INTERNATIONAL JOURNAL OF INFORMATION SECURITY SCIENCE
E. Çağlar et al., Vol.12, No.2, pp.22-41.
https://doi.org/10.55859/ijiss.1264169

Secure Communication Based On Key Generation With Quantum Reinforcement Learning

Ercan Çağlar[1] , İhsan Yılmaz[2]

[1]Department of Computer and Instructional Technologies Education, Çanakkale Onsekiz Mart University, Çanakkale, Turkey
[2]Department of Computer Engineering, Çanakkale Onsekiz Mart University, Çanakkale, Turkey
Corresponding Author: ercaglar@comu.edu.tr

Research Paper Received: 12.03.2023 Revised: 07.06.2023 Accepted: 19.06.2023

Abstract—Data security and secure communication is one of the most important issues of today. In this study, a quantum-based method for secure communication is proposed. In the proposed method, the necessary secret key in communication is generated locally by each participant through quantum gates. The quantum gates are taught by using quantum reinforcement learning (QRL). The proposed study is simulated using the Qiskit library for Python. The proposed study performs the learning action with an accuracy of 87.95% for 195 gates, 85.47% for 128 gates, 83.59% for 64 gates, 76.25% for 32 gates. As the key size increases, the performance of the method increases. The participants do not share the secret key in the presented method. Thus, the communication becomes more secure. In the study, the method is also examined in terms of security. Security analysis shows that the proposed method provides secure communication.

Keywords—quantum reinforcement learning, key generation, quantum key distribution, quantum cryptography

1. Introduction

Data security and secure communication is one of the most important issues of today. The secret keys are used to encrypt and decrypt any message in encryption methods. Different secret keys must be used for each communication. Sharing the secret key used in communication can cause security problems. Generating secret keys locally with the machine learning (ML) methods will offer a solution to security threats from key sharing.

There are three types of learning methods for machine learning such as supervised, unsupervised and reinforced learning (RL). The input and output data pairs are used in supervised learning; unsupervised learning uses only input data. The RL uses a scalar value called a reward to evaluate input-output data pairs [1]. The quantum version of RL, quantum reinforcement learning (QRL), is used in

many fields and to improve the performance of the Quantum Key Distribution (QKD) methods. There are many studies in the literature that use QKD for classification. Ren et al. [2] utilised the Random Forest classification method in QKD. Zhang et al.[3] suggested a supporting machine learning MDI-QKD system. Chin et al. [4] developed a machine learning method based on Bayesian inference for the estimation of phase noise in CV-QKD systems. Giordano and Martin-Delgado [5] proposed an artificial intelligence algorithm with RL to generate an entangled state. There are few studies on QRL in the literature [6], [7], [8]. Albarr´an-Arriagada et al.[9] designed a measurement-based adaptation protocol with QRL. A fair comparison of RL and QRL is given in references. [10], [11].

In this study, a method using QRL is proposed to generate the secret key locally. The quantum gates used in secret key generation are taught by any participant to another participant using QRL. The learning action is performed by selecting from the quantum gates Identity (I), Not (X) and CNOT. These quantum gates are used to generate the key. Both participants apply the same quantum gates to the quantum state. They perform a quantum measurement operation on the quantum state to obtain the secret key. It is a prerequisite for the method that the participants know which quantum gates to apply. In order for the secret key to occur in both participants, the participants must apply the same quantum gates to the quantum state. The quantum measurement is performed on the quantum state to obtain the secret key. The participants need to know in advance which quantum gates they will implement before key generation, and the quantum gates are learned using by QRL. One of the participants teaches the quantum gates applied to the other using the QRL method. The learning is achieved via the quantum channel based on the principles of quantum mechanics. Some quantum gates may be incorrect due to the superposition principle of the quantum mechanics. The quantum gates are applied for two different error correction operations, and then, the incorrect quantum gates are ignored. After error correction operations and ignored gates, the same quantum gates will be obtained in both participants. Secure communication is provided when the quantum gates of both parties are the same.

The rest of the paper is organised as follows: Section 2 presents preliminary information about the rotation gates. The Key Generation with Quantum Reinforcement Learning algorithm for secret key transmission is described in Section 3. The proposed secure communication method is presented in Section 4. Section 5 discusses the security analysis of the proposed method. Finally, Section 6 provides a conclusion.

2. Preliminaries

In this section, preliminary information about the quantum rotation gates is given. The quantum rotation gates are used to prepare the superposition of the quantum state and reobtain the initial state. The R_y gate is a single qubit rotation around the y axis. The R_y gate is shown as follows:

$$R_y(\theta) = \begin{pmatrix} \cos\frac{\theta}{2} & -\sin\frac{\theta}{2} \\ \sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{pmatrix} \tag{1}$$

Let us show the gate R_y for angles $\frac{\pi}{3}$ and $-\frac{\pi}{3}$.

$$R_y\left(\frac{\pi}{3}\right) = \begin{pmatrix} \cos\frac{\pi}{6} & -\sin\frac{\pi}{6} \\ \sin\frac{\pi}{6} & \cos\frac{\pi}{6} \end{pmatrix} = \begin{pmatrix} \frac{\sqrt{3}}{2} & -\frac{1}{2} \\ \frac{1}{2} & \frac{\sqrt{3}}{2} \end{pmatrix} \tag{2}$$

$$\begin{aligned} R_y\left(-\frac{\pi}{3}\right) &= \begin{pmatrix} \cos\left(-\frac{\pi}{6}\right) & -\sin\left(-\frac{\pi}{6}\right) \\ \sin\left(-\frac{\pi}{6}\right) & \cos\left(-\frac{\pi}{6}\right) \end{pmatrix} \\ &= \begin{pmatrix} \cos\frac{\pi}{6} & \sin\frac{\pi}{6} \\ -sin\frac{\pi}{6} & \cos\frac{\pi}{6} \end{pmatrix} = \begin{pmatrix} \frac{\sqrt{3}}{2} & \frac{1}{2} \\ -\frac{1}{2} & \frac{\sqrt{3}}{2} \end{pmatrix} \end{aligned} \tag{3}$$

Let us show the superposition state by applying the $R_y\left(\frac{\pi}{3}\right)$ to the $|0\rangle$

$$\begin{aligned} R_y\left(\frac{\pi}{3}\right)|0\rangle &= \begin{pmatrix} \frac{\sqrt{3}}{2} & -\frac{1}{2} \\ \frac{1}{2} & \frac{\sqrt{3}}{2} \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} \\ &= \begin{pmatrix} \frac{\sqrt{3}}{2} \\ \frac{1}{2} \end{pmatrix} = \frac{\sqrt{3}}{2}|0\rangle + \frac{1}{2}|1\rangle \end{aligned} \tag{4}$$

Let us obtain the initial state by applying the $R_y\left(-\frac{\pi}{3}\right)$ to the $\frac{\sqrt{3}}{2}|0\rangle + \frac{1}{2}|1\rangle$.

$$\begin{aligned} R_y\left(-\frac{\pi}{3}\right)\left(\frac{\sqrt{3}}{2}|0\rangle + \frac{1}{2}|1\rangle\right) &= \begin{pmatrix} \frac{\sqrt{3}}{2} & \frac{1}{2} \\ -\frac{1}{2} & \frac{\sqrt{3}}{2} \end{pmatrix} \begin{pmatrix} \frac{\sqrt{3}}{2} \\ \frac{1}{2} \end{pmatrix} \\ &= \begin{pmatrix} \frac{3}{4} + \frac{1}{4} \\ -\frac{\sqrt{3}}{2} + \frac{\sqrt{3}}{2} \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} = |0\rangle \end{aligned} \tag{5}$$

3. Key Generation with Quantum Reinforcement Learning

The QRL consists of three main elements, agent, state space and reward, as in conventional RL. Factors in the Markov Decision Process (MDP) to create a QRL system are represented through the principles of quantum mechanics. States and actions in RL algorithms are represented as orthogonal bases in QRL. In the QRL, they are called eigen states and eigen actions[1]. In our study, according to MDP, state space S is represented by two qubits. Action space A is represented by gates {Identity (I), NOT (X) and CNOT}, and r is represented by reward function {0,1}. Each choice is independent and does not affect another. Two qubit states are used to learn one gate. Therefore, the 2n-qubit states are used to learn n gates.

This study utilises a secure quantum channel for data transmission between two parties. It is assumed that there is no data loss in the quantum channel. We will call the sending party initiating the communication, "Alice"; the receiving party, "Bob"; and the third party intervening and listening to the communication, "Eve".

Alice and Bob follow the steps bellow for the QRL (Figure 1). The algorithm works as follows:

Step 1: Alice prepares 2n quantum states, selects n gates, and determines 2n angles for rotation.

Step 2: Alice applies the rotation gate to the quantum state using a different angle for each qubit. Alice sends the superposition of quantum state to Bob (Figure 1a).

Step 3: Bob selects n candidate gates and applies the gates to the quantum state that Alice sends. (Figure 1b).

Step 4: Alice applies her gates to the quantum state. The qubits in which Bob and Alice apply the same gate become the quantum state in Fig. 1a. If a gate is applied to the quantum state twice, the quantum state turns back to the initial state. (Figure 1c).

Step 5: Alice applies the rotation gate with negative angles to the quantum state. The qubits to which Bob and Alice apply the same gate become as they were initially prepared (Figure 1d).

Step 6: After Alice measures the quantum state, she compares the measurement result with the data set she used to create the quantum state. According to the measurement result, the reward is determined (Figure 1e).

