_{*n*}, respectively. For each received qubit, Bob_{*i*} uses r_i^{ij} to record his operation. If his operation is **Measure-flip**, $r_i^{ij} = 1$; if not, $r_i^{ij} = 0$. Then, the states of $|a_1^j\rangle, |a_2^j\rangle, \dots, |a_n^j\rangle$ are converted to $|a_1^j \oplus r_1^{ij}\rangle, |a_2^j \oplus r_2^{ij}\rangle, \dots, |a_n^j \oplus r_n^{ij}\rangle$. After that, Alice measures the qubits sent by Bob_{*i*}, and the measurement results are labeled as $m_1^j, m_2^j, \dots, m_n^j$, where $m_i^j = a_i^j \oplus r_i^{ij}$. According to the equation (7) and $m_0^j = 0$, it holds that

$$m_i^{ij} = m_i^j \oplus 0 = a_i^j \oplus r_i^{ij}. \quad (9)$$

Then, we consider the case that Alice keeps $|1\rangle$ (i.e. $m_0^j = 1$) in her hand and sends $|\bar{a}_1^j\rangle, |\bar{a}_2^j\rangle, \dots, |\bar{a}_n^j\rangle$ to Bob₁, Bob₂, ..., Bob_{*n*}, respectively. After Bob_{*i*}'s operations (i.e. r_i^{ij}), the states of qubits are converted to $|\bar{a}_1^j \oplus r_1^{ij}\rangle, |\bar{a}_2^j \oplus r_2^{ij}\rangle, \dots, |\bar{a}_n^j \oplus r_n^{ij}\rangle$. After that, Alice measures the qubits sent by Bob_{*i*}. The corresponding measurement results are denoted as $m_1^j, m_2^j, \dots, m_n^j$, where $m_i^j = \bar{a}_i^j \oplus r_i^{ij} = 1 \oplus a_i^j \oplus r_i^{ij}$. According to the equation (7) and $m_0^j = 1$, it holds that

$$m_i^{ij} = m_i^j \oplus 1 = 1 \oplus a_i^j \oplus r_i^{ij} \oplus 1 = a_i^j \oplus r_i^{ij}. \quad (10)$$

Thus, based on the equations (9) and (10), it holds that $m_i^{ij} = a_i^j \oplus r_i^{ij}$. According to the steps of the protocol, after obtaining m_i^{ij} , Alice will declare it to Bob₁, Bob₂, ..., Bob_n via a classical channel. Utilizing the values of m_i^{ij} and r_i^{ij} , Alice's secret message k_j can be recovered by calculating

$$\begin{aligned} k_j &= (m_1^{ij} \oplus r_1^{ij}) \times 2^{n-1} + (m_2^{ij} \oplus r_2^{ij}) \times 2^{n-2} + \dots + (m_n^{ij} \oplus r_n^{ij}) \times 2^0 \\ &= (a_1^j \oplus r_1^{ij} \oplus r_1^{ij}) \times 2^{n-1} + (a_2^j \oplus r_2^{ij} \oplus r_2^{ij}) \times 2^{n-2} + \dots \\ &\quad + (a_n^j \oplus r_n^{ij} \oplus r_n^{ij}) \times 2^0 = a_1^j \times 2^{n-1} + a_2^j \times 2^{n-2} + \dots + a_n^j \times 2^0. \end{aligned} \quad (11)$$

It can be clearly seen from equation (11) that 'classical' users can cooperate to recover the secret information k_j shared by Alice by using their respective secret information r_i^{ij} and the information m_i^{ij} published by Alice.

Therefore, the output of our protocol is correct. By using this protocol, Alice can share specific messages to the 'classical' parties (Bob_i, $i = 1, 2, \dots, n$), and only the 'classical' parties cooperate they can recover Alice's messages.

4. Security analysis

Decoy photon technology, derived from the BB84 protocol, would detect most eavesdropping [44, 45]. Thus, most typical external and internal attacks are invalid to our protocol. The detailed analysis is shown as follows.

4.1. The intercept-resend attack

The intercept-resend attack is a typical eavesdropping method. The attacker will intercept the transmitted particles and resends the particles prepared by herself to the target user. Suppose an external eavesdropper, Eve, uses the intercept-resend attack to obtain some useful information. Without loss of generality, consider Eve attacking particles transmitted between Alice and Bob_i. Eve may first intercept all the qubits sent from Alice to Bob_i in Step 2. Then, she generates fake qubits in basis $\{|0\rangle, |1\rangle\}$, and sends these fake qubits to Bob_i. After Bob_i performing the operations on these qubits, Eve catches and measures the qubits sent by Bob_i to obtain his operations. However, Eve's attack is invalid since the order of the qubits sent from Bob_i to Alice is entirely secret for Eve. That is, Eve cannot distinguish which qubit is measure-flipped and which is reflected. More seriously, Eve's fake qubits are not identical to Alice's decoy photons, which will make Eve's attack discovered by Alice during the eavesdropping checking in Step 4.

4.2. The measure-resend attack

Eve may launch the measure-resend attack to steal some useful information. She first intercepts all the qubits sent by Alice, and measures them in basis $\{|0\rangle, |1\rangle\}$. Then she

sends the measured qubits to Bob_i directly. After that, Bob_i performs the **Measure-flip** operation or the **Reflect** operation on the received qubits. Subsequently, Eve intercepts the qubits sent from Bob_i to Alice, and measures these qubits to extract some useful information. However, Alice will detect Eve's attack in the eavesdropping checking. Specifically, if Bob_i chooses the **Measure-flip** operation, Eve's attack induces no errors. If Bob_i chooses the **Reflect** operation, Alice can easily detect Eve's attack because Eve's attack destroys the states of $|+\rangle$ and $|-\rangle$. Therefore, adopting the measure-resend attack, Eve will unavoidably be found by Alice.

