arXiv:2508.05487v1 [quant-ph] 7 Aug 2025

Efficient Mediated Multiparty Semi-Quantum Secret Sharing Protocol Based on Single-Qubit Reordering

Mustapha Anis Younes [*1], Sofia Zebboudj [†2], and Abdelhakim Gharbi [‡3]

[1,2]Université de Bejaia, Faculté des Sciences Exactes, Laboratoire de Physique Théorique, 06000 Bejaia, Algérie
[2]ENSIBS, Université de Bretagne Sud, 56000 Vannes, France

Abstract

Typical multiparty semi-quantum secret sharing (MSQSS) protocols require the dealer to possess full quantum capabilities, while the classical users usually need to perform three operations. To address this practical limitation, this paper introduces a new mediated MSQSS protocol that enables Alice, a classical user, to share a secret with M classical Bobs, with the assistance of an untrusted third party (TP) who may attempt any possible attack to steal Alice's secret. Furthermore, the classical participants require only two capabilities instead of three, namely: (a) performing measurements in the Z basis; and (b) reordering qubits. The proposed scheme offers significant advantages over existing mediated QSS protocols: (1) it is the first mediated SQSS protocol to adopt single qubits, instead of entangled states, as the quantum resource, which makes it more practical and easier to implement; (2) It achieves higher qubit efficiency. Security analysis also demonstrates that the protocol is secure against well-known attacks.

Keywords— Semi-quantum cryptography; Multiparty mediated semi-quantum secret sharing; single qubits; Dishonest third party.

1 Introduction

Secret sharing is a procedure that allows a dealer to share a secret among several participants. Invented independently by Shamir [19] and Blakley [2] in 1979, it involves splitting the secret into multiple parts (called shadows) and distributing them to the participants. This is done in such a way that no individual part reveals any intelligible information about the original secret. Only when a sufficient number of participants combine their shadows can the secret be reconstructed. The security of classical secret sharing (CSS) protocols relies on computational complexity and hard mathematical problems, which makes them vulnerable to quantum computing attacks [6, 17]. On the other hand, quantum secret sharing (QSS) can overcome this challenge by relying on the fundamental laws of quantum physics.

In 1999, Hillery et al. [9] introduced the first QSS protocol based on GHZ states. Since then, numerous QSS protocols and experimental implementations have been proposed [34, 26, 1, 18, 12, 33, 20], leveraging the properties of various quantum resources. However, these protocols typically require participants to possess full quantum capabilities, which is difficult to achieve in practice [7], as not everyone can afford expensive quantum devices.

To address this issue, Boyer et al. [5] introduced the concept of a "semi-quantum environment", which includes two types of users: quantum and classical. According to the definition, quantum users possess full quantum capabilities, whereas classical users are restricted to performing the following operations: (1) reflect particles without disturbance; (2) measure qubits in the Z basis $\{|0\rangle, |1\rangle\}$; (3) prepare qubits

[*]Corresponding Author: mustaphaanis.younes@univ-bejaia.dz
[†]sofia.zebboudj@univ-ubs.fr
[‡]abdelhakim.gharbi@univ-bejaia.dz

in the Z basis; and (4) reorder qubits. In 2007, Boyer et al. [5, 3] proposed the first semi-quantum key distribution (SQKD) protocol. Since then, various SQKD protocols have been developed [35, 4, 25, 27, 11], allowing a quantum user to share secret keys with a classical user. In 2015, Krawec [13] introduced the mediated model, which involves an untrusted, fully quantum third party (TP) acting as a mediator to help two classical participants establish a secure key, further reducing the quantum burden on the users.

In 2011, Li et al. [15] proposed the first semi-quantum secret sharing (SQSS) protocol, in which a quantum dealer can share secret information with two classical participants using GHZ-type states. Following this, various SQSS protocols have been proposed [28, 14, 31, 22, 21, 10, 30, 8, 29, 16, 32], many of which can accommodate multiple participants. Although these protocols are lighter than fully quantum ones, they share a major restriction: the dealer must always be the quantum user. It is therefore interesting, from both theoretical and experimental perspectives, to explore whether a classical user can assume the role of the dealer.

This restriction was first tackled by Tsai et al. [23] in 2021. Their approach, based on the mediated model and leveraging the properties of GHZ states, introduced the first mediated multiparty quantum secret sharing (MQSS) protocol. It enables a classical user to securely share a secret with other classical users, with the assistance of an adversarial, fully quantum third party (TP). However, this protocol suffers from extremely low qubit efficiency. In 2023, Tsai et al. [24] proposed another mediated MQSS protocol based on a measurement property of graph states. This new protocol achieves a qubit efficiency that is 2^{M-1} times higher than the first scheme, where M is the number of participants. Although both protocols place all participants on equal footing in terms of capabilities, the TP still requires heavy quantum resources. In practice, the cost and complexity of generating and maintaining such entangled states remain prohibitively high. Ideally, protocols where both the TP and the participants require only minimal quantum capabilities, such as handling single-qubit states, would be far more practical.

To reduce TP's quantum burden, this paper introduces the first mediated multiparty semi-quantum secret sharing protocol (MSQSS) based on single qubits. In the proposed scheme, TP is only required to: (1) generate qubits in the state $|+\rangle$, and (2) measure qubits in the $Z = \{|0\rangle, |1\rangle\}$ and $X = \{|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}, |-\rangle = (|0\rangle - |1\rangle)/\sqrt{2}\}$ bases. As for the classical participants, they only need two capabilities: (a) measuring qubits in the Z basis, and (b) reordering qubits. As a result, our protocol is more practical for real-world implementation. Furthermore, the use of the qubit reordering operation minimizes the number of discarded particles in the protocol, resulting in higher qubit efficiency compared to previous mediated QSS protocols. Our protocol also adopts a circular qubit transmission method, making it more scalable than tree-based methods, especially in multiparty scenarios. Finally, security analyses shows that the protocol is secure and can resist well-known attacks, such as the intercept-resend attack, fake-state attack, entanglement-measure attack, Trojan horse attacks, and collusion attacks.

The remainder of this paper is organized as follows. Section 2 describes the proposed protocol in detail. Section 2.2 provides a concrete example of the protocol. The security analysis is presented in Section 3. Section 4 discusses the efficiency analysis and provides a comparison with other similar schemes. Finally, a conclusion is given in section 5.

