Advanced Quantum Technologies

Multiparty-to-Multiparty Semi-quantum Secret Sharing Protocol

--Manuscript Draft--

Manuscript Number:	qute.202400617
Article Type:	Research Article
Corresponding Author:	Chun-Wei Yang, Ph.D. China Medical University Taichung, TAIWAN
Order of Authors:	Chia-Wei Tsai, Ph.D.
	Chun-Hsiang Wang
	Jason Lin, Ph.D.
	Chun-Wei Yang, Ph.D.
Keywords:	quantum secret sharing protocol; semi-quantum; graph state; quantum Trojan horse attacks
Abstract:	This study proposes the first multiparty-to-multiparty semi-quantum secret sharing (MMSQSS) protocol within a restricted quantum environment. Unlike existing fully quantum secret sharing (QSS) protocols, this protocol allows protocol participants with limited quantum capabilities—including (1) measuring a single qubit in the Z-basis and (2) performing single-qubit unitary operations—to participate, significantly reducing implementation costs. By employing one-way qubit transmission, the proposed MMSQSS protocol not only simplifies the quantum communication process but also effectively defends against quantum Trojan horse attacks. The correctness and security analyses demonstrate that the proposed MMSQSS protocol is robust against various well-known attack strategies. Simulation experiments confirm the feasibility of the protocol for various numbers of participants. It maintains high levels of efficiency and security even as the number of participants increases. Moreover, compared with existing protocols, the proposed MMSQSS protocol lowers the barrier to practical quantum communication deployment by reducing the quantum resources required for protocol participants.

Multiparty-to-Multiparty Semi-quantum Secret Sharing Protocol

Chia-Wei Tsai[1, a], Chun-Hsiang Wang[1, b], Jason Lin[2, c], and Chun-Wei Yang[3, *]

[1]Department of Computer Science and Information Engineering, National Taichung University of Science and Technology, No.129, Sec. 3, Sanmin Rd., North Dist., Taichung 40401, Taiwan, R.O.C.
[2]Department of Computer Science and Engineering, National Chung Hsing University, No. 145, Xingda Rd., South District, Taichung 40227, Taiwan.
[3]Master Program for Digital Health Innovation, College of Humanities and Sciences, China Medical University, No. 100, Sec. 1, Jingmao Rd., Beitun Dist., Taichung 406040, Taiwan.

[a]cwtsai@nutc.edu.tw
[b]jam930725@gmail.com
[c]jasonlin@nchu.edu.tw
[*]cwyang@mail.cmu.edu.tw

Abstract

This study proposes the first multiparty-to-multiparty semi-quantum secret sharing (MMSQSS) protocol within a restricted quantum environment. Unlike existing fully quantum secret sharing (QSS) protocols, this protocol allows protocol participants with limited quantum capabilities—including (1) measuring a single qubit in the Z-basis and (2) performing single-qubit unitary operations—to participate, significantly reducing implementation costs. By employing one-way qubit transmission, the proposed MMSQSS protocol not only simplifies the quantum communication process but also effectively defends against quantum Trojan horse attacks. The correctness and security analyses demonstrate that the proposed MMSQSS protocol is robust against various well-known attack strategies. Simulation experiments confirm the feasibility of the protocol for various numbers of participants. It maintains high levels of efficiency and security even as the number of participants increases. Moreover, compared with existing protocols, the proposed MMSQSS protocol lowers the barrier to practical quantum communication deployment by reducing the quantum resources required for protocol participants.

Keywords: quantum secret sharing protocol, semi-quantum, graph state, quantum Trojan horse attacks.

1. Introduction

Secret sharing is a cryptographic technique that secures information by splitting it into multiple parts, often referred to as “agents.” Each agent, on its own, does not reveal any information about the secret; however, when sufficient agents cooperate with each other, the original secret can be reconstructed. Therefore, this cryptographic method is advantageous in situations where sensitive information needs to be protected but simultaneously needs to be recoverable by a group of authorized participants. To achieve secret sharing, Shamir [1] adopted polynomial interpolation to propose the classical secret sharing (CSS) protocols in 1979. In Shamir’s quantum secret sharing (QSS) protocol, a secret is divided into shadows using a polynomial of degree $k-1$, where k is the minimum number of shadows needed to reconstruct the secret. The polynomial coefficients are randomly generated, with the constant term being the secret. Each agent receives a shadow corresponding to a unique point on the polynomial. At least *k* agents (points) are required to reconstruct the secret. Although Shamir's CSS offers theoretical information security, it has certain limitations. Specifically, (1) the size of each secret share must be at least equal to that of the original secret and (2) securely distributing these large secret shares poses significant challenges. To address these issues, certain mathematical approaches, such as the geometric plane and Chinese Remainder Theorem, have been employed to develop computationally secure CSS protocols [2, 3]. Compared with information-theoretically secure CSS protocols, these computationally secure protocols are more feasible for implementation in practical network environments. However, computationally secure CSS protocols may become vulnerable in computing scenarios involving quantum mechanics, particularly if quantum computers can solve the underlying mathematical problems. In response to the vulnerability of classical secret sharing (CSS) protocols with the advent of quantum computers, Hillery et al. [4] leveraged the quantum entanglement properties of the Greenberger–Horne–Zeilinger (GHZ) state [5] to propose the first quantum secret sharing (QSS) protocol in 1997. Because the security of Hillery et al.'s QSS protocol is based on quantum mechanics, the computational power of quantum computers cannot affect the security of the protocol. Subsequently, numerous studies [6-21] have proposed various QSS protocols using different quantum states/properties or implemented QSS protocols.

However, these QSS protocols only let a secret owner (known as a "dealer") share their secret with 2~m agents. Therefore, QSS protocols cannot be used for specific applications. For instance, imagine a military research unit developing a dangerous new weapon. To ensure safe use, weapon activation requires a secret key. To prevent any single researcher from having complete control over this secret key—because they might leak it—the key must be generated collectively by all researchers involved. In addition, the military cannot allow a single officer to hold the entire key. Instead, the key must be divided into multiple parts that are entrusted to different officers. Only when all the officers holding these key fragments convene can the key be reconstructed, allowing it to be activated. The aforementioned QSS protocols are unsuitable for this application. To address this issue, the concept of multiparty-to-multiparty quantum secret sharing (MMQSS) was proposed in which two groups of m and n participants exist. All m participants in group 1 collectively generate the secret message and share it with n participants in group 2. No subset of either group could correctly recover the secret message without the cooperation of the entire set of either group 1 or group 2. In line with the concept of MMQSS, the studies in [22-32] proposed various MMQSS protocols that utilize different quantum resources or properties.

In 2005, Yan and Gao [22] introduced the first MMQSS protocol employing single photons to share secrets between two groups of different sizes; the secret could only be recovered if all the participants in each group cooperated. However, Li et al. [23] identified a security issue within the protocol: the last participant of group 1 could maliciously replace the secret message without being detected, and suggested how to fix it. Since then, various studies have emerged and different MMQSS protocols have been proposed. Han et al. [24] developed an MMQSS protocol using continuous variable operations instead of special discrete unitary operations to encode secrets that prevent certain types of special attacks. [25, 26] further improved the security of the MMQSS protocol using two and three conjugate bases, respectively. In 2010, Shi et al. [27] introduced an MMQSS protocol using Bell states and Bell measurements in which a trusted third party (TP) was assumed to securely generate and distribute quantum resources to all participants. Sheng et al. [28] used squeezed states to propose a new protocol and analyzed its security under various lossy channel conditions. Qin et al. [29] used entangled states to propose a new scheme distinct from previous studies, which allowed participants in one group to transmit their shared secret to participants in another group while both groups could keep their shared secret, and each group could reconstruct the secret independently. However, the study was limited by the same number of participants in both groups.