3.1. Teaching the gates required for Key Generation

In this section, the gates used to generate the secret key, are taught to Bob with QRL by Alice. Each gate is taught independently of the others. There are n different learning actions for n gates. Alice determines the n gates she will use to generate the secret key from the {I, X, CNOT} gates. The

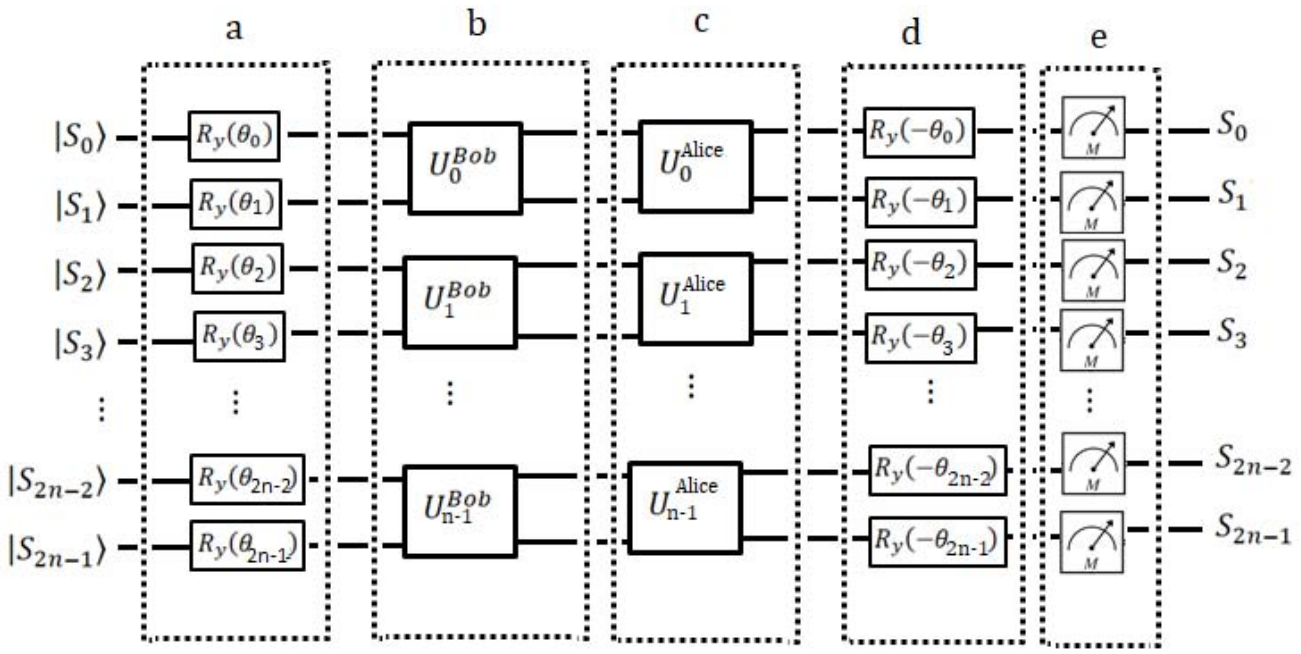

Figure 1. a. Application of rotation gates to quantum states by Alice, b. Bob's application of candidate gates to quantum states sent by Alice. c. Alice's application of her gates to quantum states sent after being modified by Bob, d. Application of rotation gates with negative angles to quantum states by Alice, e. Measurement of quantum states by Alice.

gates can be shown as follows:

$$U_i^{Alice} = u_0, u_1, .., u_{n-1} \;;\quad i = 1...n-1 \qquad u_i \;\in \{I, X, CNOT\} \tag{6}$$

Bob randomly selects n candidate gates from {I, X, CNOT} gates. The gates can be shown as follows:

$$U_i^{Bob} = u_0^b, u_1^b, \ldots, u_{n-1}^b \;;\quad i = 1...n-1 \qquad u_i \;\in \{I, X, CNOT\} \tag{7}$$

Alice prepares a 2n qubit quantum state for the n gates as follows:

$$S = s_0 s_1 \ldots s_{2n-1} \;;\; s_i \;\in \{0,1\}\,; i = 0...2n-1 \qquad |\psi\rangle = |s_0 s_1 s_2 s_3 \ldots s_{2n-2} s_{2n-1}\rangle \tag{8}$$

Alice obtains the superposition state with different amplitudes by applying 2n Rotation gates at different angles to the quantum state as follows:

$$\begin{aligned} |\psi'\rangle = R_y(\theta)\,|\psi\rangle &= \bigotimes_{i=0}^{2n-1} R_y(\theta_i)\,|s_i\rangle \\ &= R_y(\theta_0)\,|s_0\rangle \bigotimes R_y(\theta_1)\,|s_1\rangle \bigotimes \\ &\ldots \bigotimes R_y(\theta_{2n-1})\,|s_{2n-1}\rangle \\ &= |s_0' s_1' s_2' \ldots s_{2n-1}'\rangle \quad s' = \alpha\,|0\rangle + \beta\,|1\rangle \end{aligned} \tag{9}$$

Alice sends the obtained quantum state $|\psi'\rangle$ to Bob. When a superposition quantum state as in Equation (9) is measured, the measurement result is either 0 or 1. If Eve or Bob measures state $|\psi'\rangle$, they cannot obtain state $|\psi\rangle$ as in Equation (8). Hence the data security is ensured.

$$\begin{aligned}|\psi^{''}\rangle = U_i^{Bob}|\psi'\rangle &= \bigotimes_{i=0}^{n-1} u_i^b |s_{2i}^{'} s_{2i+1}^{'}\rangle \\ &= u_0^b |s_0^{'} s_1^{'}\rangle \bigotimes u_1^b |s_2^{'} s_3^{'}\rangle \bigotimes \\ &\quad ... \bigotimes u_{n-1}^b |s_{2n-2}^{'} s_{2n-1}^{'}\rangle \\ &= |s_0^{'} s_1^{''} s_2^{'} s_3^{''} .. s_{2n-2}^{'} s_{2n-1}^{''}\rangle\end{aligned} \tag{10}$$

Bob applies the candidate gates to the quantum state $|\psi'\rangle$ as in Equation (10). $|s_0^{'}\rangle, |s_2^{'}\rangle, \ldots, |s_{2n-2}^{'}\rangle$ qubits are defined as control qubits. $|s_1^{'}\rangle, |s_3^{'}\rangle, \ldots, |s_{2n-1}^{'}\rangle$ qubits are defined as target qubits. Since the control qubit will not be used for the I and X gates, the gates are applied as I$\bigotimes$I and I$\bigotimes$X to the 2-qubit state.

Bob sends the obtained quantum state $|\psi^{''}\rangle$ to Alice. Alice applies her own gates to the quantum state $|\psi^{''}\rangle$ as follows:

$$\begin{aligned}|\psi^{'''}\rangle = U_i^{Alice}|\psi^{''}\rangle &= \bigotimes_{i=0}^{n-1} u_i |s_{2i}^{'} s_{2i+1}^{''}\rangle \\ &= u_0 |s_0^{'} s_1^{''}\rangle \bigotimes u_1 |s_2^{'} s_3^{''}\rangle \bigotimes \\ &\quad ... \bigotimes u_{n-1} |s_{2n-2}^{'} s_{2n-1}^{''}\rangle \\ &= |s_0^{'} s_1^{'''} s_2^{'} s_3^{'''} .. s_{2n-2}^{'} s_{2n-1}^{'''}\rangle\end{aligned} \tag{11}$$

Alice obtains the quantum state $|\psi^{'''}\rangle$ as in Equation (11). Quantum gates are reversible gates. By applying the same gate to a quantum state twice, we can bring the quantum state to its initial state. When the same gates are selected by Alice and Bob, the quantum states will become as in Equation (9). Selecting different gates means that a different quantum state will occur than in Equation (9). In other words, if $s_1^{'''}$ is equal to $s_1^{'}$, the same gate is used. If $s_1^{'''}$ is not equal to $s_1^{'}$, a different gate is used. In the next step, Alice applies the rotation gate with negative angles to the quantum state $|\psi^{'''}\rangle$ as follows:

$$\begin{aligned}|\psi^{''''}\rangle = R_y(-\theta)|\psi^{'''}\rangle &= \bigotimes_{i=0}^{2n-1} R_y(-\theta_i)|s_i^{'''}\rangle \\ &= R_y(-\theta_0)|s_0^{'}\rangle \bigotimes R_y(-\theta_1)|s_1^{'''}\rangle \bigotimes ... \\ &\quad \bigotimes R_y(-\theta_{2n-2})|s_{2n-2}^{'}\rangle \bigotimes R_y(-\theta_{2n-1})|s_{2n-1}^{'''}\rangle \\ &= |s_0^{''} s_1^{''''} s_2^{''} s_3^{''''} ... s_{2n-2}^{''} s_{2n-1}^{''''}\rangle \\ S^{'} &= s_0^{''} s_1^{''''} s_2^{''} s_3^{''''} ... s_{2n-2}^{''} s_{2n-1}^{''''}\end{aligned} \tag{12}$$

When the rotation gate is applied with a negative of the angle in Equation (9), the quantum state becomes a non-superposition state. However, since the amplitudes of the qubits to which Alice and Bob applied different gates are distorted, these qubits are in superposition. When the superpositioned qubit is measured, it will return 0 or 1. In the next step, Alice measures the quantum state in Equation (12). Through this measurement, a classical data of 2n bits is obtained by Alice. She compares the 2n bits classical data in Equation (12) with the 2n bit classical data in Equation (8). For bits of the same value, she marks the reward value as "1", and "0" for bits of different value. She sends the reward value to Bob. Then she creates a new quantum state $|\psi\rangle$ and repeats the steps. Bob does not change the gates for qubits with a reward value of "1" for the new quantum state. He changes the gate which applies to qubits with a reward value of "0". He chooses a different gate than the one he chose earlier. This algorithm repeats until all reward values are "1". When all reward values are "1", the steps are repeated by applying the NOT gate to the control qubit. If all of the reward values remain as "1", error checks are started. Otherwise, iteration continues for bits with a reward value of 0.

In each iteration, Alice announces 50% of the gates which have a reward value of "0". Alice and Bob certainly do not choose the same gate when the reward value is "0". If they chose the same gate, the reward value would be "1" with 100% probability.

Bob compares the gate that Alice announced to his own. If the two gates are the same, Bob announces the presence of Eve. This will be further discussed in the security analysis (Section 5).

Let us exemplify the above steps for the value of n=4 as follows:

Step 1 Alice has four gates: $U_i^{Alice} = \{X, CNOT, I, X\}$. She creates 8 qubits quantum states for 4 gates, like $|\psi\rangle = |01101011\rangle$.