2 The proposed protocol

In this paper, we propose a new mediated semi-quantum QSS scheme, where Alice, a classical entity wants to share a secret with M classical Bobs with the help of an untrusted third-party (TP) who might attempt any possible attack to steal Alice's secret without being detected. Namely, Alice is capable to perform the following operations:

1. Generate and measure qubits in the $Z = \{|0\rangle, |1\rangle\}$ basis.
2. Reorder qubits via different delay lines.

On the other hand, the classical Bobs are only capable of performing two operations, namely:

- Measuring qubits in the Z basis.
- Reordering qubits.

As for TP, he is only required to perform the following operations:

1. Generate qubits in the state $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$.
2. Measure qubits in the X and Z basis, such as

$$X = \{|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\} \tag{1}$$

The proposed protocol adopts a circular qubit transmission method. Additionally, there exist a public authenticated classical channel between the participants. Since the TP is considered adversarial, the classical channel between him and the participants do not necessarily need to be authenticated.

2.1 Steps of the protocols

Let S be a classical bit string that Alice wants to share, with L its length. The procedure of our proposed MSQSS protocol unfolds as follows:

2.1.1 Step 01: (Preparation by TP)

TP generates a sequence S_{TP} of $N = 4L(1 + M\epsilon)$ qubits, where:

- L is the desired length of the final secret key.
- M is the number of participants.
- ϵ is a parameter that satisfies $\epsilon < 1$.

Each qubit in the sequence is prepared in the state $|+\rangle$, and the sequence is then transmitted to Alice.

2.1.2 Step 02: (Alice's operations)

Upon receiving the sequence S_{TP}, Alice randomly selects half of the qubits to measure in the Z basis. She then replaces those qubits with newly generated ones in the same state she found. For convenience, we refer to those qubits as *SIFT* particles, and the remaining ones as *CTRL* particles. Alice ends up with a new sequence, denoted as S_A. Before transmitting the sequence to Bob_1, Alice reorders randomly the N qubits. Note that the specific rearrangement order of the qubits is only known to Alice. The resulting sequence, denoted as S'_A, is then sent to Bob_1.

2.1.3 Step 03: (Participants' operations)

After receiving the sequence S'_A from Alice, Bob_1 randomly selects a fraction of size $4N\epsilon$ of the sequence and performs a Z basis measurement on those qubits. He saves the positions of the measured qubits along with the corresponding measurement outcomes in his classical register. Next, Bob_1 randomly reorders the remaining qubits, creating a new sequence S_{B_1}, which he sends to Bob_2. Upon receiving the sequence, Bob_2 performs the same operations as Bob_1 and sends his resulting sequence to the next Bob. Each subsequent Bob follows the same procedure, except for the last one who sends his sequence S_{B_M} back to TP.

Note that when N is large enough, it is sufficient for each Bob to select a subset approximately half the length of the secret to estimate the error rate with Alice. Therefore, setting $\epsilon = 1/8$ or less, for example, is a choice that is both valid and reasonable.

2.1.4 Step 04: (TP's operations)

When TP receives the sequence S_{B_M} from Bob_M, he randomly chooses to measure each qubit in either the X basis or the Z basis. After performing the measurements, he publicly announces both the measurement basis and the corresponding outcome for each qubit.

2.1.5 Step 05: (Eavesdropping check)

In this step, Alice conducts an eavesdropping check with the M participants using the authenticated public channel. Alice requests all classical participants to reveal the positions of the qubits they measured, along with their corresponding measurement outcomes as follows:

- Bob_1 announces the positions of the qubits he measured as well as the measurement outcome for each qubits.
- For the remaining participants (Bob_i, $i \geq 2$), the information must be revealed in the following manner:
  1. Bob_i first reveals the positions of the measured qubits.
  2. The previous participants, starting from Bob_{i-1} and moving in reverse order, disclose the transposition order of these announced qubits, so Alice can accurately perform her security check.
  3. After that, Bob_i reveals the corresponding measurement outcome for each qubit.

For each participant, Alice compares the announced measurement outcomes with the corresponding states in her original sequence.

- For the *SIFT* particles, Bob_i's ($i \geq 1$) outcomes must match the states that Alice found in step 02.
- For *CTRL* particles, Alice verifies if Bob_i's outcomes are evenly distributed between $|0\rangle$ and $|1\rangle$.

If the error rate for the *SIFT* qubits or the deviation rate for the *CTRL* qubits exceeds a preset threshold, Alice aborts the protocol.

2.1.6 Step 06: (TP's honesty check)

In this step, Alice verifies the honesty of TP. She begins by requesting Bob_M to reveal the transposition order of the qubits that TP measured in the X basis. Each remaining participant, starting from the last and proceeding in reverse order, then publicly announces the transposition order of these qubits. Once this is over, Alice publicly announces the position of the *CTRL* particles in her sequence S'_A. Following this, Bob_1 reveals the transposition order of these qubits, and each remaining participant, in turn, publicly announces the transposition order for these qubits.

It is important to emphasize that Alice does not reveal her measurement outcomes for the *SIFT* qubits, nor does she disclose the correct reordering for these qubits.

Depending on the operation performed by TP and the specific qubit involved, four equally likely cases arise:

1. **Case 01: (X-*CTRL*)** TP performed an X basis measurement on a *CTRL* qubit. This case is used for eavesdropping detection. For TP to pass the check, he must consistently announce the measurement result $|+\rangle$; otherwise, Alice and the participants will abort the protocol.
2. **Case 02: (X-*SIFT*)** TP performed an X basis measurement on a *SIFT* qubit. In this case, Alice and the participants expect TP to announce both the measurement results $|+\rangle$ and $|-\rangle$ with equal probability. Alice checks whether the results are evenly distributed, and if the deviation rate exceeds a predetermined threshold, she aborts the protocol.
3. **Case 03: (Z-*CTRL*)** TP performed a Z basis measurement on a *CTRL* qubit. In this case, Alice and the participants expect TP to announce both the measurement results $|0\rangle$ and $|1\rangle$ with equal probability. Alice verifies whether the results are evenly distributed, and if the deviation exceeds a predetermined threshold, she aborts the protocol.
4. **Case 04: (Z-*SIFT*)** TP performed a Z basis measurement on a *SIFT* qubit. The qubits in this case are used to establish the secret sharing key. The measurement outcomes announced by TP correspond to Alice's original measurement outcomes, that we denoted as K_i^A, but are randomly shuffled due to the reordering performed by Alice and the participants. Alice's secret key can only

be reconstructed if Alice and all classical participants cooperate by sharing their transposition order of these qubits.

