symmetry

MDPI

*Article*

# A Secured Half-Duplex Bidirectional Quantum Key Distribution Protocol against Collective Attacks

**Manal Khawasik [1,2,*], Wagdy Gomaa El-Sayed [1], M. Z. Rashad [3] and Ahmed Younes [1,2,4]**

[1] Department of Mathematics and Computer Science, Faculty of Science, Alexandria University, Alexandria 21544, Egypt
[2] Alexandria Quantum Computing Group, Faculty of Science, Alexandria University, Alexandria 21544, Egypt
[3] Department of Computer Science, Faculty of Computers and Information Systems, Mansoura University, Mansoura 35516, Egypt
[4] School of Computer Science, University of Birmingham, Birmingham B15 2TT, UK
* Correspondence: manal.khawasik@alexu.edu.eg

**Abstract:** Quantum Key Distribution is a secure method that implements cryptographic protocols. The applications of quantum key distribution technology have an important role: to enhance the security in communication systems. It is originally inspired by the physical concepts associated with quantum mechanics. It aims to enable a secure exchange of cryptographic keys between two parties through an unsecured quantum communication channel. This work proposes a secure half-duplex bidirectional quantum key distribution protocol. The security of the proposed protocol is proved against collective attacks by estimating the interception of any eavesdropper with high probability in both directions under the control of the two parties. A two-qubit state encodes two pieces of information; the first qubit represents the transmitted bit and the second qubit represents the basis used for measurement. The partial diffusion operator is used to encrypt the transmitted qubit state as an extra layer of security. The predefined symmetry transformations induced by unitary in conjunction with the asymmetrical two-qubit teleportation scheme retain the protocol's secrecy. Compared to the previous protocols, the proposed protocol has better performance on qubit efficiency.

**Keywords:** collective attack; intercept attack; parameter estimation; quantum cryptography; quantum key distribution

check for updates

**Citation:** Khawasik, M.; El-Sayed, W.G.; Rashad, M.Z.; Younes, A. A Secured Half-Duplex Bidirectional Quantum Key Distribution Protocol against Collective Attacks. *Symmetry* **2022**, *14*, 2481. https://doi.org/10.3390/sym14122481

Academic Editor: Jeng-Shyang Pan

Received: 20 October 2022
Accepted: 17 November 2022
Published: 23 November 2022

## 1. Introduction

Quantum computing has affected many areas such as machine learning, optimization problems, material synthesis, and communication systems, specifically Quantum Key Distribution (QKD) [1–7]. QKD is an important aspect of quantum cryptography [8]. It allows exchanging cryptographic keys between two parties named Alice (A) and Bob (B). The two parties trust each other, but they do not have access to a secure communication channel [9]. The strength of QKD is that it uses the laws of quantum physics, especially the properties of light and photons, that are used to introduce methods for the secure distribution of encryption keys over communication networks [10].

In quantum physics, polarized light can be used to exchange information by encoding the values of classical bits into quantum objects. Each bit is represented by a pulse which is emitted and sent to the receiver as light signals. These pulses typically involve millions of light particles known as photons [10]. Eavesdroppers usually try to observe or detect information about the transmitted photons that would change the photon state. The transmission is then perturbed and causes a transmission interruption [11].

The measurement of the quantum state causes the state to be destroyed when an eavesdropper detects the photon and registers the bit value. Consequently, Eve prepares a new photon according to the information she received and then sends the photon to the receiver side [12]. The two parties can detect the attack where the receiver chooses a bit splitter that receives a photon from the sender randomly. On the other hand, Eve is not supposed to determine exactly which basis to perform the measurement in order to intercept the communication transmission. The eavesdropper can only guess the basis in a random manner, and if the guessing is wrong, then Bob would receive a muddled state that is disturbed by Eve who will consequently lose control over the communication channel [13].

In 2017, a semi-quantum version of the B92 protocol was presented where the sender party transmits one qubit to the receiver, which is a classical party. This protocol provides a security proof against collective and general attacks using fewer quantum resources [14]. In 2019, Po-Hua et al. proposed a mediated semi-QKD protocol that shares a secret key between two classical parties. This protocol uses a third untruthful party to generate single photon and perform Bell measurement [15]. In 2020, a QKD scheme against collective rotation channel noise was introduced. This protocol uses polarization and transverses the spatial modes of photons. The linear optical elements are used to measure two-single photon states to obtain the keys [9]. In 2021, Nitin Jain et al. demonstrated a QKD system that can generate composable keys that are secured against collective attacks. A machine learning framework for phase compensation was implemented to retain the excess noise under the null key length threshold [16]. In 2022, a semi-QKD protocol based on logical qubits was presented, two physical qubit entangled states are used, and the measurement of a single physical qubit is performed by the quantum communicant [17]. Xu et al. proposed a QKD protocol with random post-selection that reduces the error events with an enhanced detection efficiency [18]. Luis et al. proposed a method that obtains a complete reconciliation in QKD; this method determines the transmitted errors in a reverse reconciliation and corrects all of them, which is invariant to the error rate. However, this method is still not applicable on the collective attack [19].

This paper proposes a half-duplex bidirectional QKD protocol that is secured against collective attacks. The proposed QKD protocol provides a parameter estimation that can be completely estimated under the control of the two parties. This protocol is also secured against the intercepted attack where the sender prepares a two-qubit state that combines two main data, the bit and basis values. The partial diffusion quantum operator is applied to hide the two qubit state from the superposition against the direct measurement of an eavesdropper [20].

The remaining of this paper is organized as follows: Section 2 introduces the main basic tools used for developing the proposed protocol. Section 3 presents the structure of the proposed protocol in addition to a security proof of a collective attack and parameter estimation. Section 4 shows the discussion and results of this work. Finally, the main conclusion of this work is introduced in Section 5.

## 2. Basics and Main Methods

This section presents the main idea of quantum key distribution and the basic tools and operators used for developing the proposed protocol.

### 2.1. Quantum Key Distribution

In QKD, the two parties have a quantum communication channel (QCC) in addition to a classical channel. The basic principles of quantum physics are utilized where Alice and Bob can transmit qubits to each other using photons to ensure the secrecy of achieving random keys. In the classical channel, post processing methods are implemented to analyze any eavesdropping behaviors and estimate statistics required to rectify interceptions occurred in the QCC [11].

QKD starts from the QCC where the preparation and measurement of qubits take place randomly in different bases. This step is followed by data sifting, parameter estimation, error correction and privacy amplification in the authenticated classical channel that are implemented to determine which measurement results could lead to secret key bits [8]. Incompatible measurements are discarded from the raw key during the key sifting step;

the discarded bits have different photon polarization of their equivalent qubits. In the parameter estimation stage, Alice and Bob estimate the security parameters of the QCC in order to statistically predict the information about their key that is attacked by Eve. The error rate is produced from the parameter estimation stage and is compared by a certain threshold. If the value of the error rate is greater than the threshold, then the protocol is aborted because this indicates that there is an attack or a channel noise; in both cases, the iteration is stopped to guarantee the secrecy of the protocol. On the other hand, if the error rate is less than a certain threshold value, then the protocol continues toward the error correction stage [21].

According to the estimation parameters, the leakage information is estimated; then, Alice and Bob have to remove the errors from their shared key to reconcile their key. This is achieved during the error correction step by implementing an appropriate classical error reconciliation algorithm. During the error correction step, appropriate classical error reconciliation algorithms are used to remove errors of the shared key. These algorithms use the statistical parameters of the parameter estimation step. The conditional Von Neumann entropy associated with the conditional Shannon entropy can be used to compute the key rate [14]. Furthermore, other error reconciliation methods can be applied that correct all the errors that are produced in regular binary frames transmitted over a noisy QCC despite the error rate of the quantum channel [19].

Privacy amplification is then applied to the raw key to reduce the information that Eve has gathered up about the key. In this stage, the correlation between the key and Eve is stopped, and the two parties transform their identical shared key into a new shrinked key unknowable to Eve. The development of quantum communications can be enhanced when using powerful teleportation schemes. Combining quantum teleportation with QKD strategies can remove some implicit noisy effects, and hence, enhance the secrecy of the quantum communications channels [22]. Figure 1 shows schematically the main stages of main QKD protocol.

