Enhanced SIFT Operations in Mediated Semi-Quantum Key Distribution: Protocol Design and Simulation

Arowolo Praise O.[a], Yuan Tian[a,*1], *GenqingBian*[a], Jian Li[b]

[a] *College of Information and Control Engineering Xi'an University of Architecture and Technology Xi'an 710055 Shaanxi China*
[b] *School of Cyberspace Security Beijing University of Post and Telecommunications Beijing 100086 China*

Abstract

Quantum cryptography promises secure communication, yet fully quantum protocols face significant implementation challenges. Mediated Semi-Quantum Key Distribution (MSQKD) protocols addresses this by allowing classical users with limited quantum abilities to establish secure keys with assistance from an untrusted quantum server. This paper presents an efficient MSQKD protocol using single photons, achieving enhanced practicality and security. By incorporating SIFT and CTRL operations (where classical users discard, replace, and reflect qubits without disturbance) the protocol strengthens security and reduces the quantum overhead on the third party (TP), achieving a qubit efficiency of 1/12. Advanced security mechanisms, including decoy state testing and quantum channel testing, further safeguard communication. A noise model is introduced to assess robustness under real-world conditions, with IBM's Qiskit simulations confirming the protocol's resilience against various attacks. This work provides a promising, practical solution for secure quantum communication in realistic scenarios.

Keywords: quantum cryptography, quantum key distribution, mediated semi-quantum protocol, qubit efficiency

1. Introduction

Quantum technologies have transformed secure communication, promising cryptographic systems that are theoretically unbreakable. Quantum cryp-

[1] Email: tinyuen@xauat.edu.cn

tography, leveraging the principles of quantum mechanics, offers a paradigm shift from classical cryptographic methods which was proposed by by Bennett and Brassard (1). At the forefront of this quantum revolution stands Quantum Key Distribution (QKD), a pioneering technology designed to secure communication channels against both classical and quantum adversaries.

Quantum cryptography is the art and science of exploiting quantum mechanical effects in order to perform cryptographic tasks. While the most well-known example of this discipline is QKD, there exist many other applications such as quantum money, randomness generation, secure two- and multi-party computation and delegated quantum computation (2). Traditional QKD protocols, while secure, pose significant implementation challenges due to their reliance on complex quantum operations and entangled states. Mediated Semi-Quantum Key Distribution (MSQKD) protocols mitigate these challenges by involving an untrusted TP to assist classical users with limited quantum capabilities.

Semi-quantum key distribution was introduced because it provides a more feasible and efficient approach for secure communication, leveraging quantum principles while mitigating some of the challenges associated with fully quantum systems. The SQKD protocol allows a "classical" participant with limited quantum capability to share a secret key securely with a trusted quantum participant. A "classical" participant means one can only perform some of the following four operations: (1) Preparing qubits in the basis $\{|0\rangle, |1\rangle\}$. (2) Measuring qubits in the basis $\{|0\rangle, |1\rangle\}$.(3) Reflecting qubits without disturbance. (4) Reordering the qubits.

Many other semi-quantum protocols have also been presented, such as SQKD(3; 4; 5; 6; 7; 8; 9; 10), semi-quantum communications(11; 12), semi-quantum secret sharing protocols (SQSS)(13; 14),semi-quantum key agreement(SQKA) (15; 16), semi-quantum identity authentication (SQIA) (17; 18; 19) and semi-quantum private comparisons (SQPC)(20; 21; 22; 23). This hybrid solution allows for the integration of quantum-resistant classical algorithms, making it more adaptable to existing infrastructure and paving the way for widespread adoption of quantum-secure communication protocols.

MSQKD protocols offer a middle ground by reducing the quantum requirements for end users. In MSQKD protocols, two limited-quantum users, Alice and Bob, establish a shared key with the help of an untrusted quantum third party, TP. The users have some limited quantum capabilities, while TP possesses full quantum powers.

The first MSQKD protocol was proposed by Krawec in 2015 (6), utilizing bell basis generated by TP. Classical users could only measure incoming qubits in the Z-basis or reflect them. This protocol had a qubit efficiency of 1/24. The key aspect of this protocol is that classical users do not require quantum memory or any sophisticated quantum operations. While the efficiency was low, Kravec's protocol paved the way for mediated protocols that require limited quantum capabilities from end users.

In 2018, Liu et al. (7) proposed an improved mediated semi-quantum key distribution protocol using bell states generated by TP. In this protocol, TP generates entanglement qubit pairs in one of the four Bell states and sends one qubit from each pair to both Alice and Bob. Upon receiving the qubits, Alice and Bob independently and randomly choose to either measure the qubit in the Z basis and send the result back to TP, or reflect the qubit back to TP without measurement. TP performs Bell measurements on the received particles to get measurement results, which can be used later by the classical participants to share a session key, detect eavesdroppers, or detect malicious action of the TP A key advantage of this protocol is the increased qubit efficiency of 1/8 compared to Krawec's protocol (6). By using this method, Liu et al.'s protocol(7) reduced the quantum resource overhead for the third party.

During 2019, Lin et al. (24) proposed another mediated semi-quantum key distribution protocol using single photons generated by the TP. In this protocol, TP prepares single photon qubits in the X basis and transmits them to the classical participants. Upon receiving the photons, the classical participants independently and randomly choose to perform either the SIFT operation (measure and resend the qubit in the Z basis) or the CTRL operation (reflect the received photon without tampering) before sending it back to TP. After receiving the qubits from the classical participants, TP performs a Bell state measurement and announces the results. The classical participants perform the necessary processes to check for TP's honesty or that of any eavesdropper. Lin et al.'s protocol reduced the quantum operation requirements for classical users while also reducing the burden of TP in generating bell states. Compared to prior protocols, it relied on single-photon generation by TP. The qubit efficiency was comparable to Liu et al.'s(7) protocol at 1/24.

Despite advancements, existing MSQKD protocols still face practical and security limitations. For instance, Krawec's protocol (2015) and Liu et al.'s protocol (2018) rely on Bell states, increasing the quantum overhead for the TP and limiting efficiency. Lin et al.'s protocol (2019) improved practicality by using single photons but did not address certain security vulnerabilities comprehensively. Recent advancements in semi-quantum key distribution, such as Mediated Semi-Quantum Key Distribution with Improved Efficiency by Guskind and Krawec (2022)(10) and An Efficient Semi-Quantum Key Distribution Protocol and Its Security Proof Ye et al. (2022)(25), have focused on improving qubit efficiency and security for semi-quantum protocols. While Guskind and Krawec's protocol achieves high efficiency, it sacrifices noise tolerance, limiting its robustness in practical applications. Similarly, Ye et al. propose an efficient SQKD protocol that balances quantum resource requirements with noise considerations but lacks certain security features like our integrated decoy state testing and quantum channel testing. This paper builds on these advancements by introducing a protocol that optimizes qubit efficiency while maintaining noise resilience and robust security mechanisms, making it a more practical solution for secure communication. Table 4 further details specific comparisons in efficiency, noise tolerance, and security mechanisms between our protocol and recent advancements like those by Guskind and Krawec (2022) and Ye et al. (2022)

The mediated semi-quantum protocol proposed in this paper draws on these existing protocols(6; 24; 7; 26). The motivation for this study is to bridge these gaps by designing a more efficient MSQKD protocol that reduces quantum resource demands on the TP and increases security through novel mechanisms like SIFT operations, decoy state testing, and quantum channel testing. We use single photons instead of entangled Bell states, significantly enhancing qubit efficiency to 1/12 (double that of previous protocols) while reducing quantum overhead for the third party (TP). The protocol incorporates advanced security mechanisms, including SIFT operations, decoy state testing, and quantum channel testing, to reinforce security. These mechanisms allow classical users to discard and replace qubits and verify a portion of the Bell measurement results, ensuring honesty from the TP and strengthening the protocol's robustness against various attacks. To further enhance its practical applicability, a noise model is included to assess performance under real-world conditions, demonstrating resilience against practical challenges. Finally, comprehensive security analysis, supported by experimental simulations using IBM's Qiskit framework, confirms the protocol's feasibility, operational accuracy, and effectiveness in secure quantum communication environments.

