EPiC Series in Computing

Volume 106, 2025, Pages 70–83

Proceedings of the 20th Asia Joint
Conference on Information Security

Circular Quantum Secret Sharing Based on SWAP Gates

Pei-Shiun Tsai[1], Tzu-Yu Liao[1, *], Wei-Rung Chen[1], Jason Lin[1, *],
and Iuon-Chang Lin[2]

[1] Department of Computer Science and Engineering,
National Chung Hsing University, Taichung, Taiwan

[2] Department of Management Information Systems,
National Chung Hsing University, Taichung, Taiwan

s111056016@mail.nchu.edu.tw
s111065019@mail.nchu.edu.tw
g112056043@mail.nchu.edu.tw
jasonlin@nchu.edu.tw
iclin@nchu.edu.tw

Abstract

Most existing quantum secret sharing (QSS) protocols can be classified into two types of transmission structures: tree-type and circular-type. Compared to circular-type protocols, tree-type QSS protocols are more difficult to implement in practice due to photon energy loss over long distances, rendering them unsuitable when parties are widely separated. However, circular-type protocols still face two major challenges: (1) maintaining the energy of transmitted photons across a long chain of intermediate nodes is infeasible, and (2) reliance on relay transmission makes them vulnerable to Trojan horse attacks. To address these issues, we propose two novel circular-type QSS protocols based on SWAP gates. The proposed protocols are immune to Trojan horse attacks and offer a practical solution for relay transmission, enabling the long-distance distribution of shadow keys to each agent.

Keywords: Quantum secret sharing, circular transmission, SWAP gates, Trojan horse attacks, single photons

1 Introduction

In a secret sharing scheme [1-4], agents are required to collaborate by disclosing their individual secret shares in order to jointly reconstruct the dealer's original secret. This mechanism can be utilized to establish a shared key between a dealer and multiple agents, and is applicable to various cryptographic protocols, including symmetric encryption [5, 6]. For instance, in a three-party scenario,

A. Yamada, H.K. Kim, Y. Wang and T.-T. Tsai (eds.), AsiaJCIS 2025 (EPiC Series in Computing, vol. 106), pp. 70–83

suppose a dealer Alice holds a secret key K_A, which is divided into two shares, K_B and K_c, and distributed to two agents. This division satisfies the relationship $K_A = K_B \oplus K_C$, where $\oplus$ denotes the bitwise Exclusive-OR (XOR) operation, thereby completing the secret sharing process. When the dealer intends to securely transmit a plaintext message $Plaintext_A$ to the agents, the message is encrypted using the key K_A, producing the ciphertext $Cipher_A = Plaintext_A \oplus K_A$, which is then made publicly accessible to the agents. To recover the original message $Plaintext_A$, the agents must cooperate to reveal their respective secret shares and reconstruct the original key K_A. The recovered key can then be applied to the public ciphertext $Cipher_A$, enabling successful decryption of the plaintext.

In conventional secret sharing, secrets are often represented as binary strings and distributed via classical channels. However, these classical schemes rely on computational hardness assumptions, such as the difficulty of factoring large integers [7] or solving discrete logarithms [8], for their security guarantees. With the rapid development of quantum computing, these assumptions are no longer reliable, as algorithms like Shor's algorithm [9] could efficiently break many widely used cryptographic systems. Consequently, current classical secret sharing is now considered vulnerable in the presence of quantum adversaries.

To address this future threat, quantum cryptography introduces a fundamentally different paradigm, offering unconditional security grounded in the laws of quantum mechanics. One of the most significant breakthroughs is the development of quantum key distribution (QKD) [10-12]. The BB84 protocol [11], proposed by Bennett and Brassard in 1984, was the first QKD scheme. It allows two agents to generate a shared key through the transmission of quantum states prepared in non-orthogonal bases, with any eavesdropping attempts being inherently detectable. Later, in 1992, the B92 protocol [12] was introduced as a simplified alternative using only two non-orthogonal quantum states. While conceptually more minimal, B92 still ensures security through quantum principles such as the no-cloning theorem and measurement disturbance. Both BB84 and B92 form the basis for various quantum communication tasks, including quantum secret sharing (QSS), which extends classical secret sharing into the quantum domain by enabling secrets to be encoded into quantum states and shared over quantum channels with unconditional security.

QSS enables the secure distribution of secrets by encoding classical information into quantum states and transmitting them through quantum channels. In QSS protocols, the dealer's secret is typically represented as a binary string $S = (s_0 s_1 \dots s_n)$, where each bit $s_i \in \{0, 1\}$, for $i \in \{0, 1, 2, \dots, n\}$. The secret is then mapped to quantum states, and is shared among agents by using quantum properties such as entanglement, superposition, quantum unitary operations and quantum measurement. Depending on the communication topology, QSS protocols can be broadly classified into two categories: tree-type and circular-type structures, as shown in Figure 1.