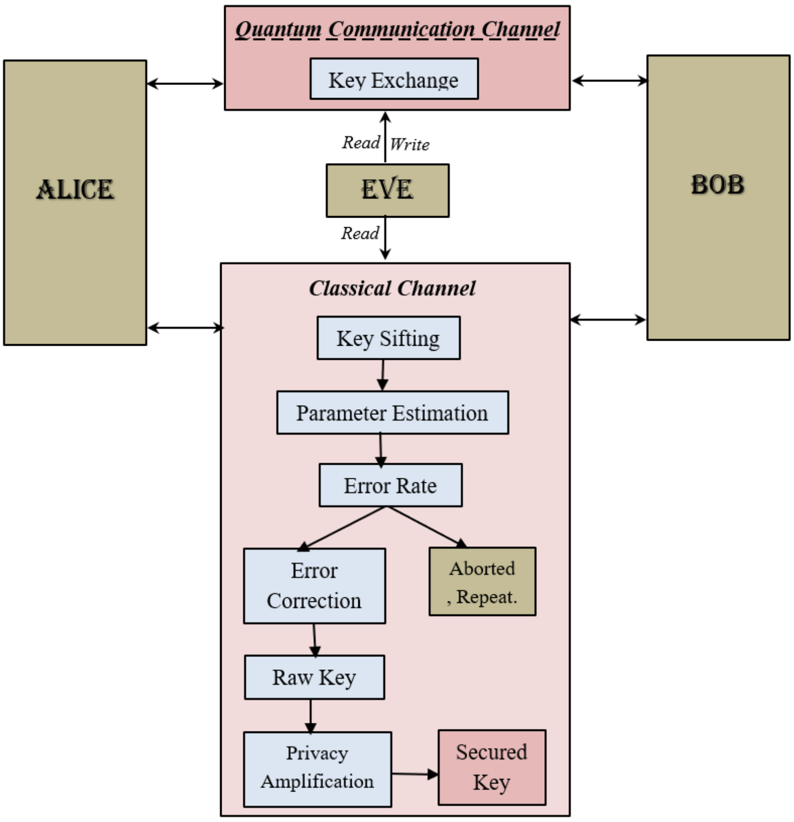


**Figure 1.** Main stages of the QKD protocol. The two parties share a quantum communication channel for key exchange, in addition to an authorized classical channel.

### 2.2. Partial Diffusion Operator

The partial diffusion operator is a quantum operator that is used to hide quantum states from a superposition to increase the security level in communication systems [23]. It can be represented by the following equation:

$$\mathcal{D}_{\mathcal{P}} = (W^{\otimes n} \otimes I)(2\,|0\rangle\,\langle 0| - I)(W^{\otimes n} \otimes I), \tag{1}$$

where $W$ denotes the Walsh Hadamard gate, the vector $|0\rangle$ is of length $2^{n+1}$, and $I_n$ represents the identity matrix. The partial diffusion operator performs the inversion about the mean on the subspace of the system entangled with $|0\rangle$, which is followed by performing a phase shift of $-1$ on the subspace of the system entangled with $|1\rangle$ in order to differentiate the hidden states from the selected states. The oracle $U_f$ is an operator that evolves to be true for the selected states [20]. The operator $U_f$ is applied to determine the selected and hidden states where $U_f\,|x,0\rangle \rightarrow |x, f(x)\rangle$. Figure 2 illustrates the implementation circuit of $\mathcal{D}_{\mathcal{P}}$.

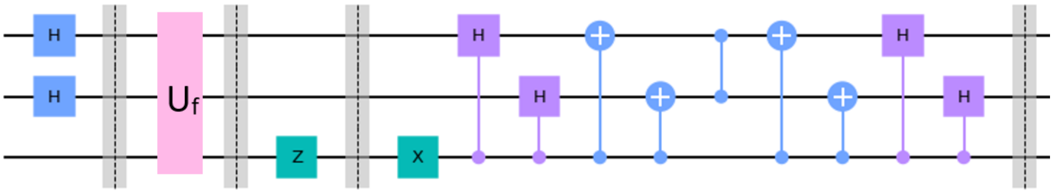


**Figure 2.** The partial diffusion quantum operator. The inversion about the mean and the phase shift are performed to hide specific states from the superposition.

It evaluates to true for the target states and false otherwise. $\mathcal{D}_{\mathcal{P}}$ is expressed by the following equation:

$$\sum_{j=0}^{N-1} (-\beta_j + 2\,\langle\beta\rangle)(|j\rangle \otimes |0\rangle) - \sum_{j=0}^{N-1} \alpha_j(|j\rangle \otimes |1\rangle), \tag{2}$$

where $\beta$ is a complex number and $\langle\beta\rangle = \frac{1}{N}\sum_{j=0}^{N-1}\beta_j$ represents the mean of the amplitudes of the states in the superposition [23]. For example, applying the quantum operator $\mathcal{D}_{\mathcal{P}}$ on the 2-qubit system $|\psi\rangle = \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)$ is to convert $|\psi\rangle$ to a superposition of any two states contained in this system that can be substituted by the other two states by substituting and restoring them. The states to be hidden and the states to be selected are chosen depending on the data exchange requirements.

The hidden states can be restored using the Grover's quantum operator $G$ that performs the inversion about the mean [24]. Figure 3 presents the quantum circuit of the Grover's operator for a 2-qubit system.

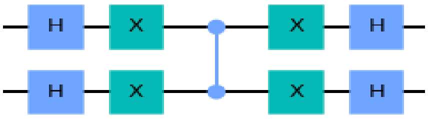


**Figure 3.** The circuit implementation of Grover's quantum operator on 2 qubits. This operator is applied once to restore the hidden states.

## 3. Theoretical Work

The usage of QKD can be presented by analyzing the collective attack and parameter estimation steps of the protocol. In collective attacks, Eve performs the same operation each iteration of the quantum communication stage. It is the channel side leakage of information introduced by imperfect devices in the transmission and measurement of quantum states [9]. Section 3.1 presents the main structure and steps of the proposed half-duplex bidirectional QKD protocol. Section 3.2 presents the steps of the collective attack executed by Eve in both the forward and reverse directions.

### *3.1. The Structure of the Proposed Protocol*

This protocol utilizes a half-duplex bidirectional quantum channel, forward $(fwd)$ and reverse $(rvs)$ in addition to an Authenticated Classical Channel (ACC). Alice starts the QKD protocol with two random classical bit strings $s$ and $t$, each of size $N = \lfloor(4+\delta)n\rfloor$, where s comprises the bit values 0 or 1, while t denotes basis $Z$ and basis $X$, which are denoted by o and 1, respectively, and n denotes the raw key bits and then encodes them into quantum bits according to the values of each bit in strings $s$ and $t$ where

$$|\Phi\rangle = \otimes_{l=1}^{N} |\phi_{s_l t_l}\rangle = |s_l t_l\rangle + |\tilde{s_l} t_l\rangle\,, \tag{3}$$

where $s_l$ is the $l$th bit of $s$ and $\tilde{s_l}$ denotes the bitwise complement of $s$. The effect of this procedure is that Alice encodes s as determined by t as a block of 2-qubit states. The classical bit 0 in string $s$ is encoded into $|\phi_0\rangle = |00\rangle + |10\rangle$ or $|\phi_1\rangle = |01\rangle + |11\rangle$ when the value of the corresponding bit in string $t$ is 0 or 1, respectively. The classical bit 1 in string $s$ is encoded into $|\phi_0\rangle$ or $|\phi_1\rangle$ when the value of the corresponding bit in string $t$ is 0 or 1, respectively.

Alice then applies the partial diffusion quantum operator for hiding the prepared quantum states that comprises the bit and basis values by other two qubit states within the superposition as an extra security level [20]. This makes the message safe by direct measurement from an eavesdropper. The state is now ready to be transmitted to Bob using the asymmetrical two-qubit teleportation configuration $\mathcal{T}$ that consists of five particles. Alice comprises the two-qubit state that she intends to transmit to Bob in addition to the third qubit that is entangled with Bob in a GHZ state [25]. Alice sends to Bob through the ACC the Grover quantum operator $\mathcal{G}$ and the predefined unitary transform $U_s$ where $s \in \{0,1\}$. Bob saves his results as a raw key where $R$ denotes the size of Alice's and Bob's raw keys. Figure 4 demonstrates the forward direction steps of the proposed protocol for one iteration.

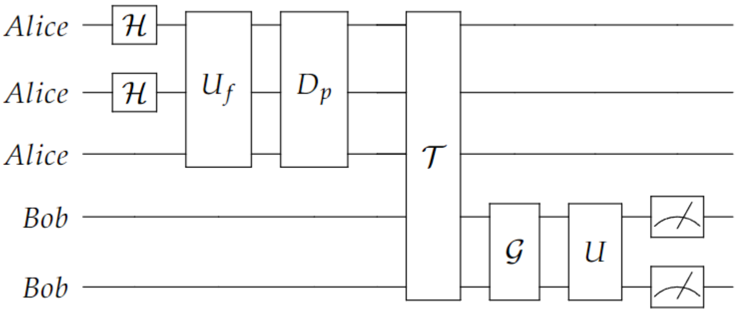


**Figure 4.** The steps of the forward direction of proposed half-duplex bidirectional QKD protocol for one iteration. The first three registers are under the control of Alice, whereas the fourth and fifth registers are under Bob's control.