The remainder of this paper is organized as follows: Section 2 describes the proposed protocol in detail and gives an illustrative example of the protocol in action. Section 3 presents the security analyses. Section 4 shows the simulation results and the implementation of the noise model and how it affects the protocol compared to Lin's protocol (24). Section 5 offers a comparison and discussion of the proposed protocol with existing protocols. Finally, Section 6 concludes the paper and outlines future research directions.

2. The Proposed Protocol

Inspired by Lin et al. (24) protocol which was proposed in 2019, this section outlines our proposed MSQKD approach. We assume that the quantum channels connecting TP with Alice and Bob are ideal, meaning they are free from loss and noise. Additionally, we consider the classical channel between Alice and Bob to be secure, allowing data to be viewed but not altered. The TP, however, is considered untrusted and capable of any attack to compromise the key distribution.

The creation of a new MSQKD protocol is motivated by the need to address the practical and security challenges present in existing protocols. Many current protocols depend on complex quantum operations or entangled states, making them difficult to implement in practical scenarios. Our goal is to develop a more feasible and secure MSQKD protocol by leveraging single photons and incorporating sophisticated security features.

Before explaining the protocol steps, we will review some background information essential for its comprehension. Firstly, the Bell states (27) can be represented as follows:

$$\begin{aligned}
|\phi^+\rangle &= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = \frac{1}{\sqrt{2}}(|++\rangle + |--\rangle),\\
|\phi^-\rangle &= \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) = \frac{1}{\sqrt{2}}(|+-\rangle + |-+\rangle),\\
|\psi^+\rangle &= \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) = \frac{1}{\sqrt{2}}(|++\rangle - |--\rangle),\\
|\psi^-\rangle &= \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) = \frac{1}{\sqrt{2}}(|-+\rangle - |+-\rangle)
\end{aligned} \tag{1}$$

The set $\{|0\rangle, |1\rangle\}$ represents qubits in the Z basis, and the set $\{|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\}$ denotes qubits in the X basis.

According to Equation (1), if we perform a Bell measurement on two qubits on a Z basis, then the measurement result can be predicted as follows:

$$
\begin{aligned}
|00\rangle &= \frac{1}{\sqrt{2}}(|\phi^+\rangle + |\phi^-\rangle),\\
|01\rangle &= \frac{1}{\sqrt{2}}(|\psi^+\rangle + |\psi^-\rangle),\\
|10\rangle &= \frac{1}{\sqrt{2}}(|\psi^+\rangle - |\psi^-\rangle),\\
|11\rangle &= \frac{1}{\sqrt{2}}(|\phi^+\rangle - |\phi^-\rangle).
\end{aligned} \tag{2}
$$

By Equation (2), if we perform a Bell measurement on the state $|00\rangle$, for example, we will obtain either $|\phi^+\rangle$ or $|\phi^-\rangle$. If another measurement result is obtained, it implies that the original state $|00\rangle$ could have been disturbed by eavesdroppers, or the measurement could be a forged one. These possibilities will be used to check for eavesdropping attacks as well as to verify the honesty of the TP in the proposed Semi-Quantum Key Distribution (SQKD) protocol. The steps of the proposed SQKD protocol are described as follows:

Step 1: TP generates 2N single photons and sends the sequence N of single photons to Alice and Bob respectively. These photons are prepared in the X-basis as $|+\rangle$. The states are defined as $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, facilitating the initialization phase of the quantum communication.

Step 2: Alice and Bob receive the photons and independently decide the operation to perform on each photon (CTRL or SIFT) and log these positions with the initial positions. In the CTRL operation, the photon is reflected back to TP without any disturbance. In the SIFT operation, a photon is discarded and replaced with a new photon in the Z-basis, which is sent back to TP. The choice can be random or predetermined based on the security needs.

Step 3: For photons undergoing the SIFT Operation, enhancements include Decoy state testing, where some SIFT qubits are prepared as decoy states, known only to Alice and Bob, to test for eavesdropping and ensure TP's honesty in handling and measurement. Additionally, Quantum channel testing uses qubits to test the integrity of the quantum channel by sending test states that help detect interference or alterations. After deciding on the operation (CTRL or SIFT), before sending the photons back to TP, Alice and Bob reorders the sequence of qubits and updates the new positions with their respective operations. This can be done randomly or based on a predetermined algorithm that both Alice and Bob share.

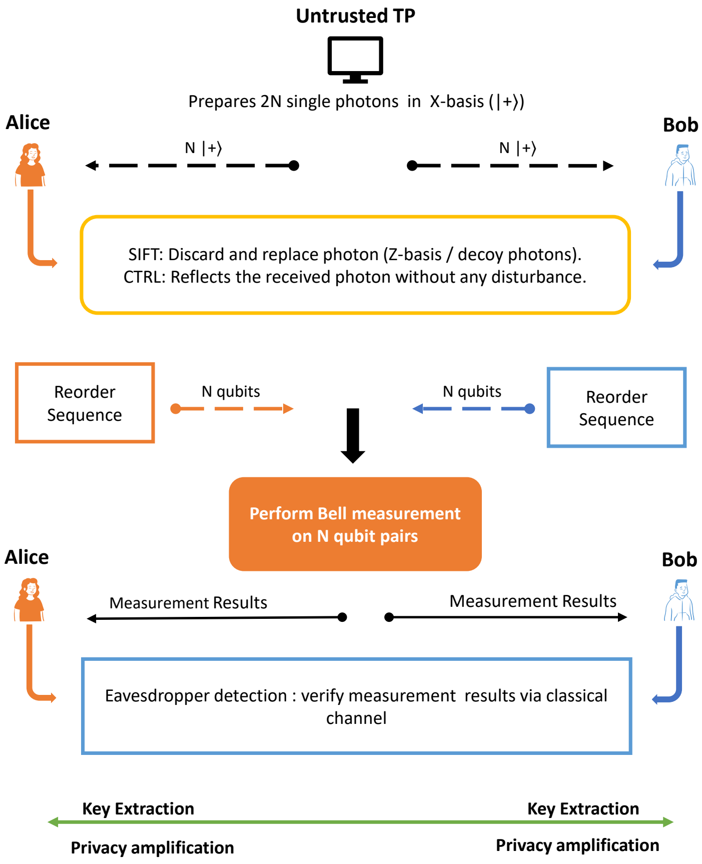

Untrusted TP
Prepares 2N single photons in X-basis (|+⟩)
Alice
Bob
N |+⟩
N |+⟩
SIFT: Discard and replace photon (Z-basis / decoy photons).
CTRL: Reflects the received photon without any disturbance.
Reorder Sequence
N qubits
N qubits
Reorder Sequence
Perform Bell measurement on N qubit pairs
Alice
Bob
Measurement Results
Measurement Results
Eavesdropper detection : verify measurement results via classical channel
Key Extraction
Key Extraction
Privacy amplification
Privacy amplification

Figure 1: Proposed Mediated SQKD Protocol

Step 4: TP receives the qubits back from Alice and Bob unaware of the new sequence order. A Bell state measurement is performed on each pair of returned qubits. Subsequently, TP announces the results of these measurements to both Alice and Bob.

Step 5: Using an authenticated classical channel, Alice and Bob disclose the type of operation (CTRL or SIFT) performed and positions on each qubit without revealing the specific states used in CTRL operations. They verify TP's announced results based on the expected outcomes for both CTRL and SIFT operations, checking for consistency and integrity. Alice and Bob discuss the correctness of the bell measurement result provided by TP as explained in the table 1 below.

Step 6: Alice and Bob extract the raw key from the sequences where both have performed the SIFT operation. This operation is crucial because it involves measuring the photon's state and then sending a corresponding state back to TP. Below is the process by which the raw key bits are formed:

- If Alice measures $|0\rangle$ and sends a photon in state $|0\rangle$ and Bob does the same, any resultant Bell state $|\phi^+\rangle$ or $|\phi^-\rangle$ from TP's measurement confirms their measurements, and $|0\rangle$ is used as the raw key bit.