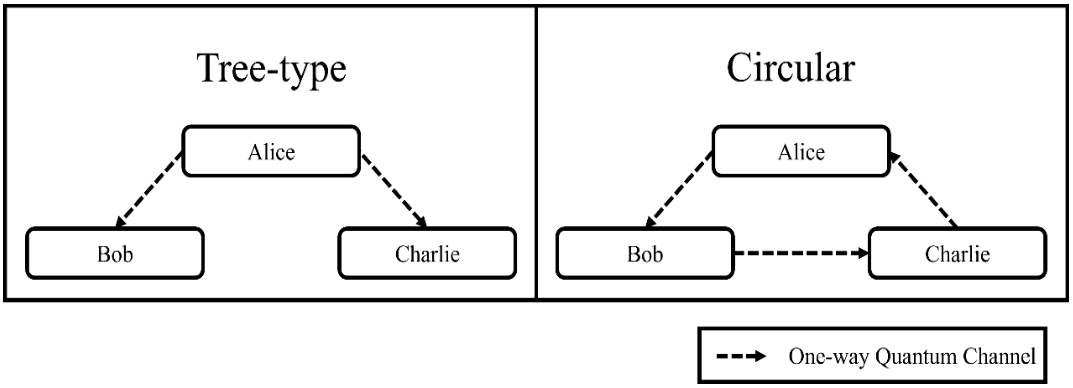

Figure 1: Illustration of tree-type and circular-type transmission structures in QSS

In 1999, Hillery et al. proposed the first QSS scheme based on a tree-type transmission structure using three-particle Greenberger-Horne-Zeilinger (GHZ) states [13]. In their scheme, entangled photons are generated by the dealer and distributed to each agent through individual quantum channels. However, due to current physical limitations [14, 15], photons cannot be transmitted over infinite distances, making tree-type QSS schemes significantly more challenging to implement in practical settings.

To overcome this limitation, Deng et al. [16] introduced a circular-type QSS protocol in 2006. In this structure, quantum states such as single photons or entangled particles are passed sequentially through all agents in a closed loop, with each agent applying a local quantum operation to embed their share of the secret. The final quantum state is then returned to the dealer, who performs a measurement to verify the integrity of the sequence or to retrieve the secret. Because the physical distance between any two neighboring agents in a circular topology is relatively short, circular-type QSS schemes are generally more feasible and cost-effective for practical implementation.

Building on this model, various circular-type QSS protocols have been proposed [17-23]. In most designs, a single photon or entangled pair is transmitted through a sequence of agents, each of whom applies a unitary operation, such as a Pauli or Hadamard gate, to encode their share. These protocols often include decoy states and basis randomization to detect eavesdropping. Alternatively, some circular-type schemes adopt a different encoding strategy by having agents reorder the photon sequences rather than perform quantum operations. These are often classified as semi-quantum secret sharing (SQSS) protocols [19-21], as they allow agents with limited quantum capabilities to participate.

Despite the advantages of circular-type QSS, several practical challenges remain. As the number of agents increases, the photon must traverse a longer path, increasing the probability of photon loss and transmission errors, challenges reminiscent of those encountered in tree-type structures. Moreover, because all agents share the same quantum channel, circular-type QSS is also vulnerable to Trojan horse attacks, such as the delay-photon Trojan horse attack [24] and the invisible-photon Trojan horse attack [25]. While these attacks can be mitigated using quantum devices like photon number splitters (PNS) and wavelength filters, such countermeasures inevitably increase system complexity and deployment cost.

In response to the two major challenges in circular-type QSS, this paper proposes a novel circular-type QSS protocol based on SWAP gates. The remainder of the paper is organized as follows: Section II introduces the SWAP gate, explains how it addresses the aforementioned issues, and presents the quantum logic gates and quantum states used in the protocol. Section III describes the proposed two QSS protocols in details. Section IV provides a preliminary security analysis of the protocol. Section V offers a comparison between our scheme and existing protocols, followed by concluding remarks.

2 Preliminaries

Before presenting the full protocol, we first introduce the essential quantum components that form its foundation. In particular, our scheme employs the SWAP gate [26–27] as a core mechanism to enable controlled transmission and secret embedding within the circular structure. This gate plays a central role in maintaining the integrity and order of quantum information as it traverses multiple agents. In addition, we define the specific quantum states and unitary operations, such as Pauli gates, used throughout the protocol. These elements collectively enable the secure encoding, transformation, and measurement of quantum secrets.

A. Properties of the SWAP gate

The SWAP gate is a type of quantum logic gate that operates on two input photons and produces two output photons. After the operation, the quantum states of the two photons are exchanged. The quantum circuit representation of the SWAP gate is shown in Figure 2.

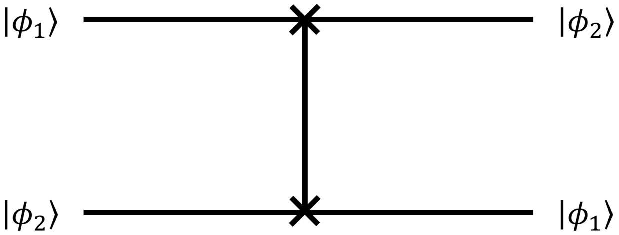

Figure 2: Circuit of the SWAP gate

The unique characteristics of the SWAP gate enable us to address both of the problems outlined in Section I. The solutions are discussed as follows:

(1) Photon Energy Loss During Transmission

Consider a scenario where Alice intends to transmit a photon to Bob, who in turn must forward it to Charlie. When Bob receives the photon from Alice, he performs the following steps, as illustrated in Figure 3.