Step 2: Alice applies the rotation gate with a different angle for each qubit. In our example we apply the rotation gate with all qubits $\frac{\pi}{3}$. $R_y\left(\frac{\pi}{3}\right)|0\rangle = \frac{\sqrt{3}}{2}|0\rangle + \frac{1}{2}|1\rangle$, $R_y\left(\frac{\pi}{3}\right)|1\rangle = -\frac{1}{2}|0\rangle + \frac{\sqrt{3}}{2}|1\rangle$

Alice applies the rotation gate to the quantum state as follows:

$$
\begin{aligned}
|\psi'\rangle &= \bigotimes_{i=0}^{2n-1} R_y\left(\frac{\pi}{3}\right)|01101011\rangle \\
&= \left(\frac{\sqrt{3}}{2}|0\rangle + \frac{1}{2}|1\rangle\right) \bigotimes \left(-\frac{1}{2}|0\rangle + \frac{\sqrt{3}}{2}|1\rangle\right) \\
&\bigotimes \left(-\frac{1}{2}|0\rangle + \frac{\sqrt{3}}{2}|1\rangle\right) \bigotimes \left(\frac{\sqrt{3}}{2}|0\rangle + \frac{1}{2}|1\rangle\right) \\
&\bigotimes \left(-\frac{1}{2}|0\rangle + \frac{\sqrt{3}}{2}|1\rangle\right) \bigotimes \left(\frac{\sqrt{3}}{2}|0\rangle + \frac{1}{2}|1\rangle\right) \\
&\bigotimes \left(-\frac{1}{2}|0\rangle + \frac{\sqrt{3}}{2}|1\rangle\right) \bigotimes \left(-\frac{1}{2}|0\rangle + \frac{\sqrt{3}}{2}|1\rangle\right) \\
&= \left(-\frac{\sqrt{3}}{4}|00\rangle + \frac{3}{4}|01\rangle - \frac{1}{4}|10\rangle + \frac{\sqrt{3}}{4}|11\rangle\right) \\
&\bigotimes \left(-\frac{\sqrt{3}}{4}|00\rangle - \frac{1}{4}|01\rangle + \frac{3}{4}|10\rangle + \frac{\sqrt{3}}{4}|11\rangle\right) \\
&\bigotimes \left(-\frac{\sqrt{3}}{4}|00\rangle - \frac{1}{4}|01\rangle + \frac{3}{4}|10\rangle + \frac{\sqrt{3}}{4}|11\rangle\right) \\
&\bigotimes \left(\frac{1}{4}|00\rangle - \frac{\sqrt{3}}{4}|01\rangle - \frac{\sqrt{3}}{4}|10\rangle + \frac{3}{4}|11\rangle\right)
\end{aligned}
$$

Step 3: Bob selects n candidate gates and applies the gates to the quantum state as follows:

$$
\begin{aligned}
U_i^{Bob} &= \{CNOT, CNOT, I, X\} \\
|\psi''\rangle &= CNOT \\
&\left(-\frac{\sqrt{3}}{4}|00\rangle + \frac{3}{4}|01\rangle - \frac{1}{4}|10\rangle + \frac{\sqrt{3}}{4}|11\rangle\right) \\
&\bigotimes CNOT \\
&\left(-\frac{\sqrt{3}}{4}|00\rangle - \frac{1}{4}|01\rangle + \frac{3}{4}|10\rangle + \frac{\sqrt{3}}{4}|11\rangle\right) \\
&\bigotimes (I \bigotimes I) \\
&\left(-\frac{\sqrt{3}}{4}|00\rangle - \frac{1}{4}|01\rangle + \frac{3}{4}|10\rangle + \frac{\sqrt{3}}{4}|11\rangle\right) \\
&\bigotimes (I \bigotimes X) \\
&\left(\frac{1}{4}|00\rangle - \frac{\sqrt{3}}{4}|01\rangle - \frac{\sqrt{3}}{4}|10\rangle + \frac{3}{4}|11\rangle\right) \\
&= \left(-\frac{\sqrt{3}}{4}|00\rangle + \frac{3}{4}|01\rangle - \frac{1}{4}|11\rangle + \frac{\sqrt{3}}{4}|10\rangle\right) \\
&\bigotimes \left(-\frac{\sqrt{3}}{4}|00\rangle - \frac{1}{4}|01\rangle + \frac{3}{4}|11\rangle + \frac{\sqrt{3}}{4}|10\rangle\right) \\
&\bigotimes \left(-\frac{\sqrt{3}}{4}|00\rangle - \frac{1}{4}|01\rangle + \frac{3}{4}|10\rangle + \frac{\sqrt{3}}{4}|11\rangle\right) \\
&\bigotimes \left(\frac{1}{4}|01\rangle - \frac{\sqrt{3}}{4}|00\rangle - \frac{\sqrt{3}}{4}|11\rangle + \frac{3}{4}|10\rangle\right)
\end{aligned}
$$

Step 4: Alice applies her gates to the quantum state as follows:

$$
\begin{aligned}
U_i^{Alice} &= \{X, CNOT, I, X\} \\
|\psi'''\rangle &= U_i^{Alice}|\psi''\rangle \\
&= (I \bigotimes X) \\
&\left(-\frac{\sqrt{3}}{4}|00\rangle + \frac{3}{4}|01\rangle - \frac{1}{4}|11\rangle + \frac{\sqrt{3}}{4}|10\rangle\right) \\
&\bigotimes CNOT \\
&\left(-\frac{\sqrt{3}}{4}|00\rangle - \frac{1}{4}|01\rangle + \frac{3}{4}|11\rangle + \frac{\sqrt{3}}{4}|10\rangle\right)
\end{aligned}
$$

$$\bigotimes(I \bigotimes I)$$
$$\left(-\frac{\sqrt{3}}{4}|00\rangle - \frac{1}{4}|01\rangle + \frac{3}{4}|10\rangle + \frac{\sqrt{3}}{4}|11\rangle\right)$$
$$\bigotimes(I \bigotimes X)$$
$$\left(\frac{1}{4}|01\rangle - \frac{\sqrt{3}}{4}|00\rangle - \frac{\sqrt{3}}{4}|11\rangle + \frac{3}{4}|10\rangle\right)$$
$$= \left(-\frac{\sqrt{3}}{4}|01\rangle + \frac{3}{4}|00\rangle - \frac{1}{4}|10\rangle + \frac{\sqrt{3}}{4}|11\rangle\right)$$
$$\bigotimes \left(-\frac{\sqrt{3}}{4}|00\rangle - \frac{1}{4}|01\rangle + \frac{3}{4}|10\rangle + \frac{\sqrt{3}}{4}|11\rangle\right)$$
$$\bigotimes \left(-\frac{\sqrt{3}}{4}|00\rangle - \frac{1}{4}|01\rangle + \frac{3}{4}|10\rangle + \frac{\sqrt{3}}{4}|11\rangle\right)$$
$$\bigotimes \left(\frac{1}{4}|00\rangle - \frac{\sqrt{3}}{4}|01\rangle - \frac{\sqrt{3}}{4}|10\rangle + \frac{3}{4}|11\rangle\right)$$
$$= \left(\frac{3}{4}|00\rangle - \frac{\sqrt{3}}{4}|01\rangle - \frac{1}{4}|10\rangle + \frac{\sqrt{3}}{4}|11\rangle\right)$$
$$\bigotimes \left(-\frac{1}{2}|0\rangle + \frac{\sqrt{3}}{2}|1\rangle\right) \bigotimes \left(\frac{\sqrt{3}}{2}|0\rangle + \frac{1}{2}|1\rangle\right)$$
$$\bigotimes \left(-\frac{1}{2}|0\rangle + \frac{\sqrt{3}}{2}|1\rangle\right) \bigotimes \left(\frac{\sqrt{3}}{2}|0\rangle + \frac{1}{2}|1\rangle\right)$$
$$\bigotimes \left(-\frac{1}{2}|0\rangle + \frac{\sqrt{3}}{2}|1\rangle\right) \bigotimes \left(-\frac{1}{2}|0\rangle + \frac{\sqrt{3}}{2}|1\rangle\right)$$

This example demonstrates that the qubits for which Alice and Bob apply the same gate, return to their form in Step 2. For the first two qubits, they apply different gates. The initial value of the first two qubits is $|01\rangle$. After they apply their gates respectively, the first two qubits become different from Step 2. The amplitude of the first two qubits changes. Now let us apply a rotation gate with negative angle. Quantum states where Alice and Bob choose the same gate become non-superposition states.

Step 5: Alice applies the rotation gate with negative angles to the quantum state as follows:

$$|\psi''''\rangle = R_y(-\theta)\,|\psi'''\rangle$$
$$= \left(R_y\left(-\frac{\pi}{3}\right) \bigotimes R_y\left(-\frac{\pi}{3}\right)\right)$$
$$\left(+\frac{3}{4}|00\rangle - \frac{\sqrt{3}}{4}|01\rangle - \frac{1}{4}|10\rangle + \frac{\sqrt{3}}{4}|11\rangle\right)$$
$$\bigotimes R_y\left(-\frac{\pi}{3}\right)\left(-\frac{1}{2}|0\rangle + \frac{\sqrt{3}}{2}|1\rangle\right)$$
$$\bigotimes R_y\left(-\frac{\pi}{3}\right)\left(\frac{\sqrt{3}}{2}|0\rangle + \frac{1}{2}|1\rangle\right)$$
$$\bigotimes R_y\left(-\frac{\pi}{3}\right)\left(-\frac{1}{2}|0\rangle + \frac{\sqrt{3}}{2}|1\rangle\right)$$
$$\bigotimes R_y\left(-\frac{\pi}{3}\right)\left(\frac{\sqrt{3}}{2}|0\rangle + \frac{1}{2}|1\rangle\right)$$
$$\bigotimes R_y\left(-\frac{\pi}{3}\right)\left(-\frac{1}{2}|0\rangle + \frac{\sqrt{3}}{2}|1\rangle\right)$$
$$\bigotimes R_y\left(-\frac{\pi}{3}\right)\left(-\frac{1}{2}|0\rangle + \frac{\sqrt{3}}{2}|1\rangle\right)$$
$$= \left(\frac{3}{8}|00\rangle - \frac{2-3\sqrt{3}}{8}|01\rangle\right.$$
$$\left. -\frac{\sqrt{3}}{4}|10\rangle + \frac{3+2\sqrt{3}}{8}|11\rangle\right)$$
$$\bigotimes|1\rangle \bigotimes|0\rangle \bigotimes|1\rangle \bigotimes|0\rangle \bigotimes|1\rangle \bigotimes|1\rangle$$
$$|\psi''''\rangle = \left(\frac{3}{8}|00\rangle - \frac{2-3\sqrt{3}}{8}|01\rangle\right.$$
$$\left. -\frac{\sqrt{3}}{4}|10\rangle + \frac{3+2\sqrt{3}}{8}|11\rangle\right) \bigotimes|101011\rangle$$

Qubits with the same gates applied are in non-superposition states. However, the first two qubits in our example are in a superposition state.