- Similarly, if Alice measures $|1\rangle$ and sends a photon in state $|1\rangle$ and Bob does the same, resulting in Bell states $|\phi^+\rangle$ or $|\phi^-\rangle$, $|1\rangle$ is used as the raw key bit.

The bit values $|0\rangle$ or $|1\rangle$ measured and sent by Alice and Bob become part of the raw key if the announced results match the expected Bell states.

Step 7: Alice and Bob perform error correction to reconcile any discrepancies in their raw key bits. Privacy amplification techniques are employed to distill a secure final key from the raw key, minimizing any potential leakage of key information to TP or eavesdroppers.

The protocol includes continuous verification mechanisms during and after key distribution to ensure the ongoing security and integrity of the quantum channel. Regular audits and updates to the protocol's security measures are recommended to adapt to new quantum threats and advancements in quantum computing.

Table 1: Expected Bell Measurement Results Based on Alice and Bob's Operations and its Usage

Alice Operation	**Bob Operation**	**Expected Bell Measurement Result**	**Explanation**	**Usage**
SIFT ($\vert 0\rangle$)	SIFT ($\vert 0\rangle$)	$\vert\phi^+\rangle$ or $\vert\phi^-\rangle$	As shown in equation (2)	Key derivation
SIFT ($\vert 0\rangle$)	SIFT ($\vert 1\rangle$)	$\vert\psi^+\rangle$ or $\vert\psi^-\rangle$	As shown in equation (2)	Key derivation
SIFT ($\vert 1\rangle$)	SIFT ($\vert 0\rangle$)	$\vert\psi^+\rangle$ or $\vert\psi^-\rangle$	As shown in equation (2)	Key derivation
SIFT ($\vert 1\rangle$)	SIFT ($\vert 1\rangle$)	$\vert\phi^+\rangle$ or $\vert\phi^-\rangle$	As shown in equation (2)	Key derivation
CTRL	CTRL	$\vert\phi^+\rangle$ or $\vert\psi^+\rangle$	Since both photons were reflected without any disturbance	To detect eavesdropping or dishonest TP
CTRL	SIFT (any)	Any result (random)	Bob's random replacement influences the measurement unpredictably, regardless of Alice's CTRL operation.	None
SIFT (any)	CTRL	Any result (random)	Similar to the previous row, Alice's random replacement results in any possible Bell state.	None

2.1. Example

In the previous section, we summarized the fundamental steps of the proposed mediated semi-quantum key distribution protocol. Although this overview provides a general understanding, a detailed example can further enhance clarity by offering a concrete insights into the complexities of quantum processes.

First, The TP prepares a sequence of 10 single photons in the X-basis, specifically in the states The states are defined as $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ The TP sends these photons one by one to Alice and Bob through secure quantum channels. Upon receiving a photon, Alice and Bob independently choose between two operations: the CTRL operation and the SIFT operation.

SIFT Operation: Alice (or Bob) discards the received photon and replaces it with a new qubit prepared in the Z-basis. This new qubit is then sent back to the TP. Some qubits are replaced with decoy qubits, whose states are predetermined and known to Alice and Bob.

CTRL Operation: Alice (or Bob) reflects the received qubit without any disturbance back to the TP.

After the operations are performed, the sequence of qubits are reordered; only Alice and Bob know the right order with the respective operations performed on the qubits. For this example, we use the scenarios shown in Table 2 below:

The TP receives the qubit sequence sent back by Alice and Bob and performs a Bell state measurement on each pair of photons as shown in table 2. The TP then announces the measurement results to Alice and Bob. Alice and Bob use an authenticated classical channel to disclose the types of operations (CTRL or SIFT) they performed on each photon without revealing the specific qubits generated in the SIFT operations. They verify the TP's announced results based on the expected outcomes for both CTRL and SIFT operations, checking for consistency and integrity. As shown in table 3

Alice and Bob extract the raw key from the sequences where they both performed the SIFT operation. In our example, photons 1 and 4 can be used for this purpose. The decoy photons were used in the protocol, These decoy photons have known states that Alice and Bob can compare against the TP's announced results. If the TP's results do not match the expected outcomes for these decoy states, it indicates potential tampering or eavesdropping.

At position 7 , where both CTRL operations were performed (reflected without any measurement), Alice and Bob would detect dishonesty or an attack if the bell measurement result provided by TP doesn't match the required result as specified in equation 2. Alice and Bob perform error correction to reconcile any discrepancies in their raw key bits. Privacy amplification techniques are then employed to distill a secure final key from the raw key, minimizing any potential leakage of key information to the TP or eavesdroppers.

Through this example, we demonstrate how the proposed MSQKD protocol enables Alice and Bob to securely establish a shared key with the assistance of the TP, while ensuring the integrity and confidentiality of the communication through various verification and security mechanisms.

Table 2: Scenario of Alice and Bob's Operations

Photon	**TP to Alice**	**TP to Bob**	**Alice's Operation**	**Bob's Operation**
1	$\|+\rangle$	$\|+\rangle$	SIFT, replaces with decoy $\|0\rangle$, sends to TP	SIFT, replaces with decoy $\|0\rangle$, sends to TP
2	$\|+\rangle$	$\|+\rangle$	CTRL, reflects $\|+\rangle$	SIFT, sends $\|1\rangle$
3	$\|+\rangle$	$\|+\rangle$	SIFT, replaces with decoy $\|1\rangle$, sends to TP	CTRL, reflects $\|+\rangle$
4	$\|+\rangle$	$\|+\rangle$	SIFT, sends $\|0\rangle$	SIFT, sends $\|0\rangle$
5	$\|+\rangle$	$\|+\rangle$	CTRL, reflects $\|+\rangle$	SIFT, sends $\|1\rangle$
6	$\|+\rangle$	$\|+\rangle$	SIFT, replaces with decoy $\|0\rangle$, sends to TP	CTRL, reflects $\|+\rangle$
7	$\|+\rangle$	$\|+\rangle$	CTRL, reflects $\|+\rangle$	CTRL, reflects $\|+\rangle$
8	$\|+\rangle$	$\|+\rangle$	SIFT, sends $\|0\rangle$	SIFT, sends $\|0\rangle$
9	$\|+\rangle$	$\|+\rangle$	CTRL, reflects $\|+\rangle$	SIFT, sends $\|1\rangle$
10	$\|+\rangle$	$\|+\rangle$	SIFT, sends $\|1\rangle$	CTRL, reflects $\|+\rangle$

Table 3: Verification of Alice and Bob's Operations

Photon	**Alice's Operation**	**Bob's Operation**	**Verification**
1	SIFT with decoy $\|0\rangle$	SIFT with decoy $\|0\rangle$	TP announces a random Bell state result. Verified against known decoy states. If the result does not match the expected outcome, TP is dishonest or eavesdropping is detected.
2	CTRL	SIFT($\|1\rangle$)	TP announces a random Bell state result. Verified as consistent since Bob's SIFT operation randomizes the outcome.
4	SIFT	SIFT	TP announces a random Bell state result. Verified as consistent since both did CTRL operations.
7	CTRL	CTRL	TP should announce $\|\phi^+\rangle$ or $\|\psi^+\rangle$. TP announces $\|\phi^-\rangle$. Inconsistent: The result does not match the expected Bell state ($\|\phi^+\rangle$ or $\|\psi^+\rangle$), indicating possible tampering or eavesdropping.

3. Security Analyses

The security of the proposed protocol is analyzed in this section. We delve into a comprehensive examination of the security measures incorporated within the protocol, aiming to assess its resilience against potential adversarial scenarios.

In this security analysis, we make the following assumptions: (i)It is assumed that the quantum channels between TP and the participants (Alice and Bob) are perfect, meaning they are non-lossy and noiseless. (ii)The classical channel between Alice and Bob is assumed to be authenticated, ensuring that any data exchanged cannot be tampered with, although it can be viewed by an eavesdropper. (iii)The TP is not trusted and is assumed to be potentially dishonest, capable of attempting any kind of attack to compromise the distributed key. However, Alice and Bob are honest and follow the protocol correctly. (iv)The quantum devices used by Alice, Bob, and TP are assumed to operate perfectly without any implementation flaws or errors. This includes the preparation and measurement of qubits.