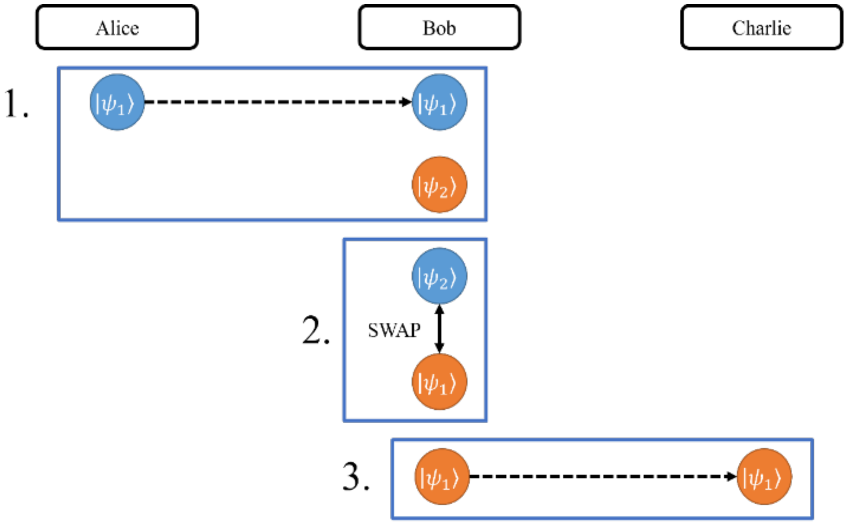

Figure 3: An example of sing the SWAP gate to extend a photon's lifespan

Step 1. Bob generates a new photon, which possesses a higher energy level than the photon received from Alice.

Step 2. He then inputs both photons into a SWAP gate. As a result, the new photon adopts the quantum state of Alice's photon, while retaining its original, higher energy.

Step 3. Bob transmits the newly swapped photon to Charlie.

By utilizing this method, the lifespan of Alice's original photon can be effectively extended through the SWAP operation, thereby mitigating energy loss during transmission.

(2) Trojan horse attacks

Suppose a SWAP gate operation is performed, as shown in Figure 3, prior to the security verification phase of the protocol. In this case, any photons injected as part of a Trojan horse attack may be inadvertently swapped into the auxiliary photon. Since injected photons can still be affected by quantum unitary operations, such as the SWAP gate, the attack may be detected if the unitary operation is applied on the photon. Specifically, if the quantum state of the auxiliary photon deviates from its expected value, this discrepancy can serve as an indicator of the presence of eavesdropper. A schematic illustration of this attack scenario is provided in Figure 4.

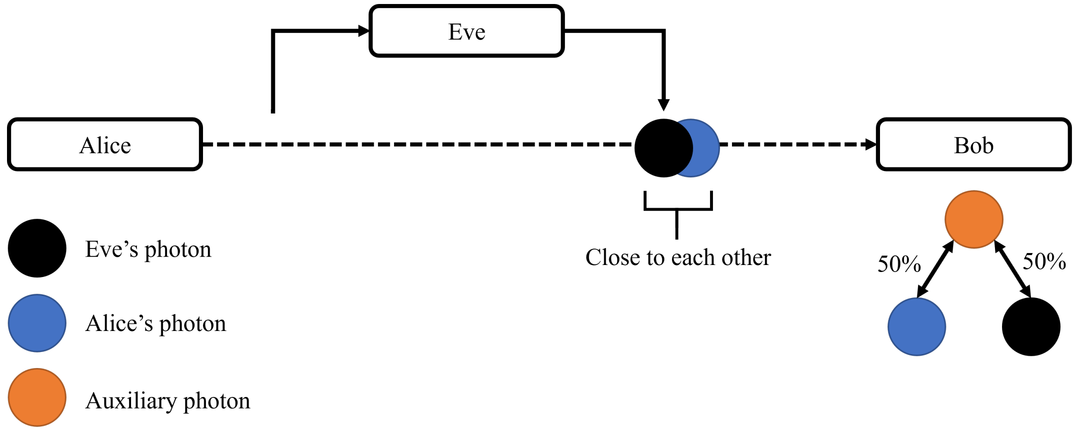

Figure 4: The use of SWAP gate to detect Trojan horse attacks

B. Quantum States and Quantum Gates

In our proposed QSS protocol, we utilize single photons prepared in either the Z basis or the X basis, corresponding to the following four quantum states: the Z basis consists of $|0\rangle$ and $|1\rangle$, while the X basis includes $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$.

In addition to the SWAP gate, two other quantum logic gates are employed in the protocol: the identity gate $I = |0\rangle\langle 0| + |1\rangle\langle 1|$, and the Pauli-X gate $X = |1\rangle\langle 0| + |0\rangle\langle 1|$. Table 1 summarizes the resulting photon states after applying these gates to input states from both the Z and X bases.

Table 1: Effects on single photon states after applying quantum gates

Quantum initial state	$\lvert 0\rangle$	$\lvert 1\rangle$	$\lvert +\rangle$	$\lvert -\rangle$
I gate	$\lvert 0\rangle$	$\lvert 1\rangle$	$\lvert +\rangle$	$\lvert -\rangle$
X gate	$\lvert 1\rangle$	$\lvert 0\rangle$	$\lvert +\rangle$	$-\lvert -\rangle$

It is worth noting that photons in the X basis remain unaffected by the application of either logic gate in terms of their measurement outcomes; their observable behavior remains unchanged. Moreover, photons prepared in either the Z or X basis retain their original basis after the gate operations, they are not transformed from one basis to another.

3 Proposed Circular QSS Protocols

This section introduces the two proposed circular QSS protocols based on SWAP gates in details. A four-party setting is used as an illustrative example to describe the step-by-step process of the two schemes. In the protocol environment, Alice acts as the dealer, while Bob, Charlie, and David serve as the agents. The secret to be shared by Alice is a cryptographic key, denoted as K_A, which she divides into three secret shares: K_B, K_C, and K_D to be distributed to Bob, Charlie, and David, respectively. Photon transmission follows a circular path in the order: Alice → Bob → Charlie → David → Alice, as shown in Figure 5.