4.3. The entangle-measure attack

The entangle-measure attack attack is one of the typical attack methods. Specifically, Eve will perform (U_E, U_F) on the target qubit and her probe $|0\rangle_E$ and then she will measure her probe to extract useful information. Here, U_E is the attack operator applied on the qubits sent from Alice to Bob_i while U_F is the attack operator applied on the qubits sent from Bob_i to Alice. The effect of (U_E, U_F) on the target qubit is described as follows [20]:

$$\begin{aligned} U_E|0, 0\rangle_{TE} &= \alpha|0, e_0\rangle + \beta|1, e_1\rangle, \\ U_E|1, 0\rangle_{TE} &= \beta|0, e_2\rangle + \alpha|1, e_3\rangle, \end{aligned} \quad (12)$$

and

$$\begin{aligned} U_F|0, e_\omega\rangle_{TE} &= \mu_\omega|0, e_{0,\omega}^0\rangle + \nu_\omega|1, e_{0,\omega}^1\rangle, \\ U_F|1, e_\omega\rangle_{TE} &= \nu_\omega|0, e_{1,\omega}^0\rangle + \mu_\omega|1, e_{1,\omega}^1\rangle, \end{aligned} \quad (13)$$

where T and E represent the target qubit and Eve's probe, respectively. Since U_E and U_F are unitary, which imply $|\alpha|^2 + |\beta|^2 = 1$, $|\mu_\omega|^2 + |\nu_\omega|^2 = 1$, and $\omega = 0, 1, 2, 3$.

Firstly, we analyze the effect of (U_E, U_F) on the decoy photons. The effect of U_E on the decoy photons sent by Alice is shown as follows.

$$\begin{aligned} U_E|0, 0\rangle_{TE} &= \alpha|0, e_0\rangle + \beta|1, e_1\rangle, \\ U_E|1, 0\rangle_{TE} &= \beta|0, e_2\rangle + \alpha|1, e_3\rangle, \\ U_E|+, 0\rangle_{TE} &= \frac{1}{\sqrt{2}}(\alpha|0, e_0\rangle + \beta|1, e_1\rangle + \beta|0, e_2\rangle + \alpha|1, e_3\rangle), \\ U_E|-, 0\rangle_{TE} &= \frac{1}{\sqrt{2}}(\alpha|0, e_0\rangle + \beta|1, e_1\rangle - \beta|0, e_2\rangle - \alpha|1, e_3\rangle). \end{aligned} \quad (14)$$

In Step 4, Alice and Bob_i do the eavesdropping checking. When Bob_i chooses the **Measure-flip** operation on the qubits $|0\rangle$ and $|1\rangle$, his measurement results should be identical to Alice's initial states. If Eve wants to be undetected, U_E needs to satisfy the conditions: $\beta = 0$ and $\alpha = 1$. Thus, the equation (14) can be reduced to

$$\begin{aligned}
U_E|0,0\rangle_{TE} &= |0,e_0\rangle, \\
U_E|1,0\rangle_{TE} &= |1,e_3\rangle, \\
U_E|+,0\rangle_{TE} &= \frac{1}{\sqrt{2}}(|0,e_0\rangle + |1,e_3\rangle), \\
U_E|-,0\rangle_{TE} &= \frac{1}{\sqrt{2}}(|0,e_0\rangle - |1,e_3\rangle). \quad (15)
\end{aligned}$$

Next, Eve performs U_F on the decoy photons sent by Bob_i. According to the [30], Eve performing U_F depends on the knowledge acquired by U_E . Due to the **Reorder** operation of Bob_i, the order of decoy photons sent from Alice to Bob_i is different from that Bob_i sent to Alice. Hence, there are two cases need to be analyzed.

Case 1: After the **Reorder** operation, the order of some decoy photons is not changed. According to the equation (15), Eve's probe $|0\rangle_E$ is changed to $|e_0\rangle$ or $|e_3\rangle$. When Bob_i chooses the **Reflect** operation, the effect of U_F is shown as follows,

$$\begin{aligned}
U_F|0,e_0\rangle_{TE} &= \mu_0|0,e_{0,0}^0\rangle + \nu_0|1,e_{0,0}^1\rangle, \\
U_F|1,e_3\rangle_{TE} &= \nu_3|0,e_{1,3}^0\rangle + \mu_3|1,e_{1,3}^1\rangle, \\
U_F \left[\frac{1}{\sqrt{2}}(|0,e_0\rangle_{TE} + |1,e_3\rangle_{TE}) \right] \\
&= \frac{1}{2}|+\rangle (\mu_0|e_{0,0}^0\rangle + \nu_0|e_{0,0}^1\rangle + \nu_3|e_{1,3}^0\rangle + \mu_3|e_{1,3}^1\rangle) \\
&\quad + \frac{1}{2}|-\rangle (\mu_0|e_{0,0}^0\rangle - \nu_0|e_{0,0}^1\rangle + \nu_3|e_{1,3}^0\rangle - \mu_3|e_{1,3}^1\rangle), \\
U_F \left[\frac{1}{\sqrt{2}}(|0,e_0\rangle_{TE} - |1,e_3\rangle_{TE}) \right] \\
&= \frac{1}{2}|+\rangle (\mu_0|e_{0,0}^0\rangle + \nu_0|e_{0,0}^1\rangle - \nu_3|e_{1,3}^0\rangle - \mu_3|e_{1,3}^1\rangle) \\
&\quad + \frac{1}{2}|-\rangle (\mu_0|e_{0,0}^0\rangle - \nu_0|e_{0,0}^1\rangle - \nu_3|e_{1,3}^0\rangle + \mu_3|e_{1,3}^1\rangle). \quad (16)
\end{aligned}$$

When Bob_i chooses the **Measure-flip** operation, the effect of U_F is (Here, we focus on the situation that qubits $|0\rangle$ and $|1\rangle$ are flipped to $|1\rangle$ and $|0\rangle$.)

$$\begin{aligned}
U_F|1,e_0\rangle_{TE} &= \nu_0|0,e_{1,0}^0\rangle + \mu_0|1,e_{1,0}^1\rangle, \\
U_F|0,e_3\rangle_{TE} &= \mu_3|0,e_{0,3}^0\rangle + \nu_3|1,e_{0,3}^1\rangle. \quad (17)
\end{aligned}$$