Bob prepares a new state based on his measurement and retransmits to Alice through the reverse direction using $\mathcal{T}$. Alice performs the same unitary transformation she sent to Bob and then measures the system and saves her measurement as a raw key. The protocol's communication stage consists of the following steps:

Step 1. Alice starts with two random classical bit strings $s$ and $t$, each string is of size $N$ where $N = \lfloor(4+\delta)n\rfloor$ where $\delta$ is a parameter $> 0$.

Step 2. Alice encodes $s$ and $t$ into a $\lfloor(4+\delta)n\rfloor$ superposition of two states where the second qubit represents the basis used for measurement, whereas the first qubit represents the bit value. The prepared qubits are then $|\phi_0\rangle$ or $|\phi_1\rangle$.

Step 3. Alice performs a partial diffusion quantum operator that is used as an extra security level by substituting the prepared qubits by other qubits from the superposition.
Step 4. The two-qubit state is teleported from Alice to Bob through the $fwd$ direction of the unauthorized QCC.
Step 5. Bob performs the Grover's quantum operator followed by the predefined unitary transformation sent by Alice through ACC and performs his measurement.
Step 6. Bob prepares a two-qubit state based on his measurement and retransmits the qubit through the $rvs$ direction of the QCC.
Step 7. Alice performs the same predefined unitary transformation sent to Bob.

Table 1 illustrates the different combinations of the bit and basis values, their equivalent two qubit states, and the predefined unitary transformation. The unitary transformation $U_0$ applies the Hadamard gate $H$ that transforms $|0\rangle$ into the symmetric linear combination $|0\rangle + |1\rangle$ while it transforms $|1\rangle$ into the anti-symmetric linear transform $|0\rangle - |1\rangle$. Furthermore, the unitary transformation $U_1$ applies the symmetric effect of the phase flip gate followed by the Hadamard gate. Figure 5 demonstrates the reverse direction steps of the proposed QKD protocol for one iteration.

**Table 1.** Encoding classical bits and basis measurement into two-qubit state. In each iteration, the bit and basis are encoded into a 2-qubit state; then, a predefined symmetry transformation is applied.

| Bit | Basis | Encoded 2-Qubit State | Unitary Transformation |
|---|---|---|---|
| 0 | Z | $\lvert\phi_0\rangle$ | $U_0$ |
| 1 | Z | $\lvert\phi_0\rangle$ | $U_1$ |
| 0 | X | $\lvert\phi_1\rangle$ | $U_0$ |
| 1 | X | $\lvert\phi_1\rangle$ | $U_1$ |

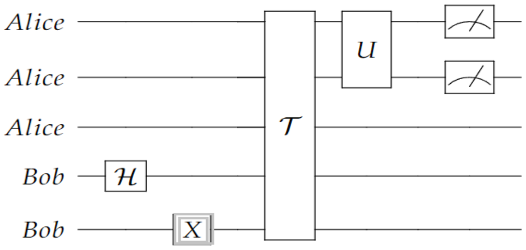


**Figure 5.** The steps of the reverse direction of the proposed half-duplex bidirectional QKD protocol for one iteration. Bob transmits the prepared state to Alice through the reverse direction using asymmetry 2-qubit teleportation scheme $\mathcal{T}$.

After repeating the protocol's steps $N$ times, the sifting procedure is performed. For each iteration, Alice will compare the bit and basis values $s$ and $t$ through the ACC with Bob's measurement values after performing $U_s$ in order to establish their shared raw key $R$. The amount of discarded qubits is denoted by $M$, where $M = N - R$.

### 3.2. Collective Attack

For one iteration of the protocol, by setting the measurement to be $Z$-basis, $\mathcal{H}_T$ represents the two-dimensional Hilbert space modeling the qubits in the transit space. The Eve's private ancilla is represented by $\mathcal{H}_E$ where the qubits prepared by Eve are denoted by $|E\rangle$. The Eve's ancilla qubit states after the forward attack are denoted by $|e_j\rangle$ where $j$ denotes the state's index. The states $|e^k_{i,j}\rangle$ are arbitrary states that resulted from the reverse attack where $i$ denotes the original qubit that is transmitted through the system, $j$ denotes the index of the ancilla qubit resulted from the $fwd$ direction attack, and $k$ represents the ancillary qubits that are entangled with the original system. The quantum operators $U_{fwd}$ and $U_{rvs}$ are unitary operators that perform the attack operation and act on $\mathcal{H}_T \otimes \mathcal{H}_E$. $U_{fwd}$ is used to attack qubits that are transmitted from Alice to Bob (forward direction) while $U_{rvs}$ is used to attack qubits that are returning from Bob to Alice (Reverse direction). The following equations demonstrate the most general form of the collective attack and illustrate the effect of performing $U_{fwd}$ and $U_{rvs}$ on the first transmitted qubit.

$$U_{fwd}(|0\rangle \otimes |E\rangle) = |0\rangle_A \otimes |e_0\rangle_E + |1\rangle_A \otimes |e_1\rangle_E \tag{4}$$

$$U_{fwd}(|1\rangle \otimes |E\rangle) = |0\rangle_A \otimes |e_2\rangle_E + |1\rangle_A \otimes |e_3\rangle_E \tag{5}$$

$$U_{rvs}(|0\rangle \otimes |e_j\rangle) = |0\rangle \otimes |e^0_{0,j}\rangle + |1\rangle \otimes |e^1_{0,j}\rangle \tag{6}$$

$$U_{rvs}(|1\rangle \otimes |e_j\rangle) = |0\rangle \otimes |e^0_{1,j}\rangle + |1\rangle \otimes |e^1_{1,j}\rangle \tag{7}$$

The state $|j\rangle \otimes |E\rangle$ is subjected to Eve's unitary transformation that changes the state sent by Alice. The following steps present the analysis of a single iteration of the proposed QKD protocol. It describes the case that Alice sends a $Z$-basis state where the two parties perform a measurement is in the same basis:

Step 1. The quantum state that represents the qubit prepared by Alice is

$$|\psi\rangle_A = \frac{1}{\sqrt{2}}(|0\rangle_A + |1\rangle_A) \otimes |0\rangle\,, \tag{8}$$

where the sender prepares a qubit state of the form $|00\rangle + |10\rangle$.

Step 2. Eve attacks the qubit transmitted from Alice. The unitary attack operator $U_{fwd}$ is applied in the forward direction using Equations (4) and (5). For simplifying the analysis, we focus on attacking the first qubit.

$$U_{fwd}\,|\psi\rangle_A = |\psi\rangle_{AE} = \frac{1}{2}(|0\rangle_A\,|e_0\rangle_E + |1\rangle_A\,|e_1\rangle_E + |0\rangle_A\,|e_2\rangle_E + |1\rangle_A\,|e_3\rangle_E). \tag{9}$$

Step 3. Bob performs his measurement, the probability of measuring the system in state $|0\rangle$ is $\langle\psi_{AE}|M_0M_0^\dagger|\psi_{AE}\rangle$ where $M_0 = |0\rangle$. This is represented by the following equation

$$\begin{aligned}\langle\psi_{AE}\,|0\rangle\,\langle 0|\,\psi_{AE}\rangle =& (\langle 0|0\rangle\,\langle e_0|e_0\rangle + \langle 1|0\rangle\,\langle e_1|e_1\rangle + \langle 0|0\rangle\,\langle e_2|e_2\rangle + \langle 1|0\rangle\,\langle e_3|e_3\rangle) + \\ & (\langle 0|0\rangle\,\langle e_0|e_0\rangle + \langle 0|1\rangle\,\langle e_1|e_1\rangle + \langle 0|0\rangle\,\langle e_2|e_2\rangle + \langle 0|1\rangle\,\langle e_3|e_3\rangle).\end{aligned} \tag{10}$$

while the probability of measuring the system in state $|1\rangle$ is $\langle\psi_{AE}|M_1M_1^\dagger|\psi_{AE}\rangle$ where $M_1 = |1\rangle$. This is represented by the following equation

$$\begin{aligned}\langle\psi_{AE}\,|1\rangle\,\langle 1|\,\psi_{AE}\rangle =& (\langle 0|1\rangle\,\langle e_0|e_0\rangle + \langle 1|1\rangle\,\langle e_1|e_1\rangle + \langle 0|1\rangle\,\langle e_2|e_2\rangle + \langle 1|1\rangle\,\langle e_3|e_3\rangle) + \\ & (\langle 1|0\rangle\,\langle e_0|e_0\rangle + \langle 1|1\rangle\,\langle e_1|e_1\rangle + \langle 1|0\rangle\,\langle e_2|e_2\rangle + \langle 1|1\rangle\,\langle e_3|e_3\rangle).\end{aligned} \tag{11}$$