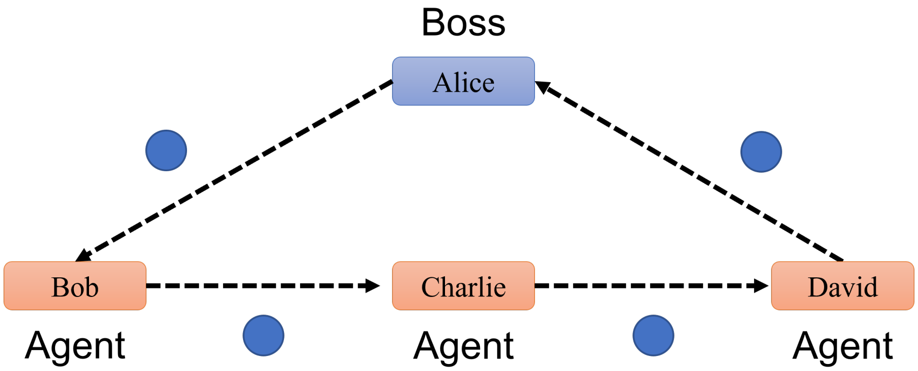

Figure 5: The environment of the proposed QSS protocols

A. The Circular QSS Protocol Based on Single Photons with Agents Measurement Capability

Step 1. Alice prepares a sequence of Nsingle photons, consisting of M photons in the Z basis and K photons in the X basis, such that $N = M + K$, or simplicity, we denote the sequence of N photons as $S = (s_1, s_2, s_i \dots, s_n)$, where $1 \leq i \leq n$, and each s_i represents the quantum state of the i-th photon. After generating the photon sequence, Alice records the initial basis and quantum state of each photon. She then sends the sequence S to Bob via a quantum channel.

Step 2. After receiving the photon sequence S from Alice, Bob generates a corresponding set of N auxiliary photons, denoted as $S^{aux} = (s_1^{aux}, s_2^{aux}, s_i^{aux} \dots, s_n^{aux})$. Bob then applies a SWAP gate operation to each pair consisting of a received photon and its corresponding auxiliary photon. As a result, the quantum states of the auxiliary photons are updated to reflect those of the original photons, yielding $S^{aux} = (s_1, s_2, s_i \dots, s_n)$, as shown in Figure 6.

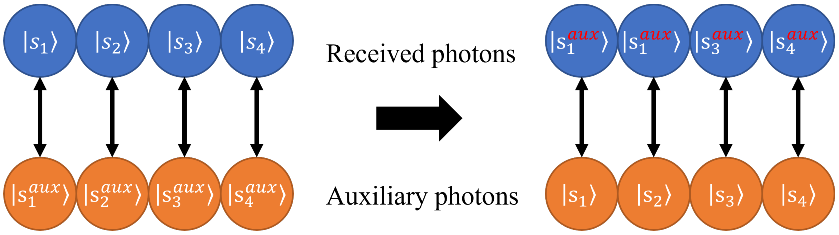

Figure 6: State transfer between received and auxiliary photons via SWAP gate

Step 3. Alice and Bob perform a security check on the L photons in S^{aux} that were originally prepared in the X basis. Alice informs Bob of the positions of these L photons, and Bob proceeds to measure the corresponding photons in the X basis. Bob reports the measurement results back to Alice. Alice compares Bob's measurement outcomes with the original quantum states she had prepared. If the sensed error rate is within normal thresholds, this process goes into the next step. Otherwise, this procedure stops and the protocol will be restarted.

Step 4. The L photons used for security checking, such as s_1 and s_2, are removed from S^{aux}, resulting in a reduced sequence $S^{aux} = (s_3, \ldots, s_n)$. Bob then applies a quantum logic gate to each remaining photon in S^{aux}. Specifically, for each photon s_i , a unitary operation $U_i^B \in \{I, X\}$ is applied, yielding a new photon sequence denoted as $S^{new} = (U_3^B s_3, \ldots, U_n^B s_n)$. Finally, Bob sends the sequence $S^{new}$to Charlie through a quantum channel. The example of the step is illustrated in Figure 7.

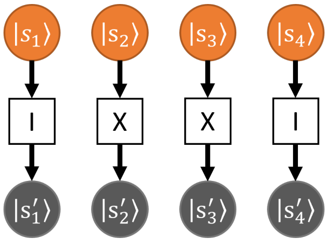

Figure 7: Example of photon encryption using I and X gates

Step 5. Charlie performs the same procedures as Bob, specifically Steps 2 through 4. After executing the SWAP gate operations, conducting the security check, and applying a sequence of unitary operations $U_i^C \in \{I, X\}$, Charlie obtains the photon sequence $(U_3^C U_3^B s_3, \ldots, U_n^C U_n^B s_n)$, which is then transmitted to David. David likewise performs the same steps as Bob. After his operations, the resulting photon sequence becomes $(U_3^D U_3^C U_3^B s_3, \ldots, U_n^D U_n^C U_n^B s_n)$, which he then sends back to Alice via the quantum channel.

Step 6. Alice repeats the procedure described in Step 2 to reconstruct the auxiliary sequence. She then measures on the photons: those originally prepared in the Z basis, as well as the remaining photons in the X basis. A subset of the Z-basis photons is used for security verification. For these photons, Alice requests that all agents publicly disclose the related unitary operations U_i^x they applied during the protocol. She then compares the expected measurement outcomes, with her actual measurement results. For the remaining X-basis photons, Alice directly compares the measurement results with the original quantum states. If the error rate is within normal thresholds, this process continues. Otherwise, this procedure is aborted.

