An efficient multi-party quantum secret sharing protocol based on single photon

Content & Services Team

IOP Publishing, Temple Circus, Temple Way, Bristol BS1 6HG, UK

E-mail: submissions@iop.org

August 2017

Abstract. This paper introduces an efficient multi-party quantum secret sharing (MQSS) protocol based on single photon. The protocol utilizes single photon and local unitary operations for efficient and secure secret distribution among multiple participants. By reducing the dependence on complex quantum entanglement, the protocol lowers the technical barriers and costs associated with implementation. Participants in our protocol are not required to perform quantum measurements, simplifying the process. A distinctive feature is the protocol's ability to share secrets without revealing individual shares, thereby ensuring that the distributor has no knowledge of the participants' secret shares. The efficiency of the protocol can reach 100% in the absence of eavesdropping. The protocol is capable of withstanding common attack scenarios, and simulations have verified the feasibility of the protocol.

Keywords: Multi-party quantum secret sharing, Single photon, Local unitary operation, Simulation

1. Introduction

With the advent of quantum computing [1–3], quantum information science has seen increased interest in secure communication protocols leveraging quantum mechanics. Among these, quantum secret sharing (QSS) is a key protocol for distributing a secret among multi-parties, ensuring confidentiality and reconstruction only when a sufficient number collaborate. QSS prevents any single party from accessing the full secret, enhancing security for multi-party computations. In banking, for instance, QSS can distribute a sensitive key such that no individual can access it alone, only revealing it when the designated group collaborates.

The inception of QSS can be traced back to the groundbreaking work by Hillery et al. [4] in 1999, who first proposed a protocol leveraging the entanglement properties of the Greenberger-Horne-Zeilinger (GHZ) states to distribute a secret among multi-parties. In the same year, Karlsson et al. [5] proposed a QSS protocol based on entangled states. In 2004, Xiao et al. [6] extended the protocol originally proposed by Hillery et al., enabling the process of secret sharing among any number of participants, thereby

establishing the foundation for what is now known as multi-party quantum secret sharing (MQSS) protocols. Afterwards, a large number of scholars engaged in the research of MQSS protocols, and a series of innovative MQSS protocols [7–35] emerged one after another, which greatly enriched the research achievements in this field . For example, in the year 2011, Hwang et al. [15] put forward an MQSS protocol based on GHZ states. Through the utilization of quantum dense coding and the technique of decoy single photons. During 2013, Chen et al. [16] proposed an MQSS protocol based on the GHZ states. In this protocol, Alice prepares to encode the secret information, and Bob selects the shared information according to his preference. Ain et al. in the year 2017 [19] proposed a quantum secret sharing protocol. It involves the sender distributing EPR pairs, receivers performing measurement , the sender generating new pairs and teleporting. Zhang et al. [22] in 2019 proposed a novel quantum secret sharing model based on multi-party entangled states. They presented two specific protocols, analyzed their security against existing attacks, and summarized a general model. In 2021, Zhou et al. [25] proposed a dynamic multi-party to multi-party quantum secret sharing protocol (DMMQSS) based on GHZ states, which permits the flexible addition or removal of participants to adapt to diverse scenarios. In 2023, Kuo et al. [30] proposed an efficient MQSS protocol based on a novel structure and single photon. This protocol constructs an independent quantum secure direct communication path for each participant. One year later, Gao [31] discovered that the KTYC protocol proposed by Kuo et al. has a security vulnerability in the multi-party case, where two dishonest agents can collude to steal Alice's secret. Then Gao proposed an improved protocol and analyzed its security and efficiency. In 2024, Du et al. [33] proposed an efficient MQSS protocol based on measuring-basis-encrypted. They encrypted the basis information of the qubits received by each agent with the sub-secrets of other agents. Also in 2024, Li et al. [34] proposed an authenticated dynamic MQSS protocol based on the Chinese remainder theorem. They employed quantum digital signatures for identity authentication, transmitted information among participants based on GHZ states.

A multitude of MQSS protocols have been proposed. However, they often face a critical limitation: the distributor must be aware of all participants' secrets beforehand. In the context of the banking industry, this undoubtedly poses potential risks to the bank's information security. Once the distributor's system is breached, the secrets of all participants will be completely exposed, which may lead to serious financial losses and a crisis of customer trust. In recent years, some protocols have begun to address this issue. The protocols in [36–39] both satisfy the characteristic that the distributor does not know the participants' secret shares. In 2010, Shi et al. [36] proposed a MQSS protocol between two groups of members using EPR pairs as resources, in which members obtain the shared key through Bell measurements without local unitary operations. In 2022, Tsai et al. [37] proposed a mediated MQSS protocol that allows n restricted quantum users to share a secret with the assistance of a semi-honest third-party (TP) with full quantum capabilities. The year 2023, You et al. [38] introduced a DMMQSS protocol based on single photons and local unitary operation. A semi-honest TP is utilized

to prepare all quantum resources and distribute particle sequences to the respective recipients. Each agent encodes their secret share using only single photons and local unitary operations. The process is simplified as it does not require verification of the secret shares when add or remove agents. One year later, Xin et al. [39] proposed an MQSS protocol based on EPR pairs. In this protocol, the distributor prepares a sequence of EPR paires and splits it into two subsequences, which are then sent to each participant. The participants encode the secret using Pauli operators. All of the above protocols share a common characteristic, distributor is unaware of each participant's secret share .