Additionally, an advanced version of the MMQSS protocol, a dynamic multiparty to multiparty quantum secret sharing (DMMQSS) protocol, was proposed by Zhou et al. [30] using the GHZ state in which participants can join or leave any secret sharing session without compromising the integrity and security of the protocol. Zhou et al.'s DMMQSS protocol allows the number of participants to vary before quantum resources are measured, thus significantly improving the flexibility and applicability. In 2023, You et al. [31] proposed a more practical DMMQSS protocol based on single photons that incurred fewer security risks than [30]. Moreover, the scheme did not require the verification of secret shares when adding a new participant. Later, Tian et al. [32] utilized Bell states to propose a DMMQSS protocol and verified its correctness through simulations using IBM's Qiskit platform [33].

Although MMQSS protocols can address the problem of sharing secrets between participants in two groups, they face challenges in practical implementation. In other words, these protocols always assume that the participants have complete quantum capabilities/devices. However, the implementation costs of some quantum capabilities/devices are high (e.g., storing a qubit or maintaining entanglement for a long time) under current quantum technologies. If all protocol participants are equipped with expensive quantum devices, the implementation will not be economically feasible. Therefore, enabling the participants to use easily implemented quantum capabilities to achieve quantum communication protocols is an important research issue. To address this issue, Boyer et al. introduced the innovative concept of a semi-quantum environment, comprising two types of users: classical users, who have limited quantum capabilities, and quantum users, who have full quantum capabilities. The first semi-quantum key distribution (SQKD) protocol was proposed by Boyer et al. [34, 35]. Thereafter, various semi-quantum communication (SQC) protocols [36-47] have been proposed based on semi-quantum environments. Semi-quantum environments can be classified into four types according to the quantum capabilities of classical users, as summarized in **Table 1**.

Table 1. Four types of semi-quantum environments

Environment	Capabilities of classical user
Measure and resend	(1) generate qubits in Z-basis (2) measure qubits in Z-basis (3) reflect qubits without introducing any disturbance
Randomization-based	(1) measure qubits in Z-basis (2) reorder qubits by employing different delay lines (3) reflect qubits without introducing any disturbance
Measurement-free	(1) generate Z-basis qubits (2) reorder qubits by employing different delay lines (3) reflect qubits without introducing any disturbance
Restricted quantum (Operation-based)	(1) generate qubits in Z-basis (2) perform single-qubit operation

An important branch of SQC protocols is the secret sharing protocol, which can be divided into two types: semi-quantum secret sharing (SQSS) [36-42] and mediated semi-quantum secret sharing (MSQSS)[46, 47] protocols. An SQSS protocol allows a quantum user (a dealer) to share secret messages with multiple classical users (agents), whereas an MSQSS protocol enables a classical user (a dealer) to share secret messages with multiple classical users (agents) with the help of a quantum TP. Although the two types of SQSS protocols can achieve secret sharing tasks in a semi-quantum environment, these SQSS protocols cannot allow multiple dealers to share secret messages with various agents. Therefore, this study adopts the property of the graph state to propose the first multiparty-to-multiparty semi-quantum secret sharing (MMSQSS) protocol. In the proposed MMSQSS protocol, *m* classical dealers can generate a secret message and share it with *n* classical agents with the assistance of a dishonest TP (a quantum user). Classical dealers and agents have only two quantum capabilities: (1) Z-basis measurement and (2) single-qubit operations (i.e., capabilities in a restricted quantum environment). Moreover, unlike other SQSS protocols that rely on round-trip qubit transmission, classical dealers and agents do not require additional quantum devices to protect against quantum Trojan horse attacks because of the adoption of one-way qubit transmission. In other words, the quantum capabilities and devices are lower than when using round-trip qubit transmission. Correctness and security analyses are performed to validate the proposed MMSQSS protocol and its feasibility is demonstrated using a simulation method.

The remainder of this paper is organized as follows: **Section 2** addresses the measurement property of the quantum complete graph state and thereafter describes the proposed MMSQSS protocol. **Section 3** presents correctness and security analyses of the proposed protocol. A comparison of experimental results is presented in **Section 4**. Finally, **Section 5** outlines concluding remarks and recommendations for further investigation.

2. Proposed MMSQSS Protocol

In this section, we begin by explaining the properties of the complete graph state, followed by an introduction to the proposed MMSQSS protocol.

2.1 Introduction of the complete graph state

A graph state is an important entanglement state [48, 49] that has been applied to various communication and computation applications. The following quantum system can represent any *n*-qubit graph state with graph format $G = (V, E)$, where V (vertices) and E (edges) denote a set of qubits and entanglement relationships, respectively.

$$|G\rangle = \prod_{(i,j)\in E} CZ^{\{i,j\}}|+\rangle^{\otimes n}, \tag{1}$$

where $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $CZ^{\{a,b\}}$ denotes performing a controlled-Z (CZ) gate (as shown in the following equation) on the qubit pair (a, b).

$$CZ = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix} = |00\rangle\langle 00| + |01\rangle\langle 01| + |10\rangle\langle 10| - |11\rangle\langle 11| \tag{2}$$

A complete graph state is a particular type of graph state representing a multiqubit quantum system in which all qubits are mutually entangled [47]. An n-qubit complete graph state can be represented as follows:

$$|K\rangle = \prod_{1\le i<j\le n} CZ^{\{i,j\}}|+\rangle^{\otimes n} = \left(\frac{1}{\sqrt{2}}\right)^{n} \sum_{x=0}^{2^n-1} (-1)^{\Delta}|x\rangle, \tag{3}$$

where $\Delta = \left\lfloor \frac{Hw(x)}{2} \right\rfloor mod\ 2$, and $Hw(x)$ denotes the Hamming weight of x.

Our previous study [47] proposed a measurement property of multiqubit complete graph states in Z-basis $(|0\rangle, |1\rangle)$ and X-basis $\left(|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\right)$ measurements. This study utilizes this property as a general formula. Assume using a basis set $B = \{b_1, b_2, \dots, b_n\}$ to measure an *n*-qubit complete graph state, where $b_i \in \{X, Z\}$ and $1 \leq i \leq n$. If $b_i = X$, the *i*-th qubit of the complete graph state is measured in the X-basis; otherwise, it is measured in the Z-basis. According to different bases, we can separate the basis set into two sets $B_x = \{i | 1 \leq i \leq n, b_i = X\}$ and $B_z = \{i | 1 \leq i \leq n, b_i = Z\}$. Here, this study encodes the measurement results $|0\rangle$ and $|+\rangle$ as the classical bit 0, and $|1\rangle$ and $|-\rangle$ as the classical bit 1. The measurement result of the *i*-th qubit is denoted as mr_i, where $mr_i \in \{0,1\}$. Then, we calculate $m_x = \bigoplus_{i \in B_x} mr_i$ and $m_z = \bigoplus_{i \in B_z} mr_i$. When $|B_x| = 2t + 1$, the complete graph state has the following measurement property (**Eq. (4)**), where $|B_x|$ denotes that the number of elements in B_x, t is an integer and $0 \leq t < \frac{n}{2}$.

$$m_x = (t \; mod \; 2) \oplus m_z, \tag{4}$$

where *mod* denotes the modulo operation, that is, when an odd number of qubits is measured in the X-basis, the measurement property is satisfied. Assuming that any qubit of the complete graph state is randomly measured in the Z- or X-basis, the probability of this property occurring is $\frac{1}{2}$. Additionally, Eq. (4) can be rewritten as Eq. (5).

$$m_x \oplus m_z = bt, \tag{5}$$

where $bt = t \; mod \; 2$. The calculation result of performing XOR operations on all measurement results is equal to $t \; mod \; 2$; this is, $m_x \oplus m_z \oplus bt = 0$.