3.1. Intercept-Resend Attack

An intercept-resend attack involves an eavesdropper, Eve intercepting qubits sent from the TP to Alice and Bob and then resending new qubits to the respective parties. The goal is to extract information about the key without it being detected. When Eve intercepts and resends new qubits to Alice and Bob, she might send qubits on either an X or Z basis.

The detection for this attack by Eve before or after the operations by the classical participants can be determined. for positions where both classical participants performed CTRL operations, Eve could go undetected if the qubit she sent was $|+\rangle$, any other value of qubit sent would bring inconsistencies, as explained in table 3, Alice and Bob have $\frac{1}{2} * \frac{1}{2}$ chance of selecting CTRL , since Eve might send qubits on either an X or Z basis, Since Eve might send qubits on either an X or Z basis, Eve has a $\frac{1}{2} * \frac{1}{2} * \frac{1}{2} = \frac{1}{8}$ chance of remaining undetected if she sends the $|+\rangle$ state. Thus, the probability of detecting Eve's intercept-resend attack under these conditions is $1 - \left(\frac{7}{8}\right)^N$, with a large N the detection probability would be close to 1.

Also at position where both participants perform SIFT operations , Alice or Bob discards the intercepted qubit and replaces it with a new qubit in the Z-basis ($|0\rangle$ or $|1\rangle$). Eve's sent qubit is irrelevant in this case, as it is discarded. The decoy qubits and the reordering of the qubits after performing their operations further reduce any eavesdropper's ability to correlate the intercepted and resent qubits with the final measurement results, making our protocol safe from this attack.

3.2. Measure-Resend Attack

The measure-resend attack is a common eavesdropping strategy in quantum key distribution (QKD) protocols. In this attack, an adversary (often called Eve) intercepts the qubits sent by the sender (TP), measures them, and then sends new qubits to the receivers (Alice and Bob) based on the measurement results.

Assuming Eve measures each intercepted qubit on a chosen basis (e.g., Z-basis or X-basis), she then resends the qubits to Alice and Bob based on her measurement results, hoping to pass undetected and gain information about the operations performed. Alice and Bob receive the qubits and proceed with their respective operations (CTRL or SIFT), followed by incorporating decoy qubits. Eve has intercepted the original qubits, measured them, and resent them. The protocol's use of random CTRL and SIFT operations and subsequent reordering of qubits add significant uncertainty for Eve. Eve cannot predict or replicate the operations performed by Alice and Bob. This randomization ensures that even if Eve successfully measures and sends the qubits to Alice and Bob, she can not gain any information because Alice and Bob perform SIFT operations, which discard and replace the qubit. Eve has no idea about this. Also, the random reordering known to only the classical participant would make it harder for Eve to keep track of the qubits measured earlier. For a qubit, there is a $\frac{1}{2}$ chance of selecting SIFT operations in step 2, which means the qubit is displaced and replaced with a new qubit. This means Eve has a $\frac{1}{2}$ chance of getting the right measurement result. Therefore , the combined probability of Eve measuring the qubit correctly and sending a correct qubit to Alice or Bob is $\frac{1}{2} * \frac{1}{2} = \frac{1}{4}$. Given that Alice and Bob use random CTRL and SIFT operations and reordering, the overall probability that Eve remains undetected after intercepting and resending qubits across N instances is $\left(\frac{3}{4}\right)^N$. As N increases, the probability of detecting Eve approaches 1. This ensures that the measure-resend attack has a high probability of being detected, thus preserving the security of the MSQKD protocol.

3.3. Double-CNOT Attack

In this section, we examine the Double-CNOT attack, where the TP (Third Party) attempts to uncover the secret key by performing CNOT operations. The attack is structured as follows:

TP initially performs a CNOT operation, using the particles sent to the participants in Step 1 as control bits and TP's ancillary particles as target bits:

$$U_{\text{CNOT}} = |00\rangle\langle 00| + |01\rangle\langle 01| + |11\rangle\langle 10| + |10\rangle\langle 11|$$

Subsequently, TP conducts a second CNOT operation with the particles sent from the participants in Step 2 as control bits and TP's ancillary particles again as target bits. The goal is to extract Alice's and Bob's operations from the ancillary particles, thereby obtaining the secret key undetected. If TP succeeds in identifying Alice's and Bob's operations in Step 2, they can measure the qubits in the Z basis (used earlier by Alice and Bob) and falsify Bell measurement results using Equation (2) to deceive Alice and Bob. If unsuccessful, TP resorts to Bell measurements on the remaining qubit pairs.

However, this attack is ineffective due to the protocol's design, which prevents TP from deducing Alice's or Bob's operations in Step 2 from the ancillary particles. Let's explore two different scenarios:

Example 1:

Assume TP starts with a particle $|+\rangle$ intended for Alice and an ancillary particle $|0\rangle$. TP performs the initial CNOT operation in Step 1, resulting in the following state:

$$U_{\text{CNOT}}|+\rangle_A|0\rangle_T = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{AT} = |\phi^+\rangle_{AT}$$

Here, A represents the particle intended for Alice, and T represents TP's ancillary qubit. After Alice's operation and TP's second CNOT operation in Step 2, the possible outcomes are:

- If Alice measures and resends $|0\rangle$:

$$U_{\text{CNOT}}|0\rangle_A|0\rangle_T = |0\rangle_A|0\rangle_T$$

- If Alice measures and resends $|1\rangle$:

$$U_{\text{CNOT}}|1\rangle_A|1\rangle_T = |1\rangle_A|0\rangle_T$$

- If Alice reflects the state:

$$U_{\text{CNOT}}\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{AT} = |+\rangle_{AT}$$

Example 2:

Suppose TP uses a particle $|0\rangle$ intended for Bob and an ancillary particle $|+\rangle$. TP performs the first CNOT operation in Step 1, yielding:

$$U_{\text{CNOT}}|0\rangle_B|+\rangle_T = \frac{1}{\sqrt{2}}(|00\rangle + |01\rangle)_{BT}$$

Here, B represents the particle for Bob, and T represents TP's ancillary qubit. After Bob's operation and TP's second CNOT operation in Step 2, the potential outcomes include:

- If Bob measures and resends $|0\rangle$:

$$U_{\text{CNOT}}|0\rangle_B|0\rangle_T = |0\rangle_B|0\rangle_T$$

- If Bob measures and resends $|1\rangle$:

$$U_{\text{CNOT}}|1\rangle_B|1\rangle_T = |1\rangle_B|1\rangle_T$$

- If Bob reflects the state:

$$U_{\text{CNOT}}\frac{1}{\sqrt{2}}(|00\rangle + |01\rangle)_{BT} = |0\rangle_{BT}$$

Alice and Bob integrate decoy states, known exclusively to them, into their transmission to detect eavesdropping and ensure TP's honesty. Should TP attempt a Double-CNOT attack, the decoy states will not produce the anticipated Bell state measurements, exposing the attack.

By randomly discarding and replacing qubits, the protocol ensures that TP cannot consistently correlate the control and target bits correctly, thereby subjecting the Double-CNOT attack useless against this protocol.

3.4. Dishonest TP Attack

In this section, we analyze the security of the proposed MSQKD protocol against a dishonest TP. A dishonest TP may attempt to compromise the security of the key distribution by either tampering with the qubits or manipulating the measurement results.

TP may alter the states of the qubits sent to Alice and Bob in an attempt to gain information about the key or introduce errors that would compromise the integrity of the key. When TP sends tampered qubits to Alice and Bob, the decoy states introduced in step 3 will help detect this. Alice and Bob will compare the measurement results for the decoy states against the expected results in step 5. Any inconsistency will reveal that TP has tampered with the qubits.

Secondly, TP may announce false Bell state measurement results to Alice and Bob, intending to mislead them about the correct states of the qubits and thus compromise the key. If TP manipulates the measurement results, the verification process through the classical channel will detect this. Alice and Bob will disclose their operations (CTRL or SIFT) and compare the announced results from TP. Since the operations and qubit positions are known only to Alice and Bob, any false announcement by TP will be detected.