Although some MQSS protocols have been proposed, in which the distributor is not aware of the participants' secret shares, most of these protocols still face several issues, such as low protocol efficiency, difficulties in quantum resource preparation, and high complexity of unitary operations. In order to overcome the above deficiencies, this paper proposes an efficient MQSS protocol. Throughout the implementation process of this protocol, the distributor is always unable to obtain the participants' secret shares, and this feature effectively protects the participants' privacy. Moreover, the quantum resources we employ are single particles and simple local unitary operations, which not only reduce the difficulty of resource preparation but also, this protocol stipulates that participants do not need to perform measurement operations, and these characteristics greatly enhance the implementability of the protocol. It is worth mentioning that in this protocol, decoy particles can be used for information transmission. In the ideal situation without eavesdropping, the efficiency of this protocol can reach 100%, which shows the significant advantages of this protocol in information transmission. Finally, in order to further verify the correctness of this protocol, we conducted simulation experiments on the IBM quantum platform, and the results show that the protocol exhibits good performance both in theory and practice.

The structure of this paper is organized as follows: Section 2 first discusses the quantum resources and operations involved in the protocol, then introduces the MQSS protocol, and provides examples to aid understanding. Section 3 analyzes the security of the protocol. Section 4 simulates the protocol process using the IBM platform. Section 5 compares this protocol with existing MQSS protocols. Section 6 summarizes the entire paper.

2. Protocol

We will introduce the quantum resources and local unitary operations, as well as the encoding and decoding rules that we utilize. In the protocol, we employ four types of single photon, which are denoted as $|0\rangle = \binom{1}{0}$,$|1\rangle = \binom{0}{1}$, $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, and $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$.

The local unitary operations we employ are the operations I and the operations U, defined as follows:

$$I = |0\rangle\langle 0| + |1\rangle\langle 1|. \tag{1}$$

$$U = |0\rangle\langle 1| - |1\rangle\langle 0|. \tag{2}$$

We do not utilize the CNOT gate or other complex operations, thereby reducing the experimental cost and difficulty. We detail the effects of the local unitary operations I and U on the four single photon. The results are summarized in Table 1, which illustrates the transformation of each quantum state under the application of these operations.

Table 1. Quantum State Transformations Under Local Unitary Operations

Quantum State	Local Unitary Operation	Result
$\|0\rangle$	$I = \|0\rangle\langle 0\| + \|1\rangle\langle 1\|$	$\|0\rangle$
$\|1\rangle$	$I = \|0\rangle\langle 0\| + \|1\rangle\langle 1\|$	$\|1\rangle$
$\|+\rangle$	$I = \|0\rangle\langle 0\| + \|1\rangle\langle 1\|$	$\|+\rangle$
$\|-\rangle$	$I = \|0\rangle\langle 0\| + \|1\rangle\langle 1\|$	$\|-\rangle$
$\|0\rangle$	$U = \|0\rangle\langle 1\| - \|1\rangle\langle 0\|$	$\|1\rangle$
$\|1\rangle$	$U = \|0\rangle\langle 1\| - \|1\rangle\langle 0\|$	$\|0\rangle$
$\|+\rangle$	$U = \|0\rangle\langle 1\| - \|1\rangle\langle 0\|$	$\|-\rangle$
$\|-\rangle$	$U = \|0\rangle\langle 1\| - \|1\rangle\langle 0\|$	$\|+\rangle$

Below, the quantum encoding rules is detailed in Table 2, where bit 0 is associated with the Identity operation I, and bit 1 with the operation U. Table 3 presents the decoding rules, translating the measured quantum states $|0\rangle$ and $|+\rangle$ to bit 0, and $|1\rangle$ and $|-\rangle$ to bit 1.

Table 2. Encoding Rules

Bit Value	Local unitary operation
0	$I = \|0\rangle\langle 0\| + \|1\rangle\langle 1\|$
1	$U = \|0\rangle\langle 1\| - \|1\rangle\langle 0\|$

Table 3. Decoding Rules

Measurement Result	Secret
$\|0\rangle$	0
$\|1\rangle$	1
$\|+\rangle$	0
$\|-\rangle$	1

2.1. Propose MQSS protocol

In this section, we provide a detailed introduction to our proposed MQSS protocol. We assume that there are a total of $n+1$ members involved in this protocol. Alice serves as the distributor, while Bob, Charlie, and subsequent participants up to the n-th participant, are considered the recipients of the secret share . The secret S, consisting of a total of m bits, is utilized for two distinct purposes. A portion of the secret, denoted as m_{info}, is allocated for the transmission of information and is calculated as $m_{\text{info}} = \frac{m}{2}$. Another portion, denoted as m_{detect}, is reserved for the detection of eavesdropping and is defined as $m_{\text{detect}} = m - m_{\text{info}}$. When no eavesdropping is detected, the segment m_{detect} can also be employed to transmit information.

Step 1: Alice prepares a sequence of m photons at random, where each photon is randomly selected from the set $\{|0\rangle, |+\rangle\}$,the sequence is denoted as $P = \{P_1, P_2, \ldots, P_m\}$. This selection is deliberate, as the states $|0\rangle$ and $|+\rangle$ are used to represent the classical bits 0 , respectively. Consequently, the sequence generated by Alice does not convey any additional information beyond the intended bit values. Subsequently, Alice reorders the sequence P randomly, resulting in a new sequence denoted as P'_a. Then Alice dispatches the sequence P'_a to Bob.

Step 2: Upon receiving the sequence P'_a, Bob first reorders it to obtain a new sequence P_b. Subsequently, Bob generates a secret bit string $b = (b_1, b_2, \ldots, b_m)$ of length m, where each b_i is randomly chosen from the set $\{0, 1\}$. Subsequently, in accordance with the predefined encoding rules, Bob applies the corresponding local unitary operations, as determined by each bit in the string $b = (b_1, b_2, \ldots, b_m)$, to each qubit in the sequence P_b. This process results in the formation of a new sequence, denoted as P'_b. Subsequently, Bob sends the sequence P'_b to the next participant, Charlie.

Step 3: Similarly, upon receiving the sequence P'_b, Charlie first reorders it to obtain P_c. He then generates his own secret bit string $c = (c_1, c_2, \ldots, c_m)$. Following the corresponding encoding rules, Charlie applies a series of local unitary operations to each qubit in P_c in sequence. After these operations, the sequence P_c is transformed into P'_c. Charlie then dispatches P'_c to the next participant in the protocol.