Step 7. Alice then compares the measurement outcomes of the remaining Z-basis photons with their originally prepared states. If a measurement result matches the initial state, it implies that the total unitary operation applied to that photon is the identity operation I, and the corresponding classical bit is encoded as 0. Conversely, if the result differs from the initial state, the total unitary operation is inferred to be the Pauli-X gate X, and the classical bit is encoded as 1. By aggregating the results from these photons, Alice reconstructs the secret key K_A. Meanwhile, Bob, Charlie, and David each hold a share of the key, denoted as K_B, K_C, and K_D, respectively. This establishes the relationship $K_A = K_B \oplus K_C \oplus K_D$. When the agents wish to recover Alice's secret. For instance, determining the total unitary operation applied to the third photon, they must each reveal their respective secret shares, specifically U_3^B , U_3^C , U_3^D . Only by combining these operations can they successfully reconstruct the corresponding bit of Alice's secret.

We now analyze the photon efficiency η_e of our first proposed QSS protocol. Photon efficiency is defined as $\eta_e = \frac{q_u}{q_t}$, where q_u denotes the number of photons used for key generation, and q_t represents the total number of photons consumed throughout the protocol. Assume there are H participants in the protocol. The dealer initially prepares N single photons, of which M are in the Z basis and K are in the X basis, satisfying $N = M + K$. Out of the M photons in Z bases, the dealer uses $\frac{M}{2}$ photons for security checking. Additionally, each participant uses $\frac{K}{H}$ photons in X bases for basis comparison and eavesdropping detection. Given the above setup, the resulting photon efficiency η_e is calculated as follows: $\eta_e = \frac{M}{2HN-(H-1)K}$.

B. The Circular QSS Protocol Based on Reordering Single Photon Sequences

Step 1. Alice prepares a sequence of N single photons, consisting of M photons in the Z basis and K photons in the X basis, such that $N = M + K$, or simplicity, we denote the sequence of N photons as $S = (s_1, s_2, s_i \dots, s_n)$, where $1 \le i \le n$, and each s_i represents the quantum state of the i^{th} photon. After generating the photon sequence, Alice records the initial basis and quantum state of each photon. She then sends the sequence S to Bob via a quantum channel.

Step 2. Upon receipt of sequence S from Alice, Bob generates a corresponding set of N auxiliary photons, denoted as $S^{aux} = (s_1^{aux}, s_2^{aux}, s_i^{aux} \dots, s_n^{aux})$. He applies a SWAP gate operation to each pair consisting of a received photon and its corresponding auxiliary photon. After the SWAP operations, Bob proceeds with the protocol using the updated auxiliary sequence $S^{aux} = (s_1, s_2, s_i \dots, s_n)$.

Step 3. Bob reorders the photons in the sequence S^{aux} particles according to a randomly chosen permutation, which he records for future reference. The resulting sequence will be $S'^{aux} = \{s_1', s_2', s_i', \dots, s_n'\}$. He then applies a unitary operation $U_i^B \in \{I, X\}$ to each photon s_i' in S'^{aux}, resulting in a new photon sequence $S^{new} = (U_1^B s_1', \dots, U_n^B s_n')$. This modified sequence is then transmitted to Charlie via a quantum channel.

Step 4. Charlie and David independently repeat the procedures outlined in Steps 2 and Steps 3. After David completes his operations, he will send the photon sequence back to Alice via the quantum channel.

Step 5. Upon receiving the final photon sequence, Alice replicates the SWAP gate operations as in Step 2 to reconstruct a new auxiliary sequence, denoted as $S^{aux} = S'$. She requires all the agents to publish their individual messages of rearranging orders of all qubit in random order, so that the sequence may be restored to its original ordering. Based on the collective information from the agents, each participant can reconstruct the original photon positions and the corresponding sequence of unitary operations. Alice then proceeds to measure each photon, those initially prepared in the Z-basis are measured directly, while the remaining photons are measured in the X-basis.

Step 6. A subset of the Z-basis photons is designated for security verification. For these photons, Alice instructs all agents to disclose the specific unitary operations U_i^x applied during the protocol. She compares the expected outcomes with her actual measurement results. For the X-basis photons, Alice compares her measurement results with the initial quantum states. If the observed error rate remains below an acceptable threshold, the protocol proceeds; otherwise, it is aborted.

Step 7. Alice compares the measurement outcomes of the remaining Z-basis photons with their corresponding initial states. A matching outcome indicates that the collective unitary operation is equivalent to the identity I, and the associated classical bit is interpreted as 0. Conversely, if the outcome differs from the initial state, the overall transformation corresponds to a Pauli-X operation X, and the bit is interpreted as 1. Aggregating the outcomes yields Alice's secret key K_A. Meanwhile, Bob, Charlie, and David each hold a share of the key, denoted as K_B, K_C, and K_D, respectively. This establishes the relationship $K_A = K_B \oplus K_C \oplus K_D$. To reconstruct any specific bit of Alice's key, for instance, the unitary operations applied to the third photon—each agent must reveal their respective operations U_3^B, U_3^C, U_3^D. Only through the collaborative disclosure of all these elements can the corresponding bit of Alice's secret be successfully retrieved.

We proceed to evaluate the photon efficiency η_e of our second proposed QSS protocol. Assume there are H participants in the protocol. The dealer initially prepares N single photons, consisting of M photons in the Z basis and K photons in the X basis, satisfying $N = M + K$. Out of the M photons in Z bases, the dealer uses $\frac{M}{2}$ photons for security checking. Since each of these photons passes through all H participants, the total photon consumption is $(H+1)N$. Based on this configuration, the photon efficiency of the protocol is given by: $\eta_e = \frac{M}{2(H+1)N}$.