The probability of detecting a dishonest TP is high due to the combined use of decoy states, random reordering, and classical verification. Even if TP attempts to manipulate the results or tamper with the qubits, these mechanisms ensure that any discrepancies will be identified,, Hence our protocol safe from these kinds of attack

4. Protocol Simulation with Qiskit

In this section , we conduct an experimental simulation of the proposed MSQKD protocol using IBM's Qiskit, aimed at demonstrating it's feasibility and correctness and how the protocol is supposed to work. to simplify the presentation , we will disregard any potential eavesdropping or attacks in the subsequent procedures.

During the simulation TP produced 5 single photons at random each to both Alice and Bob, We utilize Qiskit to construct quantum circuits simulating various MSQKD protocol steps. First, we initialize quantum registers, where each register represents a qubit. By applying Hadamard and X gates initially to produce the $|+\rangle$ and $|-\rangle$ states. Next, TP performs a Bell state measurement using CNOT and Hadamard gates and measures the qubits in the Z-basis. The quantum circuit is drawn and displayed using Qiskit visualization tools

To ensure the accuracy of the simulation, we simulated the protocol 1024 times and recorded the simulation results.

4.1. Simulation Setup

- Quantum Channel: ideal, non-lossy, and noiseless channels between the TP and Alice/Bob.

- Classical Channel: an authenticated channel between Alice and Bob for result verification.

- Photon Preparation: The TP prepares $2N$ single photons in the X-basis ($|+\rangle$) and sends N photons each to Alice and Bob.

- Operations: Alice and Bob randomly choose to perform CTRL or SIFT operations on the received photons.

- Bell Measurements: The TP performs Bell state measurements on the returned qubits.

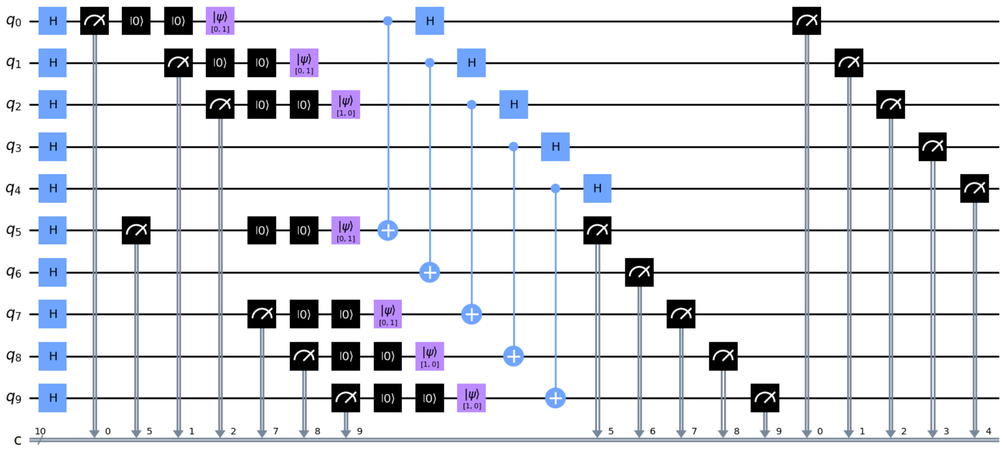
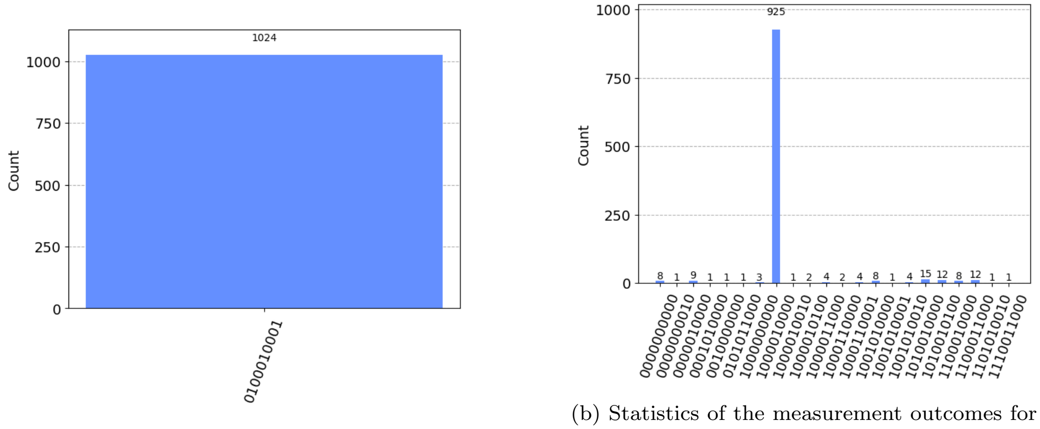


Figure 2: The process of simulation



(a) Statistics of the measurement outcomes for the simulation after 1024 times

(b) Statistics of the measurement outcomes for the simulation after 1024 times with noise model implemented

Figure 3: Comparison of measurement outcomes with and without noise model

4.2. Results

- Qubit Efficiency: The simulation confirmed the protocol's improved qubit efficiency of 1/12.
- Operational Feasibility: The simulations validated the correctness and feasibility of the proposed protocol in a quantum computing environment.

4.3. Implementation of the Noise model

In the proposed MSQKD protocol, we used a depolarizing noise model to simulate the effects of noise on quantum operations. Depolarizing noise is a common and well-studied noise model in quantum computing, representing a scenario where a quantum state is replaced with the maximally mixed state with a certain probability, thereby introducing errors in the system. The noise model was implemented using Qiskit's noise module. Two types of depolarizing errors were defined:

- Single Qubit Gate Error: This error affects single qubit gates (u1, u2, u3) with a specified noise level.
- Two Qubit Gate Error: This error affects the two qubit gate (cx) with a specified noise level.

The defined depolarizing errors were then added to the noise model for all qubits using the '"add_all_qubit_quantum_error method"'. The incorporation of the depolarizing noise model into the simulation of the MSQKD protocol allows us to evaluate its robustness and performance in realistic scenarios where quantum operations are subject to noise.

In this section , we analyze the performance of our protocol with Lin protocol (24). The false positive rate is a critical metric in evaluating the performance of eavesdropper detection methods, as it indicates the percentage of times the protocol falsely identifies the presence of an eavesdropper when there is none. Lower false positive rates are desirable because they imply that the protocol is better at accurately distinguishing between eavesdropper and non-eavesdropper scenarios.

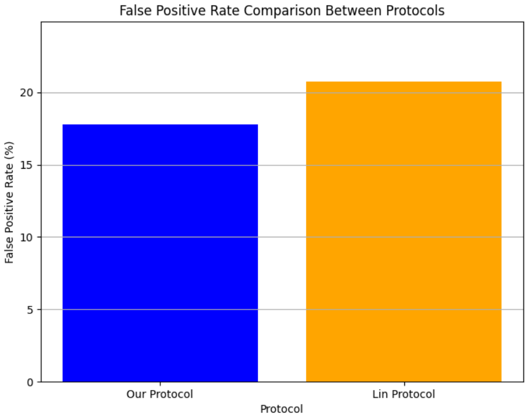


Figure 4: Comparison of False Positive Rates Between Protocols

As shown in fig4 , The false positive rate for "Our Protocol" is calculated to be 17.78 percent , This value indicates that in 17.78 percent of the cases where there is no eavesdropper present, "Our Protocol" incorrectly flags an eavesdropper, while for "Lin Protocol" is slightly higher at 20.75 percentage , This means that "Lin Protocol" incorrectly detects an eavesdropper in 20.75 percent of the cases when there is actually no eavesdropper present. A lower false positive rate for "Our Protocol" suggests that it is more reliable in avoiding false alarms compared to "Lin Protocol." This indicates better performance in practical applications where minimizing false positives is crucial, such as in secure communications and cryptographic protocols. The difference in false positive rates (3 percent) highlights a notable improvement in detection accuracy with "Our Protocol."