This process is repeated with each subsequent participant performing analogous operations. The sequence progresses through the group, with each participant applying their local unitary operations based on their secret bit string. Eventually, after the n-th participant completes their operations, the sequence is transformed into P'_n. Finally, the n-th participant returns the sequence P'_n to Alice.

Step 4: Upon receiving the sequence P'_n, Alice first discloses the initial order of the sequence P' as it was prepared. Subsequently, Alice requests each participant, from Bob to the n-th participant, to reveal the order of their respective rearranged sequences. With this collective information, Alice then reorders P'_n to align the qubits with their original preparation order, resulting in the sequence P'', where the order of the qubits is $P'' = (P_1, P_2, \ldots, P_m)$.

Following this, Alice measures each qubit in sequence and, adhering to the decoding

rules, extracts the final secret $S = (S_1, S_2, \ldots, S_m)$.

Step 5: Based on the original order of the particles disclosed by Alice and the n participants, Bob can reorder his own sub-secret string b to obtain the final sub-secret string b'. The order of each bit in b' corresponds to the order of the particles after Bob's rearrangement, ensuring that his $b' = (b_1, b_2, \ldots, b_m)$ aligns with the local unitary operations corresponding to the original sequence $P = (P_1, P_2, \ldots, P_m)$.

Similarly, the remaining $n-1$ participants perform the same operation to derive their final sub-secret strings $(c', d', \ldots, n')$. Ultimately, the n participants collaborate to reconstruct the secret S through the XOR operation:

$$S = b' \oplus c' \oplus \cdots \oplus n'. \tag{3}$$

Step 6: We have elected to place the eavesdropping detection process as the final step in our protocol. Alice randomly selects m_{detect} positions from the sequence P'' for the purpose of eavesdropping detection. She then compares the measurement outcomes of these qubits with the corresponding bits recovered by the participants. Should the error rate among the sampled bits exceed a predetermined threshold, the secret S is deemed compromised and is discarded. Alternatively, if the error rate is within acceptable limits, the secret is validated and accepted as the shared secret among the participants.

2.2. Example of the Proposed MQSS Protocol

In this section, we present a simple example to illustrate the proposed MQSS protocol. The protocol involves five members: Alice, Bob, Charlie, David, and Edward. Alice acts as the distributor, while Bob, Charlie, David, and Edward are the participants. The parameters are defined as $n = 4$, $m = 4$, $m_{\text{info}} = 2$, and $m_{\text{detect}} = 2$. The specific steps of the protocol are outlined below:

Step 1: Alice prepares a sequence of four single particles, denoted as $P = \{P_1, P_2, P_3, P_4\}$, where each particle is randomly selected to be either $|0\rangle$ or $|+\rangle$. Assuming Alice generates a sequence $P = \{|0\rangle, |+\rangle, |+\rangle, |0\rangle\}$. Subsequently, Alice rearranges the sequence P to form a new sequence P'. For instance, let $P' = \{P_1, P_3, P_4, P_2\} = \{|0\rangle, |+\rangle, |0\rangle, |+\rangle\}$. Alice then sends P' to Bob.

Step 2: Upon receiving P', Bob reorders the sequence to form $P_b = \{P_1, P_4, P_2, P_3\}$. He then randomly selects a subsequence of secret bits $b = (b_1, b_2, b_3, b_4) = (1, 1, 0, 0)$. Based on the predefined rules, Bob performs local unitary operations on P_b. Specifically, he applies the operation U to P_1 and P_4, while applying the identity operation I to P_2 and P_3. As a result, the sequence P_b is transformed into $P'_b = \{|0\rangle, |+\rangle, |0\rangle, |+\rangle\}$. Bob then sends P'_b to Charlie.

Step 3: Similarly, upon receiving P'_b, Charlie reorders it to obtain $P_c = \{P_2, P_3, P_1, P_4\}$. He then randomly selects his own subsequence of secret bits $c = (c_1, c_2, c_3, c_4) = (0, 1, 0, 1)$. According to these secret bits, Charlie performs a sequence of local unitary operations . Specifically, the operation I is applied to P_2, the operation

U to P_3, the operation I to P_1, and the operation U to P_4. Consequently, the sequence P_c is transformed into $P_c' = \{|+\rangle, |-\rangle, |1\rangle, |0\rangle\}$. Charlie then sends P_c' to David.

Step 4: Upon receiving P_c', David reorders it to obtain $P_d = \{P_1, P_4, P_3, P_2\}$. David selects his subsequence of secret bits $d = (d_1, d_2, d_3, d_4) = (0, 0, 1, 0)$. He then applies the corresponding local unitary operations to each particle in the sequence P_d. After completing the above operations, P_d is transformed into $P_d' = \{|1\rangle, |0\rangle, |+\rangle, |+\rangle\}$. Subsequently, David sends P_d' to Edward.

Step 5: Similarly, Edward performs operations analogous to those of the previous participants. He first reorders P_d' to form $P_e = \{P_2, P_1, P_3, P_4\}$. Next, he selects his subsequence of secret bits, assuming $e = (e_1, e_2, e_3, e_4) = (1, 1, 1, 0)$. According to the corresponding local unitary operations, Edward applies the U operation to P_2, P_1, and P_3, and the identity operation I to P_4. Consequently, P_e is transformed into $P_e' = \{|-\rangle, |0\rangle, |-\rangle, |0\rangle\}$. Finally, Edward sends P_e' back to Alice.