4 Security Analysis

The following section analyzes the security of the proposed QSS protocols. In the context of QSS protocols, four common types of attacks must be considered. External attackers may launch intercept-resend attacks, entanglement-measurement attacks, or Trojan horse attacks. In addition to these external threats, internal attackers may attempt collusion attacks by collaborating dishonestly to compromise the protocol.

A. Intercept-resend attack

In a circular QSS protocol, participants transmit secret information through quantum channels. An external attacker, commonly referred to as Eve, may attempt to eavesdrop on the secret information by intercepting photons traveling through these channels. The attack proceeds as follows: when Alice transmits photons to Bob, Eve intercepts the photons and performs measurements on them. To avoid detection, Eve then sends an equal number of replacement photons to Bob, prepared according to her measurement outcomes. A similar interception strategy may be applied to other quantum channels as well, such as the channel between Bob and Charlie.

In both of the proposed QSS protocols, several decoy photons randomly chosen from the set $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ are inserted into the photon sequence. Consequently, an eavesdropper, Eve, cannot determine the basis associated with each photon. Although Eve may still attempt to intercept and resend the photons, the probability of her correctly measuring the state of a single photon is $\frac{3}{4}$. Therefore, the probability that eavesdropping is detected through the security check is given by $1-\left(\frac{3}{4}\right)^n$, where n denotes the total number of decoy photons inserted into the sequence. It is obvious that as n becomes sufficiently large, the probability of detecting Eve approaches 1.

B. Entanglement-measurement attack

An external eavesdropper, Eve, may attempt to obtain secret information by employing an entanglement-measurement attack. The procedure is as follows. Suppose Eve intends to eavesdrop on a photon transmitted from Alice to Bob. Eve first prepares an auxiliary photon in the state $|E\rangle$. As the photon from Alice passes through, Eve entangles it with her auxiliary photon by performing a joint unitary operation U on the two-photon system. The resulting system state can be expressed as follows:

$$U|0\rangle|E\rangle = \alpha_0|0\rangle|E_0\rangle + \alpha_1|1\rangle|E_1\rangle \tag{1}$$

$$U|1\rangle|E\rangle = \beta_0|0\rangle|E_0'\rangle + \beta_1|1\rangle|E_1'\rangle \tag{2}$$

where $|\alpha_0|^2 + |\alpha_1|^2 = |\beta_0|^2 + |\beta_1|^2 = 1$. In order to avoid detection during the eavesdropping check, it is required that $\alpha_1 = \beta_0 = 1$. Then, we can use these requirements to get the following expressions:

$$U|+\rangle|E\rangle = \frac{1}{2}[|+\rangle(\alpha_0|E_0\rangle + \beta_1|E_1'\rangle) + \ |-\rangle(\alpha_0|E_0\rangle - \beta_1|E_1'\rangle)] \tag{3}$$

$$U|-\rangle|E\rangle = \frac{1}{2}[|+\rangle(\alpha_0|E_0\rangle - \beta_1|E_1'\rangle) + \ |-\rangle(\alpha_0|E_0\rangle + \beta_1|E_1'\rangle)] \tag{4}$$

Similarly, Eve will remain undetected if the following condition is satisfied, where $\alpha_0|E_0\rangle - \beta_1|E_1'\rangle = 0$ (i.e., $\alpha_0|E_0\rangle = \beta_1|E_1'\rangle$).

For Eve to avoid detection, all of the constraints derived from Equations (1) to (4) must be simultaneously satisfied. These conditions can be collectively summarized as follows:

$$U|0\rangle|E\rangle = \alpha_0|0\rangle|E_0\rangle \tag{5}$$

$$U|1\rangle|E\rangle = \beta_1|1\rangle|E_1'\rangle = \alpha_0|0\rangle|E_0\rangle \tag{6}$$

$$U|+\rangle|E\rangle = \frac{1}{2}|+\rangle(\alpha_0|E_0\rangle + \beta_1|E_1'\rangle) = \alpha_0|+\rangle|E_0\rangle \tag{7}$$

$$U|-\rangle|E\rangle = \frac{1}{2}|-\rangle(\alpha_0|E_0\rangle + \beta_1|E_1'\rangle) = \alpha_0|-\rangle|E_0\rangle \tag{8}$$

where Eve can only obtain information from $|E_0\rangle$. Therefore, Eve does not have sufficient information to distinguish the state of the photon which Alice transmit to Bob. The same applies to any pair of adjacent participants in the protocol.

C. Trojan horse attacks

In a Trojan horse attack, the eavesdropper, Eve, introduces her own photons into the quantum channel. For instance, during the transmission of secret information from Alice to Bob, Eve injects additional undetectable photons into the channel. This makes detection by Bob more difficult. After Bob applies his unitary operations, Eve retrieves her inserted photons and can thereby infer Bob's secret information.

To defend against this type of attack, all participants in both of our proposed QSS protocols employ SWAP gate operations. The probability that one of Eve's inserted photons is swapped with an auxiliary photon is $\frac{1}{2}$, and the probability that the swapped photon has the same state as Alice's original photon is $\frac{1}{2}$. Consequently, the probability of detecting Eve's presence is given by $1 - \left(\frac{3}{4}\right)^n$, where n denotes the total number of decoy photons within a sequence. As n increases, the detection probability approaches 1.

D. Collusion attack

It is possible that in a circular QSS protocol, multiple dishonest insiders may collaborate to launch a collusion attack. In the following context, we assume that Bob* and David* denote dishonest participants, where Bob* is the first agent in the sequence and David* is the last agent in the protocol. To illustrate the attack method, we consider a four-party scenario involving Alice, Bob*, Charlie, and David*.