To ensure security, Alice randomly selects a few of these bits and reveals their positions. Bob_1 then discloses the transposition order of these bits, followed by each remaining participant. Alice compares TP's outcomes with her own and if they do not align, the protocol is aborted and restarted. It is important to note that Alice only reveals the positions of those bits and not the outcomes.

2.1.7 Step 08: (Secret sharing)

Once Alice confirms the absence of any eavesdropping or dishonest behavior from TP, she discloses her rearrangement order for the *SIFT* qubits belonging to *Case 04*. However, she does not reveal the corresponding measurement outcomes.

Alice now possess a random bit string K^A of length L, which serves her as a secret key. She then uses K_i to encrypt her secret bit string S as follows:

$$C_i = S_i \oplus K_i^A, \quad \text{for each } i \in \{1, 2, \cdots, N\} \tag{2}$$

Alice then announces C through the authenticated classical channel to share her secret information. When all classical Bobs cooperate by sharing their rearrangement orders, they can reconstruct Alice's secret key K^A from TP's measurement outcomes and decrypt C to retrieve her final secret.

2.2 An example

Now, we present an example of the proposed multiparty MSQSS protocol, where Alice intends to share a secret of length $N = 5$ with two participants, Bob and Charlie. We take $\epsilon = \frac{1}{6}$. In this example, we suppose that TP and the participants are honest.

2.2.1 TP's preparation

Suppose TP prepares a sequence of 26 qubits, each in the state $|+\rangle$ and sends it Alice.

2.2.2 Alice's operations

Upon receiving the sequence, Alice applies the a Z basis measurement to the qubits in positions $(1, 2, 3, 6, 7, 10, 13, 15, 16, 18, 19, 23, 24, 25, 26)$. After her operations, she can end up with the following sequence:

$$\begin{aligned} S_A = \{&|0\rangle_1, |1\rangle_2, |1\rangle_3, |+\rangle_4, |+\rangle_5, |0\rangle_6, |1\rangle_7, |+\rangle_8, |+\rangle_9, |0\rangle_{10}, |+\rangle_{11}, |+\rangle_{12}, \\ &|0\rangle_{13}, |+\rangle_{14}, |1\rangle_{15}, |0\rangle_{16}, |+\rangle_{17}, |0\rangle_{18}, |0\rangle_{19}, |+\rangle_{20}, |+\rangle_{21}, |+\rangle_{22}, |1\rangle_{23}, |1\rangle_{24}, |0\rangle_{25}, |1\rangle_{26}\}. \end{aligned} \tag{3}$$

She shuffles this sequence by the following table:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 11 & 12 & 13 & 14 & 15 & 16 & 17 & 18 & 19 & 20 \\ 21 & 22 & 23 & 24 & 25 & 26 & & & & \end{pmatrix} \longrightarrow \begin{pmatrix} 22 & 19 & 15 & 5 & 12 & 14 & 3 & 21 & 4 & 20 \\ 16 & 6 & 11 & 1 & 8 & 7 & 9 & 13 & 23 & 17 \\ 18 & 24 & 10 & 2 & 26 & 25 & & & & \end{pmatrix} \tag{4}$$

This should read as: first qubit was displaced to position 22, second qubit to position 19, third qubit to position 15 $\cdots$ etc. Therefore, the sequence of qubits turns into:

$$\begin{aligned} S'_A = \{&|+\rangle_{14}, |1\rangle_{24}, |1\rangle_7, |+\rangle_9, |+\rangle_4, |+\rangle_{12}, |0\rangle_{16}, |1\rangle_{15}, |+\rangle_{17}, |1\rangle_{23}, |0\rangle_{13}, |+\rangle_5, \\ &|0\rangle_{18}, |0\rangle_6, |1\rangle_3, |+\rangle_{11}, |+\rangle_{20}, |+\rangle_{21}, |1\rangle_2, |0\rangle_{10}, |+\rangle_8, |0\rangle_1, |0\rangle_{19}, |+\rangle_{22}, |1\rangle_{26}, |0\rangle_{25}\}. \end{aligned} \tag{5}$$

The subscript in each vector refers to the initial position of the qubit in Alice's original sequence S_A. In the rest of the example, we keep those subscripts to keep track of how Alice's original qubits are being reordered.

Alice sends the sequence S'_A to Bob.

2.2.3 Bob's operations

When Bob receives S'_A, he randomly selects the qubits at the position 3, 25, and 26 to measure in the Z basis. Therefore, he obtains:

$$|1\rangle_7 \overset{Measure}{\longrightarrow} |1\rangle_7 , \tag{6}$$

$$|1\rangle_{26} \overset{Measure}{\longrightarrow} |1\rangle_{26} , \tag{7}$$

$$|0\rangle_{25} \overset{Measure}{\longrightarrow} |0\rangle_{25} . \tag{8}$$

After discarding those qubits from S'_A, Bob ends up with the following sequence:

$$\begin{aligned} S_B = \{&|+\rangle_{14} , |1\rangle_{24} , |+\rangle_9 , |+\rangle_4 , |+\rangle_{12} , |0\rangle_{16} , |1\rangle_{15} , |+\rangle_{17} , |1\rangle_{23} , |0\rangle_{13} , |+\rangle_5 , \\ &|0\rangle_{18} , |0\rangle_6 , |1\rangle_3 , |+\rangle_{11} , |+\rangle_{20} , |+\rangle_{21} , |1\rangle_2 , |0\rangle_{10} , |+\rangle_8 , |0\rangle_1 , |0\rangle_{19} , |+\rangle_{22} \}. \end{aligned} \tag{9}$$

Bob shuffles this sequence by the order:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 11 & 12 & 13 & 14 & 15 & 16 & 17 & 18 & 19 & 20 \\ 21 & 22 & 23 & & & & & & & \end{pmatrix} \longrightarrow \begin{pmatrix} 13 & 17 & 15 & 8 & 4 & 5 & 21 & 14 & 12 & 19 \\ 3 & 2 & 18 & 23 & 10 & 6 & 16 & 9 & 11 & 1 \\ 22 & 7 & 20 & & & & & & & \end{pmatrix} \tag{10}$$

This should read as: first qubit in S_B was displaced to position 13, second qubit to position 17 $\cdots$ etc. Therefore, the sequence of qubits turns into:

$$\begin{aligned} S'_B = \{&|+\rangle_8 , |0\rangle_{18} , |+\rangle_5 , |+\rangle_{12} , |0\rangle_{16} , |+\rangle_{20} , |0\rangle_{19} , |+\rangle_4 , |1\rangle_2 , |+\rangle_{11} , |0\rangle_{10} , |1\rangle_{23} , \\ &|+\rangle_{14} , |+\rangle_{17} , |+\rangle_9 , |+\rangle_{21} , |1\rangle_{24} , |0\rangle_6 , |0\rangle_{13} , |+\rangle_{22} , |1\rangle_{15} , |0\rangle_1 , |1\rangle_3 \}. \end{aligned} \tag{11}$$

Bob proceeds to send this sequence to Charlie.