From Equations (10) and (11), the state after measuring the system in the $Z$-basis as expected is as follows

$$|\Psi\rangle_B = \frac{1}{2}\,|0\rangle_B\,(|0\rangle_A\,|e_0\rangle_E + |0\rangle_A\,|e_2\rangle_E) + \frac{1}{2}\,|1\rangle_B\,(|1\rangle_A\,|e_1\rangle_E + |1\rangle_A\,|e_3\rangle_E). \tag{12}$$

Step 4. Bob sends the prepared 2-qubit states back to Alice, Eve interrupts and applies the reverse attack unitary operator $U_{rvs}$. From Equations (6) and (7), the system can be represented as

$$\begin{aligned}|\Psi\rangle_{BE} = U_{rvs}\,|\psi_B\rangle =& \frac{1}{2\sqrt{2}}\,|0\rangle_B\,(|0\rangle_A\,|e^0_{0,0}\rangle_E + |1\rangle_A\,|e^1_{0,0}\rangle_E + |0\rangle_A\,|e^0_{0,2}\rangle_E + |1\rangle_A\,|e^1_{0,2}\rangle_E) + \\ & \frac{1}{2\sqrt{2}}\,|1\rangle_B\,(|0\rangle_A\,|e^0_{1,1}\rangle_E + |1\rangle_A\,|e^1_{1,1}\rangle_E + |0\rangle_A\,|e^0_{1,3}\rangle_E + |1\rangle_A\,|e^1_{1,3}\rangle_E).\end{aligned} \tag{13}$$

Step 5. Eve passes the attacked qubit states to Alice who measures the $Z$-basis as in step 1. The probability of measuring the system in state $|0\rangle$ is $\langle\Psi|M_0M_0^{\dagger}|\Psi\rangle$ and can be represented as

$$\begin{aligned}\langle\Psi\,|0\rangle\,\langle0|\,\Psi\rangle = {} & \langle0|_B\,(\langle0|0\rangle\,\langle e^0_{0,0}|e^0_{0,0}\rangle + \langle1|0\rangle\,\langle e^1_{0,0}|e^1_{0,0}\rangle + \langle0|0\rangle\,\langle e^0_{0,2}|e^0_{0,2}\rangle + \\ & \langle1|0\rangle\,\langle e^1_{0,2}|e^1_{0,2}\rangle) + \langle1|_B\,(\langle0|0\rangle\,\langle e^0_{1,1}|e^0_{1,1}\rangle + \langle1|0\rangle\,\langle e^1_{1,1}|e^1_{1,1}\rangle + \\ & \langle0|0\rangle\,\langle e^0_{1,3}|e^0_{1,3}\rangle + \langle1|0\rangle\,\langle e^1_{1,3}|e^1_{1,3}\rangle)\,|0\rangle_B\,(\langle0|0\rangle\,\langle e^0_{0,0}|e^0_{0,0}\rangle + \\ & \langle0|1\rangle\,\langle e^1_{0,0}|e^1_{0,0}\rangle + \langle0|0\rangle\,\langle e^0_{0,2}|e^0_{0,2}\rangle + \langle0|1\rangle\,\langle e^1_{0,2}|e^1_{0,2}\rangle) + |1\rangle_B \\ & (\langle0|0\rangle\,\langle e^0_{1,1}|e^0_{1,10}\rangle + \langle0|1\rangle\,\langle e^1_{1,1}|e^1_{1,1}\rangle + \langle0|0\rangle\,\langle e^0_{1,3}|e^0_{1,3}\rangle + \\ & \langle0|1\rangle\,\langle e^1_{1,3}|e^1_{1,3}\rangle).\end{aligned} \tag{14}$$

Similarly, the probability of measuring the system in state $|1\rangle$ is $\langle\Psi|M_1M_1^{\dagger}|\Psi\rangle$ and can be represented as

$$\begin{aligned}\langle\Psi\,|1\rangle\,\langle1|\,\Psi\rangle = {} & \langle0|_B\,(\langle0|1\rangle\,\langle e^0_{0,0}|e^0_{0,0}\rangle + \langle1|1\rangle\,\langle e^1_{0,0}|e^1_{0,0}\rangle + \langle0|1\rangle\,\langle e^0_{0,2}|e^0_{0,2}\rangle + \langle1|1\rangle \\ & \langle e^1_{0,2}|e^1_{0,2}\rangle) + \langle1|_B\,(\langle0|1\rangle\,\langle e^0_{1,1}|e^0_{1,1}\rangle + \langle1|1\rangle\,\langle e^1_{1,1}|e^1_{1,1}\rangle + \langle0|1\rangle \\ & \langle e^0_{1,3}|e^0_{1,3}\rangle + \langle1|1\rangle\,\langle e^1_{1,3}|e^1_{1,3}\rangle)\,|0\rangle_B\,(\langle1|0\rangle\,\langle e^0_{0,0}|e^0_{0,0}\rangle + \langle1|1\rangle\,\langle e^1_{0,0}|e^1_{0,0}\rangle \\ & + \langle1|0\rangle\,\langle e^0_{0,2}|e^0_{0,2}\rangle + \langle1|1\rangle\,\langle e^1_{0,2}|e^1_{0,2}\rangle) + |1\rangle_B\,(\langle1|0\rangle\,\langle e^0_{1,1}|e^0_{1,1}\rangle \\ & + \langle1|1\rangle\,\langle e^1_{1,1}|e^1_{1,1}\rangle + \langle1|0\rangle\,\langle e^0_{1,3}|e^0_{1,3}\rangle + \langle1|1\rangle\,\langle e^1_{1,3}|e^1_{1,3}\rangle).\end{aligned} \tag{15}$$

By analyzing the system using Equations (14) and (15) yields:

$$\begin{aligned}\Psi = {} & |0\rangle\,\langle0|_A\,(|0\rangle\,\langle0|_B\,|e^0_{0,0}\rangle\,\langle e^0_{0,0}| + |0\rangle\,\langle0|_B\,|e^0_{0,2}\rangle\,\langle e^0_{0,2}| + |1\rangle\,\langle1|_B\,|e^0_{1,1}\rangle \\ & \langle e^0_{1,1}| + |1\rangle\,\langle1|_B\,|e^0_{1,3}\rangle\,\langle e^0_{1,3}|) + |1\rangle\,\langle1|_A\,(|0\rangle\,\langle0|_B\,|e^1_{0,0}\rangle\,\langle e^1_{0,0}| + |0\rangle\,\langle0|_B\,|e^1_{0,2}\rangle \\ & \langle e^1_{0,2}| + |1\rangle\,\langle1|_B\,|e^1_{1,1}\rangle\,\langle e^1_{1,1}| + |1\rangle\,\langle1|_B\,|e^1_{1,3}\rangle\,\langle e^1_{1,3}|).\end{aligned} \tag{16}$$

Figure 6 illustrates the steps of the collective attack executed by Eve in both the $fwd$ and $rvs$ directions through one iteration of the proposed QKD protocol.

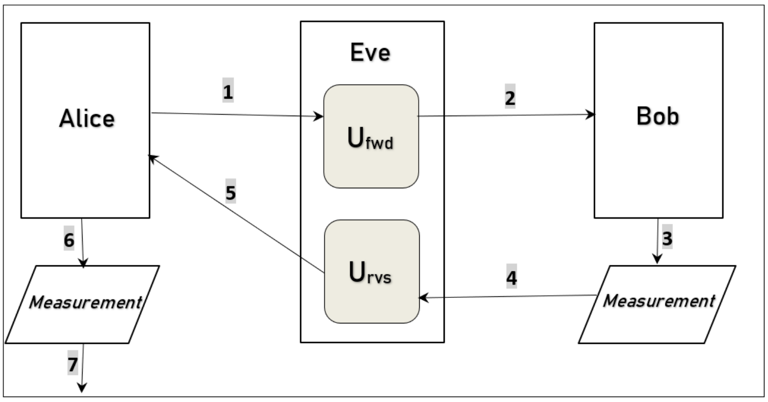


**Figure 6.** The collective attack. Eve intercepts the qubit transmitted from Alice to Bob in the forward direction using the $U_{fwd}$ operator, and Eve intercepts the qubit transmitted from Bob to Alice in the reverse direction using the $U_{rvs}$ operator.