Step 6: Alice measures the quantum state in Step 5.

Alice has $|\psi''''\rangle$. After the measurment of $|\psi''''\rangle$, Alice has "00101011", "01101011", "10101011" or "11101011". Alice has an initial value of "01101011".

Assuming that the measurement result is "00101011", let us compare "01101011" to "00101011". It is clear that the bit used to prepare the second qubit has changed from "1" to "0". Alice marks the reward for the second qubit as "0". Since the bits used to prepare the other qubits have not changed, Alice marks them as "1". She sends Bob the reward value "10111111". Since the reward value of the second qubit is "0", she creates a new quantum state $|\psi\rangle$ and repeats the steps. Bob does not change the gates which apply to qubits with a reward value of "1" for the new quantum state. He changes the gate which applies to qubits with a reward value of "0". He chooses a different gate than the one he chose earlier. He chooses the CNOT gate for the first two qubits in the first iteration. For this reason, he chooses either gate I or X in the second iteration. Alice and Bob repeat the steps until all reward values are "1".

Assuming that the measurement result is "01101011", let us compare "01101011" to "01101011". Since both data are the same, Alice marks all of the reward values as "1". Table 1 shows that the reward value can be "1" even if different gates are selected. Alice repeats the steps after applying the NOT gate to the control qubits in the quantum state $|\psi\rangle$. In this case, since Alice and Bob use different gates, the reward value is expected to be "0". Bob changes the gate which applies to qubits with a reward value of "0". However, since the rotation gate is applied, the quantum state is in superposition. Therefore, as in our example, the reward value can be "1". In our example for the first two qubits, Alice chooses gate X and Bob chooses gate CNOT. While the reward value is expected to be 0, it takes the value 1 due to superposition. Repeating the steps by applying the NOT gate to the control qubit, Alice's gate CNOT behaves like Bob's gate X. The reward value will be "1" with 100% probability. The superposition principle of quantum states caused Bob to accept the incorrect gate. When accepted incorrect gates are detected through the error checks in Section 3.2, the detected gates are then cancelled.

Table 1.
Situations where Alice and Bob choose different gates.

First Quantum State*	Bob's gate	The Transmitted Quantum State	Alice's gate	Last Quantum State	Reward
$\|00\rangle$	I	$\|00\rangle$	CNOT	$\|00\rangle$	1
$\|01\rangle$	I	$\|01\rangle$	CNOT	$\|01\rangle$	1
$\|10\rangle$	I	$\|10\rangle$	CNOT	$\|11\rangle$	0
$\|11\rangle$	I	$\|11\rangle$	CNOT	$\|10\rangle$	0
$\|00\rangle$	X	$\|01\rangle$	CNOT	$\|01\rangle$	0
$\|01\rangle$	X	$\|00\rangle$	CNOT	$\|00\rangle$	0
$\|10\rangle$	X	$\|11\rangle$	CNOT	$\|10\rangle$	1
$\|11\rangle$	X	$\|10\rangle$	CNOT	$\|11\rangle$	1
$* \ \|q_0 q_1\rangle$, $q_0 : Control\ qubit \quad q_1 : Target\ qubit$					

3.2. Error Corrections for Key

The previous section reveals that Bob may accept incorrect gates. The reason for this error is that different gates are chosen by Alice and Bob. Two parties must detect and cancel incorrect gates. Therefore, two different error checks are required. The first of these error checks detects situations where one party selects the "Identity" gate and the other selects the "NOT" gate. The other error check detects situations where one party selects the "CNOT" gate and the other selects the "Identity" or "NOT" gate.

3.2.1 Identity-NOT Error Check

This error check method is for situations where one of the parties selects the "Identity" and the other selects the "NOT" gate. Both parties generate the secret key with Quantum computing. This secret key is used to encrypt the message by XOR operation. Both parties exchange encrypted messages and detect incorrect gates. Then, incorrect gates are cancelled by participants.

Alice and Bob's gates are as follows:

$$U_i^{Alice} = u_0, u_1, .., u_{n-1} \; ; u_i \; \in \{I, X, CNOT\} \; ;$$
$$U_i^{Bob} = u_0^b, u_1^b, \ldots, u_{n-1}^b \; ; u_i^b \; \in \{I, X, CNOT\} \; ;$$
$$i = 1...n-1$$

Algorithm for Identity-NOT error check works as follows:

Step 1: Alice prepares 2n qubits'quantum state to generate the secret key as follows:

$$\begin{aligned} S = s_0 s_1 \ldots s_{2n-1} \; ; \; s_i \; \in \{0,1\} \, ; i = 0...2n-1 \\ |\psi\rangle = |s_0 s_1 s_2 s_3 \ldots s_{2n-2} s_{2n-1}\rangle \\ Control \; Qubits : s_0, s_2, \ldots, s_{2n-2} \; ; \\ Target \; Qubits : s_1, s_3, \ldots, s_{2n-1} \end{aligned} \tag{13}$$

Step 2: Accepting the $s_0, s_2, \ldots, s_{2n-2}$ qubits are control qubits, Alice applies her own gates to $|\psi\rangle$ as follows:

$$\begin{aligned} |\psi^{'}\rangle = U_i^{Alice} |\psi\rangle = \bigotimes_{i=0}^{n-1} u_i \, |s_{2i} s_{2i+1}\rangle \\ = u_0 \, |s_0 s_1\rangle \bigotimes u_1 \, |s_2 s_3\rangle \bigotimes \\ \ldots \bigotimes u_{n-1} \, |s_{2n-2} s_{2n-1}\rangle \\ = |s_0 s_1^{'} s_2 s_3^{'} .. s_{2n-2} s_{2n-1}^{'}\rangle \end{aligned} \tag{14}$$

Step 3: Alice measures the target qubits in the quantum state and obtains secret key as follows:

$$K^{Alice} = k_0 k_1 \ldots k_{n-1} \; ; \; k_i \; \in \{0,1\} \, ; i = 0...n-1 \tag{15}$$

Step 4: Alice reconstructs the same quantum state she used to create the secret key. Then she sends it to Bob. Accepting the $s_0, s_2, \ldots, s_{2n-2}$ qubits are control qubits, Bob applies his own gates to $|\psi\rangle$ as follows:

$$\begin{aligned} |\psi^{'}\rangle = U_i^{Bob} |\psi\rangle = \bigotimes_{i=0}^{n-1} u_i^b \, |s_{2i} s_{2i+1}\rangle \\ = u_0^b \, |s_0 s_1\rangle \bigotimes u_1^b \, |s_2 s_3\rangle \bigotimes \\ \ldots \bigotimes u_{n-1}^b \, |s_{2n-2} s_{2n-1}\rangle \\ = |s_0 s_1^{''} s_2 s_3^{''} .. s_{2n-2} s_{2n-1}^{''}\rangle \end{aligned} \tag{16}$$

Step 5: Bob measures the quantum state. Bob keeps the measurement results of the target qubits as a secret key. Bob keeps the measurement results of the Control qubits in the ControlBits array as follows:

$$\begin{aligned} K^{Bob} = k_0^{Bob} k_1^{Bob} \ldots k_{n-1}^{Bob} \; ; \; k_i^{Bob} \; \in \{0,1\} \, ; \\ ControlBits^{Bob} = \; s_0, s_2, \ldots, s_{2n-2} \; ; \\ s_{2i} \; \in \{0,1\} \, ; i = 0..n-1 \end{aligned} \tag{17}$$

Both Alice and Bob generate a key by applying their gates to the quantum state. If both have the same gates, the generated key must be same. If both have the same key, the encrypted text can be decrypted by the other. Both use XOR on classical bits to encrypt and decrypt the message.

Step 6: Alice prepares n-bit classical data as follows:

$$M = m_0 m_1 \ldots m_{n-1} \; ; \; m_i \; \in \{0,1\} \, ; i = 0...n-1 \tag{18}$$

Step 7: Alice applies the "XOR" operation to the message in Equation (18) and the key in Equation (15). The encrypted message is generated as follows:

$$\begin{aligned} C = \left(k_0 \bigoplus m_0\right) \left(k_1 \bigoplus m_1\right) \ldots \left(k_{n-1} \bigoplus m_{n-1}\right) \\ C = c_0 c_1 \ldots c_{n-1} \; ; \quad c_i \; \in \{0,1\} \, ; \; i = 0...n-1 \end{aligned} \tag{19}$$

Step 8: She sends the encrypted message to Bob. Our expectation is that Bob reaches the original message using his own key. Then Bob applies the "XOR" operation to the encrypted message in Equation (19) and the key in Equation (17). Thus, the decrypted message is created as follows:

$$M^{'} = \left(k_0^{Bob} \bigoplus c_0\right)\left(k_1^{Bob} \bigoplus c_1\right) \dots \left(k_{n-1}^{Bob} \bigoplus c_{n-1}\right)$$
$$M^{'} = m_0^{'} m_1^{'} \dots m_{n-1}^{'} \;\; ; \;\; m_i^{'} \in \{0,1\}\,; i = 0...n-1 \tag{20}$$

Step 9: Bob uses the ControlBits array in Equation (17) as the control qubit, the $M^{'}$ message in Equation (20) as the target qubit and prepares a quantum state. He applies his own gates to the quantum state as follows:

$$|\varphi\rangle = |s_0 m_0^{'} s_2 m_1^{'} \dots s_{2n-2} m_{n-1}^{'}\rangle \;\; ; \;\; s_{2i} \in \{0,1\}\,; \; m_i^{'} \in \{0,1\}\,; i = 0..n-1$$
$$|\varphi^{'}\rangle = U_i^{Bob} |\varphi\rangle = \bigotimes_{i=0}^{n-1} u_i^b |s_{2i} m_i^{'}\rangle = u_0^b |s_0 m_0^{'}\rangle \bigotimes u_1^b |s_2 m_1^{'}\rangle \bigotimes \dots \bigotimes u_{n-1}^b |s_{2n-2} m_{n-1}^{'}\rangle = |s_0 m_0^{''} s_2 m_1^{''} \dots s_{2n-2} m_{n-1}^{''}\rangle \tag{21}$$