Suppose Bob* and David* intend to acquire Charlie's information, thereby enabling them to reconstruct Alice's secret without Charlie's cooperation. The detailed procedure is as follows:

Initially, Bob* holds a photon sequence S consisting of n photons. Rather than forwarding S directly to Charlie as specified by the protocol, Bob* instead sends S to David*. In parallel, Bob* prepares a counterfeit photon sequence S' , also consisting of n photons randomly chosen from the set $\{|0\rangle,\ |1\rangle\}$ and transmits S' to Charlie.

Upon receiving S', Charlie follows the standard protocol procedures by applying his unitary operations to each photon and then sending the modified sequence to David*. After receiving S', David* collaborates with Bob* to determine the specific unitary operations that Charlie applied. To complete the attack, David* subsequently applies both Charlie's and his own prescribed unitary operations to the original photon sequence S(the one initially retained by Bob*) and then forwards it to Alice.

Through this process, Bob* and David* successfully obtain Alice's secret without requiring Charlie's participation, thereby compromising the security of the protocol.

In the first proposed QSS protocol, all agents are required to perform a security check during Step 3. When Charlie receives the photon sequence S', each photon has a probability of $\frac{1}{2}$ of being in the same state as its corresponding photon in the original sequence. Consequently, the probability that a collusion attack by dishonest agents is detected is given by $1-\left(\frac{1}{2}\right)^{n}$, where n denotes the number of photons selected for checking. It is evident that as n becomes sufficiently large, the probability of detecting such an attack approach 1.

In the second proposed QSS protocol, since all agents are required to reorder the photon sequence they received, it becomes infeasible for dishonest participants to infer the positions of Charlie's unitary operations. As a result, Bob* and David* are unable to recover Charlie's shadow information and reconstruct Alice's secret.

5 Performance Comparison

In Table 2, we conduct a comparative analysis between our proposed QSS protocol and several existing schemes, based on a set of key evaluation criteria. These include whether agents are required to generate photons, which can significantly impact implementation complexity. We also assess whether agents need the ability to apply quantum logic gates, and evaluate the average number of gates used per agent to estimate the operational overhead. Another important aspect is whether agents are required to perform photon measurements, as this affects the demands on quantum hardware. The types of quantum resources required is also evaluated, such as single photons or Bell states, since different photon types present different levels of experimental difficulty. Furthermore, we examine whether quantum memory is needed for storing photons during the protocol, which may limit feasibility in current technological contexts. We also analyze the security of each protocol against Trojan horse attacks, evaluating whether effective countermeasures are integrated into the design. Lastly, we determine whether the protocol is capable to distribute photons in long-distance scenario using practical methods.

Table 2: Comparison of different QSS protocols

	Deng et al.'s QSS [16]	Wang et al.'s QSS [17]	Gao's QSS [18]	Gao et al.'s QSS [19]	Ye et al.'s QSS [21]	Our 1st proposed QSS	Our 2nd proposed QSS
Photon generation by agents	✗	✗	✗	✓	✓	✓	✓
Use of quantum logic gates by agents	✓	✓	✓	✗	✗	✓	✓
Measurement capabilities required by agents	✓	✓	✓	✗	✗	✓	✗
Average number of quantum gates used per agent	1	1	2	0	0	2	2
Quantum resources	Single photon	Single photon	Bell States	Bell States	Single photon	Single photon	Single photon
Quantum memory	✗	✓	✗	✗	✗	✗	✗
Method for defending against Trojan horse attacks	PNS/Wavelength Filter	PNS/Wavelength Filter	PNS/Wavelength Filter	PNS/Wavelength Filter	PNS/Wavelength Filter	SWAP gates	SWAP gates
Suitability for long-distance transmission	✗	✗	✗	✗	✗	✓	✓

While our proposed QSS protocols require agents to both generate photons and perform quantum gate operations, they offer strong resilience against Trojan horse attacks through cost-effective measures, avoiding the higher hardware demands associated with methods such as photon number splitting (PNS) and wavelength filtering. Another advantage of our QSS protocols is being able to do long-distance distribution in a practical way. Since our protocol is designed to transmit photons using SWAP gates, we can make sure the photons in the protocol will maintain their energy throughout the procedures.

It is worth noting that a similar approach was proposed by Lin et al. [23] in 2013, which defends against Trojan horse attacks using CNOT gates and relies on generating multi-particle entangled states, such as GHZ states. While effective, these methods involve significantly higher costs due to the complexity of preparing and maintaining stable entanglement among multiple photons. In contrast, our protocol employs SWAP gates and operates with single-photon states, which are easier to generate and manipulate, offering a more practical and scalable solution.

6 Conclusion

This study proposed two novel multi-party QSS protocols leveraging SWAP gates to enhance both practicality and security. The first protocol is based on single photons and assumes agents with measurement capabilities, while the second relies on reordering single-photon sequences. Through rigorous security analysis, we demonstrated that both protocols resist common attacks. Notably, the integration of SWAP gates enables effective defense against Trojan horse attacks and helps maintain photon energy throughout the process, facilitating practical implementation. Compared to existing QSS schemes, our approach offers a more feasible pathway toward real-world deployment.

In future work, we plan to further improve the performance and resilience of our protocols. Key directions include enhancing photon efficiency and reducing the quantum capabilities required by agents, making the schemes more accessible in resource-limited quantum networks.

Acknowledgements

This work was partially supported by the National Science and Technology Council, Taiwan, R.O.C. (Grant Nos. NSTC 113-2221-E-005-086, NSTC 113-2622-H-005-001, and NSTC 113-2634-F-005-001-MBK).