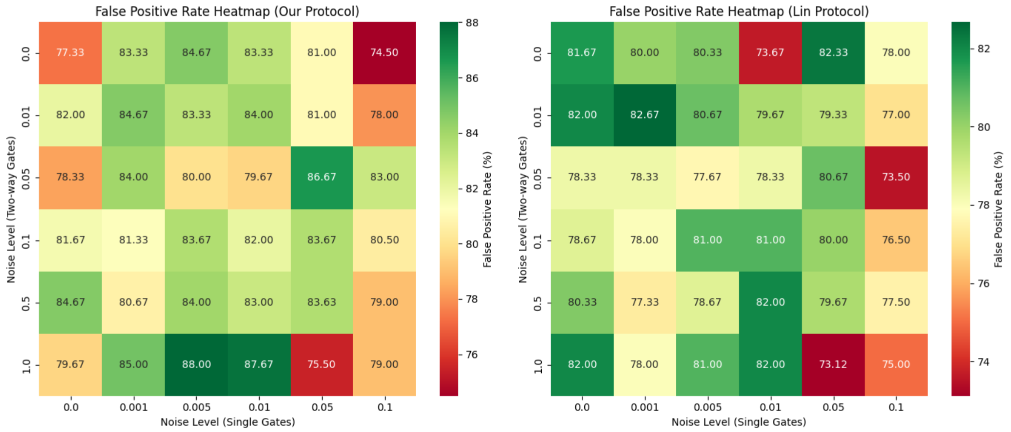


Figure 5: False Positive heat map Between Protocols

The heat maps presented in Figure5 display the false positive rates for "Our Protocol" and "Lin Protocol" across varying noise levels in single gates and two-way gates.

For "Our Protocol," the false positive rates range from 74.50 percent to 88.00 percent . The lowest false positive rate of 74.50 percent is observed at the highest noise level (0.1) for single gates with no noise in two-way gates, whereas the highest false positive rate of 88.00 percent is observed at the noise level of 0.005 for single gates and the highest noise level (1.0) for two-way gates. This suggests that "Our Protocol" is relatively more robust against noise in single gates when two-way gate noise is minimal, but its performance declines significantly with moderate noise in single gates and high noise in two-way gates.

In comparison, the "Lin Protocol" shows false positive rates ranging from 73.12 percent to 82.67 percent . The lowest false positive rate of 73.12 percent is observed at the highest noise level (1.0) for two-way gates with a moderate noise level (0.05) in single gates. Conversely, the highest false positive rate of 82.67 percent occurs at the lowest noise level (0.0) for single gates and minimal noise in two-way gates (0.01). This indicates that "Lin Protocol" tends to maintain a lower and more stable false positive rate across various noise levels, with some increase in false positives when both single and two-way gate noise are minimal.

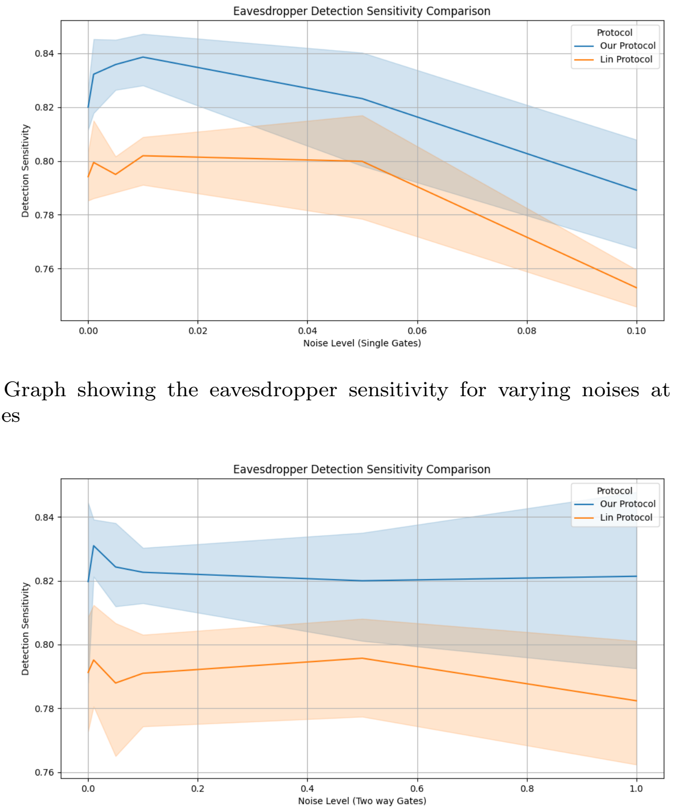
Overall, the heat maps highlight the noise resilience of both protocols, with "Our Protocol" demonstrating more variability in false positive rates under different noise conditions, while "Lin Protocol" maintains more consistent performance but with generally higher false positive rates at minimal noise levels.

We evaluate the sensitivity of our proposed MSQKD protocol to eavesdropping, in comparison to the Lin protocol (24). Sensitivity analysis is conducted to determine how effectively each protocol can detect the presence of an eavesdropper under varying noise conditions. To perform this evaluation, we conducted a series of simulations and analyzed the resulting data. We calculated the detection sensitivity for each protocol by grouping the simulation data based on noise levels and computing the mean eavesdropper detection rate.

We performed each simulation 100 times to ensure the statistical reliability of our results. We considered various configurations of the quantum system by using different numbers of qubits. Specifically, we tested systems with 4, 6, 8, 10, 12, and 14 qubits. This range allows us to observe how the detection sensitivity scales with the size of the quantum system. For single-qubit gates, we applied a range of noise levels: 0 (no noise), 0.001, 0.005, 0.01, 0.05, and 0.1. These noise levels represent different degrees of gate imperfections and environmental interference that might affect the fidelity of single-qubit operations in a real-world quantum system.Similarly, for two-qubit gates, we used noise levels of 0 (no noise), 0.01, 0.05, 0.1, 0.5, and 1.0. These values are chosen to study the impact of two-qubit gate errors, which are typically more prone to noise and errors compared to single-qubit gates. Below is the comparison between both protocols and how it's been affected by the noise level at different gates;

According to the results in 6a both protocols show a decline in detection sensitivity as the noise level for single gates increases, showing the way noise can affect the detection of eavesdroppers in the simulation, Our Protocol maintains a higher sensitivity than the Lin Protocol across all noise levels. The shaded regions indicate the variance in detection sensitivity. For Our Protocol, there is more significant variance at lower noise levels, but it becomes more consistent as noise increases while Lin Protocol shows relatively consistent variance but with a more pronounced decrease in sensitivity compared to Our Protocol.

Similarly , in 6b Both protocols exhibit a decline in detection sensitivity as the noise level for two-way gates increases. Our Protocol starts at a



(a) Graph showing the eavesdropper sensitivity for varying noises at Single Gates

(b) Graph showing the eavesdropper sensitivity for varying noises at Two-Way Gates

Figure 6: Eavesdropper Detection Sensitivity Comparison between our protocol and Lin protocol(24)

higher sensitivity (approximately 0.82) and ends around 0.80 as noise levels increase from 0 to 1.0 while Lin Protocol starts at a lower sensitivity (approximately 0.80) and shows a slight decrease, ending around 0.78. The shaded regions around the lines represent the variance or confidence intervals in the detection sensitivity. Our Protocol has a wider variance at lower noise levels, indicating more fluctuation, but this variance narrows as noise increases while Lin Protocol shows a more consistent variance throughout.

Our Protocol consistently outperforms the Lin Protocol in terms of eavesdropper detection sensitivity across all noise levels for both single-qubit and two-qubit gates. The variance in detection sensitivity is higher at lower noise levels for both protocols, especially for Our Protocol. These results suggest that while both protocols experience a decline in detection sensitivity with increased noise, Our Protocol is more robust and maintains higher sensitivity, making it potentially more reliable in noisy environments.

5. Comparison and Discussion

This section provides an in-depth comparison between the proposed Mediated SQKD protocol and existing protocols, specifically the seminal MSQKD protocols by Krawec (6), Liu et al. (7) Lin et al. (24) and other recent works .