If Eve wants to be undetected by Alice, then after the U_F attack, the states of the particles received by Alice should be opposite to their initial states. That is, U_F must satisfy the conditions:

$$\nu_0 = \nu_3 = 0, \quad \mu_0 = \mu_3 = 1, \quad |e_{0,0}^0\rangle = |e_{1,3}^1\rangle. \quad (18)$$

Case 2: After the **Reorder** operation, the order of some decoy photons is changed. Here, we focus on the decoy photons reflected by Bob_i. Suppose Alice sends qubits $|0\rangle$ and $|+\rangle$ to Bob_i, and Bob_i sends qubits $|+\rangle$ and $|0\rangle$ to Alice. Based on the equation (15), performing U_E on the qubits $|0\rangle$ and $|+\rangle$, the states become to

$$U_E|0,0\rangle_{TE} U_E|+,0\rangle_{TE} = \frac{1}{\sqrt{2}}|0,e_0\rangle (|0,e_0\rangle + |1,e_3\rangle). \quad (19)$$

For the received qubits, Bob_i performs **Reflect** operation and swaps the positions of these two qubits. Then the states change to $\frac{1}{\sqrt{2}}(|0,e_0\rangle|0,e_0\rangle + |1,e_0\rangle|0,e_3\rangle)$. After performing U_F , the states become

$$\begin{aligned}
&\frac{1}{\sqrt{2}} [(\mu_0|0,e_{0,0}^0\rangle + \nu_0|1,e_{0,0}^1\rangle)(\mu_0|0,e_{0,0}^0\rangle + \nu_0|1,e_{0,0}^1\rangle) \\
&\quad + (\nu_0|0,e_{1,0}^0\rangle + \mu_0|1,e_{1,0}^1\rangle)(\mu_3|0,e_{0,3}^0\rangle + \nu_3|1,e_{0,3}^1\rangle)]. \quad (20)
\end{aligned}$$

Substituting equation (18) into equation (20), we can derive

$$\begin{aligned}
&\frac{1}{\sqrt{2}} (\mu_0|0,e_{0,0}^0\rangle\mu_0|0,e_{0,0}^0\rangle + \mu_0|1,e_{1,0}^1\rangle\mu_3|0,e_{0,3}^0\rangle) \\
&= \frac{1}{2}(|+\rangle + |-\rangle)|e_{0,0}^0\rangle|0,e_{0,0}^0\rangle + \frac{1}{2}(|+\rangle - |-\rangle)|e_{1,0}^1\rangle|0,e_{0,3}^0\rangle \\
&= \frac{1}{2}|+,0\rangle (|e_{0,0}^0\rangle|e_{0,0}^0\rangle + |e_{1,0}^1\rangle|e_{0,3}^0\rangle) + \frac{1}{2}|-,0\rangle \\
&\quad \times (|e_{0,0}^0\rangle|e_{0,0}^0\rangle - |e_{1,0}^1\rangle|e_{0,3}^0\rangle). \quad (21)
\end{aligned}$$

If Eve wants to be undetected in this case, Alice's measurement results of these two qubits must be $|+\rangle$ and $|0\rangle$. That is, U_F must satisfy the conditions:

$$|e_{0,0}^0\rangle = |e_{0,3}^0\rangle, \quad |e_{0,0}^1\rangle = |e_{1,0}^1\rangle. \quad (22)$$

Putting everything together, if Eve's attack introduces no errors, it must satisfy:

$$\begin{aligned}
\alpha = \mu_0 = \mu_3 = 1, \quad \beta = \nu_0 = \nu_3 = 0, \\
|e_{0,0}^0\rangle = |e_{0,3}^0\rangle = |e_{1,0}^1\rangle = |e_{1,3}^1\rangle. \quad (23)
\end{aligned}$$

Now, we analyze the effect of (U_E, U_F) on the qubits from the GHZ state $|G_k^+\rangle$. Assume Eve performs (U_E, U_F) on the i th qubit in $|G_k^+\rangle$, where the i th qubit is denoted as $|a_i^j\rangle$ and $a_i^j \in \{0, 1\}$. If Bob_i performs the **Reflect** operation on the received qubit, after performing (U_E, U_F) , the state of $|a_i^j\rangle$ will evolve into

$$U_F U_E |a_i^j\rangle |0\rangle_E = \begin{cases} \mu_0|0,e_{0,0}^0\rangle + \nu_0|1,e_{0,0}^1\rangle & |a_i^j\rangle = |0\rangle \\ \nu_3|0,e_{1,3}^0\rangle + \mu_3|1,e_{1,3}^1\rangle & |a_i^j\rangle = |1\rangle \end{cases}. \quad (24)$$

If Bob_i performs the **Measure-flip** operation on the received qubit, after performing (U_E, U_F) , the state of $|a_i^j\rangle$ will evolve into

$$U_F U_E |a_i^j\rangle |0\rangle_E = \begin{cases} \nu_0|0,e_{1,0}^0\rangle + \mu_0|1,e_{1,0}^1\rangle & |a_i^j\rangle = |0\rangle \\ \mu_3|0,e_{0,3}^0\rangle + \nu_3|1,e_{0,3}^1\rangle & |a_i^j\rangle = |1\rangle \end{cases}. \quad (25)$$

Applying equation (23) into equations (24) and (25), we have

$$U_F U_E |a_i^j\rangle = |a_i^j\rangle |e_{0,0}^0\rangle. \quad (26)$$

Thus, to avoid introducing errors, Eve's probe should be unassociated with the target qubit. That is to say, no matter what

state the target qubit is in, Eve can only get the same result from her probe. Therefore, our protocol can withstand the entangle-measure attack.

4.4. The Double-CNOT attack

Semi-quantum protocols are susceptible to the Double-CNOT attack, which can be described as follows. Eve firstly intercepts the particle sent by Alice. Then, she performs the first attack $U_{\text{CNOT}} = |00\rangle\langle 00| + |01\rangle\langle 01| + |10\rangle\langle 10| + |11\rangle\langle 11|$, where the intercepted particle is the control bit and her ancillary particle $|0\rangle_E$ is the target bit. After that, Eve intercepts the particle sent by Bob_{*i*} and executes the second U_{CNOT} on the intercepted particle and her ancillary particle again. Finally, Eve measures her ancillary particle to obtain some useful information.