2.2 Proposed protocol

Before explaining the proposed protocol, we outline its assumptions and define its environment for this MMSQSS protocol. These assumptions involve two groups: *N* dealers (i.e., Alice$_1$, Alice$_2$, …, Alice$_N$) and *M* agents (i.e., Bob$_1$, Bob$_2$, …, Bob$_M$). These $N + M$ participants are classical users with limited quantum capabilities, specifically (1) performing a Z-basis $\{|0\rangle, |1\rangle\}$ measurement, and (2) applying a Hadamard operation $H = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$. Each participant (a dealer) in group 1 has an *n*-bit sub-key K_{Alice_i}, they collectively generate a *n*-bit master key, $K_{Master} = \bigoplus_{i=1}^{N} K_{Alice_i}$, then they share the master key with the *M* participants in group 2 with the help of a quantum TP owning complete quantum capabilities. TP is dishonest in providing a more realistic scenario. In other words, without violating the principles of quantum mechanics, TP can perform various attacks, including colluding with a certain number of malicious dealers ($\leq N - 1$) or malicious agents ($\leq M - 1$) to steal the secret sub-keys of other dealers or the secret shadows of other agents. No subset of either group could correctly recover the secret message without the cooperation of the entire set of either group 1 or group 2. This study uses the schematic (shown in **Fig.1**) to represent the tasks of the proposed protocol. In addition, this study assumes the existence of an authenticated classical channel between participants, where attackers can only eavesdrop on transmitted messages but cannot modify them.

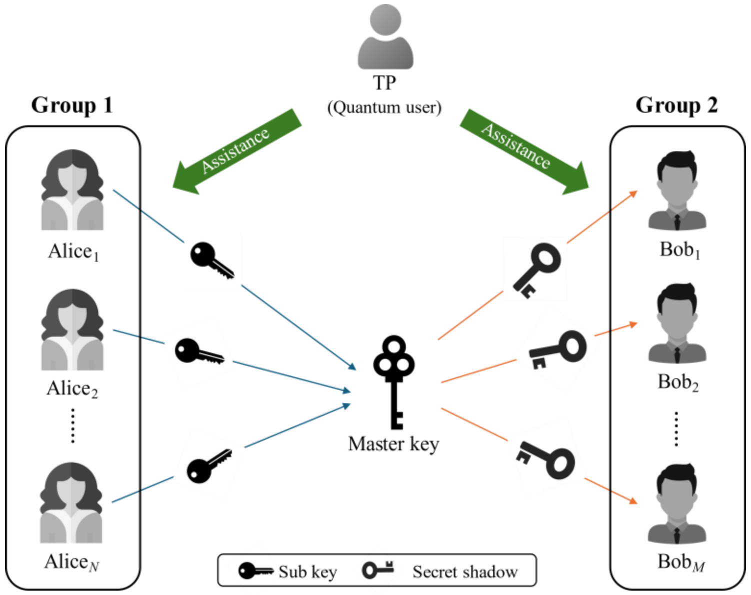


Figure 1. Schematic of the proposed MMSQSS protocol

The processes of the proposed MMSQSS protocol are outlined as follows:

Step 1. TP generates a complete graph state with $N + M$ qubits, and thereafter TP distributes the first N photons to each Alice$_i$ and the remaining to each Bob$_j$, where $1 \leq i \leq N$ and $1 \leq j \leq M$.

Step 2. When each Alice$_i$ (Bob$_j$) receives this qubit, they can select between two handling approaches: (1) measuring the qubit in Z-basis $\{|0\rangle, |1\rangle\}$ immediately, or (2) performing H operation on the qubit first and thereafter measuring it in the Z-basis $\{|0\rangle, |1\rangle\}$. Subsequently, Alice$_i$ (Bob$_j$) encodes the measurement results into classical bits, where $|0\rangle$ is encoded as 0, and the other outcome is 1.

The two steps are executed at least *4n* times to ensure that both dealers and agents obtain sufficient measurement results to complete the multiparty secret sharing task successfully.

Step 3. All the participants announce their handling approaches for each round. If the number of participants selecting the second handling approach in a round is even, the measurement results are discarded. If it is odd, specifically in the format $2t + 1$, they will keep the measurement results and record the coefficient t. Because each participant selects the handling approaches randomly, this study assumes that the ratio of useful measurement results is 0.5. In other words, each Alice$_i$ (Bob$_j$) holds the measurement result sequence $MR_{Alice_i} = \left\{mr^1_{Alice_i}, mr^2_{Alice_i}, \dots, mr^{2n}_{Alice_i}\right\}$ ($MR_{Bob_j} = \left\{mr^1_{Bob_j}, mr^2_{Bob_j}, \dots, mr^{2n}_{Bob_j}\right\}$), and a positive integer sequence $T = \{t^1, t^2, \dots, t^{2n}\}$, referring to the coefficient t of $2t + 1$ for the corresponding rounds.

Step 4. All the participants discuss and select *l* positions from the measurement result sequences randomly to form a CHECK sequence. For each position *p* of the CHECK sequence, each participant simultaneously announces their corresponding bits using authenticated channels. The participants then verify whether $\left(\oplus_{i=1}^{N} mr_{A_i}^{p}\right) \oplus \left(\oplus_{j=1}^{M} mr_{B_j}^{p}\right) = t^p \ mod \ 2$ holds true or not. If the error rate exceeds a predefined threshold, the protocol is terminated; otherwise, it proceeds to the next stage. In this study, half the measurement results are selected as check bits (l = *n*).

Step 5. Each Alice$_i$ (Bob$_j$) takes the remaining values of MR_{Alice_i} (MR_{Bob_j}) as the classical bit sequence $S_{Alice_i} = \{s^1_{Alice_i}, s^2_{Alice_i}, \dots, s^n_{Alice_i}\}$ ($S_{Bob_j} = \{s^1_{Bob_j}, s^2_{Bob_j}, \dots, s^n_{Bob_j}\}$), and they also calculate the remaining values of T to form a new binary sequence $BT = \{bt^1, bt^2, \dots, bt^n\}$, where $bt^x = t^x \ mod \ 2$. Each Alice$_i$ calculates $E_{Alice_i} = K_{Alice_i} \oplus S_{Alice_i}$ and announces this calculation result to all agents using the authenticated classical channels, where K_{Alice_i} denotes the sub-key of Alice$_i$ with *n* classical bits.

Step 6. When the agents intend to recover the master key of the dealers, they must cooperate to calculate the following equation:

$$\begin{aligned}&(\oplus_{i=1}^{N} E_{Alice_i}) \oplus \left(\oplus_{j=1}^{M} S_{Bob_j}\right) \oplus BT \\ &= \oplus_{i=1}^{N}(K_{Alice_i} \oplus S_{Alice_i}) \oplus \left(\oplus_{j=1}^{M} S_{Bob_j}\right) \oplus BT \\ &= (\oplus_{i=1}^{N} K_{Alice_i}) \oplus (\oplus_{i=1}^{N} S_{Alice_i}) \oplus \left(\oplus_{j=1}^{M} S_{Bob_j}\right) \oplus BT \qquad (6)\end{aligned}$$

According to Eq. (5), we can determine that $(\oplus_{i=1}^{N} S_{Alice_i}) \oplus \left(\oplus_{j=1}^{M} S_{Bob_j}\right) \oplus BT$ is 0. Thus, Eq. (6) can be rewritten as Eq. (7). Therefore, these agents correctly recover the master keys of the dealers.

$$\begin{aligned}&(\oplus_{i=1}^{N} E_{Alice_i}) \oplus \left(\oplus_{j=1}^{M} S_{Bob_j}\right) \oplus BT \\ &= \oplus_{i=1}^{N} K_{Alice_i} = K_{Master} \qquad (7)\end{aligned}$$

3. Correctness and Security Analyses

In this section, we first analyze the correctness of the proposed MMSQSS protocol to demonstrate that the master key can be successfully recovered with the cooperation of all the agents. Security analyses are provided to show that the proposed protocol is robust against various well-known attack scenarios.