In Krawec's protocol and others, the classical participants have the same quantum capabilities, which include measuring the qubits in Z-basis and reflecting the qubits.in our protocol we use the enhanced SIFT operation whereby the qubits are replaced by new qubits at random also distinguishes this protocol from other protocols , adding more layers to it's unpredictability and also reordering the qubit sequence making it harder for TP or an eavesdropper to gain or keep track of any information. Unlike Krawec's protocol and Liu et al.'s protocol, which use Bell states, TP in the proposed protocol uses single photons as the quantum resource without using any entanglement state. This reduces TP's burden in generating quantum resources and makes the protocol more practical. In terms of qubit efficiency, Liu's protocol has the best efficiency, while Liu's protocol boasts better qubit efficiency. The practical implications of this difference must be considered in the context of overall system complexity, security robustness, and ease of implementation. The proposed protocol's improved qubit efficiency of 1/12 compared to the previous 1/24 represents a significant enhancement in the practical application of quantum cryptographic methods. This improved efficiency means that fewer quantum resources are required to achieve the same level of security, making the protocol more feasible for real-world implementation. The qubit efficiency is defined as

$$\eta = \frac{n}{m}$$

where n denotes the total number of shared classical bits, and m denotes the total number of qubits generated in the protocols.

Initially, TP generates 2N qubits and sends them to Alice and Bob. since the SIFT operation involves discarding the received photon and replacing it with a new qubit. Therefore, if Alice and Bob each handle N qubits, the total number of SIFT operations across both will be

$$2N \times \frac{1}{2} = N,$$

assuming each qubit has an equal probability of undergoing SIFT. The measure and resend operations do not change the total number of qubits. Each SIFT operation generates a new qubit. Therefore, if Alice and Bob each perform $\frac{N}{2}$ SIFT operations on average:

$$\text{Additional qubits generated} = N$$

So, the total number of qubits generated (m) becomes:

$$m = 2N + N = 3N$$

Shared classical bits are derived from the SIFT operation. Assuming Alice and Bob each perform SIFT on half of their qubits:

$$n = \frac{N}{4}$$

Using the revised total number of qubits generated:

$$\eta = \frac{n}{m}$$

$$\eta = \frac{\frac{N}{4}}{3N} = \frac{1}{12}$$

So, the revised qubit efficiency for the proposed protocol, accounting for the additional qubits generated by the CTRL operation, is:

$$\eta = \frac{1}{12}$$

Table 4 presents a comparison of various mediated semi-quantum key distribution (MSQKD) protocols, focusing on their technical capabilities, qubit efficiency, noise tolerance, and quantum resource requirements. These protocols demonstrate significant advancements over time, particularly in qubit efficiency. For instance, our protocol achieves a qubit efficiency of 1/12, doubling the efficiency of early protocols like Krawec (2015) with minimal resource demands. At Ye et al's(25) paper , Q represents the Error rate.

Table 4: Comparison of Quantum Key Distribution Protocols

Protocol	**TP Capabilities**	**Classical Capabilities**	**Quantum Resource**	**Qubit Efficiency**	**Noise Tolerance**
Krawec (2015) (6)	Prepare Bell states, Bell measurement	Generation, Measurement, Reflection	Bell states	$\frac{1}{24}$	Not addressed
Liu (2018) (7)	Prepare Bell states, Bell measurement	Generation, Measurement, Reorder	Bell states	$\frac{1}{8}$	Not addressed
Lin (2019) (24)	Single photons in X basis, Bell measurement	Generation, Measurement, Reflection	Single photons	$\frac{1}{24}$	Limited
Guskind and Krawec (2022) (10)	Single-photon preparation, Bell measurement	Measure, Reflect, Reorder	Single photons, bell states	$\frac{1}{12}$	Moderate
Ye et al. (2022) (25)	Prepare single-particle states, Bell measurement	Measurement , Reflection, Reorder	Bell states	$\frac{1-Q}{4}$	Moderate
Zhou (2024) (8)	Measurement-free, single-particle state	Generation, Reflection	Single-particle state	$\frac{1}{8}$	Improved
Our Protocol	Single photons in X basis, Bell measurement	Generation, Reflection, Reorder	Single photons	$\frac{1}{12}$	Extensive

Quantum resources have become more manageable in newer protocols, with recent developments favoring single photons over the more complex and resource-intensive Bell states. Additionally, noise tolerance has seen improvements; protocols by Zhou (2024) and our protocol explicitly address noise resilience, making them more practical for real-world applications compared to earlier methods.

The security mechanisms also vary across protocols, with recent methods incorporating advanced features such as decoy state testing and quantum channel testing, which enhance protection against eavesdropping and other attacks. This comparison illustrates a clear trend in MSQKD protocol development toward greater efficiency, security, and practicality, with our protocol showcasing strong performance across these factors.

6. Conclusion

Utilizing the properties of single photons and Bell measurements, we have developed a new MSQKD protocol that enables two classical participants to securely share a secret key with the assistance of an untrusted TP. Unlike Krawec's and Liu et al.'s protocols, which rely on Bell states, our proposed protocol is more practical as it only requires the TP to generate single photons without the need for entanglement. The enhanced qubit efficiency of 1/12 further increases the practicality by reducing quantum resource requirements and improving overall efficiency.

The MSQKD protocol was successfully simulated using IBM Qiskit, confirming the feasibility of its implementation. To ensure robustness in real-world conditions, we included a noise model to analyze its impact on the protocol's performance. Our security analysis indicates that the proposed protocol can withstand various well-known attacks. For Trojan Horse attacks or other implementation-dependent threats, specific detection devices can be employed, which we suggest for future research. The unconditional security of some semi-quantum key distribution protocols has been previously explored, and applying these proof methods to our SQKD protocol is a critical direction for future work. Additionally, investigating the use of discovered properties to design other quantum protocols and further reducing the quantum burden on TP are promising areas for future research.

Acknowledgements

Project supported by the Natural Science Basic Research Program of Shaanxi (Program No. 2024JC-YBQN-0688). We also would like to thank the anonymous reviewers for their detailed review and valuable comments, which have enhanced the quality of this paper.

References

[1] C. H. Bennett, G. Brassard, A. K. Ekert, Quantum cryptography, Scientific American 267 (4) (1992) 50–57.

[2] A. Broadbent, C. Schaffner, Quantum cryptography beyond quantum key distribution, Designs, Codes and Cryptography 78 (2016) 351–382.

[3] X. Zou, D. Qiu, L. Li, L. Wu, L. Li, Semiquantum-key distribution using less than four quantum states, Physical Review A 79 (5) (2009) 052312.

[4] K.-F. Yu, C.-W. Yang, C.-H. Liao, T. Hwang, Authenticated semi-quantum key distribution protocol using bell states, Quantum Information Processing 13 (2014) 1457–1465.

[5] Q. Li, W. H. Chan, S. Zhang, Semiquantum key distribution with secure delegated quantum computation, Scientific reports 6 (1) (2016) 19898.

[6] W. O. Krawec, Mediated semiquantum key distribution, Physical Review A 91 (3) (2015) 032323.

[7] Z.-R. Liu, T. Hwang, Mediated semi-quantum key distribution without invoking quantum measurement, Annalen der Physik 530 (4) (2018) 1700206.

[8] S. Zhou, Q.-M. Xie, N.-R. Zhou, Measurement-free mediated semi-quantum key distribution protocol based on single-particle states, Laser Physics Letters 21 (6) (2024) 065207.

[9] N.-R. Zhou, K.-N. Zhu, X.-F. Zou, Multi-party semi-quantum key distribution protocol with four-particle cluster states, Annalen der Physik 531 (8) (2019) 1800520.

[10] J. Guskind, W. O. Krawec, Mediated semi-quantum key distribution with improved efficiency, Quantum Science and Technology 7 (3) (2022) 035019.

[11] Y.-P. Luo, T. Hwang, Authenticated semi-quantum direct communication protocols using bell states, Quantum Information Processing 15 (2016) 947–958.

[12] C. Shukla, K. Thapliyal, A. Pathak, Semi-quantum communication: protocols for key agreement, controlled secure direct communication and dialogue, Quantum Information Processing 16 (2017) 1–19.