Step 6: Upon receiving P_e', Alice announces the original order of each particle in her prepared sequence and requests all participants to disclose the order of particles after their respective rearrangements. Using this information, Alice rearranges P_e' to align the particle sequence with the original order in which she generated it. As a result, P_e' is transformed into $P_a'' = \{P_1, P_2, P_3, P_4\} = \{|0\rangle, |-\rangle, |-\rangle, |0\rangle\}$. Alice then measures each particle in P_a'' and decodes the results according to the predefined rules, obtaining the overall secret $S = (0, 1, 1, 0)$.

Step 7: Based on the particle order information disclosed by all participants, Bob, Charlie, David, and Edward can rearrange their respective sub-secrets to derive their final secrets. Thus, Bob's secret b becomes $b' = (1, 0, 0, 1)$, Charlie's secret c becomes $c' = (0, 0, 1, 1)$, David's secret d becomes $d' = (0, 0, 1, 0)$, and Edward's secret e becomes $e' = (1, 1, 1, 0)$. Finally, all participants collaboratively reconstruct the overall secret S using the XOR operation:

$$S = b' \oplus c' \oplus d' \oplus e' = (0, 1, 1, 0). \tag{4}$$

3. Security analysis

This section provides a security analysis of the proposed protocol, focusing on both outside and inside attacks.

3.1. Outside attack

Outside attack pertain to the scenarios where an unauthorized adversary, such as Eve, attempts to eavesdrop on the communication without legitimate access to the system. Eve may attempt to gain access to the secret S through various common attack strategies, including intercept-resend attack, measurement-resend attack, entangle–measure attack, and Trojan horse attack.

3.1.1. Intercept–resend attack To attempt to acquire the secret S, the interceptor Eve may intercept the sequence P'_n that the last participant, the n-th participant, is about to send back to Alice, and then forward a prepared fake particle sequence to Alice. However, Eve is unaware of the measurement basis for each particle in the sequence P'_n at this point. Therefore, the probability that the fake sequence prepared by Eve does not match the measurement basis of the corresponding particles in P'_n is $\frac{1}{2}$, and the probability that they are equal is also $\frac{1}{2}$. When Alice receives the fake sequence and sorts the particles back to their initial order, the probability of introducing an error at each position after measurement is $\frac{1}{2}$. Given the length of our secret is m, in step 6 of the protocol, Alice has a probability of $\rho_1 = 1 - \left(\frac{1}{2}\right)^m$ to detect Eve's presence. From Figure 1, it can be obtained that when $m = 5$, the value of ρ_1 is 0.9687. When $m = 20$, the value of ρ_1 is 0.9999. Therefore, when m is large enough, Eve's eavesdropping behavior will be detected. Moreover, Eve cannot glean any useful information from P'_n because she lacks knowledge of the initial order of the particles and the corresponding measurement basis for each particle, which are both randomly determined to her.

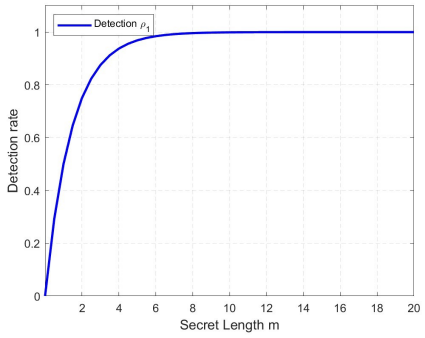

Figure 1. Probability of detected eavesdropping ρ_1 .

3.1.2. Measurement-resend attack In an attempt to intercept the secret S, Eve may intercept the sequence P'_n that the n-th participant is about to send to Alice and measure it. Based on the measurement outcomes, Eve can generate particles that match the measured states and resend them to Alice. However, her success is not guaranteed. When Eve randomly measures P'_n using either the Z-basis or the X-basis, for a single particle, if she chooses the correct basis, she can evade eavesdropping detection. If she chooses incorrectly, for instance, when the particle is $|0\rangle$ and she measures in the X-basis, according to the principles of quantum superposition, the measurement outcomes will be $|+\rangle$ or $|-\rangle$ with equal probability of $\frac{1}{2}$ each. Consequently, by the encoding rules, there is still a $\frac{1}{2}$ chance to escape eavesdropping detection. Therefore, for a single particle, Eve has a probability of $\frac{1}{2} + \frac{1}{2} \times \frac{1}{2} = \frac{3}{4}$ to evade eavesdropping detection. When the secret length is m, the probability that Eve is detected is $\rho_2 = 1 - \left(\frac{3}{4}\right)^m$. From Figure 2, it can be obtained that when $m = 5$, the value of ρ_2 is 0.7627. When $m = 20$, the value of ρ_2 is 0.9968. Therefore, when m is large enough, Eve's eavesdropping behavior

will be detected. Furthermore, since Eve is unaware of the initial order of the particles, she cannot correctly confirm the sequence of each particle in K'_n, and thus she cannot obtain the secret S.

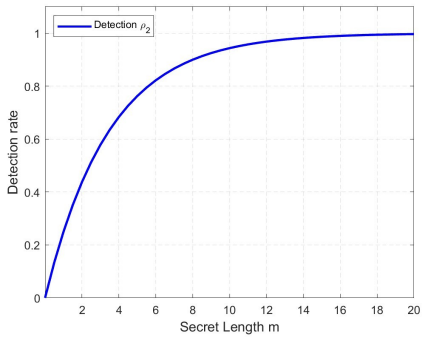

Figure 2. Probability of detected eavesdropping ρ_2 .