After the *rev* attack, Eve passes the qubit to the sender who performs the measurement, and thus, the mutual information between Eve and Bob can be achieved by tracing out

Alice's system and leaving the systems of Bob and Eve as illustrated in the following equation:

$$\rho_{BE} = \frac{1}{2}\,|0\rangle\,\langle 0|_B \otimes (|e^0_{0,0}\rangle\,\langle e^0_{0,0}| + |e^1_{0,0}\rangle\,\langle e^1_{0,0}| + |e^0_{0,2}\rangle\,\langle e^0_{0,2}| + |e^1_{0,2}\rangle\,\langle e^1_{0,2}|) + \\ \frac{1}{2}\,|1\rangle\,\langle 1|_B \otimes (|e^0_{1,1}\rangle\,\langle e^0_{1,1}| + |e^1_{1,1}\rangle\,\langle e^1_{1,1}| + |e^0_{1,3}\rangle\,\langle e^0_{1,3}| + |e^1_{1,3}\rangle\,\langle e^1_{1,3}|). \tag{17}$$

### *3.3. Parameter Estimation Stage*

The two parties can estimate the interception of Eve in the $fwd$ and $rvs$ directions during the parameter estimation stage. Alice generates a set of random bits and encodes them by measuring them randomly in the $Z$ or $X$-bases. Alice then sends the encoded qubits through the shared QCC that is not secured and authorized by Eve. Before Bob receives the encoded qubits, Eve intercepts the qubits. The cases where Eve measures in a different basis from Alice's will change the qubits states. Eve then passes on the qubits to the receiver side where the qubits are measured. If Alice and Bob measure in the same basis, this means that Bob has a probability of 50% to receive the correct bit. The two parties discard the useless bits of different measured bases in the sifted key step to obtain their raw keys. Alice then chooses a random selection of her sifted key and Bob chooses the same selection part; then, they compare the selected parts to detect Eve's interception. The expectation value of a probability of the quantum state can be determined from the quantity $P_{m,b,a}$ where the parameter $m$ denotes to the encoded qubit equivalent to the bit of the message sent by Alice, and the parameters $b$ and $a$ represent the bases Bob and Alice used to measure, respectively. The probability $P_{m,b,a}$ can be used to estimate the value $\langle e^k_{i,j}|e^k_{i,j}\rangle$ which is used to calculate the amplitude of each state [26]. For example, to estimate $P_{1,1,0}$, Alice initially sends the bit 1 which according to Table 1 is encoded into the qubit state $|00\rangle + |10\rangle$ where

$$|\psi\rangle_A = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |0\rangle\,. \tag{18}$$

If Eve's measurement value after her attack in the $fwd$ direction is $|10\rangle$, then the qubit state according to (5) is changed to be

$$U_{fwd}\,|\psi\rangle_A = |\psi\rangle_{AE} = (|0\rangle\,|e_2\rangle + |1\rangle\,|e_3\rangle) \otimes |1\rangle\,, \tag{19}$$

where $\langle e_2|e_2\rangle + \langle e_3|e_3\rangle = 1$. Eve passes the qubit to Bob, and the probability that Bob measures the qubit in basis 1 is $\langle e_3|e_3\rangle$ where

$$|\psi\rangle_B \otimes |\psi\rangle_{AE} = \frac{1}{\sqrt{\langle e_3|e_3\rangle}}\,|1\rangle\,|e_3\rangle\,. \tag{20}$$

Bob transmits the qubit back to Alice whereas Eve attacks it in the $rvs$ direction. According to Equation (7), where $j = 3$, this interception changes the qubit as

$$U_{rvs}(|\psi\rangle_B \otimes |\psi\rangle_{AE}) = \frac{1}{\sqrt{\langle e_3|e_3\rangle}}(|0\rangle\,|e^0_{1,3}\rangle + |1\rangle\,|e^1_{1,3}\rangle). \tag{21}$$

Eve passes on the qubits back to Alice after the attack. The probability that Alice measures the qubit in basis 0 is

$$(\frac{1}{\sqrt{\langle e_3|e_3\rangle}})^2\,\langle e^0_{1,3}|e^0_{1,3}\rangle = \frac{\langle e^0_{1,3}|e^0_{1,3}\rangle}{\langle e_3|e_3\rangle}. \tag{22}$$

The quantity $P_{m,b,a}$ can be calculated using the conditional probability formula [27]. Providing that Alice initially sends $m$, then

$$P_{m,b,a} = Pr(A_a \cap B_b) = Pr(A_a|B_b)Pr(B_b), \tag{23}$$

where $Pr(A_a)$ is the probability of the event that Alice measures $|a\rangle$, $Pr(B_b)$ is the probability of the event that Bob measures $|b\rangle$, and $Pr(A_a|B_b)$ is the probability of the event that Alice measures $|a\rangle$ in the $rvs$ direction after Bob has already measured $|b\rangle$ in the $fwd$ direction. Now, the quantity $Pr(A_a \cap B_b)$ which denotes the probability that Alice measures $|a\rangle$ and Bob measures $|b\rangle$ can be calculated. Returning to the above example,

$$P_{1,1,0} = Pr(B_1)Pr(A_0|B_1) = \langle e_3|e_3\rangle \left( \frac{e^0_{1,3}|e^0_{1,3}}{\sqrt{\langle e_3|e_3\rangle}} \right) = \langle e^0_{1,3}|e^0_{1,3}\rangle \,. \tag{24}$$

Equations (19)–(23) can be executed to estimate other cases. Table 2 summarizes the estimation values of probabilities when Alice initially sends $|0\rangle$. Parameter estimation results when Alice initially sends $|1\rangle$ are summarized in Table 3. Eve cannot obtain any information using the ancillary particles, and if Eve wants to make the ancillary qubits distinguishable, then his attack will be detected by the two parties.

**Table 2.** Parameter estimation when Alice sends $|0\rangle$.

| $\boldsymbol{P_{m,b,a}}$ | $\boldsymbol{Pr(B_b)}$ | $\boldsymbol{Pr(A_a|B_b)}$ | $\boldsymbol{Pr(A_a \cap B_b)}$ |
|---|---|---|---|
| $P_{0,0,0}$ | $\langle e_0|e_0\rangle$ | $\frac{\langle e^0_{0,0}|e^0_{0,0}\rangle}{[\sqrt{\langle e_0|e_0\rangle}]^2}$ | $\langle e^0_{0,0}|e^0_{0,0}\rangle$ |
| $P_{0,0,1}$ | $\langle e_0|e_0\rangle$ | $\frac{\langle e^1_{0,0}|e^1_{0,0}\rangle}{[\sqrt{\langle e_0|e_0\rangle}]^2}$ | $\langle e^1_{0,0}|e^1_{0,0}\rangle$ |
| $P_{0,1,0}$ | $\langle e_1|e_1\rangle$ | $\frac{\langle e^0_{1,1}|e^0_{1,1}\rangle}{[\sqrt{\langle e_1|e_1\rangle}]^2}$ | $\langle e^0_{1,1}|e^0_{1,1}\rangle$ |
| $P_{0,1,1}$ | $\langle e_1|e_1\rangle$ | $\frac{\langle e^1_{1,1}|e^1_{1,1}\rangle}{[\sqrt{\langle e_1|e_1\rangle}]^2}$ | $\langle e^1_{1,1}|e^1_{1,1}\rangle$ |

**Table 3.** Parameter estimation when Alice sends $|1\rangle$.

| $\boldsymbol{P_{m,b,a}}$ | $\boldsymbol{Pr(B_b)}$ | $\boldsymbol{Pr(A_a|B_b)}$ | $\boldsymbol{Pr(A_a \cap B_b)}$ |
|---|---|---|---|
| $P_{1,0,0}$ | $\langle e_2|e_2\rangle$ | $\frac{\langle e^0_{0,2}|e^0_{0,2}\rangle}{[\sqrt{\langle e_2|e_2\rangle}]^2}$ | $\langle e^0_{0,2}|e^0_{0,2}\rangle$ |
| $P_{1,0,1}$ | $\langle e_2|e_2\rangle$ | $\frac{\langle e^1_{0,2}|e^1_{0,2}\rangle}{[\sqrt{\langle e_2|e_2\rangle}]^2}$ | $\langle e^1_{0,2}|e^1_{0,2}\rangle$ |
| $P_{1,1,0}$ | $\langle e_3|e_3\rangle$ | $\frac{\langle e^0_{1,3}|e^0_{1,3}\rangle}{[\sqrt{\langle e_3|e_3\rangle}]^2}$ | $\langle e^0_{1,3}|e^0_{1,3}\rangle$ |
| $P_{1,1,1}$ | $\langle e_3|e_3\rangle$ | $\frac{\langle e^1_{1,3}|e^1_{1,3}\rangle}{[\sqrt{\langle e_3|e_3\rangle}]^2}$ | $\langle e^1_{1,3}|e^1_{1,3}\rangle$ |

The key rate against collective attack [28] can be calculated using the following equation: $r(\rho_{ABE}) = I(A : B) - \chi(B : E)$ where $I(A : B) = H(A) + H(B) - H(A,B)$ and $\chi(B : E) = H(B) + S(E) - S(B,E)$. The mutual information denoted by $I(A : B)$ is a measure of the correlations between two systems; it is used to quantify the amount of bits that Alice and Bob have to discard from their mutual data for error correction [14].