However, Alice will detect Eve's attack in the eavesdropping checking since her attack will change the decoy photons' states. For the decoy photons, after performing the U_{CNOT} operation, the qubit systems become:

$$U_{\text{CNOT}}(|0\rangle_A|0\rangle_E) = |00\rangle_{AE}, \quad (27)$$

$$U_{\text{CNOT}}(|1\rangle_A|0\rangle_E) = |11\rangle_{AE}, \quad (28)$$

$$U_{\text{CNOT}}(|+\rangle_A|0\rangle_E) = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{AE}, \quad (29)$$

$$U_{\text{CNOT}}(|-\rangle_A|0\rangle_E) = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)_{AE}, \quad (30)$$

where the subscripts *A* and *E* represent the Alice's qubit and Eve's ancillary particle, respectively. To eliminate the errors caused by the U_{CNOT} , Eve needs to perform the U_{CNOT} again on the same control bit and the target bit. However, the qubit sent by Bob_{*i*} is not the same as the qubit sent by Alice because Bob_{*i*} performs the **Reorder** operation on the qubit sending to Alice. That is, Eve cannot eliminate the errors introduced by the U_{CNOT} operation. Thus, Eve's attack will inevitably introduce errors.

For example, assume that the *j*th qubit sent by Alice is $|+\rangle_A$ while the *j*th qubit sent by Bob_{*i*} is $|0\rangle_B$. After performing the Double-CNOT attack, the qubit systems are transformed as

$$\begin{aligned} & U_{\text{CNOT}}|0\rangle_B[U_{\text{CNOT}}(|+\rangle_A|0\rangle_E)] \\ &= \frac{1}{\sqrt{2}}(|000\rangle + |011\rangle)_{BAE} \\ &= \frac{1}{\sqrt{2}}|0\rangle_B(|+\rangle|+\rangle + |-\rangle|-\rangle)_{AE} \end{aligned} \quad (31)$$

Consider the scenario where Bob chooses the **Reflect** operation for $|+\rangle_A$. After undergoing the Double-CNOT attack, Alice will perform measurements on the particle reflected by Bob in the basis $\{|+\rangle, |-\rangle\}$. As indicated by equation (31), Alice's measurement results will randomly be in either $|+\rangle_A$ or $|-\rangle_A$, rather than being guaranteed to be in $|+\rangle_A$. During eavesdropping detection, Alice will discover this error. Therefore, Eve's attack will introduce errors and be detected by Alice with a non-zero probability.

4.5. The Trojan horse attack

In our protocol, each qubit is transmitted twice. To extract Alice's and Bob's secret, Eve may perform Trojan horse attacks [46–48] which mainly include the delay-photon attack and the invisible photon attack. Fortunately, by equipping with wavelength filters and photon number splitters [49, 50], the Trojan horse attacks can be effectively defended. As a result, our protocol can withstand the Trojan horse attacks.

4.6. The participant attack

In SQSS protocols, dishonest 'classical' users also pose a threat to the security of the protocol. They attempt to obtain the secret information acquired by other users through attack methods, thus independently reconstructing the shared secret information. Here, we analyze an extreme case where $n - 1$ dishonest participants conspire to steal Alice's secret without the honest participant's help. Assume that Bob_{*t*} ($t = 1, 2, \dots, n$ and $t \neq i$) is dishonest and Bob_{*i*} is honest. According to the steps of the protocol, Bob_{*t*} will obtain part of the secret information, but this still cannot help them recover the secret information shared by Alice. To obtain the secret of Alice, the dishonest participants need to get the operations of Bob_{*i*}. Bob_{*t*} may launch attacks on the transmitted qubits between Alice and Bob_{*i*}. However, in our protocol, there is not any qubit transmitted between Bob_{*i*} and Bob_{*t*}. Obviously, Bob_{*t*} is thoroughly independent of Bob_{*i*}. Thus, Bob_{*t*} essentially acts as an external eavesdropper when she attacks the transmitted qubits between Alice and Bob_{*i*}. Based on the above analysis of Eve's attacks, Alice will detect Bob_{*t*}'s attacks with a non-zero probability. Therefore, our protocol can withstand the participant attack.

5. Simulation and discussion

In this section, we will use IBM Qiskit to conduct circuit simulation of the proposed protocol and discuss the protocol performance. It is worth noting that, throughout the entire circuit simulation phase, we focus primarily on simulating the circuit corresponding to $(n + 1)$ -qubit GHZ state.

5.1. Simulation based on IBM Qiskit

The designed protocol is capable of enabling n 'classical' users to share secret information. For the sake of implementing simulations and demonstrating the correctness of the protocol, here, we use a three-party scenario (i.e. $n = 3$) as an example to conduct circuit simulation of the protocol.

Firstly, let us introduce some basic settings for the three-party MSQSS protocol. Suppose there are three 'classical' users, Bob₁, Bob₂, and Bob₃, and one quantum user, Alice. In this protocol, Alice intends to share the secret information $k = 5$ with the 'classical' users. The secret information can only be recovered when all 'classical' users cooperate with each other.

According to the protocol's requirements, in the three-party MSQSS protocol scenario, Alice needs to prepare the 4-qubit