2.2.4 Charlie's operations

Charlie randomly selects the qubits at positions 2, 6, and 13 of S'_B to measure in the Z basis, which means that Charlie measures the qubits $|0\rangle_{18}$, $|+\rangle_{20}$, and $|+\rangle_{14}$, respectively. Charlie can obtain the following outcomes:

$$|0\rangle_{18} \overset{Measure}{\longrightarrow} |0\rangle_{18} , \tag{12}$$

$$|+\rangle_{20} \overset{Measure}{\longrightarrow} |1\rangle_{20} , \tag{13}$$

$$|+\rangle_{14} \overset{Measure}{\longrightarrow} |0\rangle_{14} . \tag{14}$$

After discarding those qubits from S'_B, she ends up with the following sequence:

$$\begin{aligned} S_C = \{&|+\rangle_8 , |+\rangle_5 , |+\rangle_{12} , |0\rangle_{16} , |0\rangle_{19} , |+\rangle_4 , |1\rangle_2 , |+\rangle_{11} , |0\rangle_{10} , |1\rangle_{23} , \\ &|+\rangle_{17} , |+\rangle_9 , |+\rangle_{21} , |1\rangle_{24} , |0\rangle_6 , |0\rangle_{13} , |+\rangle_{22} , |1\rangle_{15} , |0\rangle_1 , |1\rangle_3 \}, \end{aligned} \tag{15}$$

which she shuffles by the following order:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 11 & 12 & 13 & 14 & 15 & 16 & 17 & 18 & 19 & 20 \end{pmatrix} \longrightarrow \begin{pmatrix} 7 & 5 & 1 & 20 & 8 & 18 & 12 & 6 & 15 & 9 \\ 13 & 10 & 11 & 17 & 16 & 4 & 3 & 19 & 2 & 14 \end{pmatrix} \tag{16}$$

Therefore, Charlie ends up with the sequence S'_C as follow:

$$\begin{aligned} S'_C = \{&|+\rangle_{12}, |0\rangle_1, |+\rangle_{22}, |0\rangle_{13}, |+\rangle_5, |+\rangle_{11}, |+\rangle_8, |0\rangle_{19}, |1\rangle_{23}, |+\rangle_9, \\ &|+\rangle_{21}, |1\rangle_2, |+\rangle_{17}, |1\rangle_3, |0\rangle_{10}, |0\rangle_6, |1\rangle_{24}, |+\rangle_4, |1\rangle_{15}, |0\rangle_{16}\}. \end{aligned} \tag{17}$$

Charlie sends this sequence to TP.

2.2.5 TP's operations

Upon receiving S'_C, TP performs the X basis measurement in the positions $(1, 2, 3, 5, 8, 10, 14, 17, 18)$ and the Z basis measurement in the remaining positions. Then TP announces his measurement basis for each qubit as well as his measurement outcomes. If TP is honest, he announces the following sequence:

$$\begin{aligned} S'_{TP} = \{&|+\rangle_{12}, |-\rangle_1, |+\rangle_{22}, |0\rangle_{13}, |+\rangle_5, |1\rangle_{11}, |0\rangle_8, |+\rangle_{19}, |1\rangle_{23}, |+\rangle_9, \\ &|1\rangle_{21}, |1\rangle_2, |0\rangle_{17}, |+\rangle_3, |0\rangle_{10}, |0\rangle_6, |-\rangle_{24}, |+\rangle_4, |1\rangle_{15}, |0\rangle_{16}\}. \end{aligned} \tag{18}$$

2.2.6 Eavesdropping check

Following Alice's request, Bob and Charlie announces the positions and outcomes of their selected qubits as indicated in the steps of the protocol. Alice verifies if their outcomes on the *SIFT* qubits are aligned with her own, which is the case in the following situation. and that Charlie's outcomes on the *CTRL* qubits are evenly distributed, which is also satisfied.

It is important to note that Bob must take into account his discarded qubits on S_B to determine the correct corresponding positions of Charlie's selected qubits.

Based on this verification, Bob and Charlie pass the public discussion.

2.2.7 TP's honesty check

By using their respective transposition tables (Tables 10 and 16), Bob and Charlie publicly announce, in reverse order, the correct transposition of the qubits that TP measured in the X basis. Note that they must account for the discarded qubits in order to determine the correct reordering. Then, after Alice announces the positions of the *CTRL* particles, Bob and Charlie publish their transposition orders for the qubits at those corresponding positions. Based on the operations of Alice and TP, we obtain the following four subsequences of S'_{TP}:

1. Subset where TP measured the *CTRL* qubits in the X basis:

$$S_{CX} = \{|+\rangle_{12}, |+\rangle_{22}, |+\rangle_5, |+\rangle_9, |+\rangle_4\}. \tag{19}$$

   As we can see, all TP's measurement results are the state $|+\rangle$ as they should be.

2. Subset where TP measured the *SIFT* qubits in the X basis:

$$S_{SX} = \{|-\rangle_1, |+\rangle_{19}, |+\rangle_3, |-\rangle_{24}\}. \tag{20}$$

   As we can see, we have an even distribution for the states $|+\rangle$ and $|-\rangle$.

3. Subset where TP measured the *CTRL* qubits in the Z basis:

$$S_{CZ} = \{|1\rangle_{11}, |0\rangle_8, |1\rangle_{21}, |0\rangle_{17}\}. \tag{21}$$

   As we can see, we have an even distribution for the states $|0\rangle$ and $|1\rangle$.

4. Subset where TP measured the *SIFT* qubits in the Z basis:

$$S_{SZ} = \{|0\rangle_{13}, |1\rangle_{23}, |1\rangle_{2}, |0\rangle_{10}, |0\rangle_{6}, |1\rangle_{15}, |0\rangle_{16}\}. \tag{22}$$

Alice uses the measurement outcomes of the 2^{nd} and 6^{th} qubits of her sequence S_A as test bits, which correspond to the 3^{rd} and 5^{th} qubits of S_{SZ}. As we can see, TP announced the correct measurement results.