The quantum mutual information between Bob and Eve that quantifies the amount of privacy amplification that is necessary to eliminate the information obtained by Eve is represented by $\chi(B : E)$. From the conditional Shannon entropy,

$$H(A|B) = H(A,B) - H(B), \text{ then }, I(A:B) = H(A) - H(A|B) \tag{25}$$

In the case that Alice and Bob estimate the error rate in the $Z$-basis, the probability that Alice's raw key bit is 0 equals

$$P_{m,b,0} = P_{0,0,0} + P_{0,1,0} + P_{1,0,0} + P_{1,1,0}, H(A) = H(P_{m,b,0}, 1 - P_{m,b,0}). \tag{26}$$

The quantity $H(A|B)$ can be computed using the combination of estimated probabilities of Alice's raw key bit and Bob's raw key bit where

$$P_{m,0,0} = \frac{1}{2}(P_{0,0,0} + P_{1,0,0}), P_{m,0,1} = \frac{1}{2}(P_{0,0,1} + P_{1,0,1}), \tag{27}$$

$$P_{m,1,0} = \frac{1}{2}(P_{1,1,0} + P_{0,1,0}), P_{m,1,1} = \frac{1}{2}(P_{0,1,1} + P_{1,1,1}). \tag{28}$$

By analyzing out the system of (13), $\rho_{BE}$ can be represented as follows

$$\frac{1}{2}|0\rangle\langle 0| \otimes (|e^0_{0,0}\rangle\langle e^0_{0,0}| + |e^1_{0,0}\rangle\langle e^1_{0,0}| + |e^0_{0,2}\rangle\langle e^0_{0,2}| + |e^1_{0,2}\rangle\langle e^1_{0,2}|) + \frac{1}{2}|1\rangle\langle 1| \otimes (|e^0_{1,1}\rangle\langle e^0_{1,1}| + |e^1_{1,1}\rangle\langle e^1_{1,1}| + |e^0_{1,3}\rangle\langle e^0_{1,3}| + |e^1_{1,3}\rangle\langle e^1_{1,3}|) \tag{29}$$

The Von Neumann entropy $S(B,E) = S(\rho_{BE})$ can then be computed as

$$H(\frac{1}{2}\langle e^0_{0,0}|e^0_{0,0}\rangle + \frac{1}{2}\langle e^1_{0,0}|e^1_{0,0}\rangle + \frac{1}{2}\langle e^0_{0,2}|e^0_{0,2}\rangle + \frac{1}{2}\langle e^1_{0,2}|e^1_{0,2}\rangle + \frac{1}{2}\langle e^0_{1,1}|e^0_{1,1}\rangle + \frac{1}{2}\langle e^1_{1,1}|e^1_{1,1}\rangle + \frac{1}{2}\langle e^0_{1,3}|e^0_{1,3}\rangle + \frac{1}{2}\langle e^1_{1,3}|e^1_{1,3}\rangle) \tag{30}$$

From Tables 2 and 3, the equation can be rewritten as

$$S(\rho_{BE}) = H(P_{0,0,0} + P_{0,0,1} + P_{1,0,0} + P_{1,0,1} + P_{0,1,0} + P_{0,1,1} + P_{1,1,0} + P_{1,1,1}) \tag{31}$$

that can be estimated and computed by the two parties Alice and Bob. From the joint von Neumann entropy,

$$S(B,E) = S(\rho_{BE}) = H(B) + \sum P(B)S(\rho^B_E), H(B) - S(B,E) = -\sum P(B)S(\rho^B_E), \tag{32}$$

The mutual information between B and E can be deduced from the following equation [29]

$$\chi(B:E) = S(\rho_E) - \sum P(B)S(\rho^B_E) \tag{33}$$

Finally, this equation can be rewritten in terms of quantities on systems A and B as follows

$$\chi(B:E) = S(\rho_{AB}) - \sum P(B)S(\rho_B), \tag{34}$$

and the initial state $\rho^{ABE}$ is

$$\rho^{ABE} = \sum_{j=1}^{n} P_j |j\rangle\langle j|^A \otimes \sigma^{BE}_j \tag{35}$$

where each $\sigma_j$ is a Hermitian operator.

## 4. Results and Discussion

The proposed QKD protocol can be explored in a straightforward manner by analyzing the steps of the protocol, as shown in Figure 4. The steps of the proposed QKD protocol are statistically analyzed and simulated using the Qiskit software [30]. The simulation circuit has $five$ quantum registers; the first three qubits are under the control of Alice, while the fourth and fifth qubits are under Bob's control. Alice prepares $|\Phi\rangle$ and communicates with Bob using the shared public QCC through the asymmetrical two-qubit teleportation scheme. Bob receives the two-qubit state and measures it; then, he prepares a new state based on his measurement. Alice reveals the symmetry transformation she used for encoding the string $a$. The two parties start the protocol with $N$ bits and check the communication to detect the existence of eavesdropping.

The generation of a raw key exchanged between the two parties is executed where the qubits are exchanged between the sender and the receiver through unsecured quantum channel, and eavesdropping attacks are expected to occur. Figure 7 illustrates the circuit implementation of the $fwd$ direction where Alice transmits a bit value $\in \{0, 1\}$ where the state $|00\rangle + |10\rangle$ or $|01\rangle + |11\rangle$ are prepared, respectively, to be sent through the communication channel.

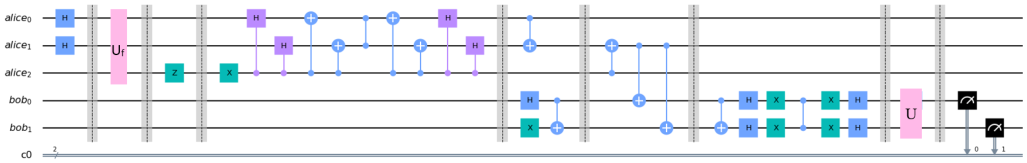
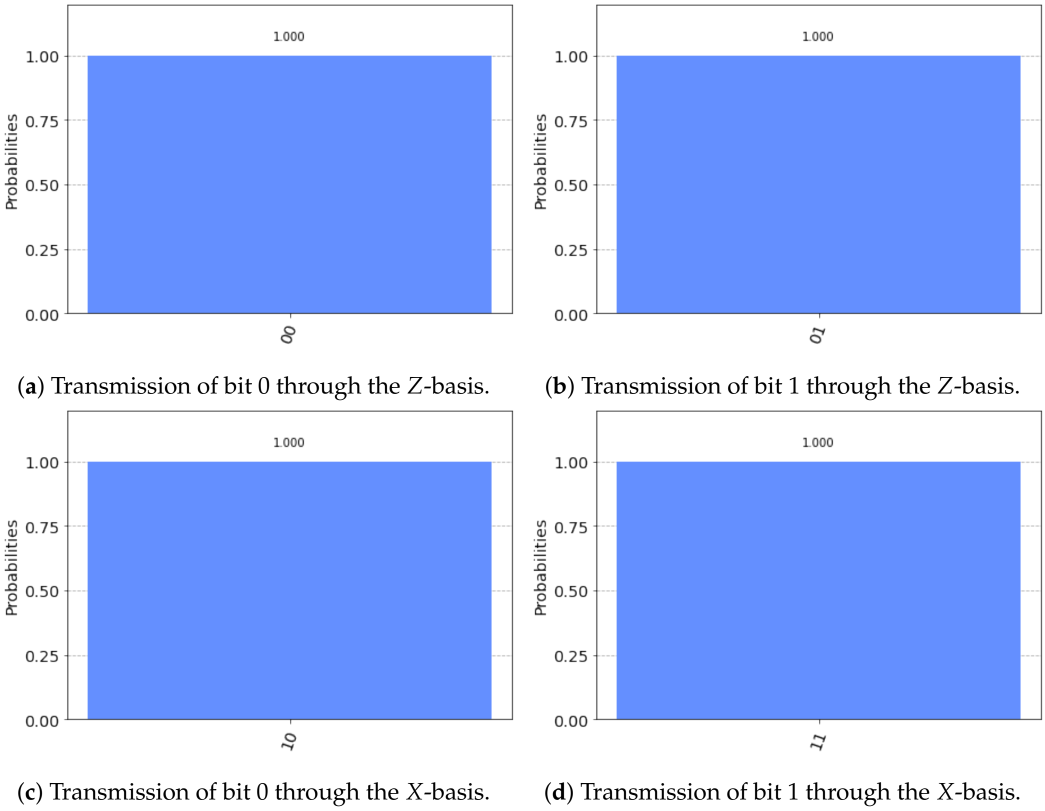


**Figure 7.** The circuit implementation of the forward direction in the proposed QKD protocol.

If Alice transmits a bit of the message after encoding it into a 2-qubits and there is no eavesdropping attack, then the qubit will be received as it is. Figure 8a,b present the measurement values when Alice transmits $|00\rangle + |10\rangle$ and unitary transformations $U_0$ and $U_1$, respectively. Figure 8c,d present the measurement values when Alice transmits $|01\rangle + |11\rangle$ and unitary transformations $U_0$ and $U_1$, respectively.