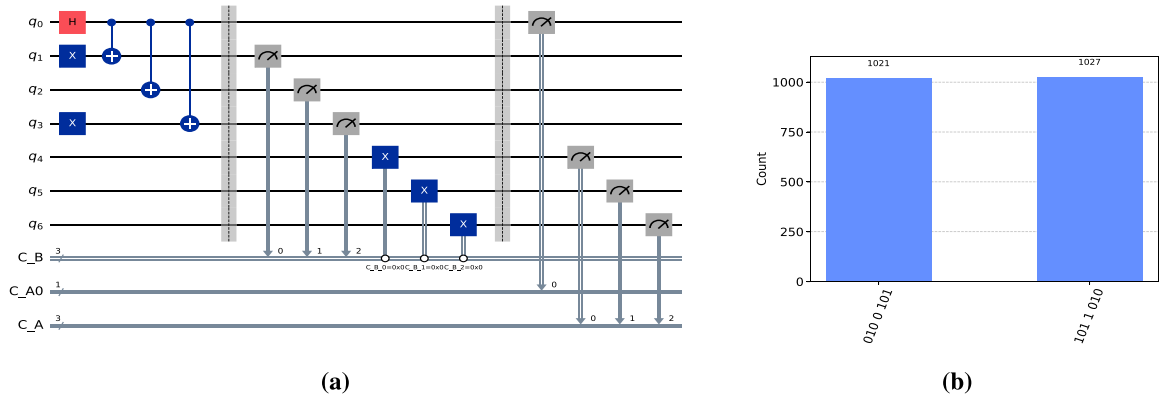


Figure 1. Quantum circuit diagram corresponding to all ‘classical’ users performing measure-flip operations. Registers (q_0, q_1, q_2, q_3) are used to generate 4-qubits GHZ state $|G_{k=5}^+\rangle$. Registers (q_4, q_5, q_6) are used by ‘classical’ users to prepare new quantum states after performing measure-flip operations. Classical register C_B records the measurement results of ‘classical’ users on the received particles, C_A0 records the measurement results of particles retained by Alice, and C_A records the measurement results of particles after being operated on by ‘classical’ users.

GHZ state $|G_{k=5}^+\rangle = \frac{1}{\sqrt{2}}(|0101\rangle + |1010\rangle)$ as the transmission qubits. Following the steps of protocol, she keeps the first qubit while sending the remaining three qubits to Bob₁, Bob₂, and Bob₃, respectively. Then, the classical users Bob₁, Bob₂, and Bob₃ will randomly perform **Measure-flip** or **Reflect** on the received particles and record the corresponding operation type. After that, Alice will measure the received particles in basis $\{|0\rangle, |1\rangle\}$.

Below, we simulate the circuit for the aforementioned process. Here, we consider three scenarios: one where all ‘classical’ users perform a **Measure-flip** operation on the received particles, another where they execute **Reflect** operations on all received particles, and the last one that both **Measure-flip** and **Reflect** operations are performed on the received particles.

Figure 1 shows the corresponding quantum circuit and simulation results when all ‘classical’ users perform **Measure-flip** operations. In figure 1(a), the section before the first barrier represents Alice preparing the quantum state $|G_{k=5}^+\rangle$, the middle section illustrates ‘classical’ users preparing particles in the opposite state after measuring the received particles, and the final part represents Alice performing single-particle measurements on the received particles. The simulation results indicate that the designed circuit meets the requirements of the protocol. Taking the first column of figure 1(b) as an example, the measurement result is ‘010 0 101’, which represents Alice’s measurement result of the measure-flipped particles as ‘010’, the measurement result of the particle retained in her hand as ‘0’, and the measurement results of Bob₁, Bob₂, and Bob₃ as ‘101’. Because Bob₁, Bob₂, and Bob₃ all performed **Measure-flip** operations, thus Alice’s measurement results should be opposite to Bob’s measurement results, and the simulation results also confirm this. Additionally, the measurement results of the particles retained in Alice’s hand and received by Bob₁, Bob₂, and Bob₃ as ‘0101’ are consistent with the measurement results of $|G_{k=5}^+\rangle$.

In order to be consistent with the protocol description, in this case, Alice’s measurement results of the received particles and the particle kept in her own hands can be recorded with the symbol $m_1 = 0, m_2 = 1, m_3 = 0, m_0 = 0$, respectively. The operations corresponding to Bob₁, Bob₂, and Bob₃ are represented by the symbol $r'_1 = 1, r'_2 = 1, r'_3 = 1$ respectively. Then, according to protocol step 5, Alice will use the value of m_0 to perform the XOR operation on m_1, m_2 and m_3 to obtain $m'_1 = m_0 \oplus m_1 = 0, m'_2 = m_0 \oplus m_2 = 1$ and $m'_3 = m_0 \oplus m_3 = 0$ and publish them to the ‘classical’ user. Finally, Bob₁, Bob₂, and Bob₃ can recover Alice’s secret information $k = 5$ as follows:

$$\begin{aligned} k &= (m'_1 \oplus r'_1) \times 2^2 + (m'_2 \oplus r'_2) \times 2 + \dots + (m'_3 \oplus r'_3) \times 2^0 \\ &= (0 \oplus 1) \times 2^2 + (1 \oplus 1) \times 2 + \dots + (0 \oplus 1) \times 2^0 \\ &= 5. \end{aligned} \quad (32)$$

Then, we consider the case that ‘classical’ users perform **Reflect** operations on all received particles. Figure 2 shows the corresponding quantum circuit and simulation results of this case. In this scenario, Alice essentially performs single-particle measurements on the 4-qubit GHZ state $|G_{k=5}^+\rangle$. Assuming Alice obtains the measurement result of ‘1’ for the particle she retains, then the other three particles’ results will be ‘010’. This outcome is consistent with the first column of the simulation results shown in figure 2(b). Therefore, it indicates that the designed circuit meets the requirements of the protocol. Let $m_0 = 1, m_1 = 0, m_2 = 1$ and $m_3 = 0$ represent Alice’s measurement results. Then, after XOR operation, we can get $m'_1 = m_0 \oplus m_1 = 1, m'_2 = m_0 \oplus m_2 = 0$ and $m'_3 = m_0 \oplus m_3 = 1$. Moreover, in this case, Bob₁, Bob₂, and Bob₃ perform **Reflect** operations, thus leading to the conclusion that $r'_1 = 0, r'_2 = 0, r'_3 = 0$. Integrating all the information, the ‘classical’ users can calculate Alice’s secret information as follows:

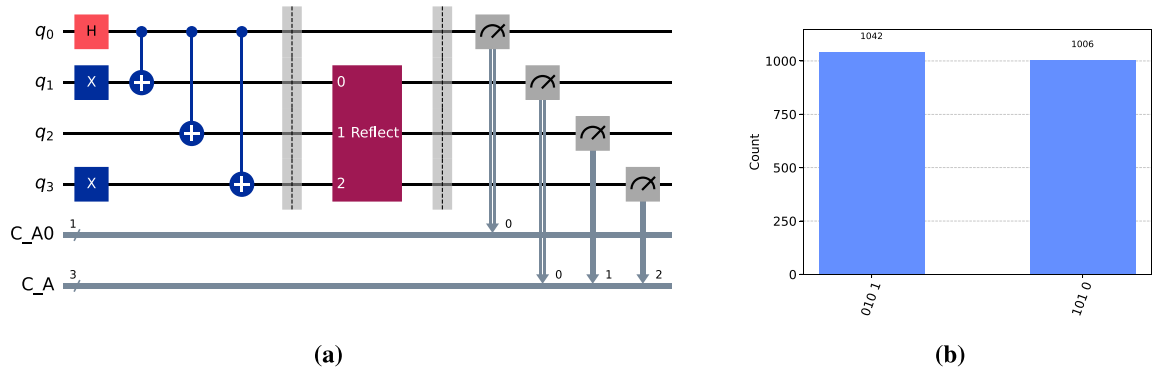


Figure 2. Quantum circuit diagram corresponding to all ‘classical’ users performing reflect operations.

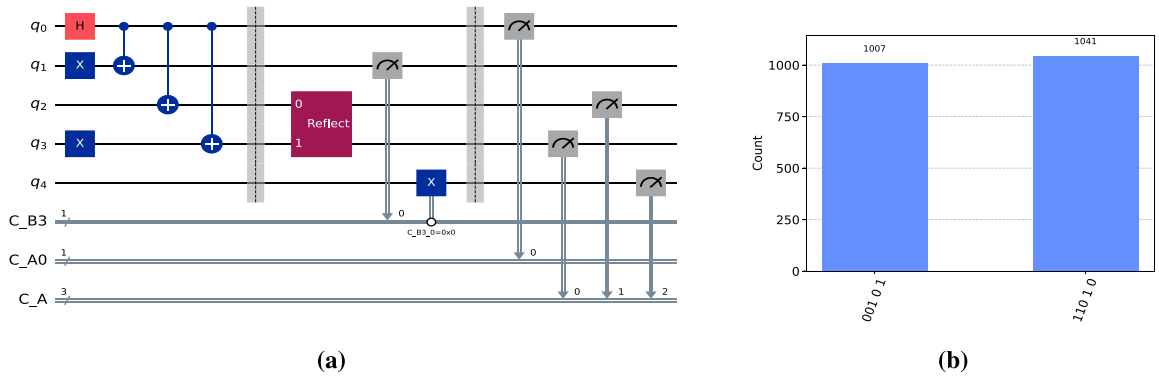


Figure 3. Quantum circuit diagram corresponding ‘classical’ user performs measure-flip and reflect operations.

$$\begin{aligned}
 k &= (m'_1 \oplus r'_1) \times 2^2 + (m'_2 \oplus r'_2) \times 2 + \dots + (m'_3 \oplus r'_3) \times 2^0 \\
 &= (1 \oplus 0) \times 2^2 + (0 \oplus 0) \times 2 + \dots + (1 \oplus 0) \times 2^0 \\
 &= 5.
 \end{aligned} \tag{33}$$

$$\begin{aligned}
 k &= (m'_1 \oplus r'_1) \times 2^2 + (m'_2 \oplus r'_2) \times 2 + \dots + (m'_3 \oplus r'_3) \times 2^0 \\
 &= (0 \oplus 1) \times 2^2 + (0 \oplus 0) \times 2 + \dots + (1 \oplus 0) \times 2^0 \\
 &= 5.
 \end{aligned} \tag{34}$$

Furthermore, we consider a more general scenario where ‘classical’ users perform random **Measure-flip** or **Reflect** operations on the received particles. Here, we assume that Bob₁, Bob₂, and Bob₃ respectively apply **Measure-flip**, **Reflect**, and **Reflect** operations to the received particles. The circuit simulation for scenarios corresponding to different operations is similar. Figure 3 illustrates the corresponding quantum circuit and simulation results for this scenario. Similarly, we assume that Alice retains the measurement result of 0 on her own particles, i.e. the result recorded in register C_A0 is 0, corresponding to the first column in figure 3(b). From the simulated results in figure 3, it can be observed that the measurement results of the particles after Bob₁, Bob₂, and Bob₃’s operations are 001, indicating consistency with the operations performed. Let $m_0 = 0, m_1 = 0, m_2 = 0$ and $m_3 = 1$ represent Alice’s measurement results. Then, after XOR operation, we can get $m'_1 = m_0 \oplus m_1 = 0$, $m'_2 = m_0 \oplus m_2 = 0$ and $m'_3 = m_0 \oplus m_3 = 1$. Moreover, following the ‘classical’ users’ operation, we can obtain $r'_1 = 1, r'_2 = 0, r'_3 = 0$. Integrating all the information, the ‘classical’ users can calculate Alice’s secret information as follows:

Above, we performed circuit simulations on three situations where ‘classical’ users perform **Measure-flip** and **Reflect** operations on the receiving particles, and verified the correctness of the protocol. The results show that the designed protocol is feasible and correct.

5.2. Discussion

This part will evaluate the performance of the protocol in terms of scalability, qubit efficiency, and shared secret information types.

Firstly, the proposed MSQSS protocol can meet the requirement of secret sharing among any number of ‘classical’ users, which is a significant advantage compared to traditional two-party SQSS protocols [31–36] that can only accommodate two ‘classical’ users, thus having certain limitations. Additionally, the designed protocol exhibits scalability. It can dynamically adjust according to actual needs to accommodate information sharing among different numbers of users. Therefore, whether it is for small-scale or large-scale secret information sharing requirements, the protocol can flexibly adapt and provide reliable solutions for users.

Table 2. The comparisons between MSQSS protocols.