3.1.3. Entangle–measure attack Eve may attempt to compromise the key S through an attack based on entangle–measure attack. In this strategy, Eve intercepts the particle sequence P'_n intended to be sent to Alice by the n-th participant and prepares an equal number of ancillary particles $|\varepsilon\rangle$ corresponding to the secret length m. Eve then applies a unitary operation U_F to entangle the ancillary particles with the intercepted sequence P'_n. By measuring the ancillary particles $|\varepsilon\rangle$, Eve aims to infer the key information. However, the intercepted sequence P'_n transforms into the following states:

$$U_F(|0\rangle|\varepsilon\rangle) = p|0\rangle|f_{00}\rangle + q|1\rangle|f_{01}\rangle. \tag{5}$$

$$U_F(|1\rangle|\varepsilon\rangle) = r|0\rangle|f_{10}\rangle + s|1\rangle|f_{11}\rangle. \tag{6}$$

$$\begin{aligned} U_F(|+\rangle|\varepsilon\rangle) = \frac{1}{2}\big[&|+\rangle(p|f_{00}\rangle + q|f_{01}\rangle + r|f_{10}\rangle + s|f_{11}\rangle) \\ &+ |-\rangle(p|f_{00}\rangle - q|f_{01}\rangle + r|f_{10}\rangle - s|f_{11}\rangle)\big]. \end{aligned} \tag{7}$$

$$\begin{aligned} U_F(|-\rangle|\varepsilon\rangle) = \frac{1}{2}\big[&|+\rangle(p|f_{00}\rangle + q|f_{01}\rangle - r|f_{10}\rangle - s|f_{11}\rangle) \\ &+ |-\rangle(p|f_{00}\rangle - q|f_{01}\rangle - r|f_{10}\rangle + s|f_{11}\rangle)\big]. \end{aligned} \tag{8}$$

Specifically, $|f_{00}\rangle$, $|f_{01}\rangle$, $|f_{10}\rangle$, and $|f_{11}\rangle$ are the four states defined by U_F.'If Eve wants to avoid being detected, the following must be satisfied:

$$U_F(|0\rangle|\varepsilon\rangle) = p|0\rangle|f_{00}\rangle. \tag{9}$$

$$U_F(|1\rangle|\varepsilon\rangle) = s|1\rangle|f_{11}\rangle. \tag{10}$$

Additionally, the complex coefficients p, q, r, and s must obey the normalization conditions:

$$|p|^2 + |q|^2 = |r|^2 + |s|^2 = 1. \tag{11}$$

From these equations, it can be derived that:

$$q = r = 0. \tag{8}$$

This leads to the following equations:

$$p|f_{00}\rangle - q|f_{01}\rangle + r|f_{10}\rangle - s|f_{11}\rangle = 0. \tag{9}$$
$$p|f_{00}\rangle + q|f_{01}\rangle - r|f_{10}\rangle - s|f_{11}\rangle = 0. \tag{10}$$

From this, it can be further deduced that $p|f_{00}\rangle = s|f_{11}\rangle$. As a result, Eve cannot extract any useful information without introducing detectable errors.

3.1.4. Trojan horse attack During the protocol process, Eve might attempt Trojan horse attacks, including invisible photon attacks and delayed photon attacks [40, 41]. To defend against invisible photon attacks, all participants in the protocol can utilize wavelength filters to screen the photons. Furthermore, to counter delayed photon attacks, members can employ photon number splitters to distinguish the received photons. Consequently, our MQSS protocol is fortified to resist Trojan horse attacks.

3.2. Inside attack

Inside attacks pose a significant threat to quantum communication protocols, as they originate from trusted insiders with legitimate access to the system. These participants can exploit their knowledge and access to disrupt the protocol or extract sensitive information. We will discuss potential internal attacks and the measures our protocol implements to mitigate these risks.

In our protocol, assuming there are n participants, the number of dishonest members among the participants ranges from 1 to $n-1$. We discuss two separate cases here: the first case where there is only one dishonest participant, and the second case where there is only one honest participant.

3.2.1. Only one participant is dishonest In our assumption, the n-th participant is the dishonest member who attempts to recover the secret on his own. Therefore, before sending p'_n to Alice, he may employ the aforementioned eavesdropping techniques. However, according to the previous analysis, the eavesdropping attempts of the n-th participant can be detected, and he is unaware of the ordering and local unitary operations performed by the other participants on the sequence. Consequently, he cannot extract valid information from the sequence p'_n.

3.2.2. Only one participant is honest At most $n-1$ participants are dishonest. Here, we assume Bob to be the sole honest participant. In this scenario, the other $n-1$ participants attempt to recover the secret without Bob's involvement, or they may attempt to acquire Bob's secret. Since they are unaware of the sorting operations and

local unitary transformations that Bob has applied to the sequence, they cannot obtain Bob's secret. Similarly, based on the aforementioned analysis, their eavesdropping behavior will be detected.

4. Simulation

To validate and demonstrate the quantum protocol, we utilize Qiskit [42–44], an open-source software framework developed and maintained by IBM, which is widely used in the field of quantum computing. IBM, a renowned leader in quantum computing, has made significant contributions through Qiskit, providing researchers and developers with a powerful tool for quantum computing exploration. Qiskit offers a comprehensive set of tools and libraries, enabling users to perform various tasks, such as quantum circuit construction, simulation, and the implementation and testing of quantum algorithms. In this experiment, we employed Qiskit, leveraging IBM's expertise and infrastructure, to simulate and showcase the working principles of the MQSS protocol.

In this quantum circuit diagram, the quantum bits q_0 to q_3 correspond to the particles P_1 to P_4 in Section 2.2 of the MQSS protocol. The X gates in the circuit represent the local unitary operations U applied to the corresponding particles. Each particle undergoes a series of local operations and reorderings, ultimately leading to Alice measuring the final quantum state to recover the overall shared secret.

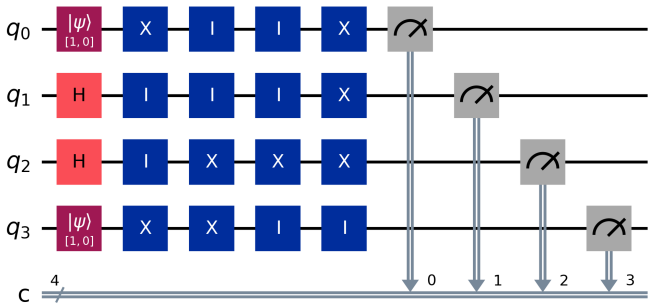

Figure 3. MQSS Protocol Example 2.2 Quantum Circuit.