Step 10: Bob measures the target qubits in the quantum state in Equation (21) and obtains the secret key as follows:

$$K^{Bob^{'}} = k_0^{Bob^{'}} k_1^{Bob^{'}} \dots k_{n-1}^{Bob^{'}} \;\; ; \;\; k_i^{Bob^{'}} \in \{0,1\}\,; \; i = 0..n-1 \tag{22}$$

Step 11: Bob applies the "XOR" operation to the decrypted message in Equation (20) and the key in Equation (22). Thus, the encrypted message is as follows:

$$C^{'} = \left(k_0^{Bob^{'}} \bigoplus m_0^{'}\right)\left(k_1^{Bob^{'}} \bigoplus m_1^{'}\right) \dots \left(k_{n-1}^{Bob^{'}} \bigoplus m_{n-1}^{'}\right)$$
$$C^{\prime} = c_0^{'} c_1^{'} \dots c_{n-1}^{'} \;\; ; \;\; c_i^{'} \in \{0,1\}\,; \; i = 0...n-1 \tag{23}$$

Step 12: Then he sends the encrypted message in Equation (23) to Alice. Alice prepares a quantum state using the control qubits in Equation (13) and the original message M in Equation (18). She applies her own gates to the quantum state as follows:

$$|\Phi\rangle = |s_0 m_0 s_2 m_1 \dots s_{2n-2} m_{n-1}\rangle \;\; ; \;\; s_{2i} \in \{0,1\}\,; \; m_i \in \{0,1\}\,; i = 0..n-1$$
$$|\Phi^{'}\rangle = U_i^{Alice} |\Phi\rangle = \bigotimes_{i=0}^{n-1} u_i |s_{2i} m_i\rangle = u_0 |s_0 m_0\rangle \bigotimes u_1 |s_2 m_1\rangle \bigotimes \dots \bigotimes u_{n-1} |s_{2n-2} m_{n-1}\rangle = |s_0 m_0^{'''} s_2 m_1^{'''} \dots s_{2n-2} m_{n-1}^{'''}\rangle \tag{24}$$

Step 13: Alice measures the target qubits in the quantum state in Equation (24) and obtains the secret key as follows:

$$K^{Alice^{'}} = k^{\prime}{}_0 k^{\prime}{}_1 \dots k^{\prime}{}_{n-1} \;\; ; \;\; k^{\prime}{}_i \in \{0,1\}\,; \; i = 0...n-1 \tag{25}$$

Step 14: $K^{Bob^{'}}$ in Equation (22) and $K^{Alice^{'}}$ in Equation (25) have the same value. Alice applies the "XOR" operation to the encrypted message in Equation (23) and the key in Equation (25). Thus, the decrypted message is as follows:

$$M^4 = \left(k_0^{'} \bigoplus c_0^{'}\right)\left(k_1^{'} \bigoplus c_1^{'}\right) \dots \left(k_{n-1}^{'} \bigoplus c_{n-1}^{'}\right)$$
$$M^4 = m_0^4 m_1^4 \dots m_{n-1}^4 \;\; ; \;\; m_i^4 \in \{0,1\}\,; i = 0...n-1 \tag{26}$$

$M^{\prime}$ in Equation (20) and M^4 in Equation (26) have the same value. Alice has Bob's $M^{\prime}$ message. Alice compares the original message M to message

M^4. Alice marks the gates of different bits as incorrect gates. She informs Bob to cancel them.

Let us exemplify the above steps for the value of n=4 as follows:

Alice and Bob's gates are as

$$U_i^{Alice} = \{X, CNOT, I, X\}$$
$$U_i^{Bob} = \{I,\ CNOT, I, X\}$$

Step 1:

$$|\psi\rangle = |01110110\rangle$$

Step 2:

$$|\psi'\rangle = U_i^{Alice}|\psi\rangle = (I \bigotimes X)|01\rangle \bigotimes CNOT|11\rangle \bigotimes (I \bigotimes I)|01\rangle \bigotimes (I \bigotimes X)|10\rangle$$
$$= |00\rangle \bigotimes |10\rangle \bigotimes |01\rangle \bigotimes |11\rangle = |00100111\rangle$$

Step 3:

$$K^{Alice} = 0011$$

Step 4:

$$|\psi'\rangle = U_i^{Bob}|\psi\rangle = (I \bigotimes I)|01\rangle \bigotimes CNOT|11\rangle \bigotimes (I \bigotimes)|01\rangle \bigotimes (I \bigotimes X)|10\rangle$$
$$= |01\rangle \bigotimes |10\rangle \bigotimes |01\rangle \bigotimes |11\rangle = |01100111\rangle$$

Step 5:

$$K^{Bob} = 1011, ControlBits^{Bob} = 0101$$

Step 6:

$$M = 1011$$

Step 7:

$$K^{Alice} = 0011, M = 1011$$
$$C = (0 \bigoplus 1)(0 \bigoplus 0)(1 \bigoplus 1)(1 \bigoplus 1) = 1000$$

Step 8:

$$K^{Bob} = 1011\ ,\ C = 1000$$
$$M' = (1 \bigoplus 1)(0 \bigoplus 0)(1 \bigoplus 0)(1 \bigoplus 0) = 0011$$

Let us compare Alice's original message in Step 6 to Bob's decrypted message in Step 8. It is clear that the first bits are different. This means that the first bits in the keys of two parties differ. The gate that generates this key bit needs to be cancelled. Both Alice and Bob cannot make a decision about this cancellation because they cannot know what the other's message is. Alice has the $M = 1011$ message. Bob has the $M' = 0011$ message. To make a decision, one of the parties must have both the M and M' message. We will ensure that Bob sends the M' message to Alice correctly. Therefore, Bob and Alice must have the same key. In our example, when we compare Alice's key at Step 3 to Bob's key at Step 5, we see that the first bits of the keys differ. Bob applies his gate to the target qubit that he prepared with the first bit of the M' message as follows:

$$M' = 0011\ ,\ U_i^{Bob} = \{I,\ CNOT, I, X\}$$
$$I|0\rangle = |0\rangle$$

If Bob measures the $|0\rangle$ state, he finds "0". Alice applies her gate to the target qubit she prepared with the first bit of the M message as follows:

$$M = 1011, U_i^{Alice} = \{X, CNOT, I, X\}$$
$$X|1\rangle = |0\rangle$$

If Alice measures the $|0\rangle$ state, she finds "0". Alice and Bob generated the same bit value. Alice and Bob can generate the same key if they use the message (M, M') that they have as their target qubit.

Step 9:

$$ControlBits^{Bob} = 0101\ ;\ M' = 0011$$
$$U_i^{Bob} = \{I,\ CNOT, I, X\}$$
$$|\varphi\rangle = |00100111\rangle$$

$$|\varphi'\rangle = U_i^{Bob}|\varphi\rangle = (I \bigotimes I)|00\rangle \bigotimes CNOT|10\rangle \bigotimes (I \bigotimes I)|01\rangle (I \bigotimes X)|11\rangle$$
$$= |00\rangle \bigotimes |11\rangle \bigotimes |01\rangle \bigotimes |10\rangle = |00110110\rangle$$

Step 10:

$$K^{Bob'} = 0110$$

Step 11:

$$M' = 0011 \ ; \ K^{Bob'} = 0110$$
$$C' = (0 \bigoplus 0)(1 \bigoplus 0)(1 \bigoplus 1)(0 \bigoplus 1) = 0101$$

Step 12:

$$ControlBits^{Alice} = 0101 \ ; \ M = 1011 \ ;$$
$$|\Phi\rangle = |01100111\rangle$$
$$U_i^{Alice} = \{X, CNOT, I, X\}$$
$$|\Phi'\rangle = U_i^{Alice}|\Phi\rangle$$
$$= (I \bigotimes X)|01\rangle \bigotimes CNOT|10\rangle \bigotimes (I \bigotimes I)|01\rangle \bigotimes (I \bigotimes X)|11\rangle$$
$$= |00\rangle \bigotimes |11\rangle \bigotimes |01\rangle \bigotimes |10\rangle = |00110110\rangle$$

Step 13:

$$K^{Alice'} = 0110$$

Step 14:

$$C' = 0101 \ ; \ K^{Alice'} = 0110$$
$$M^4 = (0 \bigoplus 0)(1 \bigoplus 1)(1 \bigoplus 0)(0 \bigoplus 1) = 0011$$

$M' = 0011$ in Step 8 and $M^4 = 0011$ in Step 14 have the same value. Alice has Bob's $M' = 0011$ message. Alice compares the original message $M = 1011$ to message $M^4 = 0011$. Alice marks the gates of different bits as incorrect gates. She informs Bob to cancel them.

3.2.2 CNOT-(Identity/NOT) Error Check

This error method is for situations where one of the two parties selects the "CNOT" and the other the "Identity" or "NOT" gate. Alice prepares 3 n-bit datasets and shares them with Bob. The first n-bit data set is the control bit, and the other two data sets are the target bits. Bob generates two different keys by using these datasets. By applying these keys to the message, he obtains two encrypted messages. He sends the encrypted messages to Alice. Alice generates two different keys by using these datasets. By applying these keys to the encrypted message, she obtains two decrypted messages. Then she compares the first decrypted message to the second decrypted message. She marks the gates of different bits as incorrect gates. She informs Bob to cancel them.