3.1 Correctness analysis

This study adopts the property of a complete graph state, as explained in Section 2.1, to prove the correctness of the proposed protocol. In other words, if we can prove that $(\oplus_{i=1}^{N} S_{Alice_i}) \oplus \left(\oplus_{j=1}^{M} S_{Bob_j}\right) \oplus BT$ is equal to 0, the agents will recover the master key, K_{Master} , successfully.

In the Step. 2, the participants randomly select between two approaches: one performs the Z-basis measurement, and the other performs *H* operation and Z-basis measurement, which is equal to the X-basis measurement. Therefore, based on the property described in **Section 2.1**, we can rewrite S_{Alice_i} and S_{Bob_j} as:

$$\oplus_{i=1}^{N} S_{Alice_i} = (\oplus_{i \in B_z} S_{Alice_i}) \oplus (\oplus_{i \in B_x} S_{Alice_i}) \qquad (8)$$

$$\oplus_{j=1}^{M} S_{Bob_j} = \left(\oplus_{j \in B_z} S_{Bob_j}\right) \oplus \left(\oplus_{j \in B_x} S_{Bob_j}\right) \qquad (9)$$

Hence, $(\oplus_{i=1}^{N} S_{Alice_i}) \oplus \left(\oplus_{j=1}^{M} S_{Bob_j}\right) \oplus BT$ be expressed as **Eq. (10)**:

$$(\oplus_{i=1}^{N} S_{Alice_i}) \oplus \left(\oplus_{j=1}^{M} S_{Bob_j}\right) \oplus BT$$

$$= \left(\oplus_{i\in B_z} S_{Alice_i}\right) \oplus \left(\oplus_{i\in B_x} S_{Alice_i}\right)\oplus \left(\oplus_{j\in B_z} S_{Bob_j}\right) \oplus \left(\oplus_{j\in B_x} S_{Bob_j}\right) \oplus BT$$

$$= \left(\left(\oplus_{i\in B_z} S_{Alice_i}\right)\oplus \left(\oplus_{j\in B_z} S_{Bob_j}\right)\right) \oplus \left(\left(\oplus_{i\in B_x} S_{Alice_i}\right) \oplus \left(\oplus_{j\in B_x} S_{Bob_j}\right)\right) \oplus BT$$

$$= M_z \oplus M_x \oplus BT, \tag{10}$$

where $M_z = \{m_z^1, m_z^2, \dots, m_z^n\}$ and $M_x = \{m_x^1, m_x^2, \dots, m_x^n\}$.

Based on the property of Eq. (5), we can determine that $m_z^k \oplus m_x^k \oplus bt^k = 0$ for $1 \le k \le n$. Therefore, the result of Eq. (10) is 0, that is, the result of $\left(\oplus_{i=1}^{N} S_{Alice_i}\right)\oplus \left(\oplus_{j=1}^{M} S_{Bob_j}\right) \oplus BT$ is 0, and thus the result of $\left(\oplus_{i=1}^{N} E_{Alice_i}\right)\oplus \left(\oplus_{j=1}^{M} S_{Bob_j}\right) \oplus BT$ must be $\oplus_{i=1}^{N} K_{Alice_i} = K_{Master}$ if no attack or noise occurs.

3.2 Security analysis

This paper provides a security analysis to demonstrate that the proposed MMSQSS protocol is robust against well-known attacks, including collective, collusion, and quantum Trojan horse attacks. Here, 'robust' means that the protocol participants can detect attacking behaviors with a nonzero probability. In this section, we first analyze a collective attack, then evaluate a collusion attack, and finally explain the protocol’s immunity against quantum Trojan horse attacks.

- **Collective attack**

In the proposed protocol, TP plays a crucial role in generating quantum resources and controlling transmissions, which provides TP an advantage over malicious participants or external attackers when launching attacks. This study analyzes the robustness of the proposed protocol against collective attacks initiated by TP, demonstrating that such attacks can be detected during the check phase with nonzero probability.

To launch a collective attack, TP performs a unitary operation U_e to entangle ancillary qubit $|E\rangle$ with complete graph state $|G\rangle$ with $N + M$ qubits. The quantum system after the operation can be expressed as follows:

$$U_e|G\rangle \otimes |E\rangle = a_0|0_{(2)}\rangle|e_0\rangle + a_1|1_{(2)}\rangle|e_1\rangle + \cdots + a_{2^{N+M}-1}|2^{N+M} - 1_{(2)}\rangle|e_{2^{N+M}-1}\rangle$$

$$= \sum_{j=0}^{2^{N+M}-1} a_j|j_{(2)}\rangle|e_j\rangle, \tag{11}$$

where $j_{(2)}$ denotes the binary representation of j, and $\sum_{j=0}^{2^{N+M}-1}\left|a_j\right|^2 = 1$. State $|e_j\rangle$ for all $j \in \{0, 1, \dots, 2^{N+M} - 1\}$ represents the state of ancillary qubit after U_e is applied, and $|e_x\rangle$ and $|e_y\rangle$ are orthogonal when $x \neq y$, that is, each $|e_j\rangle$ can be distinguished by TP. To pass the check in **Step 4**, TP must adjust U_e such that the state shown in **Eq. (11)** does not affect the measurement property described in **Eq. (5)**.

Suppose only one participant who performs the second handling approach exists, which involves performing an *H* operation followed by a Z-basis measurement; the system changes to:

$$H^{\{h\}} \cdot \left(\sum_{j=0}^{2^{N+M}-1} a_j|j_{(2)}\rangle|e_j\rangle\right)$$

$$= \sum_{j=0}^{2^{N+M}-1} a_j H^{\{h\}}|j_{(2)}\rangle|e_j\rangle$$

$$= \frac{1}{\sqrt{2}} \sum_{j=0}^{2^{N+M}-1} \left(a_{j_{(2)} \oplus 2^{\hat{h}}_{(2)}} \left| e_{j_{(2)} \oplus 2^{\hat{h}}_{(2)}} \right\rangle + (-1)^{\lfloor j/2^{\hat{h}} \rfloor} a_j |e_j\rangle \right) |j_{(2)}\rangle, \tag{12}$$

where $H^{\{h\}}$ denotes H operation on the h-th qubit, $\hat{h} = n - h$, $\lfloor x \rfloor$ denotes the floor function on x, and $\oplus$ denotes the bitwise XOR operation. The expected result of the XOR operation is $BT = 0$ because only one participant selects performing the second handling approach. To avoid contradictions in the measurement property, states with odd Hamming weights must be set to zero, making U_e subject to

$$a_{j_{(2)} \oplus 2^{\hat{h}}_{(2)}} \left| e_{j_{(2)} \oplus 2^{\hat{h}}_{(2)}} \right\rangle + (-1)^{\lfloor j/2^{\hat{h}} \rfloor} a_j |e_j\rangle = \vec{0}, \forall j \in \{x | Hw(x) \equiv 1(mod\ 2)\}, \tag{13}$$

where $Hw(k)$ denotes Hamming weight of k and $\vec{0}$ denotes the zero vector.