	Reference [37]	Reference [38]	Reference [39]	Our Protocol
Quantum resource	Bell states	$(n+1)$ -qubit GHZ-like states	Bell states	$(n+1)$ -qubit GHZ states
Number of classical users	n	n	n	n
Single-particle measurement	Yes	Yes	Yes	Yes
Entangled state measurement	Yes	Yes	Yes	No
The reflected particles as the secret key	No	No	No	Yes
Share specific message	No	No	No	Yes
Qubit efficiency	$\frac{1}{2^{n+1}+n2^{n-1}}$	$\frac{1}{3n+2}$	$\frac{1}{5n}$	$\frac{1}{3n+1}$

Qubit efficiency is an important metric for evaluating protocol performance. For the sake of uniform comparison, we focus on the qubit efficiency comparison between multi-party SQSS protocols [37–39]. Here, qubit efficiency is defined as $\eta = c/q$, where c denotes the shared classical bits, and q denotes the transmitted qubits. In our protocol, Alice wants to share L classical secret messages to n classical users. That is, $c = L$. For the transmitted qubits, Alice needs to generate $L(n+1)$ -qubit GHZ states and $L \times n$ decoy photons. While n classical users need to generate L qubits respectively to replace the qubits measured by them. That is, $q = L(n+1) + 2Ln$. Thus, the qubit efficiency of the proposed protocol is $\frac{1}{3n+1}$. Similarly, the qubit efficiency of references [37–39] can be calculated, and the specific results are shown in table 2.

In terms of the type of shared secret information, our protocol offers a distinct advantage that it can share specific information among n classical users, whereas the previous MSQSS protocol was limited to sharing random secret information. Sharing specific secret information is necessary in some secure multi-party scenarios, such as in the financial field or the healthcare field, where transaction information and patient privacy data shared by multiple parties need to be deterministic. Our protocol can meet the task requirements of these specific scenarios and provides users with a reliable solution for secure multi-party collaboration.

In addition, in our protocol, the secret keys are constructed by the classical users' operations. That is, both the measured qubits and reflected qubits can be used as the secret keys. While in previous MSQSS protocols, the reflected qubits are usually used for eavesdropping checks, not as secret keys. By increasing the utilization of transmission particles, the efficiency of the protocol is improved. Table 2 clearly shows that our protocol has higher qubit efficiency.

6. Conclusion

In this paper, by utilizing the $(n+1)$ -qubit GHZ states and the idea of semi-quantum, a multi-party semi-quantum secret sharing protocol is proposed, where the specific messages can be shared by quantum Alice to n 'classical' parties (Bob_{*i*}, $i = 1, 2, \dots, n$). Only the 'classical' parties cooperate together can recover Alice's messages. Unlike previous protocols that rely on measurement outcomes as keys, this protocol establishes keys among users by utilizing measure-flip and reflect operations performed by 'classical' users. This effectively improves the utilization of transmitted particles, providing a

new approach to enhance the qubit efficiency of multi-party semi-quantum protocols. Furthermore, our protocol is feasible with existing technologies since complex entanglement measurements and unitary operations are not required. The relevant circuit simulation also shows that the designed protocol is correct and feasible. The proposed protocol is resistant to most typical external and internal attacks and has advantages in terms of scalability, qubit efficiency and type of shared message. Therefore, this protocol may be more consistent with the needs of practical secret sharing tasks.

In future research, we will explore the application scenarios and performance optimization of semi-quantum secret sharing protocols. In practical secret sharing scenarios, the addition and removal of users are common occurrences. However, current research can only achieve secret sharing between fixed users. Therefore, how to dynamically realize semi-quantum secret sharing will be the focus of the next stage.

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 'ZCL21006'.

References

- [1] Preskill J 2018 Quantum computing in the NISQ era and beyond *Quantum* **2** 79
- [2] Gong L-H, Pei J-J, Zhang T-F and Zhou N-R 2024 Quantum convolutional neural network based on variational quantum circuits *Opt. Commun.* **550** 129993
- [3] Liu C, Zhou S, Gong L-H and Chen H-Y 2024 Quantum private comparison protocol via 4D layered states and DQC model *Quantum Inf. Process.* **23** 156
- [4] Huang W, Wen Q-Y, Liu B, Su Q, Qin S-J and Gao F 2014 Quantum anonymous ranking *Phys. Rev. A* **89** 032325
- [5] Deng F G, Zhou H Y and Long G L 2006 Circular quantum secret sharing *J. Phys. A: Math. Theor.* **39** 14089–99
- [6] Markham D and Sanders B C 2008 Graph states for quantum secret sharing *Phys. Rev. A* **78** 042309
- [7] Wang T-Y, Wen Q-Y, Chen X-B, Guo F-Z and Zhu F-C 2008 An efficient and secure multiparty quantum secret sharing scheme based on single photons *Opt. Commun.* **281** 6130–4
- [8] Yang C W and Tsai C W 2020 Efficient and secure dynamic quantum secret sharing protocol based on bell states *Quantum Inf. Process.* **19**