After the eavesdropping detection passes, TP, Bob, and Charlie have access to the following result ($'01010'$). By sharing their own rearrangement order, Bob and Charlie can obtain Alice's bit string $K =' 00101'$.

3 Security analysis

In this section, we examine the security of the proposed protocol. Given that TP possesses greater capabilities than any external or internal eavesdropper, we focus on the scenario where TP acts as the primary adversary. To steal Alice's secret, TP might employ various attacks. Our analysis demonstrates that the protocol remains secure against well-known strategies, including the fake states attack, intercept-resend attack, entanglement-measure attack, and Trojan horse attacks. Additionally, we address the potential threat of collusion, where TP collaborates with one or more participants to compromise Alice's secret.

3.1 Fake states attack

In this attack, TP prepares qubits in states other than $|+\rangle$, as required of him in step 1 of the protocol. Suppose TP prepares his sequence in the Z basis $\{|0\rangle, |1\rangle\}$. Although this strategy allows him to control the content of Alice's secret key, he cannot distinguish the *SIFT* particles from the *CTRL* particles. As a result, although TP's attack goes undetected during the initial eavesdropping check between Alice and the participants, it will be detected with probability $1 - (7/8)^L$ during the honesty check. This probability converges to 1 as L becomes sufficiently large.

3.2 Intercept-resend attack

In this attack, TP attempts to learn the rearrangement order of each participant. To do so, he intercepts the sequence S'_A sent by Alice to Bob_1 and stores it in his quantum memory. He then sends a fake sequence of particles to each Bob_i in turn. After a participant completes his operations, TP intercepts the fake sequence and measures it in an attempt to deduce the participant's rearrangement order. Once TP has retrieved and measured all the fake sequences, he applies the inferred rearrangement orders to the stored sequence S'_A and sends it back to Alice. However, this attack is bound to fail. To demonstrate this, we examine the following two strategies:

- *The fake sequences are composed of qudits:* without loss of generality, suppose that TP prepares the qubits in his fake sequences in the Z basis. In this scenario, TP cannot distinguish whether two qubits in the same state but at different positions have been exchanged. For example, consider the sequence $\{|1\rangle, |1\rangle, |0\rangle, |0\rangle\}$. If it is reordered to $\{|1\rangle, |0\rangle, |1\rangle, |0\rangle\}$, TP cannot tell whether the first $|1\rangle$ remained in place or was moved to the third position. When the sequence is large, the probability of correctly guessing the transposition order becomes negligible. Furthermore, this attack would inevitably be detected during the eavesdropping check between Alice and the participants, since TP's fake sequences do not match Alice's original sequence S'_A. As a result, the participants' measurement outcomes in step 3 of the protocol would not necessarily align with the outcomes Alice recorded in step 2. Therefore, TP cannot gain any useful information using this strategy.
- *The fake sequences are composed of qubits:* in this strategy, TP uses n-level quantum states to prepare his fake sequences. To deduce Bob_1's rearrangement order, for instance, TP prepares the sequence $\{|0\rangle_N, |1\rangle_N, |2\rangle_N, \cdots, |N-1\rangle_N\}$, where the subscript N is to denote that they are N dimensional vectors. After Bob_1 completes his operations, TP retrieves the sequence and measures

the particles in the $Z^{(N)} = \{|0\rangle_N, |1\rangle_N, \cdots, |N-1\rangle_N\}$ basis. Since all the states in the sequence are mutually orthogonal, TP can determine Bob_1's rearrangement order with certainty. If Bob_1's actions consisted solely of reordering the particles, TP's strategy would succeed. However, Bob_1 also randomly selects a subset of particles to measure in the two-level Z basis $\{|0\rangle, |1\rangle\}$. In that case, TP's attack is bound to be detected since Bob_1's outcomes won't be aligned with Alice's results in step 02 of the protocol. The same reasoning applies to the other Bobs, meaning that TP cannot obtain any useful information using this strategy without being detected.

3.3 Entanglement-measure attack

The entanglement-measure attack of TP is modeled by the unitary operations (U_F, U_R), where U_F is used to attack the particles sent by Alice to Bob_1, and U_R is used to attack the particles sent by Bob_M to TP. Note that TP does not attack the particles he sends to Alice, as they do not carry any information about Alice's secret or the participants' secret shadows. Furthermore, TP uses a different auxiliary probe, denoted as F and R respectively, for each unitary operation. The reason is that, since the sequence sent by Alice is reordered by the participants, TP cannot determine which ancilla F corresponds to each retrieved particle.

Theorem 1. *Suppose TP performs an attack (U_F, U_R) on the particles traveling from Alice to Bob_1 and from Bob_M back to him, where F and R are TP's auxiliary probes. TP introduces no error during the eavesdropping check if and only if the final states of his probes are independent of his measurement results on the qubits received by Bob_M. As a result, TP gains no information about Alice's shared secret.*

Proof. TP intercepts S'_A from Alice and applies U_F to each traveling qubit along with its associated ancilla F, initially prepared in some arbitrary normalized state $|f\rangle$. The composite system then evolves as follows:

$$U_F(|0\rangle|f\rangle) = \alpha|0\rangle|f_0\rangle + \beta|1\rangle|f_1\rangle, \tag{23}$$
$$U_F(|1\rangle|f\rangle) = \beta|0\rangle|f_2\rangle + \alpha|1\rangle|f_3\rangle, \tag{24}$$

such as $|\alpha|^2 + |\beta|^2 = 1$, and $|f_i\rangle$ are states that TP can distinguish. By linearity, we obtain

$$U_F(|+\rangle|f\rangle) = \frac{1}{\sqrt{2}}|0\rangle\big(\alpha|f_0\rangle + \beta|f_2\rangle\big) \tag{25}$$
$$+ \frac{1}{\sqrt{2}}|1\rangle\big(\beta|f_1\rangle + \alpha|f_3\rangle\big) \tag{26}$$

In order for TP to pass the eavesdropping check between Alice and the participants in **Step 05** of the protocol, he must adjust U_F accordingly. Specifically, TP must set $\beta = 0$ to ensure that the participants do not obtain invalid outcomes, and $\alpha = 1$ to satisfy the normalization condition. Under these constraints, the above equations reduce to:

$$U_F(|0\rangle|f\rangle) = |0\rangle|f_0\rangle, \tag{27}$$
$$U_F(|1\rangle|f\rangle) = |1\rangle|f_3\rangle, \tag{28}$$
$$U_F(|+\rangle|f\rangle) = \frac{1}{\sqrt{2}}\big(|0\rangle|f_0\rangle + |1\rangle|f_3\rangle\big) \tag{29}$$