Alice and Bob's gates are as follows:

$$U_i^{Alice} = u_0, u_1, .., u_{n-1} \ ; u_i \ \in \{I, X, CNOT\} \ ; \ i = 1...n-1$$
$$U_i^{Bob} = u_0^b, u_1^b, \ldots, u_{n-1}^b \ ; u_i^b \ \in \{I, X, CNOT\} \ ; \ i = 1...n-1$$

Algorithm for CNOT-(Identity/NOT) error check works as follows:

Step 1: Alice shares the following 3 n-bit classical data with Bob as follows:

$$S^1 = s_0^1 s_1^1 \ldots s_{n-1}^1 \ ; \ s_i^1 \ \in \{0,1\} \ ; i = 0...n-1 \quad (27)$$
$$S^2 = s_0^2 s_1^2 \ldots s_{n-1}^2 \ ; \ s_i^2 \ \in \{0,1\} \ ; i = 0...n-1 \quad (28)$$
$$S^3 = s_0^3 s_1^3 \ldots s_{n-1}^3 \ ; \ s_i^3 \ \in \{0,1\} \ ; i = 0...n-1 \quad (29)$$

Step 2: Both parties prepare the first quantum state using the control bits in Equation (27) and the target bits in Equation (28) as follows:

$$|\psi^1\rangle = |s_0^1 s_0^2 s_1^1 s_1^2 \ldots s_{n-1}^1 s_{n-1}^2\rangle \ ; \ |s_i^1 s_i^2\rangle \ \in \{0,1\} \ ; i = 0...n-1 \quad (30)$$

Step 3: Both prepare the second quantum state using the target bits in Equation (29) and the NOT applied version of the control bits in Equation (27):

$$|\psi^2\rangle = |NOT\left(s_0^1\right) s_0^3 NOT\left(s_1^1\right) s_1^3 \ldots NOT\left(s_{n-1}^1\right) s_{n-1}^3\rangle \quad |s_i^1 s_i^3\rangle \ \in \{0,1\}; i = 0...n-1 \tag{31}$$

Step 4: Alice applies her own gates to the quantum state in Equation (30) and the quantum state in Equation (31) as follows:

$$|\psi_1^{Alice}\rangle = U_i^{Alice}|\psi^1\rangle = \bigotimes_{i=0}^{n-1} u_i |s_i^1 s_i^2\rangle = u_0|s_0^1 s_0^2\rangle \bigotimes u_1|s_1^1 s_1^2\rangle \bigotimes ... \bigotimes u_{n-1}|s_{n-1}^1 s_{n-1}^2\rangle = |s_0^1 s_0^{2'} s_1^1 s_1^{2'} \ldots s_{n-1}^1 s_{n-1}^{2'}\rangle \tag{32}$$

$$|\psi_2^{Alice}\rangle = U_i^{Alice}|\psi^2\rangle = \bigotimes_{i=0}^{n-1} u_i |NOT\left(s_i^1\right) s_i^3\rangle = u_0|NOT\left(s_0^1\right) s_0^3\rangle \bigotimes u_1|NOT\left(s_1^1\right) s_1^3\rangle \bigotimes ... \bigotimes u_{n-1}|NOT\left(s_{n-1}^1\right) s_{n-1}^3\rangle = |NOT\left(s_0^1\right) s_0^{3'} ...NOT\left(s_{n-1}^1\right) s_{n-1}^{3'}\rangle \tag{33}$$

Step 5: Bob applies his own gates to the quantum state in Equation (30) and the quantum state in Equation (31) as follows:

$$|\psi_1^{Bob}\rangle = U_i^{Bob}|\psi^1\rangle = \bigotimes_{i=0}^{n-1} u_i^b |s_i^1 s_i^2\rangle = u_0^b|s_0^1 s_0^2\rangle \bigotimes u_1^b|s_1^1 s_1^2\rangle \bigotimes ... \bigotimes u_{n-1}^b|s_{n-1}^1 s_{n-1}^2\rangle = |s_0^1 s_0^{2'} s_1^1 s_1^{2'} \ldots s_{n-1}^1 s_{n-1}^{2'}\rangle \tag{34}$$

$$|\psi_2^{Bob}\rangle = U_i^{Bob}|\psi^2\rangle = \bigotimes_{i=0}^{n-1} u_i^b |NOT\left(s_i^1\right) s_i^3\rangle = u_0^b|NOT\left(s_0^1\right) s_0^3\rangle \bigotimes u_1^b|NOT\left(s_1^1\right) s_1^3\rangle \bigotimes ... \bigotimes u_{n-1}^b|NOT\left(s_{n-1}^1\right) s_{n-1}^3\rangle = |NOT\left(s_0^1\right) s_0^{3'} \ldots NOT\left(s_{n-1}^1\right) s_{n-1}^{3'}\rangle \tag{35}$$

Step 6: Alice measures the target qubits in the quantum state in Equation (32) and obtains the secret key as follows:

$$K^{Alice_1} = k_0^{Alice_1} k_1^{Alice_1} \ldots k_{n-1}^{Alice_1}; \quad k_i^{Alice_1} \in \{0,1\}; i = 0..n-1 \tag{36}$$

Step 7: Alice measures the target qubits at the quantum state in Equation (33) and obtains the secret key as follows:

$$K^{Alice_2} = k_0^{Alice_2} k_1^{Alice_2} \ldots k_{n-1}^{Alice_2}; \quad k_i^{Alice_2} \in \{0,1\}; i = 0..n-1 \tag{37}$$

Step 8: Bob measures the target qubits at the quantum state in Equation (34) and obtains the secret key as follows:

$$K^{Bob_1} = k_0^{Bob_1} k_1^{Bob_1} \ldots k_{n-1}^{Bob_1}; \quad k_i^{Bob_1} \in \{0,1\}; i = 0..n-1 \tag{38}$$

Step 9: Bob measures the target qubits at the quantum state in Equation (35) and obtains the secret key as follows:

$$K^{Bob_2} = k_0^{Bob_2} k_1^{Bob_2} \ldots k_{n-1}^{Bob_2}; \quad k_i^{Bob_2} \in \{0,1\}; i = 0..n-1 \tag{39}$$

Step 10: One of Bob's keys has the same value as Alice's key but the other has a different value. So, one of Bob's keys is valid and the other is invalid. Encrypting message with both keys separately he creates two encrypted messages. Then he sends these encrypted messages to Alice. If Alice decrypts the encrypted message using her own keys, she obtains two different messages. She can detect incorrect gates by comparing messages. Now let us show how Bob prepares a message as follows:

$$M = m_0 m_1 \ldots m_{n-1}; \ m_i \in \{0,1\}; i = 0...n-1 \tag{40}$$

Step 11: Bob applies the "XOR" operation to the message in Equation (40) and the key in Equation

(38). Thus, the encrypted message is created as follows:

$$C^1 = \left(k_0^{Bob_1} \bigoplus m_0\right)\left(k_1^{Bob_1} \bigoplus m_1\right) \ldots \left(k_{n-1}^{Bob_1} \bigoplus m_{n-1}\right)$$
$$C^1 = c_0^1 c_1^1 \ldots c_{n-1}^1 \; ; \quad c_i^1 \in \{0,1\} \; ; \; i = 0...n-1 \tag{41}$$

Step 12: Bob applies the "XOR" operation to the message in Equation (40) and the key in Equation (39). Thus, the encrypted message is created as follows:

$$C^2 = \left(k_0^{Bob_2} \bigoplus m_0\right)\left(k_1^{Bob_2} \bigoplus m_1\right) \ldots \left(k_{n-1}^{Bob_2} \bigoplus m_{n-1}\right)$$
$$C^2 = c_0^2 c_1^2 \ldots c_{n-1}^2 \; ; \quad c_i^2 \in \{0,1\} \; ; \; i = 0...n-1 \tag{42}$$

Step 13: Then Bob sends encrypted messages C^1 and $C^2$to Alice. Alice applies the "XOR" operation to the encrypted message in Equation (41) and the key in Equation (36). Thus, the decrypted message is created as follows:

$$M^1 = \left(k_0^{Alice_1} \bigoplus c_0^1\right)\left(k_1^{Alice_1} \bigoplus c_1^1\right) \ldots \left(k_{n-1}^{Alice_1} \bigoplus c_{n-1}^1\right)$$
$$M^1 = m_0^1 m_1^1 \ldots m_{n-1}^1 \; ; \quad m_i^1 \in \{0,1\} \; ; \; i = 0...n-1 \tag{43}$$

Step 14: Alice applies the "XOR" operation to the encrypted message in Equation (42) and the key in Equation (37). Thus, the decrypted message is created as follows:

$$M^2 = \left(k_0^{Alice_2} \bigoplus c_0^2\right)\left(k_1^{Alice_2} \bigoplus c_1^2\right) \ldots \left(k_{n-1}^{Alice_2} \bigoplus c_{n-1}^2\right)$$
$$M^2 = m_0^2 m_1^2 \ldots m_{n-1}^2 \; ; \quad m_i^2 \in \{0,1\} \; ; \; i = 0...n-1 \tag{44}$$

Alice has two decrypted messages created from the same message. As proved above, upon choosing the incorrect gates, Bob will have the incorrect key and encrypt the message incorrectly. Alice will not be able to retrieve the original message for the incorrect state. Therefore, one of Alice's messages has a different content from the original message because of Bob's incorrect gate choice. The other will have the same content as the original message. Alice compares M^1 message to M^2 message. Alice marks the gates of different bits as incorrect gates. She informs Bob to cancel them.

The gates selected differently are removed from the system through error checks. In this way, it is ensured that both parties have the same gates. After this, both parties will have the information to generate the same key.

Let us exemplify the above steps for the value of n=4 as follows:

Alice and Bob's gates are as

$$U_i^{Alice} = \{X, CNOT, I, X\}$$
$$U_i^{Bob} = \{CNOT, CNOT, I, X\}$$

Step 1:

$$S^1 = 1001 \; ; \; S^2 = 0111 \; ; \; S^3 = 1100$$

Step 2:

$$|\psi^1\rangle = |10010111\rangle$$

Step 3:

$$|\psi^2\rangle = |01111000\rangle$$

Step 4:

$$|\psi_1^{Alice}\rangle = U_i^{Alice} |10010111\rangle$$
$$= (I \bigotimes X)|10\rangle \bigotimes CNOT|01\rangle \bigotimes (I \bigotimes I)|01\rangle \bigotimes (I \bigotimes X)|11\rangle$$
$$= |11\rangle \bigotimes |01\rangle \bigotimes |01\rangle \bigotimes |10\rangle = |11010110\rangle$$

$$|\psi_2^{Alice}\rangle = U_i^{Alice}\,|01111000\rangle$$
$$= (I \bigotimes X)\,|01\rangle \bigotimes CNOT\,|11\rangle$$
$$\bigotimes (I \bigotimes I)\,|10\rangle \bigotimes (I \bigotimes X)\,|00\rangle$$
$$= |00\rangle \bigotimes |10\rangle \bigotimes |10\rangle \bigotimes |01\rangle = |00101001\rangle$$