To evaluate the performance of the proposed protocol, we conducted a simulation involving 1024 iterations. During each iteration, Alice prepared a sequence of quantum states and performed measurements after all participants had applied their respective local unitary operations. The final secret recovered by Alice in each iteration was recorded.

The distribution of the recovered secrets across the 1024 iterations is depicted in Fig. 4. The results demonstrate that all possible secrets are recovered with roughly equal frequency, confirming the uniformity and fairness of the protocol in distributing secrets.

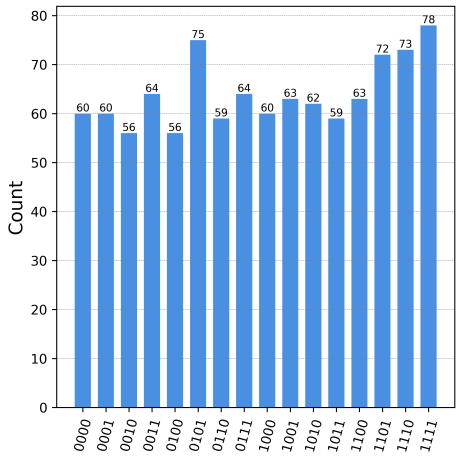

Figure 4. Distribution of secrets recovered by Alice across 1024 iterations.

5. Comparisons

To evaluate the efficiency and practicality of our proposed MQSS protocol, we conducted a comparative analysis with various existing MQSS protocols across several key aspects, including quantum resource requirements, the need for a TP, distributor can know participants' secrets, Simulation of protocol, qubit efficiency, and decoy particles can encode information. The results of this comparison are summarized in Table 4.

We propose a MQSS protocol that has certain advantages. First, the protocol is based on single photon, which simplifies the preparation of quantum resources and reduces experimental costs. Single photons do not require complex quantum entanglement preparation processes, enabling more efficient and stable generation, which is particularly valuable in experimental settings. In contrast, many existing MQSS protocols rely on multi-particle entangled states, which necessitate complex multi-particle measurements. Under current technological conditions, the implementation of such multi-particle measurements remains challenging, significantly limiting the practical applications of these protocols. Additionally, the local unitary operations employed in our protocol are relatively straightforward, consisting only of basic I and U operations, without involving complex multi-particle operations or gate operations. This simplification reduces experimental difficulty and enhances the feasibility and efficiency of the protocol.

In our proposed MQSS protocol, the distributor does not know the specific secret shares of any participant during the secret sharing process. This design effectively avoids the potential security risks associated with the distributor possessing participants' secrets, thereby further ensuring the privacy of participants' secrets and the overall security of the protocol. In addition, participants in our proposed MQSS protocol do not need to perform quantum measurements to obtain their secret shares, unlike many existing MQSS protocols that rely on quantum measurements. This approach significantly reduces resource consumption, making our protocol more efficient

and practical. Finally , in many existing MQSS protocols, the particles used for eavesdropping detection are not utilized for information transmission, resulting in low efficiency. However, our protocol makes full use of the eavesdropping detection particles m_{detect}, allowing them to also transmit information. In the absence of eavesdropping, our protocol can achieve an efficiency of up to 100%.

Table 4. Comparison results between the our protocol and existing MQSS protocols

Ref.	Quantum resources	TP usage	Distributor can know participants' secrets	Simulation of protocol	Qubit efficiency	Decoy particles can encode information
[15]	GHZ State	No	Yes	No	1/3	No
[16]	GHZ State	No	Yes	No	$1/(m+n)$	No
[30]	Single photon	No	Yes	No	$\frac{S}{M(1+2C)}$	No
[33]	Single photon	No	Yes	No	1/2	No
[34]	GHZ state	No	Yes	Yes	$\frac{r\log_2 d}{g+1+L+12t-6}$	No
[36]	EPR pair	Yes	No	No	$1/(m+n)$	No
[37]	GHZ state	Yes	No	No	$\frac{1}{2^{n+1}}$	No
[38]	Single photon	Yes	No	No	$1/\max(m,n)$	No
[39]	EPR pair	No	No	No	1	Yes
Ours	Single photon	No	No	Yes	1	Yes

We present the Qubit efficiency of several existing MQSS protocols in Figure 5. This graphical representation provides a comprehensive overview of how different protocols perform in terms of quantum bit utilization under various conditions. For the considered MQSS protocols, the number of participants n starts from 3.

It can be seen from Figure 5 that the qubit efficiencies of the protocols of Shi et.al [36], Tsai et.al [37] and You et.al [38] decrease gradually as the number of participants increases. For the protocols of Hwang et.al [15] and Du et.al [33], although