When Bob_M sends his sequence, TP attaches to each qubit a new probe, initially prepared in some arbitrary normalized state $|r\rangle$. He then applies the operation $(U_R \otimes I_F)$ to the composite system, which evolves as follows:

$$(U_R \otimes I_F)(U_F|0\rangle|f\rangle) = \gamma|0\rangle|r_0\rangle|f_0\rangle + \delta|1\rangle|r_1\rangle|f_0\rangle, \tag{30}$$
$$(U_R \otimes I_F)(U_F|1\rangle|f\rangle) = \delta|0\rangle|r_2\rangle|f_3\rangle + \gamma|1\rangle|r_3\rangle|f_3\rangle, \tag{31}$$
$$\tag{32}$$

where $|\gamma|^2 + |\delta|^2 = 1$, and $|r_i\rangle$ are states that TP can distinguish. By linearity, we obtain

$$(U_R \otimes I_F)(U_F |+\rangle |f\rangle) = \frac{1}{\sqrt{2}} |0\rangle \left(\gamma |r_0\rangle |f_0\rangle + \delta |r_2\rangle |f_3\rangle\right) \tag{33}$$

$$+ \frac{1}{\sqrt{2}} |1\rangle \left(\delta |r_1\rangle |f_0\rangle + \gamma |r_3\rangle |f_3\rangle\right) \tag{34}$$

If TP wants to pass the honesty check, then the final state of the first register must be identical to the original state sent by Alice. This implies that TP must satisfy the conditions $\delta = 0$ and $\gamma = 1$. Therefore, U_R is now defined as follows:

$$(U_R \otimes I_F)(U_F |0\rangle |f\rangle) = |0\rangle |r_0\rangle |f_0\rangle , \tag{35}$$

$$(U_R \otimes I_F)(U_F |1\rangle |f\rangle) = |1\rangle |r_3\rangle |f_3\rangle , \tag{36}$$

$$\tag{37}$$

By linearity

$$(U_R \otimes I_F)(U_F |+\rangle |f\rangle) = \frac{1}{2} |+\rangle \left(|r_0\rangle |f_0\rangle + |r_3\rangle |f_3\rangle\right) \tag{38}$$

$$+ \frac{1}{2} |-\rangle \left(|r_0\rangle |f_0\rangle - |r_3\rangle |f_3\rangle\right) \tag{39}$$

To go undetected, TP must set the incorrect terms as a zero vector, specifically:

$$|r_0\rangle |f_0\rangle = |r_3\rangle |f_3\rangle , \tag{40}$$

which means that

$$|f_0\rangle = |f_3\rangle = |F\rangle , \tag{41}$$

$$|r_0\rangle = |r_3\rangle = |R\rangle . \tag{42}$$

After inserting Eq. (41) into Eqs. (35-38), we obtain

$$\begin{cases} (U_R \otimes I_F)(U_F |0\rangle |f\rangle) = |0\rangle |R\rangle |F\rangle , \\ (U_R \otimes I_F)(U_F |1\rangle |f\rangle) = |1\rangle |R\rangle |F\rangle , \\ (U_R \otimes I_F)(U_F |+\rangle |f\rangle) = |+\rangle |R\rangle |F\rangle . \end{cases} \tag{43}$$

According to Eq. (43), when TP remains undetected during both the eavesdropping check with the participants and the honesty check, not only can he not distinguish the final states of his ancillary probes, but these states are also always independent of the *CTRL* and *SIFT* particles. As a result, TP obtains no information about Alice's shared secret key.

□

3.4 Trojan horse attack

Quantum Trojan horse attacks are common implementation attacks, in which TP inserts invisible or delayed photons into the particles he transmits to Alice. After retrieving these Trojan horse photons, TP can measure them to extract information about Alice's operations. He can use the same strategy with the other participants to obtain their secret shadows. Fortunately, the participants can easily defend against this attack by using a photon number splitter (PNS) and a wavelength filter device (WF). Therefore, the proposed protocol is secure against quantum Trojan horse attacks.

3.5 Collusion attack

In this attack, TP collaborates with some dishonest participants to obtain Alice's secret. Without loss of generality, consider the extreme scenario where only Bob_i (along with Alice of course) is honest. A first strategy is to guess Bob_i's reordering. However, since the permutation is chosen randomly and independently of the other Bobs, the probability of guessing it correctly is $1/n!$, which becomes negligible as n grows large.

A second strategy is for TP to still apply the attacks previously described, while the $M-1$ dishonest Bobs announce fake transposition orders in an attempt to avoid detection during the eavesdropping and honesty checks. However, this strategy will inevitably fail. First, TP and the dishonest Bobs do not know which qubits Bob_i will choose to measure in the Z basis, nor their states. Furthermore, they cannot distinguish the *CTRL* qubits from the *SIFT* qubits in Alice's sequence S'_A, as Alice only discloses this information after all Bobs have revealed the transposition orders of the X-*CTRL* qubits. As a result, the fake transposition orders will introduce errors during both the eavesdropping and honesty checks, causing the protocol to be aborted.

Overall, our protocol is secure against collusion attacks.

4 Efficiency analysis and comparison

In this section, we analyze the efficiency of the proposed protocol and compare its performance with existing multiparty mediated QSS protocols. The efficiency of our scheme, as well as those presented in Refs. [23, 24], can be calculated using the following formula:

$$\eta = \frac{c}{q+b}, \tag{44}$$

where c is the length of the final secret key, q is the number of qubits generated by TP, and b is the number of qubits generated by the classical participants. In the proposed scheme, TP generates $q = 4L(1+M\epsilon)$ qubits. Alice measures approximately half of these qubits in the Z basis and replaces them with newly generated ones in the same states she observed. Since she is the only classical participant who generates qubits, we have $b = 2L(1+M\epsilon)$. As for the M Bobs, they select altogether $4LM\epsilon$ qubits to measure and forward the rest to TP. At the end, only the Z-*SIFT* qubits are used as the final secret key, thus $c = L$. The qubit efficiency becomes:

$$\eta = \frac{1}{6+M\epsilon}, \tag{45}$$

We now compare the proposed protocol with other multiparty mediated QSS protocols. The comparison is drawn from four perspective: quantum resources, quantum capabilities of the participants, communication structure, and qubit efficiency. The results are summarized in Table 1.

Table 1: Comparison of proposed protocol with other Mediated MQSS schemes.