(**a**) Transmission of bit 0 through the $Z$-basis. (**b**) Transmission of bit 1 through the $Z$-basis.

(**c**) Transmission of bit 0 through the $X$-basis. (**d**) Transmission of bit 1 through the $X$-basis.

**Figure 8.** The measurement value performed by Bob in the $fwd$ direction where the first classical register represents the bit value transmitted by Alice, whereas the second classical register represents the basis used in preparing the qubit.

In the case of eavesdropping interception, the quantum channel is not secured, and the eavesdropper executes trials to measure the transmitted qubit before the receiver performs his measurement. Figure 9 illustrates the circuit implementation of the $fwd$ direction in the case of eavesdropper interception.

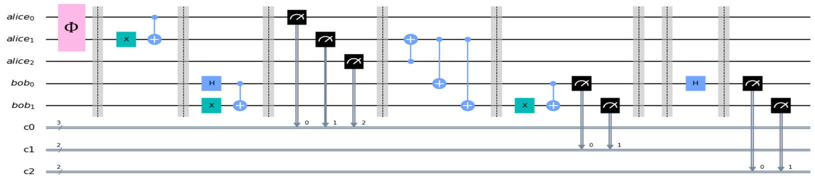
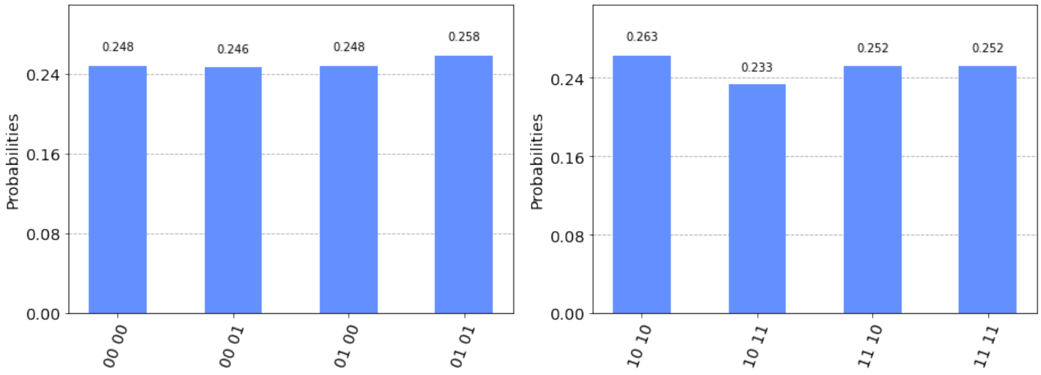


**Figure 9.** The circuit implementation of the forward direction in the case of direct measurement interception.

Eve measures the qubit state before reaching Bob, and this reduces the probability value of receiving the exact qubit state to be approximately half. The state of the qubit will be changed to $|00\rangle$ or $|10\rangle$ if Alice prepared a $Z$-basis state which is presented in Figure 10a, and if Alice prepared a $X$-basis state, then the state will be changed to be $|01\rangle$ or $|11\rangle$, which is presented in Figure 10b.



(**a**) Eve's interception of $Z$-basis state.

(**b**) Eve's interception of $X$-basis state.

**Figure 10.** The measurement values in the case of eavesdropping interception in the $fwd$ direction where the first and second classical registers denote Bob's measurement values whereas the third and fourth classical registers denote Eve's measurement values.

After all the qubits are measured, Alice and Bob reveal the information about their raw keys through a classical communication channel. Bits with law correlation are then discarded so that the two parties share a correlated sifted key. There are two reasons for mismatching between the secret keys of the two parties: the first is the existence of noise in the communication channel, and the other reason is the interception of Eve using an attack; hence, the two parties discard these bits from the key.

The proposed protocol is compared to the protocols presented in [15,17] with respect to the qubit efficiency. The qubit efficiency $\lambda$ [31] is the ratio between the total number of the key bits established to the total number of qubits generated in the protocol and can be represented by the following equation

$$\lambda = \frac{n_c}{n_q}, \tag{36}$$

where $n_c$ represents the total number of key bits established, and $n_q$ denotes the total number of the generated qubits. In the protocol presented in [17], the total number of consumed quantum states to establish $n$ raw key bits can be approximately calculated by the following equation $N = r(6n(1+\delta) + 6n(1+\delta)/2)$, where $r$ denotes the initial quantum resource being equal to 2 because this protocol uses a two-qubit entangled state, and $\delta$ is a small parameter greater than 0. In [17], Alice prepares $6n(1+\delta)$ and Bob produces $6n(1+\delta)/2$, so $N = 2(6n+3n) = 18n$, and hence, the qubit efficiency $= \frac{n}{18n} = \frac{1}{18}$. The qubit efficiency of the protocol presented in [15] has the value $\frac{1}{24}$, where this protocol uses the properties of single photons and the Bell measurement. In the proposed protocol, in order to establish $n$ raw key bits, Alice initially prepares $N$ qubits in the $fwd$ direction which is followed by using $N/2$ qubits temporarily to mark the required states in performing the oracle and partial diffusion quantum operators. The same $\frac{N}{2}$ qubits will be used for executing the teleportation $\mathcal{T}$ scheme where an entanglement in a $GHZ$ state is established with Bob. In the $fwd$ direction, Bob prepares $N$ qubits; then, after his measurement, he prepares $N$ qubits in the $rvs$ direction that are used in the sifting operation. The qubit efficiency for this protocol is $\lambda = \frac{n}{\frac{7N}{2}} = \frac{2n}{7(4+\delta)n} \approx \frac{1}{14}$, where $\delta$ is a small parameter greater than 0. The protocol presented by Xu et al. [18] proved the security against collective attacks in the device-independent QKD protocol with random post selection, whereas our protocol successfully proved the security against collective attack with multi-state random selection in addition to using the partial diffusion quantum operator and unitary transformation operators. Table 4 compares some important features among the protocol of Lin et al. [15], that of Pan et al. [17], and the proposed half-duplex bidirectional QKD protocol.

**Table 4.** Comparison of [15,17], and our proposed half-duplex bidirectional QKD protocol.

| | **Lin et al. Protocol** | **Pan et al. Protocol** | **Proposed Protocol** |
|---|---|---|---|
| Initial quantum resource | Reflection single photons | Two-physical qubit entangled state | Superposition of two states entangled with a GHZ state |
| Number of initial quantum states | Two | Three | Two |
| Qubit efficiency | $\frac{1}{24}$ | $\frac{1}{18}$ | $\frac{1}{14}$ |

One of the advantages of this approach is that the bits and bases are represented by 2-qubit states that are hidden through the communication channel using the partial diffusion operator, and this increases the ratio between the total number of the shared qubits to the number of the consumed qubits and hence increases the qubit efficiency. Furthermore, the proposed QKD protocol provides a parameter estimation that can be completely estimated under the control of the two parties. In the future work, the security of the protocol against other eavesdropping attacks can be addressed; this might be mitigated using more advanced quantum operators and schemes.

## 5. Conclusions

Despite the fact that QKD is costly to be implemented due to the high number of required qubits to realize an efficient protocol for real applications, it is considered as one of the main important use cases in the near future for the second quantum revolution. In this work, we propose a half-duplex bidirectional QKD protocol and prove its security against collective attacks. We have addressed two main key points that count toward the impact of the proposed protocol: encoding the information and raising the qubit efficiency. For the first one, we have shown how the use of a bidirectional quantum communication enables two parties to improve the security of QKD. Bits and bases are represented by two-qubit states which are hidden through their transmission using the partial diffusion quantum operator. The Grover's quantum operator is applied once to restore the hidden states. The different security layers implemented by the mentioned symmetry transformations induced by unitary managed to make it more robust against attackers. For the second one, a powerful asymmetrical two-qubit teleportation scheme is used for transmitting the two-qubit states in the forward and reverse direction of the protocol. The teleportation scheme consists of five particles: Alice comprises the first three particles, which are also used in performing the partial diffusion operator, and the third particle is entangled with Bob in a GHZ state. The principles of probability theory are used to estimate any eavesdropper interception using the conditional Shannon entropy associated with von Neumann entropy. Compared to other protocols, the proposed scheme does have a higher qubit efficiency ratio. Despite the fact that this protocol managed to detect Eve's presence, further analytical analysis is required to determine the exact accuracy of detecting an eavesdropper especially when the diffusion operator is incorporated. Moreover, as a future direction, enhancing this protocol against noisy quantum channels would be an interesting research direction.