By analyzing the term $(-1)^{\lfloor j/2^{\hat{h}} \rfloor}$, we can further simplify **Eq. (13)**. In the case where $(-1)^{\lfloor j/2^{\hat{h}} \rfloor} = -1$, one bit of h is 1 and is flipped to 0, that is, $j_{(2)} \oplus 2^{\hat{h}}_{(2)}$ sets a bit 1 in $j_{(2)}$ to 0. Using the same method to analyze the case where $(-1)^{\lfloor j/2^{\hat{h}} \rfloor} = 1$, we can conclude that

$$\begin{cases} a_{i_{(2)}} \left| e_{i_{(2)}} \right\rangle = a_{j_{(2)}} \left| e_{j_{(2)}} \right\rangle & \forall i, j, k, Hw(j_{(2)}) \equiv 1(mod\ 2), \\ a_{j_{(2)}} \left| e_{j_{(2)}} \right\rangle = -a_{k_{(2)}} \left| e_{k_{(2)}} \right\rangle, & Hw(i_{(2)}) + 1 = Hw(j_{(2)}) = Hw(k_{(2)}) - 1 \end{cases}. \tag{14}$$

This yields the following equation:

$$a_0 |e_0\rangle = (-1)^{\delta} a_{j_{(2)}} \left| e_{j_{(2)}} \right\rangle, \tag{15}$$

where $\delta = \lfloor j/2^{\hat{h}} \rfloor\ mod\ 2$. **Eq. (11)** can be written as follows:

$$\sum_{j=0}^{2^{M+N}-1} a_j |j_{(2)}\rangle |e_j\rangle = \sum_{j=0}^{2^{M+N}-1} (-1)^{\delta} a_{j_{(2)}} \left| e_{j_{(2)}} \right\rangle |e_j\rangle$$

$$= \left(\frac{1}{\sqrt{2}^{N+M}} \sum_{j=0}^{2^{M+N}-1} (-1)^{\delta} |j_{(2)}\rangle \right) \otimes |e_0\rangle, \tag{16}$$

By comparing **Eq. (16)** with the definition of the complete graph state in **Eq. (3)**, the ancillary qubit is in a product state with a complete graph state. This implies that TP cannot obtain any information without detection.

From this analysis, TP must solve a homogeneous system of equations to adjust U_e to fit within the quantum system, the system has 2^n unknown variables and a rank of $2^n - 1$. In the case where the number of participants performing the second handling approach is odd and greater than 1, it becomes equivalent to solving a homogeneous system of equations with rank $2^n - 1$ or greater. In the case where the rank is $2^n - 1$, we have proven that TP cannot obtain any information undetected. When the rank exceeds $2^n - 1$, the system either becomes inconsistent or has only one trivial solution, $x = 0$, making it impossible for TP to gather any information without the legitimate parties being unaware.

All the analyses indicate that TP cannot obtain any information without being detected by legitimate participants, implying that the participants always have a nonzero probability of detecting a collective attack. Therefore, the robustness of the proposed MMSQSS protocol against collective attacks is confirmed.

- **Collusion attack**

To demonstrate the robustness of the proposed MMSQSS protocol against various attacks, this study examines a worst-case scenario involving a collusion attack, which is discussed in this section. In this scenario, we assume that $N-1$ dealers and $M-1$ agents are malicious, and TP may conspire with these malicious participants to recover the master key without the involvement of legitimate participants. Because the previous analysis demonstrated the robustness of the proposed MMSQSS protocol against collective attacks, this study further examines another attack strategy: a malicious TP sending fake qubits instead of the original qubits from the complete graph states to steal the secret information of legitimate participants. In this scenario, the study assumes that only two legitimate participants exist: dealer Alice$_{x,}$ and agent Bob$_y$. TP and malicious participants employ two attack strategies to steal Alice$_x$'s subkey and Bob$_y$'s shadow. The related evaluations are described as follows:

A. To steal Alice$_x$'s sub-key

In this attack strategy, TP randomly generates a *2n* qubit sequence from the four quantum states $\{|0\rangle,|1\rangle,|+\rangle,|-\rangle\}$, and sends each qubit to Alice$_x$ instead of the original qubits from the complete graph states. Next, TP generates a complete graph state with $(N+M)-1$ qubits and sends the corresponding qubits to all participants (including Bob$_y$) except Alice$_x$ (also shown in **Fig.2 (a)**). If Alice$_x$ fails to detect this attack, malicious participants can steal approximately 75% of Alice$_x$'s subkey. This is because TP knows the initial states of the qubits measured by Alice. Although Alice$_x$ uses two different measurement approaches, TP still has a 75% probability of obtaining Alice$_x$'s measurement results. However, Alice$_x$ has a probability of $1-\left(\frac{1}{2}\right)$ of detecting this attack in the check phase (**Step 4** of the proposed protocol) for each bit in the CHECK sequence. Because the length of the CHECK sequence is *l*, the probability that Alice$_x$ will detect this attack behavior is $1-\left(\frac{1}{2}\right)^{l}$. When *l* is sufficiently large, Alice$_x$ can detect malicious participants' attack behavior with approximately 100% probability.

B. To steal Bob$_y$'s shadow

To steal Bob$_y$'s shadow, TP uses a similar method, generating a fake qubit sequence and sending each qubit of this sequence to Bob$_y$. TP then generates a complete graph state with $(N+M)$ qubits and sends the corresponding qubits to all participants (including Alice$_x$) except Bob$_y$ (also shown in **Fig.2 (b))**. TP retains the qubits originally intended for Bob$_y$. If Bob$_y$ fails to detect this attack, TP can measure the stored qubits based on Bob$_y$'s handling approach from **Step 2** to obtain Bob$_y$'s shadow. Fortunately, Bob$_y$ has a probability of $1-\left(\frac{1}{2}\right)^{l}$ of detecting this attack in the check phase. Therefore, Boby can detect an attack with approximately 100% probability when *l* is sufficiently large.

Based on the above analyses, we can conclude that legal participants have a probability of $1-\left(\frac{1}{2}\right)^{l}$ of detecting a collusion attack. When $l \geq 8$ (also shown in **Fig. 3**), the detection rate approaches 100%. Therefore, the proposed MMSQSS protocol is robust even against collusion attacks.