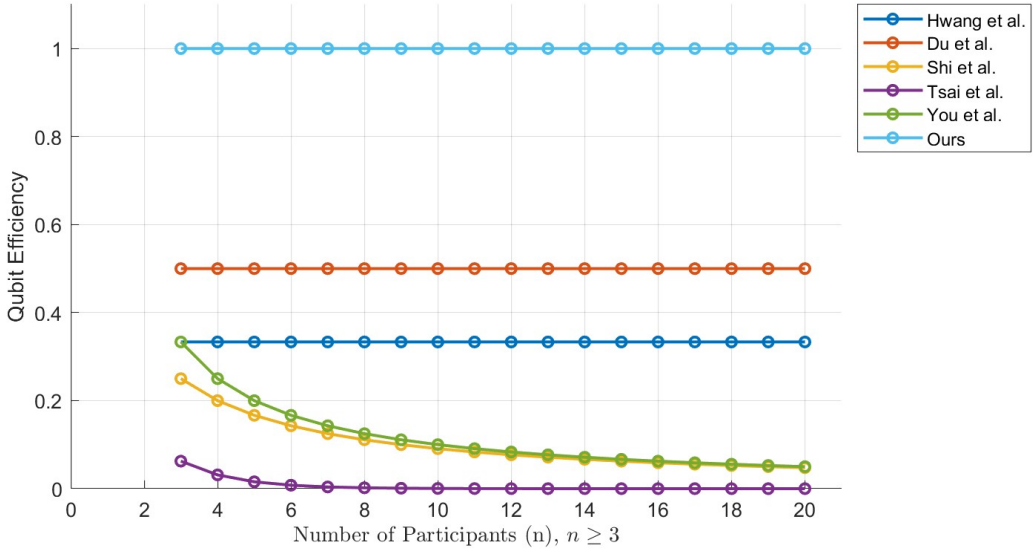

Figure 5. Quantum efficiency comparison.(Compare the qubit efficiency of our protocol with that of the protocols in [15], [33], [36], [37], [38].)

their efficiencies do not decrease with the increase of the number of participants, the efficiency values of these protocols are relatively low. In contrast, the qubit efficiency of our protocol remains 1 regardless of the number of participants.

6. Conclusion

We propose a MQSS protocol based on single photon, aimed at securely and efficiently distributing and sharing secret information among multiple participants. The protocol utilizes basic local unitary operations and single particle measurement, simplifying the preparation and manipulation of quantum resources, and reducing experimental costs and difficulties. Our protocol allows participants to engage in secret sharing without revealing any personal information to the distributor, enhancing privacy protection. By optimizing the use of quantum resources, our protocol can achieve an efficiency close to 100%. Since the participants of our protocol do not need to perform measurement operations, our protocol improves processing efficiency by reducing quantum measurements. Through simulation experiments, we have verified the effectiveness of the protocol.

Acknowledgements

[1] Andrew Steane. Quantum computing. Reports on Progress in Physics, 61(2):117, 1998.

[2] Eleanor Rieffel and Wolfgang Polak. An introduction to quantum computing for non-physicists. ACM Computing Surveys (CSUR), 32(3):300–335, 2000.

[3] Tony Hey. Quantum computing: an introduction. Computing & Control Engineering Journal, 10(3):105–112, 1999.

[4] Mark Hillery, Vladimír Bužek, and André Berthiaume. Quantum secret sharing. Physical Review A, 59(3):1829, 1999.

[5] Anders Karlsson, Masato Koashi, and Nobuyuki Imoto. Quantum entanglement for secret sharing and secret splitting. Physical Review A, 59(1):162, 1999.

[6] Li Xiao, Gui Lu Long, Fu-Guo Deng, and Jian-Wei Pan. Efficient multiparty quantum-secret-sharing schemes. Physical Review A—Atomic, Molecular, and Optical Physics, 69(5):052307, 2004.

[7] Fu-Guo Deng, Xi-Han Li, Hong-Yu Zhou, and Zhan-jun Zhang. Improving the security of multiparty quantum secret sharing against trojan horse attack. Physical Review A—Atomic, Molecular, and Optical Physics, 72(4):044302, 2005.

[8] Deng Fu-Guo, Zhou Ping, Li Xi-Han, Li Chun-Yan, and Zhou Hong-Yu. Efficient multiparty quantum secret sharing with greenberger–horne–zeilinger states. Chinese Physics Letters, 23(5):1084, 2006.

[9] Song Lin, Fei Gao, Fen-Zhuo Guo, Qiao-Yan Wen, and Fu-Chen Zhu. Comment on "multiparty quantum secret sharing of classical messages based on entanglement swapping". Physical Review A—Atomic, Molecular, and Optical Physics, 76(3):036301, 2007.

[10] Hongyang Ma, Bingquan Chen, Zhongwen Guo, and Hongsheng Li. Development of quantum network based on multiparty quantum secret sharing. Canadian Journal of Physics, 86(9):1097–1101, 2008.

[11] YuGuang Yang and QiaoYan Wen. Threshold quantum secret sharing between multi-party and multi-party. Science in China Series G: Physics, Mechanics and Astronomy, 51(9):1308–1315, 2008.

[12] Huang Da-Zu, Chen Zhi-Gang, and Guo Ying. Multiparty quantum secret sharing using quantum fourier transform. Communications in Theoretical Physics, 51(2):221, 2009.

[13] Ying Sun, Qiao-yan Wen, Fei Gao, Xiu-bo Chen, and Fu-chen Zhu. Multiparty quantum secret sharing based on bell measurement. Optics communications, 282(17):3647–3651, 2009.

[14] Xin Liao, Qiao-yan Wen, Ying Sun, and Jie Zhang. Multi-party covert communication with steganography and quantum secret sharing. Journal of Systems and Software, 83(10):1801–1804, 2010.

[15] Tzonelih Hwang, Cheng-Chieh Hwang, and Chuan-Ming Li. Multiparty quantum secret sharing based on ghz states. Physica Scripta, 83(4):045004, 2011.

[16] Rui-Ke Chen, Ying-Ying Zhang, Jian-Hong Shi, and Feng-Guang Li. A multiparty error-correcting method for quantum secret sharing. Quantum information processing, 13:21–31, 2014.

[17] Jung-Lun Hsu, Song-Kong Chong, Tzonelih Hwang, and Chia-Wei Tsai. Dynamic quantum secret sharing. Quantum Information Processing, 12:331–344, 2013.

[18] Ting-Ting Song, Qiao-Yan Wen, Fei Gao, and Hui Chen. Participant attack and improvement to multiparty quantum secret sharing based on ghz states. International Journal of Theoretical Physics, 52:293–301, 2013.

[19] Noor Ul Ain. A novel approach for secure multi-party secret sharing scheme via quantum cryptography. pages 112–116, 2017.