[13] C.-W. Yang, T. Hwang, Efficient key construction on semi-quantum secret sharing protocols, International Journal of Quantum Information 11 (05) (2013) 1350052.

[14] K.-F. Yu, J. Gu, T. Hwang, P. Gope, Multi-party semi-quantum key distribution-convertible multi-party semi-quantum secret sharing, Quantum Information Processing 16 (2017) 1–14.

[15] H.-H. Li, L.-H. Gong, N.-R. Zhou, New semi-quantum key agreement protocol based on high-dimensional single-particle states, Chinese Physics B 29 (11) (2020) 110304.

[16] C. Wang, Q. Zhang, S. Liang, H. Zhu, Secure mutual authentication quantum key agreement scheme for two-party setting with key recycling, Quantum Information Processing 23 (4) (2024) 139.

[17] H. Zhu, L. Wang, Y. Zhang, An efficient quantum identity authentication key agreement protocol without entanglement, Quantum Information Processing 19 (2020) 1–14.

[18] P. Zawadzki, Quantum identity authentication without entanglement, Quantum Information Processing 18 (1) (2019) 7.

[19] S. Jiang, R.-G. Zhou, W. Hu, Semi-quantum mutual identity authentication using bell states, International Journal of Theoretical Physics 60 (2021) 3353–3362.

[20] W.-H. Chou, T. Hwang, J. Gu, Semi-quantum private comparison protocol under an almost-dishonest third party, arXiv preprint arXiv:1607.07961 (2016).

[21] K. Thapliyal, R. D. Sharma, A. Pathak, Orthogonal-state-based and semi-quantum protocols for quantum private comparison in noisy environment, International Journal of Quantum Information 16 (05) (2018) 1850047.

[22] L.-H. Gong, Z.-J. Ye, C. Liu, S. Zhou, One-way semi-quantum private comparison protocol without pre-shared keys based on unitary operations, Laser Physics Letters 21 (3) (2024) 035207.

[23] L.-H. Gong, Z.-Y. Chen, L.-G. Qin, J.-H. Huang, Robust multi-party semi-quantum private comparison protocols with decoherence-free states against collective noises, Advanced Quantum Technologies 6 (8) (2023) 2300097.

[24] P.-H. Lin, C.-W. Tsai, T. Hwang, Mediated semi-quantum key distribution using single photons, Annalen der Physik 531 (8) (2019) 1800347.

[25] Y. Chongqiang, L. Jian, C. Xiubo, T. Yuan, H. Yanyan, An efficient semi-quantum key distribution protocol and its security proof, IEEE Communications Letters 26 (6) (2022) 1226–1230.

[26] C.-W. Tsai, C.-W. Yang, N.-Y. Lee, Lightweight mediated semi-quantum key distribution protocol, Modern Physics Letters A 34 (34) (2019) 1950281.

[27] M. A. Nielsen, I. L. Chuang, Quantum computation and quantum information, Cambridge university press, 2010.

[28] L. Chen, Q. Li, C. Liu, Y. Peng, F. Yu, Efficient mediated semi-quantum key distribution, Physica A: Statistical Mechanics and its Applications 582 (2021) 126265.

[29] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, M. Peev, The security of practical quantum key distribution, Reviews of modern physics 81 (3) (2009) 1301.

[30] C. H. Bennett, G. Brassard, Quantum cryptography: Public key distribution and coin tossing, Theoretical computer science 560 (2014) 7–11.

[31] Y. Tian, J. Li, X.-B. Chen, C.-Q. Ye, H.-J. Li, An efficient semi-quantum secret sharing protocol of specific bits, Quantum Information Processing 20 (6) (2021) 217.

[32] A. Abbas, S. Andersson, A. Asfaw, A. Corcoles, L. Bello, Y. Ben-Haim, M. Bozzo-Rey, S. Bravyi, N. Bronn, L. Capelluto, A. C. Vazquez, J. Ceroni, R. Chen, A. Frisch, J. Gambetta, S. Garion, L. Gil, S. D. L. P. Gonzalez, F. Harkins, T. Imamichi, P. Jayasinha, H. Kang, A. h. Karamlou, R. Loredo, D. McKay, A. Maldonado, A. Macaluso, A. Mezzacapo, Z. Minev, R. Movassagh, G. Nannicini, P. Nation, A. Phan, M. Pistoia, A. Rattew, J. Schaefer, J. Shabani, J. Smolin, J. Stenger, K. Temme, M. Tod, E. Wanzambi, S. Wood, J. Wootton., Learn Quantum Computation Using Qiskit, IBM, 2020.
URL `https://qiskit.org/textbook/`

[33] GitHub, Github repository, `https://github.com/Qiskit/textbook`, accessed: 2024-02-23.

[34] B. Chen, W. Yang, L. Huang, Cryptanalysis and improvement of the novel semi-quantum secret sharing scheme based on bell states, Modern Physics Letters B 32 (25) (2018) 1850294.

[35] Y. Tian, J. Wang, G. Bian, J. Chang, J. Li, Dynamic multi-party to multi-party quantum secret sharing based on bell states, Advanced Quantum Technologies 7 (7) (2024) 2400116.

[36] C.-Q. Ye, J. Li, X.-B. Chen, M. Dong, K. Ota, Measurement-based quantum sealed-bid auction, IEEE Transactions on Circuits and Systems I: Regular Papers (2023).

[37] M. Boyer, R. Gelles, D. Kenigsberg, T. Mor, Semiquantum key distribution, Physical Review A 79 (3) (2009) 032341.

[38] M. Erhard, M. Krenn, A. Zeilinger, Advances in high-dimensional quantum entanglement, Nature Reviews Physics 2 (7) (2020) 365–381.

[39] W. O. Krawec, An improved asymptotic key rate bound for a mediated semi-quantum key distribution protocol, arXiv preprint arXiv:1509.04797 (2015).

[40] S. Mutreja, W. O. Krawec, Improved semi-quantum key distribution with two almost-classical users, Quantum Information Processing 21 (9) (2022) 319.

[41] W. O. Krawec, Security proof of a semi-quantum key distribution protocol, in: 2015 IEEE International Symposium on Information Theory (ISIT), IEEE, 2015, pp. 686–690.

[42] M.-M. Wang, L.-M. Gong, L.-H. Shao, Efficient semiquantum key distribution without entanglement, Quantum Information Processing 18 (2019) 1–10.

[43] C.-W. Tsai, C.-W. Yang, Lightweight authenticated semi-quantum key distribution protocol without trojan horse attack, Laser Physics Letters 17 (7) (2020) 075202.

[44] C. Portmann, R. Renner, Cryptographic security of quantum key distribution, arXiv preprint arXiv:1409.3525 (2014).

[45] Y. Zhao, B. Qi, X. Ma, H.-K. Lo, L. Qian, Experimental quantum key distribution with decoy states, Physical review letters 96 (7) (2006) 070502.

[46] L. Yan-Feng, Semi-quantum private comparison using single photons, International Journal of Theoretical Physics 57 (2018) 3048–3055.

[47] X.-B. Wang, Quantum key distribution with asymmetric channel noise, Physical Review A—Atomic, Molecular, and Optical Physics 71 (5) (2005) 052328.

[48] X.-H. Li, F.-G. Deng, H.-Y. Zhou, Efficient quantum key distribution over a collective noise channel, Physical Review A—Atomic, Molecular, and Optical Physics 78 (2) (2008) 022321.

[49] P. N. Singh, S. Aarthi, Quantum circuits–an application in qiskit-python, in: 2021 third international conference on intelligent communication technologies and virtual mobile networks (icicv), IEEE, 2021, pp. 661–667.

[50] A. Javadi-Abhari, M. Treinish, K. Krsulich, C. J. Wood, J. Lishman, J. Gacon, S. Martiel, P. D. Nation, L. S. Bishop, A. W. Cross, et al., Quantum computing with qiskit, arXiv preprint arXiv:2405.08810 (2024).

[51] C.-Q. Ye, J. Li, X.-B. Chen, Y. Hou, M. Dong, K. Ota, Circular mediated semi-quantum key distribution, Quantum Information Processing 22 (4) (2023) 170.