Protocol	Quantum resources	Capabilities of classical participants	Communication structure	Qubit efficiency
Tsai et al. [23]	GHZ states	1. Measure $\{\|0\rangle, \|1\rangle\}$ 2. Perform Hadamard H	One-way	$\frac{1}{2^{M+1}(M+1)}$
Tsai et al. [24]	Graph states			$\frac{1}{4(M+1)}$
Our protocol	Single qubits	1. Measure $\{\|0\rangle, \|1\rangle\}$ 2. Reorder qubits	Circular	$\frac{1}{6(1+M\epsilon)}$

In terms of quantum resources, the protocols of Tsai et al. [23, 24] require TP to generate multi-particle GHZ states and complete graph states, which are difficult to produce and maintain. In contrast,

our protocol requires TP only to prepare $|+\rangle$ states and to perform single-qubit measurements in the X and Z bases. This significantly reduces TP's quantum overhead, making the proposed protocol more practical and feasible in terms of implementation.

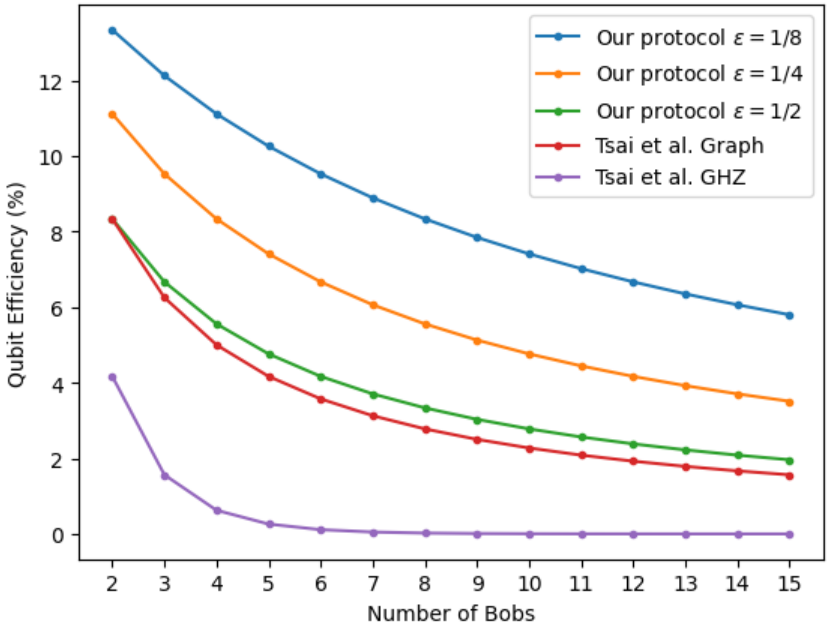

Figure 1: Qubit efficiency of the different schemes for different numbers of Bobs.

Regarding communication structure, our protocol uses a circular qubit transmission method, whereas Tsai et al.'s protocols adopt a one-way transmission method. This gives Tsai et al.'s protocols certain advantages, such as reduced qubit transmission distance. Additionally, it prevents the classical participants from needing additional devices to defend against quantum Trojan horse attacks. However, in terms of qubit efficiency, our protocol exhibits a significant advantage, especially over the protocol that is based on GHZ states. In Figure 1, we can more clearly compare the efficiency of our protocol for different values of ϵ with that of Tsai et al.'s protocols as a function of the number of classical Bobs. Specifically, for the protocol based on GHZ states, the qubit efficiency drops below 1% (i.e. 0.625%) when the number of classical Bobs reaches 4, which makes the protocol extremely inefficient. As for the protocol based on graph states, the efficiency of our protocol remains superior regardless of the number of Bobs when $\epsilon \geq 1/2$. Note that setting ϵ to this value is an extreme choice. In an ideal case, and especially when N is large, each Bob taking a small subset no larger than half the length of the secret is enough to evaluate the error rate with Alice. Therefore, setting $\epsilon = 1/8$ is a very reasonable choice.

Overall, even though Tsai et al.'s protocols shorten the qubit transmission distance and naturally ward off quantum Trojan horse attacks, our protocol demonstrates higher qubit efficiency and utilizes far cheaper quantum resources that are easier to handle, making it more feasible and efficient in terms of implementation. Furthermore, the circular communication structure gives our protocol an advantage in terms of scalability in the multiparty scenarios.

5 Conclusion

This study introduces the first mediated MSQSS protocol based on single qubits. The protocol allows classical Alice to share a secret with M classical Bobs. Compared to similar approaches, the quantum overhead of TP is significantly reduced, and the qubit efficiency is notably improved. As a result, the proposed scheme is more feasible and efficient in terms of implementation. It is also more practical than typical standard multiparty SQSS protocols, as (1) Alice does not need to possess full quantum capabilities, and (2) the classical participants only need to perform two operations (i.e. measuring in the Z basis and reordering qubits). Furthermore, security analysis shows that the protocol can resist

common attacks. In future work, it would be interesting to study the behavior of the protocol in the presence of noise.

References

[1] Saber Bagherinezhad and Vahid Karimipour. Quantum secret sharing based on reusable greenberger-horne-zeilinger states as secure carriers. 67(4):044302. ISSN 1094-1622. doi: 10.1103/physreva.67.044302.

[2] G. R. BLAKLEY. Safeguarding cryptographic keys. In *1979 International Workshop on Managing Requirements Knowledge (MARK)*. IEEE. doi: 10.1109/mark.1979.8817296.

[3] Michel Boyer, Ran Gelles, Dan Kenigsberg, and Tal Mor. Semiquantum key distribution. 79(3): 032341, . ISSN 1094-1622. doi: 10.1103/physreva.79.032341.

[4] Michel Boyer, Matty Katz, Rotem Liss, and Tal Mor. Experimentally feasible protocol for semiquantum key distribution. 96(6):062335, . ISSN 2469-9934. doi: 10.1103/physreva.96.062335.

[5] Michel Boyer, Dan Kenigsberg, and Tal Mor. Quantum key distribution with classical bob. 99(14): 140501, . ISSN 1079-7114. doi: 10.1103/physrevlett.99.140501.

[6] Isaac L. Chuang and Yoshihisa Yamamoto. Simple quantum computer. 52(5):3489–3496. ISSN 1094-1622. doi: 10.1103/physreva.52.3489.

[7] Juan Ignacio Cirac. Quantum computing and simulation: Where we stand and what awaits us. 10 (1):453–456. ISSN 2192-8606. doi: 10.1515/nanoph-2020-0351.

[8] Gan Gao, Yue Wang, and Dong Wang. Multiparty semiquantum secret sharing based on rearranging orders of qubits. 30(10):1650130. ISSN 1793-6640. doi: 10.1142/s021798491650130x.