[20] Kun-Fei Yu, Jun Gu, Tzonelih Hwang, and Prosanta Gope. Multi-party semi-quantum key distribution-convertible multi-party semi-quantum secret sharing. Quantum Information Processing, 16:1–14, 2017.

[21] Ye Chong-Qiang, Ye Tian-Yu, He De, and Gan Zhi-Gang. Multiparty semi-quantum secret sharing with d-level single-particle states. International Journal of Theoretical Physics, 58:3797–3814, 2019.

[22] Ke-jia Zhang, Xue Zhang, Heng-yue Jia, and Long Zhang. A new n-party quantum secret sharing model based on multiparty entangled states. Quantum Information Processing, 18:1–15, 2019.

[23] Kartick Sutradhar and Hari Om. Secret sharing based multiparty quantum computation for multiplication. International Journal of Theoretical Physics, 60(9):3417–3425, 2021.

[24] Yao-Hsin Chou, Guo-Jyun Zeng, Xing-Yu Chen, and Shu-Yu Kuo. Multiparty weighted threshold quantum secret sharing based on the chinese remainder theorem to share quantum information. Scientific Reports, 11(1):6093, 2021.

[25] Ri-Gui Zhou, Mingyu Huo, Wenwen Hu, and Yishi Zhao. Dynamic multiparty quantum secret sharing with a trusted party based on generalized ghz state. Ieee Access, 9:22986–22995, 2021.

[26] Mahsa Khorrampanah and Monireh Houshmand. Effectively combined multi-party quantum secret sharing and secure direct communication. Optical and Quantum Electronics, 54(4):213, 2022.

[27] Zhihui Li, Xue Jiang, and Lu Liu. Multi-party quantum secret sharing based on ghz state. Entropy, 24(10):1433, 2022.

[28] Yuguang Xu, Zexi Li, Tianhua Liu, and Hongfeng Zhu. Multi-party quantum secret sharing protocol based on ghz states entanglement swapping. International Journal of Theoretical Physics, 61(3):76, 2022.

[29] Shuaishuai Liu, Zhenguo Lu, Pu Wang, Yan Tian, Xuyang Wang, and Yongmin Li. Experimental demonstration of multiparty quantum secret sharing and conference key agreement. npj Quantum Information, 9(1):92, 2023.

[30] Shu-Yu Kuo, Kuo-Chun Tseng, Chia-Ching Yang, and Yao-Hsin Chou. Efficient multiparty quantum secret sharing based on a novel structure and single qubits. EPJ Quantum Technology, 10(1):29, 2023.

[31] Gan Gao. Cryptanalysis and improvement of efficient multiparty quantum secret sharing based on a novel structure and single qubits. EPJ Quantum Technology, 11(1):1–8, 2024.

[32] Alessio Di Santo, Walter Tiberti, and Dajana Cassioli. Security and fairness in multi-party quantum secret sharing protocol. arXiv preprint arXiv:2412.11667, 2024.

[33] Yu Tao Du and Wan Su Bao. An efficient multiparty quantum secret sharing scheme based on the measuring-basis-encrypted. The European Physical Journal Special Topics, pages 1–6, 2024.

[34] Lele Li, Zhaowei Han, Zhihui Li, Feiting Guan, and Li Zhang. Authenticable dynamic quantum multi-secret sharing based on the chinese remainder theorem. Quantum Information Processing, 23(2):46, 2024.

[35] Yu-Guang Yang, Rui-Chen Huang, Guang-Bao Xu, Yi-Hua Zhou, Wei-Min Shi, and Dan Li. New multiparty measurement-device-independent quantum secret sharing protocol based on entanglement swapping. Modern Physics Letters A, 38(32n33):2350145, 2023.

[36] RunHua Shi, LiuSheng Huang, Wei Yang, and Hong Zhong. Quantum secret sharing between multiparty and multiparty with bell states and bell measurements. SCIENCE CHINA Physics, Mechanics and Astronomy, 53:2238–2244, 2010.

[37] Chia-Wei Tsai, Chun-Wei Yang, and Jason Lin. Multiparty mediated quantum secret sharing protocol. Quantum Information Processing, 21(2):63, 2022.

[38] Zhixing You, Yunran Wang, Zhao Dou, Jian Li, Xiubo Chen, and Lixiang Li. Dynamic quantum secret sharing between multiparty and multiparty based on single photons. Physica A: Statistical Mechanics and its Applications, 624:128893, 2023.

[39] Xiangjun Xin, Fan He, Shujing Qiu, Chaoyang Li, and Fagen Li. Efficient multi-party quantum secret-sharing protocol. Chinese Journal of Physics, 92:664–674, 2024.

[40] Qing-Yu Cai. Eavesdropping on the two-way quantum communication protocols with invisible photons. Physics Letters A, 351(1-2):23–25, 2006.

[41] Nicolas Gisin, Sylvain Fasel, Barbara Kraus, Hugo Zbinden, and Grégoire Ribordy. Trojan-horse attacks on quantum-key-distribution systems. Physical Review A—Atomic, Molecular, and Optical Physics, 73(2):022320, 2006.

[42] Robert Wille, Rod Van Meter, and Yehuda Naveh. Ibm's qiskit tool chain: Working with and developing for real quantum computers. In 2019 Design, Automation & Test in Europe Conference & Exhibition (DATE), pages 1234–1240. IEEE, 2019.

[43] Naoki Kanazawa, Daniel J Egger, Yael Ben-Haim, Helena Zhang, William E Shanks, Gadi Aleksandrowicz, and Christopher J Wood. Qiskit experiments: A python package to characterize and calibrate quantum computers. Journal of Open Source Software, 8(84):5329, 2023.

[44] Paras Nath Singh and S Aarthi. Quantum circuits–an application in qiskit-python. In 2021 third international conference on intelligent communication technologies and virtual mobile networks (icicv), pages 661–667. IEEE, 2021.