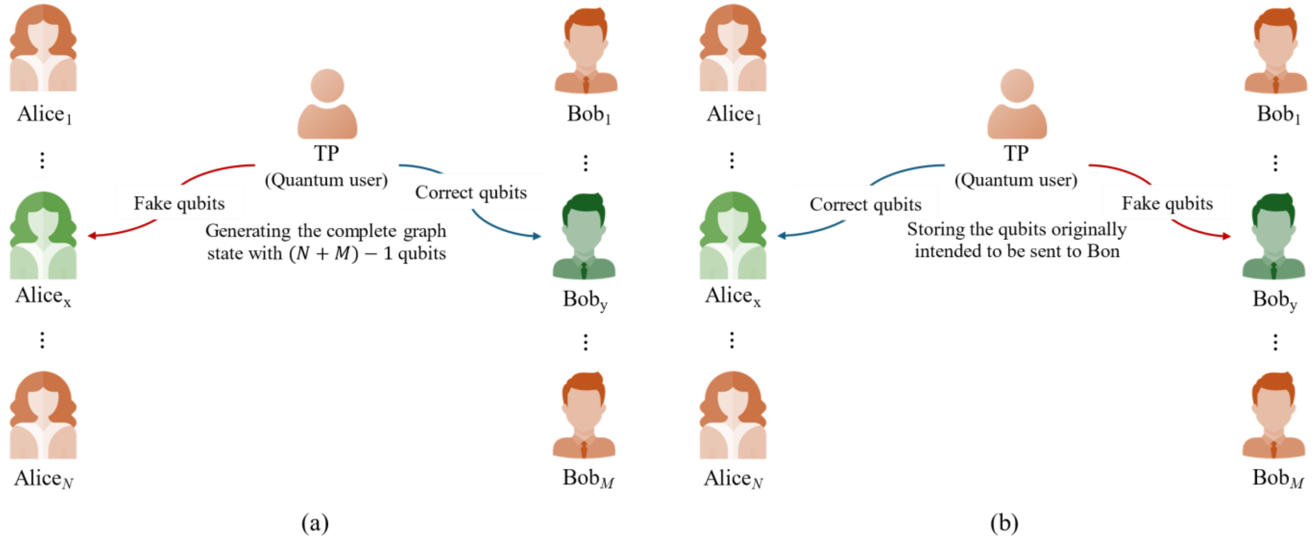


Figure 2. Two attacking strategies in the collusion attack

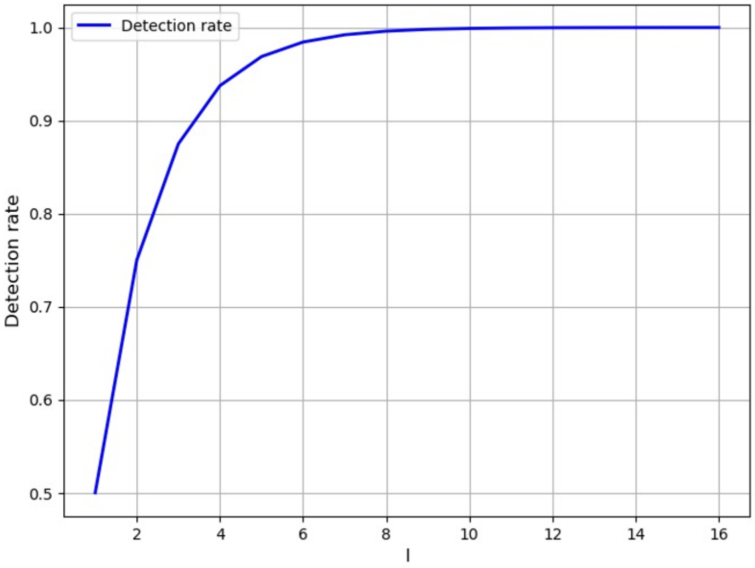


Figure 3. Trend of detection rate as l grows

- **Trojan horse attack**

Quantum Trojan horse attacks [50, 51] exploit specific system vulnerabilities, enabling attackers to secretly steal sensitive information. One method, known as a delayed photon attack, involves an attacker intercepting a qubit and sending a hidden "probing" photon along with it. This photon is delayed and remains undetected by the recipient’s equipment. After the recipient finishes its operation and returns the qubit, the attacker intercepts it again to retrieve the probing photon, revealing the recipient’s actions and secrets. Another variant of this attack utilizes invisible photons, in which the attacker adds an undetectable photon to each qubit sent to the recipient. This invisible photon undergoes the same operations as the qubit, allowing the attacker to gather information about the actions of the recipient without being detected.

Both methods effectively capture details of the recipient's operations and are most effective in two-way or circular quantum transmissions, where qubits are returned, allowing the attacker to recover hidden photons. In contrast, in one-way quantum communication, where qubits are not returned, the attacker cannot retrieve the information, rendering this approach ineffective. In other words, a quantum communication protocol that uses one-way communication to send qubits is naturally immune to quantum Trojan horse attacks. Since the proposed MMSQSS protocol employs a one-way communication model, it is inherently protected from quantum Trojan horse attacks. Moreover, this one-way approach streamlines communication by avoiding attack-related complexities and reduces the distance qubits need to travel compared to two-way or circular communication methods. As a result, the qubit transmission costs in the proposed protocol are lower than those in protocols relying on circular quantum communication.

4. Comparison and Experiment

To evaluate the performance of the proposed MMSQSS protocol, we compare it with existing MMQSS protocols across various metrics, including quantum resource usage, qubit transmission method, additional devices required to counter quantum Trojan horse attacks, and qubit efficiency. Although directly comparing the metrics could be unfair because of the different quantum environments between the proposed protocol (semi-quantum environment) and existing MSQKD protocols (quantum environment), these results offer valuable insights into the performance differences between the two quantum environments. Additionally, to demonstrate the feasibility of the proposed protocol for any number of participants, the quantum network simulator NetSquid [52] was used to implement the protocol in both ideal and noisy quantum channels.

A comparison with existing protocols [23,25-27,29-32] is summarized in **Table 2**. Because this study adopts discrete variable systems to design the quantum communication protocol, only the existing protocols using discrete variable systems are considered in this comparison. In terms of quantum sources, although the proposed protocol uses multiqubit entanglement states, making it less efficient than existing protocols that use single photons, Bell states, or GHZ states, the burden of generating these entangled states lies with the quantum user (TP). Classical users—dealers and agents—require only two quantum capabilities, and do not need to store qubits. This architecture, in which a powerful quantum user supports multiple classical users in completing a quantum communication protocol, lowers the barrier to entry into quantum communication technology and broadens its potential applications and adoption.

In terms of the qubit transmission, this study assumes that the distance of the quantum channel between each participant is the same, denoted as *d*. The one-way transmission method employed in the proposed protocol results in shorter transmission distances (only *d*) compared with existing protocols that rely on relay or circular transmissions. Furthermore, the use of one-way communication renders the proposed protocol immune to quantum Trojan horse attacks, eliminating the need for dealers and agents to equip or implement additional protective measures. However, because the agents do not possess quantum memory, the proposed protocol cannot support a mechanism for dynamically adding or removing participants. The design of a dynamic multiparty-to-multiparty semi-quantum secret sharing protocol in semi-quantum environments will be an important future work.

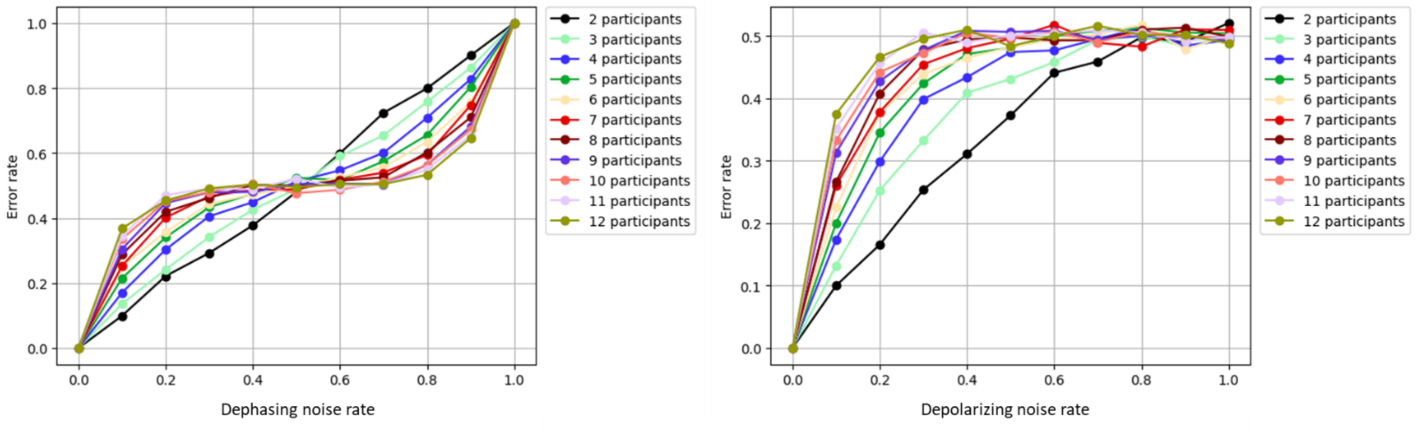
Finally, this study adopts the equation, $\eta = \frac{n}{q}$, to calculate the qubit efficiency, where n denotes the length of the master key and q denotes the number of qubits consumed to share a *n*-bit master key. Note that this study did not include the qubits used for detecting quantum Trojan horse attacks because these protocols did not explicitly mention the details of defending against quantum Trojan horse attacks; thus, the qubit efficiency could be reduced when considering quantum Trojan horse protection. In terms of the qubit efficiency, the proposed protocol is clearly not the most efficient. This is due to the limited quantum capabilities of classical users (dealers and agents), specifically, their inability to store qubits. This limitation often leads to lower qubit efficiency in SQC protocols than in fully quantum communication protocols. Notably, [27] yielded similar results to those of the proposed protocol in terms of the transmission method, resistance to Trojan horse attacks, qubit transmission distance, and qubit efficiency. However, in [27], the dealers and agents must possess Bell measurement capabilities and quantum memory. This gives the proposed protocol a practical advantage because it requires fewer quantum resources for implementation.