**Author Contributions:** Project administration, A.Y.; methodology, A.Y. and W.G.E.-S.; validation, A.Y., M.K. and W.G.E.-S.; conceptualization, M.Z.R. and M.K.; formal analysis, M.K.; investigation, A.Y. and M.K.; data curation, M.K. and A.Y.; writing the manuscript, M.K.; All authors contributed to the data collection, discussed the results and reviewed the manuscript. All authors have read and agreed to the published version of the manuscript.

**Funding:** This research received no external funding.

**Data Availability Statement:** The data presented in this study are available within the article.

**Acknowledgments:** The authors would like to thank Kareem H. El-Safty from Wigner Research Centre for Physics, Budapest, Hungary for his valuable insights and comments.

**Conflicts of Interest:** The authors declare no conflict of interest in this article.

## References

1. El-Mahalawy, A.M.; El-Safty, K.H. Classical and quantum regression analysis for the optoelectronic performance of NTCDA/p-Si UV photodiode. *Optik* **2021**, *246*, 167793. [CrossRef]
2. Okrut, O.; Cannon, K.; El-Safty, K.H.; Elsokkary, N.; Khan, F.S. Calculating Nash Equilibrium on Quantum Annealers. *arXiv* **2021**, arXiv:2112.12583.
3. Nagata, K.; Diep, D.N.; Nakamura, T. Quantum cryptography based on an algorithm for determining simultaneously all the mappings of a logical function. In *Simplified Quantum Computing with Applications*; IOP Publishing: Bristol, UK, 2022; pp. 9-1–9-11. [CrossRef]
4. Granelli, F.; Bassoli, R.; Nötzel, J.; Fitzek, F.H.; Boche, H.; da Fonseca, N.L. A Novel Architecture for Future Classical-Quantum Communication Networks. *Wirel. Commun. Mob. Comput.* **2022**, *2022*, 3770994. [CrossRef]
5. Frey, M.; Bjelaković, I.; Nötzel, J.; Stańczak, S. Semantic Security with Infinite Dimensional Quantum Eavesdropping Channel. *arXiv* **2022**, arXiv:2205.07663.
6. Tabi, Z.; El-Safty, K.H.; Kallus, Z.; Hága, P.; Kozsik, T.; Glos, A.; Zimborás, Z. Quantum optimization for the graph coloring problem with space-efficient embedding. In Proceedings of the 2020 IEEE International Conference on Quantum Computing and Engineering (QCE), Denver, CO, USA, 12–16 October 2020; pp. 56–62.
7. Zhang, W.; van Leent, T.; Redeker, K.; Garthoff, R.; Schwonnek, R.; Fertig, F.; Eppelt, S.; Scarani, V.; Lim, C.C.W.; Weinfurter, H. Experimental device-independent quantum key distribution between distant users. *arXiv* **2021**, arXiv:2110.00575.
8. Nielsen, M.A.; Chuang, I.L. *Quantum Computation and Quantum Information: 10th Anniversary Edition*; Cambridge University Press: Cambridge, UK, 2010. [CrossRef]
9. Guo, P.L.; Dong, C.; He, Y.; Jing, F.; He, W.T.; Ren, B.C.; Li, C.Y.; Deng, F.G. Efficient quantum key distribution against collective noise using polarization and transverse spatial mode of photons. *Opt. Express* **2020**, *28*, 4611–4624. [CrossRef]
10. Seminar, P. *Einstein, 1905–2005*; Birkhäuser: Basel, Switzerland, 2005; Volume 47, ISBN 978-3-7643-7435-8. [CrossRef]
11. Bennett, C.H.; Brassard, G. Quantum cryptography: Public key distribution and coin tossing. *Theor. Comput. Sci.* **2014**, *560*, 7–11. [CrossRef]
12. Grangier, P. Experiments with Single Photons. *Prog. Math. Phys.* **2006**, *47*, 135–149. [CrossRef]
13. Shi, P.; Li, N.; Wang, S.; Liu, Z.; Ren, M.; Ma, H. Quantum Multi-User Broadcast Protocol for the "Platform as a Service" Model. *Sensors* **2019**, *19*, 5257. [CrossRef]
14. Zhang, W.; Qiu, D.; Mateus, P. A single-state semi-quantum key distribution protocol and its security proof. *Int. J. Quantum Inf.* **2017**, *18*, 2050013. [CrossRef]
15. Lin, P.H.; Tsai, C.W.; Hwang, T. Mediated Semi-Quantum Key Distribution Using Single Photons. *Annalen der Physik* **2019**, *531*, 1800347. [CrossRef]
16. Jain, N.; Chin, H.M.; Mani, H.; Lupo, C.; Nikolic, D.S.; Kordts, A.; Pirandola, S.; Pedersen, T.B.; Kolb, M.; Ömer, B.; et al. Practical continuous-variable quantum key distribution with composable security. *Nat. Commun.* **2021**, *13*, 4740. [CrossRef]
17. Pan, X. Semi-Quantum Key Distribution Protocol with Logical Qubits over the Collective-Rotation Noise Channel. *Int. J. Theor. Phys.* **2022**, *61*, 77. [CrossRef]
18. Xu, F.; Zhang, Y.Z.; Zhang, Q.; Pan, J.W. Device-Independent Quantum Key Distribution with Random Postselection. *Phys. Rev. Lett.* **2022**, *128*, 110506. [CrossRef]
19. Lizama-Pérez, L.A.; López-Romero, J.M. Perfect Reconciliation in Quantum Key Distribution with Order-Two Frames. *Symmetry* **2021**, *13*, 1672. [CrossRef]
20. Younes, A. Enhancing the security of quantum communication by hiding the message in a superposition. *Inf. Sci.* **2011**, *181*, 329–334. [CrossRef]
21. Chen, Z.; Zhang, Y.; Wang, X.; Yu, S.; Guo, H. Improving Parameter Estimation of Entropic Uncertainty Relation in Continuous-Variable Quantum Key Distribution. *Entropy* **2019**, *21*, 652. [CrossRef]

22. Cardoso-Isidoro, C.; Delgado, F. Shared Quantum Key Distribution Based on Asymmetric Double Quantum Teleportation. *Symmetry* **2022**, *14*, 713. [CrossRef]
23. Younes, A.; Rowe, J.; Miller, J. Enhanced quantum searching via entanglement and partial diffusion. *Phys. D Nonlinear Phenom.* **2008**, *237*, 1074–1078. [CrossRef]
24. Grover, L.K. A Fast Quantum Mechanical Algorithm for Database Search. In Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing, STOC '96, Philadelphia, PA, USA, 22–24 May 1996; Association for Computing Machinery: New York, NY, USA, 1996; pp. 212–219. [CrossRef]
25. Khawasik, M.; Elsayed, W.; Rashad, M.; Younes, A. A Secured Quantum Two-Bit Commitment Protocol for Communication Systems. *IEEE Access* **2022**, *10*, 50218–50226. [CrossRef]
26. Li, W.; Zhao, S. Upper Bound of Collective Attacks on Quantum Key Distribution. *arXiv* **2019**, arXiv:1909.12584.
27. Krawec, W. High-Dimensional Semiquantum Cryptography. *IEEE Trans. Quantum Eng.* **2020**, *1*, 1–17. [CrossRef]
28. Devetak, I.; Winter, A. Distillation of secret key and entanglement from quantum states. *Proc. R. Soc. A Math. Phys. Eng. Sci.* **2005**, *461*, 207–235. [CrossRef]
29. Boes, P.; Eisert, J.; Gallego, R.; Müller, M.P.; Wilming, H. Von Neumann Entropy from Unitarity. *Phys. Rev. Lett.* **2019**, *122*, 210402. [CrossRef]
30. Aleksandrowicz, G.; Alexander, T.; Barkoutsos, P.; Bello, L.; Ben-Haim, Y.; Bucher, D.; Cabrera-Hernández, F.J.; Carballo-Franquis, J.; Chen, A.; Chen, C.-F.; et al. *Qiskit: An Open-Source Framework for Quantum Computing*; Zenodo: Geneva, Switzerland, 2019. [CrossRef]
31. Yang, C.W.; Hwang, T. Quantum dialogue protocols immune to collective noise. *Quantum Inf. Process.* **2013**, *12*, 2131–2142. [CrossRef]