- [9] Sutradhar K and Om H 2020 Efficient quantum secret sharing without a trusted player *Quantum Inf. Process.* **19** 73
- [10] Liao Q, Liu H and Zhu L *et al* 2021 Quantum secret sharing using discretely modulated coherent states *Phys. Rev. A* **103** 032410
- [11] Shi R H 2021 Anonymous quantum sealed-bid auction *IEEE Trans. Circuits Syst. II* **69** 414–8
- [12] Ye C-Q, Li J, Chen X-B, Dong M and Ota K 2023 Measurement-based quantum sealed-bid auction *IEEE Trans. Circuits Syst. I* **70** 5352–65
- [13] Wang J-T, Pan Y, Liu W and Li Z-Z 2022 Quantum sealed-bid auction protocol based on quantum secret sharing *Quantum Inf. Process.* **21** 278
- [14] Sutradhar K and Om H 2020 A generalized quantum protocol for secure multiparty summation *IEEE Trans. Circuits Syst. II* **67** 2978–82
- [15] Yang H-Y and Ye T-Y 2018 Secure multi-party quantum summation based on quantum fourier transform *Quantum Inf. Process.* **17** 129
- [16] Shi R-H, Mu Y, Zhong H, Cui J and Zhang S 2016 Secure multiparty quantum computation for summation and multiplication *Sci. Rep.* **6** 19655
- [17] Luo M, Li F, Liu L and Zhu S 2024 Verifiable quantum protocol for dynamic secure multiparty summation based on homomorphic encryption *J. Phys. A: Math. Theor.* **57** 115302
- [18] Boyer M, Kenigsberg D and Mor T 2007 Quantum key distribution with classical Bob *Phys. Rev. Lett.* **99** 140501
- [19] Boyer M, Gelles R, Kenigsberg D and Mor T 2009 Semiquantum key distribution *Phys. Rev. A* **79** 032341
- [20] Krawec W O 2015 Security proof of a semi-quantum key distribution protocol *IEEE Int. Symp. on Information Theory (ISIT)* (IEEE) pp 686–90
- [21] Zhou S, Xie Q M and Zhou N R 2024 Measurement-free mediated semi-quantum key distribution protocol based on single-particle states *Laser Phys. Lett.* **21** 065207
- [22] Krawec W O 2016 Security of a semi-quantum protocol where reflections contribute to the secret key *Quantum Inf. Process.* **15** 2067–90
- [23] Zhou N-R, Zhu K-N and Zou X-F 2019 Multiparty semiquantum key distribution protocol with four particle cluster states *Ann. Phys., Lpz.* **531** 1800520
- [24] Ye C Q, Li J and Chen X B *et al* 2022 An efficient semi-quantum key distribution protocol and its security proof *IEEE Commun. Lett.* **26** 1226–30
- [25] Ye C-Q, Li J, Chen X-B, Hou Y and Wang Z 2023 Security and application of semi-quantum key distribution protocol for users with different quantum capabilities *EPJ Quantum Technol.* **10** 1–23
- [26] Zou X F and Qiu D W 2014 Three-step semiquantum secure direct communication protocol *Sci. China-Phys. Mech. Astron.* **57** 1696–702
- [27] Sun Y, Yan L, Chang Y, Zhang S, Shao T and Zhang Y 2019 Two semi-quantum secure direct communication protocols based on Bell states *Mod. Phys. Lett. A* **34** 1950004
- [28] Wang P, Chen X and Sun Z 2022 Semi-quantum secure direct communication against collective-dephasing noise *Quantum Inf. Process.* **21** 352
- [29] Shi G F 2023 Semi-quantum dialogue scheme based on hyperentangled Bell states *Phys. Scr.* **98** 115120
- [30] Li Q, Chan W H and Long D Y 2010 Semiquantum secret sharing using entangled states *Phys. Rev. A* **82** 022303
- [31] Xie C, Li L Z and Qiu D W 2015 A novel semi-quantum secret sharing scheme of specific bits *Int. J. Theor. Phys.* **54** 3819–24
- [32] Xing D, Wang Y, Dou Z, Li J, Chen X and Li L 2023 Efficient semi-quantum secret sharing protocol using single particles *Chin. Phys. B* **32** 070308
- [33] Hu W W, Zhou R G and Luo J 2022 Semi-quantum secret sharing in high-dimensional quantum system using product states *Chin. J. Phys.* **77** 1701–12
- [34] He F, Xin X, Li C and Li F 2024 Security analysis of the semi-quantum secret-sharing protocol of specific bits and its improvement *Quantum Inf. Process.* **23** 51
- [35] Tian Y, Li J, Chen X-B, Ye C-Q and Li H-J 2021 An efficient semi-quantum secret sharing protocol of specific bits *Quantum Inf. Process.* **20** 217
- [36] Hou Y-Y, Xu T, Li J, Ye C-Q, Wang Z and Liu X-Y 2024 Circular semi-quantum secret sharing based on hybrid single particle and GHZ-type states *Laser Phys. Lett.* **21** 025202
- [37] Gao G, Wang Y and Wang D 2016 Multiparty semiquantum secret sharing based on rearranging orders of qubits *Mod. Phys. Lett. B* **30** 1650130
- [38] Yu K-F, Gu J, Hwang T and Gope P 2017 Multi-party semi-quantum key distribution-convertible multi-party semi-quantum secret sharing *Quantum Inf. Process.* **16** 194
- [39] Li X Y, Chang Y and Zhang S B 2020 Multi-party semi-quantum secret sharing scheme based on bell states *Int. Conf. on Artificial Intelligence and Security* (Springer) pp 280–8
- [40] Gong L-H, Ye Z-J, Liu C and Zhou S 2024 One-way semi-quantum private comparison protocol without pre-shared keys based on unitary operations *Laser Phys. Lett.* **21** 035207
- [41] Gong L-H, Li M-L, Cao H and Wang B 2024 Novel semi-quantum private comparison protocol with bell states *Laser Phys. Lett.* **21** 055209
- [42] Ye C-Q, Li J, Chen X-B, Dong M, Ota K, Khalique A and Durad M H 2024 Semi-quantum secure multiparty summation and its applications to anonymous auction and ranking *Adv. Quantum Technol.* **7** 2300347
- [43] Iqbal H and Krawec W O 2020 Semi-quantum cryptography *Quantum Inf. Process.* **19** 97
- [44] Ji Z X, Fan P R, Zhang H G and Wang H 2021 Greenberger-Horne-Zeilinger-based quantum private comparison protocol with bit-flipping *Phys. Scr.* **96** 015103
- [45] Renner R 2008 Security of quantum key distribution *Int. J. Quantum Inf.* **6** 1–127
- [46] Deng F G, Zhou P, Li X H, Li C Y and Zhou H Y 2005 Robustness of two-way quantum communication protocols against Trojan horse attack *Quantum Phys.* (arXiv:quant-ph/0508168)
- [47] Cai Q-Y 2006 Eavesdropping on the two-way quantum communication protocols with invisible photons *Phys. Lett. A* **351** 23–25
- [48] Yang C-W, Hwang T and Luo Y-P 2013 Enhancement on quantum blind signature based on two-state vector formalism *Quantum Inf. Process.* **12** 109–17
- [49] Deng F G, Li X H, Zhou H Y and Zhang Z J 2005 Improving the security of multiparty quantum secret sharing against Trojan horse attack *Phys. Rev. A* **72** 044302
- [50] Li X H, Deng F G and Zhou H Y 2006 Improving the security of secure direct communication based on the secret transmitting order of particles *Phys. Rev. A* **74** 054302