Table 2. Comparison results between the proposed protocol and existing MMQSS protocols

Ref.	**Quantum resources**	**Transmission method**	**Quantum Trojan horse attack**	**Qubit transmission distance**	**Semi-quantum environment**	**Dynamic participants**	**Qubit efficiency**
[23]	Single photon	Relay	Yes	*Md*	No	No	$\frac{1}{M}$
[25]	Single photon	Relay	Yes	*Md*	No	No	$\frac{n}{nM + \sum_{i=2}^{N} N^{i-1}(N-1)}$
[26]	Single photon	Relay	Yes	*Md*	No	No	$\frac{1}{(N+1)M}$
[27]	EPR pair	One-way	No	*d*	No	No	$\frac{1}{4(N+M)}$
[29]	GHZ state	Relay	Yes	2*d*	No	No	$\frac{1}{3M}$
[30]	GHZ state	Relay	Yes	2*d*	No	Yes	$\frac{1}{2 \times \max(N,M) + N}$
[31]	Single photon	Relay	Yes	2*d*	No	Yes	$\frac{1}{3 \times \max(N,M)}$
[32]	EPR pair	Relay	Yes	2*d*	No	Yes	$\frac{1}{6 \times \max(N,M)}$
Proposed	Graph state	One-way	No	*d*	Yes	No	$\frac{1}{4(N+M)}$

To demonstrate the feasibility of the proposed MMQSS protocol with varying numbers of participants, we implemented the protocol in scenarios involving 2–12 participants. In addition, two common types of noise, dephasing and depolarizing noise, are considered in the simulation experiment to evaluate the impact of noise on the error rates of the proposed protocol. The experimental results are summarized in **Tables 3** and **4**, and the trends in the error rates for the various scenarios are illustrated in **Fig. 4**. Because this study uses the result of the XOR operation as the master key, the probability of correctly guessing each bit of the master key randomly is 0.5. This implies that when the error rate reaches 0.5, the entanglement relationships of the graph states are completely broken by noise, preventing the participants from sharing secret messages in such a situation.

Figure 4. Error rate trends in various scenarios



(a) **(b)**

From the experimental results on dephasing noise, the error rates across all scenarios (with 2–12 participants) approach 0.5 when the dephasing noise rate reaches 0.5. As the number of participants increases, the system becomes more susceptible to noise, causing the error rate to increase more quickly than in scenarios with fewer participants. Notably, an interesting phenomenon occurs when the noise rate reaches 1.0. In this case, the error rate across all scenarios is 1.0, indicating that the participants' calculated result is the inverse of the master key. In other words, the entanglement of the graph state remains intact, and the effect of dephasing noise can be corrected through an operation. This indicates that complete graph states with any number of qubits behave as free states in a collective dephasing noise environment, where collective dephasing refers to the quantum noise that affects multiple qubits simultaneously in the same manner. However, the experimental results for depolarizing noise are intuitive. The error rates increase as the noise rates increase, and the number of participants is a key factor influencing the effect of noise. However, the free state does not occur in a depolarizing noisy environment.

Table 3. Experiment results in dephasing noise environment

Noise rate	**Number of participants**										
	2	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**
0.0	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000
0.1	0.099	0.136	0.170	0.215	0.251	0.253	0.288	0.305	0.336	0.345	0.368
0.2	0.221	0.241	0.303	0.341	0.357	0.401	0.419	0.446	0.452	0.471	0.454
0.3	0.293	0.342	0.405	0.433	0.443	0.467	0.463	0.479	0.480	0.491	0.491
0.4	0.377	0.426	0.449	0.475	0.473	0.488	0.502	0.480	0.505	0.489	0.504
0.5	0.480	0.489	0.513	0.524	0.493	0.488	0.500	0.505	0.477	0.522	0.495
0.6	0.599	0.591	0.547	0.517	0.526	0.518	0.515	0.506	0.487	0.493	0.504
0.7	0.724	0.654	0.601	0.575	0.556	0.540	0.525	0.504	0.512	0.504	0.504
0.8	0.799	0.758	0.709	0.655	0.635	0.594	0.602	0.564	0.563	0.550	0.533
0.9	0.900	0.863	0.828	0.803	0.755	0.747	0.710	0.682	0.672	0.654	0.646
1.0	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000

Table 4. Experimental results in depolarizing noise environment

Noise rate	**Number of participants**										
	2	3	4	5	6	7	8	9	10	11	12

0.0	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000
0.1	0.100	0.132	0.174	0.200	0.225	0.261	0.266	0.313	0.332	0.352	0.375
0.2	0.166	0.253	0.299	0.345	0.376	0.378	0.408	0.428	0.442	0.457	0.466
0.3	0.254	0.332	0.399	0.424	0.439	0.455	0.478	0.477	0.473	0.505	0.495
0.4	0.311	0.409	0.434	0.471	0.465	0.480	0.495	0.508	0.505	0.490	0.510
0.5	0.373	0.431	0.474	0.481	0.482	0.496	0.498	0.507	0.497	0.501	0.484
0.6	0.441	0.458	0.477	0.500	0.494	0.518	0.493	0.508	0.507	0.504	0.501
0.7	0.459	0.494	0.495	0.508	0.503	0.489	0.493	0.495	0.490	0.509	0.516
0.8	0.498	0.499	0.513	0.513	0.518	0.483	0.510	0.500	0.507	0.506	0.502
0.9	0.490	0.484	0.484	0.505	0.479	0.511	0.513	0.499	0.500	0.492	0.502
1.0	0.521	0.498	0.494	0.504	0.501	0.510	0.499	0.493	0.496	0.499	0.488

5. Conclusion

This study proposes the first MMSQSS protocol within a restricted quantum environment. The proposed protocol offers a practical solution to the high implementation costs associated with fully quantum secret sharing protocols by enabling classical users equipped with only basic quantum capabilities to participate in secure quantum communication. By utilizing one-way qubit transmission, the protocol eliminates the need for round-trip quantum communication, effectively reducing the vulnerability to quantum Trojan horse attacks and lowering implementation costs. Through detailed correctness and security analyses, this study demonstrates that the proposed MMSQSS protocol is resilient to well-known attacks, including collective, collusion, and quantum Trojan horse attacks. Furthermore, our simulation results, performed under both ideal and noisy channel conditions, confirmed the feasibility and robustness of the protocol even as the number of participants increased. These results underscore the practicality of deploying the protocol in real-world quantum communication networks, particularly in scenarios where participants have limited quantum capabilities.

Despite its advantages, the proposed protocol has limitations, particularly in its inability to add or remove participants dynamically because of the lack of quantum memory on the part of classical users. Future studies could address this limitation by developing a dynamic MMSQSS protocol that maintains security and feasibility while allowing participant flexibility. Another avenue for further investigation is the deployment of the protocol in more complex quantum network environments. The assumption in this study is that TP can transmit qubits directly to participants. In practice, the implementation of this protocol in distributed quantum networks poses additional challenges related to quantum resource management and network topology. Exploring these issues is crucial for broader applicability of the proposed protocol.