References

[1] A. Shamir, “How to share a secret,” *Communications of the ACM*, vol. 22, no. 11, pp. 612-613, 1979.

[2] H. Krawczyk, “Secret sharing made short,” Annual International Cryptology Conference (CRYPTO’ 93), Springer Berlin Heidelberg, 1993, pp. 136-146.

[3] A. Beimel, “Secret-sharing schemes: a survey,” International Conference on Coding and Cryptology, Springer Berlin Heidelberg, pp. 11-46, 2011.

[4] E. F. Brickell, “Some ideal secret sharing schemes,” Workshop on the Theory and Application of of Cryptographic Techniques, Springer Berlin Heidelberg, pp. 468-475, 1989.

[5] G. J. Simmons, “Symmetric and asymmetric encryption,” *ACM Computing Surveys*, vol. 11, no. 4, pp. 305-330, 1979.

[6] G. S. Poh, J.-J. Chin, W.-C. Yau, K.-K. R. Choo, and M. S. Mohamad, “Searchable symmetric encryption: designs and challenges,” *ACM Computing Surveys*, vol. 50, no. 3, Article 40, 2017.

[7] M. Shand and J. Vuillemin, "Fast implementations of RSA cryptography," Proceedings of IEEE 11th Symposium on Computer Arithmetic, pp. 252-259, 1993.

[8] P. Carl, "Fast, rigorous factorization and discrete logarithm algorithms," Discrete Algorithms and Complexity, S. J. David, N.Takao, N. Akihiro and S. W. Herbert, eds., pp. 119-143: Academic Press, 1987.

[9] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM Review*, vol. 41, no. 2, pp. 303-332, 1999.

[10] A. K. Ekert, "Quantum cryptography based on Bell's theorem," *Physical Review Letters*, vol. 67, no. 6, pp. 661-663, August 5, 1991.

[11] C. Bennett, and G. Brassard, "Quantum cryptography: public key distribution and coin tossing," Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing. pp. 175-179, 1984.

[12] C. H. Bennett, "Quantum cryptography using any two nonorthogonal states," *Physical Review Letters*, vol. 68, no. 21, pp. 3121-3124, May 25, 1992.

[13] M. Hillery, V. Bužek, and A. Berthiaume, "Quantum secret sharing," *Physical Review A*, vol. 59, no. 3, pp. 1829-1834, March 1, 1999.

[14] J. D. Bekenstein and M. Schiffer, "Quantum limitations on the storage and transmission of information," *International Journal of Modern Physics C*, vol. 01, no. 04, pp. 355-422, 1990.

[15] S. Pirandola, J. Eisert, C. Weedbrook, A. Furusawa, and S. L. Braunstein, "Advances in quantum teleportation," *Nature Photonics*, vol. 9, no. 10, pp. 641-652, October 1, 2015.

[16] F.-G. Deng, H.-Y. Zhou, and G. L. Long, "Circular quantum secret sharing," *Journal of Physics A: Mathematical and General*, vol. 39, no. 45, pp. 14089, October 24, 2006.

[17] T.-Y. Wang, Q.-Y. Wen, X.-B. Chen, F.-Z. Guo, and F.-C. Zhu, "An efficient and secure multiparty quantum secret sharing scheme based on single photons," Optics Communications, vol. 281, no. 24, pp. 6130-6134, December 15, 2008.

[18] G. Gao, "Secure multiparty quantum secret sharing with the collective eavesdropping-check character," *Quantum Information Processing*, vol. 12, no. 1, pp. 55-68, January 1, 2013.

[19] G. Gao, Y. Wang, and D. Wang, "Multiparty semiquantum secret sharing based on rearranging orders of qubits," *Modern Physics Letters B*, vol. 30, no. 10, 1650130, April 20, 2016.

[20] C. Xie, L. Li, and D. Qiu, "A novel semi-quantum secret sharing scheme of specific bits," *International Journal of Theoretical Physics*, vol. 54, October 1, 2015.

[21] C.-Q. Ye, and T.-Y. Ye, "Circular semi-quantum secret sharing using single particles," *Communications in Theoretical Physics*, vol. 70, no. 6, pp. 661, December 1, 2018.

[22] S. Wang, B. Liu, W. Huang, B. Xu, and Y. Li, "Memory-free quantum secret sharing protocol with collective detection," *Quantum Information Processing*, vol. 22, no. 5, pp. 181, April 28, 2023.

[23] J. Lin, and T. Hwang, "New circular quantum secret sharing for remote agents," *Quantum Information Processing*, vol. 12, no. 1, pp. 685-697, January 1, 2013.

[24] F.-G. Deng, X.-H. Li, H.-Y. Zhou, and Z.-J. Zhang, "Improving the security of multiparty quantum secret sharing against Trojan horse attack," *Physical Review A*, vol. 72, no. 4, pp. 044302, October 18, 2005.

[25] Q.-Y. Cai, "Eavesdropping on the two-way quantum communication protocols with invisible photons," *Physics Letters A*, vol. 351, no. 1, pp. 23-25, February 20, 2006.

[26] M. Fiorentino, T. Kim, and F. N. C. Wong, "Single-photon two-qubit SWAP gate for entanglement manipulation," *Physical Review A*, vol. 72, no. 1, pp. 012318, July 15, 2005.

[27] C. M. Wilmott, and P. R. Wild, "On a generalized quantum SWAP gate," *International Journal of Quantum Information*, vol. 10, no. 03, pp. 1250034, 2012.