Step 5:

$$|\psi_1^{Bob}\rangle = U_i^{Bob}\,|10010111\rangle$$
$$= CNOT\,|10\rangle \bigotimes CNOT\,|01\rangle \bigotimes$$
$$(I \bigotimes I)\,|01\rangle \bigotimes (I \bigotimes X)\,|11\rangle$$
$$= |11\rangle \bigotimes |01\rangle \bigotimes |01\rangle \bigotimes |10\rangle \;\; = |11010110\rangle$$
$$|\psi_2^{Bob}\rangle = U_i^{Bob}\,|01111000\rangle$$
$$= CNOT\,|01\rangle \bigotimes CNOT\,|11\rangle \bigotimes$$
$$(I \bigotimes I)\,|10\rangle \bigotimes (I \bigotimes X)\,|00\rangle$$
$$= |01\rangle \bigotimes |10\rangle \bigotimes |10\rangle \bigotimes |01\rangle = |01101001\rangle$$

Step 6:

$$|\psi_1^{Alice}\rangle = |11010110\rangle \;\; ; \;\; K^{Alice_1} = 1110$$

Step 7:

$$|\psi_2^{Alice}\rangle = |00101001\rangle \;\; ; \;\; K^{Alice_2} = 0001$$

Step 8:

$$|\psi_1^{Bob}\rangle = |11010110\rangle \;\; ; \;\; K^{Bob_1} = 1110$$

Step 9:

$$|\psi_2^{Bob}\rangle = |01101001\rangle \;\; ; \;\; K^{Bob_2} = 1001$$

Step 10:

$$M = 1100$$

Step 11:

$$K^{Bob_1} = 1110 \;\; ; \;\; M = 1100$$
$$C^1 = (1 \bigoplus 1)(1 \bigoplus 1)(1 \bigoplus 0)(0 \bigoplus 0) = 0010$$

Step 12:

$$K^{Bob_2} = 1001 \;\; ; \;\; M = 1100$$
$$C^2 = (1 \bigoplus 1)(0 \bigoplus 1)(0 \bigoplus 0)(1 \bigoplus 0) = 0101$$

Step 13:

$$K^{Alice_1} = 1110 \;\; ; \;\; C^1 = 0010$$
$$M^1 = (1 \bigoplus 0)(1 \bigoplus 0)(1 \bigoplus 1)(0 \bigoplus 0) = 1100$$

Step 14:

$$K^{Alice_2} = 0001 \;\; ; \;\; C^2 = 0101$$
$$M^2 = (0 \bigoplus 0)(0 \bigoplus 1)(0 \bigoplus 0)(1 \bigoplus 1) = 0100$$

Alice compares the $M^1 = 1100$ to $M^2 = 0100$ messages. Then she marks the gates of different bits as incorrect gates. She informs Bob to cancel them. In our example, the first gate will be cancelled. Alice and Bob's gates will be the same, as follows:

$$U_i^{Alice} = \{CNOT, I, X\} \;\; ; \;\; U_i^{Bob} = \{CNOT, I, X\}$$

3.3. Key Generation

This section will examine the key generation. The keys are generated by quantum gates which are taught by QRL as above (see Sections 3.1 and 3.2).

Alice and Bob have the same gates as follows:

$$U_i^{Alice} = u_0, u_1, .., u_{n-1} \; ; u_i \;\; \in \{I, X, CNOT\} \;\; ;$$
$$U_i^{Bob} = u_0, u_1, .., u_{n-1} \; ; u_i \;\; \in \{I, X, CNOT\} \;\; ;$$
$$i = 1...n-1$$

Step 1: Alice prepares the 2n-bit dataset as follows:

$$S = s_0 s_1 \ldots s_{2n-1} \;\; ; \;\; s_i \;\; \in \{0, 1\} \, ; i = 0...2n-1 \tag{45}$$

Alice sends the 2n-bit dataset in Equation (45) to Bob.

Step 2: Alice prepares a 2n qubit quantum state with the 2n-bit dataset in Equation (45) as follows:

$$|\psi\rangle = |s_0 s_1 s_2 s_3 \dots s_{2n-2} s_{2n-1}\rangle \tag{46}$$

Step 3: She applies her own gates to the quantum state as follows:

$$\begin{aligned} |\psi^{'}\rangle = U_i^{Alice} |\psi\rangle &= \bigotimes_{i=0}^{n-1} u_i |s_{2i} s_{2i+1}\rangle \\ &= u_0 |s_0 s_1\rangle \bigotimes u_1 |s_2 s_3\rangle \bigotimes \\ &\dots \bigotimes u_{n-1} |s_{2n-2} s_{2n-1}\rangle \\ &= |s_0 s_1^{'} s_2 s_3^{'} \dots s_{2n-2} s_{2n-1}^{'}\rangle \end{aligned}$$
$$|q_0 q_1\rangle,\ q_0 : Control\ qubit \quad q_1 : Target\ qubit \tag{47}$$

Step 4: Alice measures the target qubits at the quantum state and obtains the secret key as $K_{Alice} =$ "$s_1^{'} s_3^{'} s_5^{'} .. s_{2n-1}^{'}$".

Step 5: Bob prepares a 2n qubit quantum state with the 2n-bit dataset in Equation (45) as follows:

$$|\psi\rangle = |s_0 s_1 s_2 s_3 \dots s_{2n-2} s_{2n-1}\rangle \tag{48}$$

Step 6: Bob applies his gates to the quantum state as follows:

$$\begin{aligned} |\psi^{'}\rangle = U_i^{Bob} |\psi\rangle &= \bigotimes_{i=0}^{n-1} u_i |s_{2i} s_{2i+1}\rangle \\ &= u_0 |s_0 s_1\rangle \bigotimes u_1 |s_2 s_3\rangle \bigotimes \\ &\dots \bigotimes u_{n-1} |s_{2n-2} s_{2n-1}\rangle \\ &= |s_0 s_1^{'} s_2 s_3^{'} .. s_{2n-2} s_{2n-1}^{'}\rangle \end{aligned} \tag{49}$$

Step 7: Bob measures the target qubits at the quantum state and obtains the secret key as $K_{Bob} =$ "$s_1^{'} s_3^{'} s_5^{'} .. s_{2n-1}^{'}$". Both parties creates the same secret key locally. An example of key generation is shown in Figure 2:

4. Secure Communication Method

In this section, it is explained how two parties communicate securely. An example of this communication is shown in Figure 3.

Now that both parties can generate the same key, we can focus on the achievement of secure communication. First, Alice prepares the 2n-bit dataset as follows:

$$S = s_0 s_1 \dots s_{2n-1}\ ;\ s_i\ \in \{0,1\}\,; i = 0...2n-1 \tag{50}$$

Alice sends it to Bob. Both parties prepare a 2n qubit quantum state with the 2n-bit dataset in Equation (50) as follows:

$$|\psi\rangle = |s_0 s_1 s_2 s_3 \dots s_{2n-2} s_{2n-1}\rangle \tag{51}$$

Both parties apply their gates to the quantum state in Equation (51) as follows:

$$\begin{aligned} |\psi^{'}\rangle = U_i |\psi\rangle &= \bigotimes_{i=0}^{n-1} u_i |s_{2i} s_{2i+1}\rangle \\ &= u_0 |s_0 s_1\rangle \bigotimes u_1 |s_2 s_3\rangle \bigotimes \\ &\dots \bigotimes u_{n-1} |s_{2n-2} s_{2n-1}\rangle \\ &= |s_0 s_1^{'} s_2 s_3^{'} \dots s_{2n-2} s_{2n-1}^{'}\rangle \end{aligned} \tag{52}$$

Both parties measure the target qubits at the quantum state in Equation (52) and obtains the secret key as follows:

$$K = k_0 k_1 \dots k_{n-1}\ ;\ k_i\ \in \{0,1\}\,; i = 0...n-1 \tag{53}$$

Both parties obtain the shift value by adding the value of the bits in the key obtained in Equation (53) as follows:

$$t = k_0 + k_1 + \dots + k_{n-1} \tag{54}$$

Both parties have the order of the gates by shifting their gates based on the shift value in Equation (54) as follows:

$$\begin{aligned} U' &= u_{(0+t)\%n}, u_{(1+t)\%n}, .., u_{(n-1+t)\%n}\ ; \\ u_i\ &\in \{I, X, CNOT\}\ ;\quad i = 1...n-1 \\ U' &= u_0^{'}, u_1^{'}, .., u_{n-1}^{'}\ ; \\ u_i^{'}\ &\in \{I, X, CNOT\}\ ;\quad i = 1...n-1 \end{aligned} \tag{55}$$

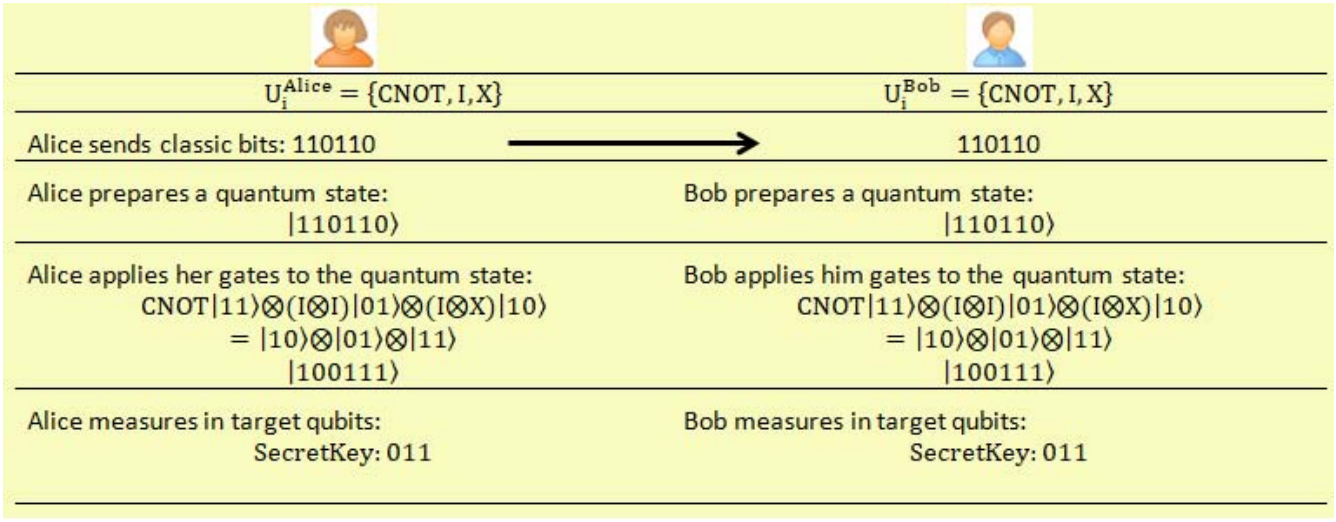

Figure 2. Example of key generation.