Declarations

Ethical approval and consent to participate

Not applicable.

Consent for publication

Not applicable.

Availability of supporting data

Data sharing is not applicable to this article as no datasets were generated or analyzed during the current study.

Competing interests

The authors declare no competing interests.

Authors' contributions

Chia-Wei Tsai: Conceptualization, Methodology, Investigation, Formal Analysis, Writing – Review & Editing.
Chun-Hsiang Wang: Methodology, Software, Formal Analysis, Writing – Original Draft.
Jason Lin: Formal Analysis, and Review manuscript.
Chun-Wei Yang: Review the manuscript and project administration.

Funding

This work was partially supported by the National Science and Technology Council, Taiwan, R.O.C. (Grant Nos. NSTC 113-2221-E-025-014, NSTC 113-2221-E-039-020, NSTC 113-2221-E-005-086, and NSTC 113-2634-F-005-001-MBK) and China Medical University, Taiwan (Grant No. CMU112-S-42).

References

[1] A. Shamir, *Commun. ACM* **1979**, 22, 612.
[2] G. R. Blakley, presented at Managing Requirements Knowledge, International Workshop on, **1979**
[3] S. Iftene, *Electronic Notes in Theoretical Computer Science* **2007**, 186, 67.
[4] M. Hillery, V. Buzek, and A. Berthiaume, *Phys. Rev. A* **1999**, 59, 1829.
[5] D. M. Greenberger, M. A. Horne, and A. Zeilinger, in *Bell's Theorem, Quantum Theory and Conceptions of the Universe*, edited by M. Kafatos (Springer Netherlands, Dordrecht, 1989), pp. 69.
[6] D. Gottesman, *Phys. Rev. A* **2000**, 61, 042311
[7] W. Tittel, H. Zbinden, and N. Gisin, *Phys. Rev. A* **2001**, 63, 042301.
[8] G. P. Guo and G. C. Guo, *Phys. Lett. A* **2003**, 310, 247.
[9] L. Xiao, G. L. Long, F.-G. Deng, and J.-W. Pan, *Phys. Rev. A* **2004**, 69, 052307.
[10] Z. J. Zhang, Y. Li, and Z. X. Man, *Phys. Rev. A* **2005**, 71, 044301
[11] S. K. Singh and R. Srikanth, *Phys. Rev. A* **2005**, 71, 012328.
[12] F.-G. Deng, H.-Y. Zhou, and G. L. Long, *Journal of Physics a-Mathematical and General* **2006**, 39, 14089.
[13] D. Markham and B. C. Sanders, *Phys. Rev. A* **2008**, 78, 042309.
[14] L. L. Liu, C. W. Tsai, and T. Hwang, *Int. J. Theor. Phys.* **2012**, 51, 2291.
[15] B. Fortescue and G. Gour, *IEEE Trans. Inf. Theory* **2012**, 58, 6659.
[16] W. Helwig, W. Cui, J. I. Latorre, A. Riera, and H.-K. Lo, *Phys. Rev. A* **2012**, 86, 052335.
[17] J. L. Hsu, S. K. Chong, T. Hwang, and C. W. Tsai, *Quantum Inf. Process.* **2013**, 12, 331.
[18] A. Maitra, S. J. De, G. Paul, and A. K. Pal, *Phys. Rev. A* **2015**, 92, 022305.
[19] A. Shen, X.-Y. Cao, Y. Wang, Y. Fu, J. Gu, W.-B. Liu, C.-X. Weng, H.-L. Yin, and Z.-B. Chen, *Sci. China Phys.* **2023**, 66, 260311.
[20] D. Rathi and S. Kumar, *Quantum Inf. Process.* **2023**, 22, 183.
[21] Q. Liao, X. Liu, B. Ou, and X. Fu, *IEEE Transactions on Communications* **2023**, 71, 6051.
[22] F.-L. Yan and T. Gao, *Phys. Rev. A* **2005**, 72, 012304.
[23] C.-M. Li, C.-C. Chang, and T. Hwang, *Phys. Rev. A* **2006**, 73, 016301.
[24] L.-F. Han, Y.-M. Liu, H. Yuan, and Z.-J. Zhang, *Chinese Phys. Lett.* **2007**, 24, 3312.
[25] F. Yan, T. Gao, and Y. Li, *Sci. China Ser. G* **2007**, 50, 572.
[26] T. Gao, F. Yan, and Y. Li, *Sci. China Ser. G* **2009**, 52, 1191.
[27] R. Shi, L. Huang, W. Yang, and H. Zhong, *Sci. China Phys.* **2010**, 53, 2238.
[28] S. Zhang, *Scientia Sinica Physica, Mechanica &amp; Astronomica* **2011**, 41, 855.
[29] H. Qin, W. K. S. Tang, and R. Tso, *Mod Phys Lett B* **2018**, 32, 1850350.
[30] R. G. Zhou, M. Huo, W. Hu, and Y. Zhao, *IEEE Access* **2021**, 9, 22986.
[31] Z. You, Y. Wang, Z. Dou, J. Li, X. Chen, and L. Li, *Phys. A* **2023**, 624, 128893.
[32] Y. Tian, J. Wang, G. Bian, J. Chang, and J. Li, *Advanced Quantum Technologies* **2024**, 7, 2400116.
[33] A. Javadi-Abhari *et al.*, **2024**, arXiv:2405.08810.

[34] M. Boyer, D. Kenigsberg, and T. Mor, *Phys. Rev. Lett.* **2007**, 99, 140501, 140501.

[35] M. Boyer, R. Gelles, D. Kenigsberg, and T. Mor, *Phys. Rev. A* **2009**, 79, 032341.

[36] Q. Li, W. H. Chan, and D. Y. Long, *Phys. Rev. A* **2010**, 82, 022303

[37] L. Z. Li, D. W. Qiu, and P. Mateus, *Journal of Physics a-Mathematical and Theoretical* **2013**, 46, 045304, 045304.

[38] C.-W. Yang and T. Hwang, *Int. J. Quant. Infor.* **2013**, 11, 1350052.

[39] C. Xie, L. Li, and D. Qiu, *Int. J. Theor. Phys.* **2015**, 54, 3819.

[40] C.-Q. Ye and T.-Y. Ye, *Commun. Theor. Phys* **2018**, 70, 661.

[41] C.-W. Tsai, C.-W. Yang, and N.-Y. Lee, *Modern Physics Letters A* **2019**, 34, 1950213.

[42] Y. Tian, J. Li, X.-B. Chen, C.-Q. Ye, and H.-J. Li, *Quantum Inf. Process.* **2021**, 20, 217.

[43] X. Zou and D. Qiu, *Sci China Phys Mech* **2014**, 57, 1696.

[44] W. O. Krawec, *Phys. Rev. A* **2015**, 91, 032323, 032323.

[45] Y.-F. Lang, *Int. J. Theor. Phys.* **2018**, 57, 3048.

[46] C.-W. Tsai, C.-W. Yang, and J. Lin, *Quantum Inf. Process.* **2022**, 21, 63.

[47] C.-W. Tsai and C.-H. Wang, *Ann. Phys.* **2023**, 535, 2300116.

[48] M. Hein, J. Eisert, and H. J. Briegel, *Phys. Rev. A* **2004**, 69, 062311.

[49] G. Berkolaiko and P. Kuchment, *Mathematical Surveys and Monographs* **2013**, 186.

[50] F. G. Deng, X. H. Li, H. Y. Zhou, and Z. J. Zhang, *Phys. Rev. A* **2005**, 72, 044302, 044302.

[51] Q. Y. Cai, *Phys. Lett. A* **2006**, 351, 23, 23.

[52] T. Coopmans *et al.*, *Communications Physics* **2021**, 4, 164.