[9] Mark Hillery, Vladimír Bužek, and André Berthiaume. Quantum secret sharing. 59(3):1829–1834. ISSN 1094-1622. doi: 10.1103/physreva.59.1829.

[10] Yan-Yan Hou, Tao Xu, Jian Li, Chong-Qiang Ye, Zhuo Wang, and Xin-Yu Liu. Circular semiquantum secret sharing based on hybrid single particle and ghz-type states. 21(2):025202. ISSN 1612-202X. doi: 10.1088/1612-202x/ad1aab.

[11] Hasan Iqbal and Walter O. Krawec. Semi-quantum cryptography. 19(3). ISSN 1573-1332. doi: 10.1007/s11128-020-2595-9.

[12] Anders Karlsson, Masato Koashi, and Nobuyuki Imoto. Quantum entanglement for secret sharing and secret splitting. 59(1):162–168. ISSN 1094-1622. doi: 10.1103/physreva.59.162.

[13] Walter O. Krawec. Mediated semiquantum key distribution. 91(3):032323. ISSN 1094-1622. doi: 10.1103/physreva.91.032323.

[14] Lvzhou Li, Daowen Qiu, and Paulo Mateus. Quantum secret sharing with classical bobs. 46(4): 045304, . ISSN 1751-8121. doi: 10.1088/1751-8113/46/4/045304.

[15] Qin Li, W. H. Chan, and Dong-Yang Long. Semiquantum secret sharing using entangled states. 82 (2):022303, . ISSN 1094-1622. doi: 10.1103/physreva.82.022303.

[16] Zhongliang Ma, Jing Li, Xianmin Wang, and Feng Liu. Semi-quantum secret sharing protocol with specific bits based on third party. 21(12):125201. ISSN 1612-202X. doi: 10.1088/1612-202x/ad821c.

[17] M. B. Plenio and P. L. Knight. Realistic lower bounds for the factorization time of large numbers on a quantum computer. 53(5):2986–2990. ISSN 1094-1622. doi: 10.1103/physreva.53.2986.

[18] Pradeep Sarvepalli. Nonthreshold quantum secret-sharing schemes in the graph-state formalism. 86 (4):042303. ISSN 1094-1622. doi: 10.1103/physreva.86.042303.

[19] Adi Shamir. How to share a secret. 22(11):612–613. ISSN 1557-7317. doi: 10.1145/359168.359176.

[20] Armin Tavakoli, Isabelle Herbauts, Marek Żukowski, and Mohamed Bourennane. Secret sharing with a single<mml:math xmlns:mml="http://www.w3.org/1998/math/mathml"><mml:mi>d</mml:mi></mml:math>-level quantum system. 92(3):030302. ISSN 1094-1622. doi: 10.1103/physreva.92.030302.

[21] Yuan Tian, Genqing Bian, Jinyong Chang, Ying Tang, Jian Li, and Chongqiang Ye. A semi-quantum secret-sharing protocol with a high channel capacity. 25(5):742, . ISSN 1099-4300. doi: 10.3390/e25050742.

[22] Yuan Tian, Jian Li, Xiu-Bo Chen, Chong-Qiang Ye, and Heng-Ji Li. An efficient semi-quantum secret sharing protocol of specific bits. 20(6), . ISSN 1573-1332. doi: 10.1007/s11128-021-03157-2.

[23] Chia-Wei Tsai, Chun-Wei Yang, and Jason Lin. Multiparty mediated quantum secret sharing protocol. 21(2). ISSN 1573-1332. doi: 10.1007/s11128-021-03402-8.

[24] Chia-Wei Tsai and Chun-Hsiang Wang. Efficient mediated quantum secret sharing protocol in a restricted quantum environment. 535(11). ISSN 1521-3889. doi: 10.1002/andp.202300116.

[25] Chih-Lun Tsai and Tzonelih Hwang. Semi-quantum key distribution robust against combined collective noise. 57(11):3410–3418. ISSN 1572-9575. doi: 10.1007/s10773-018-3854-8.

[26] Tomáš Tyc and Barry C. Sanders. How to share a continuous-variable quantum secret by optical interferometry. 65(4):042310. ISSN 1094-1622. doi: 10.1103/physreva.65.042310.

[27] Jian Wang, Sheng Zhang, Quan Zhang, and Chao-Jing Tang. Semiquantum key distribution using entangled states. 28(10):100301. ISSN 1741-3540. doi: 10.1088/0256-307x/28/10/100301.

[28] Chen Xie, Lvzhou Li, and Daowen Qiu. A novel semi-quantum secret sharing scheme of specific bits. 54(10):3819–3824. ISSN 1572-9575. doi: 10.1007/s10773-015-2622-2.

[29] Xiangjun Xin, Fan He, Chaoyang Li, and Fagen Li. Multiparty semi-quantum secret sharing protocol based on single photon sequence and permutation. 39(17n18). ISSN 1793-6632. doi: 10.1142/s0217732324500846.

[30] Ding Xing, Yifei Wang, Zhao Dou, Jian Li, Xiubo Chen, and Lixiang Li. Efficient semi-quantum secret sharing protocol using single particles. 32(7):070308. ISSN 1674-1056. doi: 10.1088/1674-1056/ace159.

[31] CHUN-WEI YANG and TZONELIH HWANG. Efficient key construction on semi-quantum secret sharing protocols. 11(05):1350052. ISSN 1793-6918. doi: 10.1142/s0219749913500524.

[32] Mustapha Anis Younes, Sofia Zebboudj, and Abdelhakim Gharbi. A lightweight and efficient multiparty semi-quantum secret sharing protocol using entangled states for sharing specific bit. 63(11). ISSN 1572-9575. doi: 10.1007/s10773-024-05834-1.

[33] I-Ching Yu, Feng-Li Lin, and Ching-Yu Huang. Quantum secret sharing with multilevel mutually (un)biased bases. 78(1):012344. ISSN 1094-1622. doi: 10.1103/physreva.78.012344.

[34] Zhan-jun Zhang, Yong Li, and Zhong-xiao Man. Multiparty quantum secret sharing. 71(4):044301. ISSN 1094-1622. doi: 10.1103/physreva.71.044301.

[35] Xiangfu Zou, Daowen Qiu, Lvzhou Li, Lihua Wu, and Lvjun Li. Semiquantum-key distribution using less than four quantum states. 79(5):052312. ISSN 1094-1622. doi: 10.1103/physreva.79.052312.