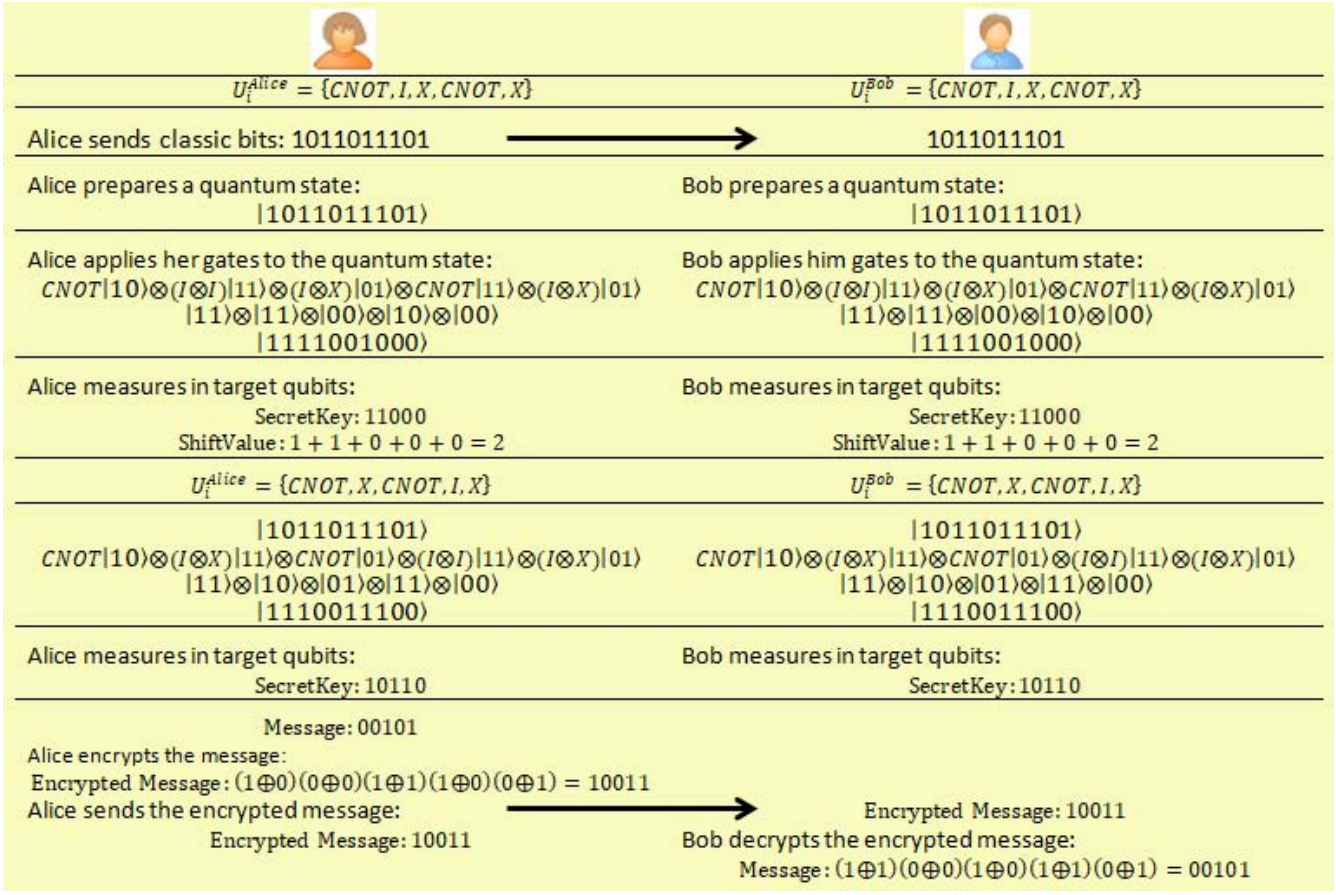

Figure 3. Example of secure communication.

In this way, the keys used in each encryption process are generated differently. Additionally each application of the gates to the same bit will differ. Thus, the eavesdroppers are also prevented from creating a sample data set. If the same gate was applied to the same bit over and over, the eavesdroppers could create a dataset and try to obtain the key information. In our method by changing the gates applied each time, security is ensured.

Both parties apply organised gates at Equation (55) to the quantum state in Equation (51) as follows:

$$\begin{aligned} |\psi^{'}\rangle = U_i^{'} |\psi\rangle &= \bigotimes_{i=0}^{n-1} u_i^{'} |s_{2i}s_{2i+1}\rangle \\ &= u_0^{'} |s_0 s_1\rangle \bigotimes u_1^{'} |s_2 s_3\rangle \bigotimes \\ &\quad ... \bigotimes u_{n-1}^{'} |s_{2n-2}s_{2n-1}\rangle \\ &= |s_0 s_1^{''} s_2 s_3^{''} ... s_{2n-2} s_{2n-1}^{''}\rangle \end{aligned} \tag{56}$$

Both parties measure the target qubits at the quantum state in Equation (56) and obtains the secret key as follows:

$$K' = k_0^{'} k_1^{'} \dots k_{n-1}^{'} \;\; ; \;\; k_i^{'} \in \{0,1\} ; i = 0...n-1 \tag{57}$$

Alice prepares n-bit classical data as follows:

$$M = m_0 m_1 \dots m_{n-1} \;\; ; \;\; m_i \;\; \in \{0,1\} ; i = 0...n-1 \tag{58}$$

Alice applies the "XOR" operation to the message in Equation (58) and the secret key in Equation (57). Thus, the encrypted message is created as follows:

$$\begin{aligned} C = \left(k_0^{'} \bigoplus m_0\right) \left(k_1^{'} \bigoplus m_1\right) \dots \left(k_{n-1}^{'} \bigoplus m_{n-1}\right) \\ C = c_0 c_1 \dots c_{n-1} \;\; ; \;\; c_i \;\; \in \{0,1\} \; ; \;\; i = 0...n-1 \end{aligned} \tag{59}$$

Then she sends the encrypted message C to Bob. He applies the "XOR" operation to the encrypted message in Equation (59) and the secret key in Equation (57). Thus, through decyrption, the original message is obtained as follows:

$$\begin{aligned} M = \left(k_0^{'} \bigoplus c_0\right) \left(k_1^{'} \bigoplus c_1\right) \dots \left(k_{n-1}^{'} \bigoplus c_{n-1}\right) \\ M = m_0 m_1 \dots m_{n-1} \;\; ; \;\; m_i \;\; \in \{0,1\} ; i = 0...n-1 \end{aligned} \tag{60}$$

5. Security Analysis

The security of the proposed study is generally as follows. Since the gates applied to create the key are not shared via any channel, the eavesdropper cannot have information about the quantum gates used.

In the learning action, the superposition state with different amplitude is used (see Equation (9)). Since the eavesdropper has no idea at what angles it is rotated and superpositioned, the quantum state cannot recover from the superposition state. If the eavesdropper measures the superposition state, she will get random information. Let us assume that Eve entangled the quantum state. Hence, Eve can have Alice's measurement results and learning outputs, but she cannot detect which gates are applied by using this informations. She can only detect whether Bob is learning successfully or not. The eavesdropper may want to act as Bob to Alice and Alice to Bob. To prevent this, Alice announces 50% of the gates marked as "0" in reward value. Bob compares his own gates to the gates that Alice announced. If there are same choices for the gates with equivalent indices, Bob announces the presence of Eve. This way, if Eve overhears the communications, she can be detected. Therefore, the learning action is terminated. We can exemplify this as follows:

Let us assume that Alice and Bob have gate X.

Step 1. Alice has bit "0". She prepares quantum state $|0\rangle$.

Step 2. She applies the rotation gate with θ angle to the quantum state $|0\rangle$ and obtains $\alpha |0\rangle + \beta |1\rangle$. She sends state $\alpha |0\rangle + \beta |1\rangle$ to Bob.

Step 3. Bob applies the X gate to $\alpha|0\rangle+\beta|1\rangle$ and he obtains $\alpha|1\rangle+\beta|0\rangle$. He sends state $\alpha|1\rangle+\beta|0\rangle$ to Alice.

Step 4. Alice applies the X gate to $\alpha|1\rangle+\beta|0\rangle$ and she obtains $\alpha|0\rangle+\beta|1\rangle$.

Step 5. Alice applies the rotation gate with θ angle to $\alpha|0\rangle+\beta|1\rangle$ and she obtains $|0\rangle$.

As shown, if both parties have the same gate, Alice obtains the initial value at the end of the learning action. In this case, Alice must mark the reward value as "1". If the reward value is marked as 0, we can realise that the quantum state has been changed by Eve.

It is hard to learn which gates generate the key. However, once learned, both parties can easily generate the same key locally. The communication is secure because of non-sharing key. Thus, a one-time pad key can be used for each communication. To obtain the message encrypted with a 512-bit key by the eavesdropper, there are 2^{512} possibilities that need to be examined. In error corrections for key, gates or message content are not shared openly. A key is only used in encryption or decryption. Incorrect gates are identified by comparisons. The messages for use in comparisons are sent by encryption.

6. Conclusions

The proposed study is simulated using the Qiskit [12] library for Python. The computer used for the simulation has an i7-11800H processor and 16 GB of RAM. The simulation could be run up to 195 gates with this hardware. The simulation results are shown in Table 2. When examining the simulation results, it should be noted that this study performed "n" independent learning actions. Today, reinforcement learning is widely preferred for determining the best move in a game or in robotics applications. Reinforcement learning seeks to find the optimal path from one point to another; the next choice depends on the previous choice. However, in our study, the choices are independent.

Table 2.
Simulation results. The simulation was run 10 times for each key sizes and the average was taken.

Key Sizes (bits)	Correct (bits)	Incorrect (bits)	Time (sec)	%
195	171.5	23.5	44.9	87.95
128	109.4	18.6	24.5	85.47
64	53.5	10.5	9.3	83.59
32	24.4	7.6	3	76.25

The proposed study performs the learning action with an accuracy of 87.95% for 195 gates, 85.47% for 128 gates, 83.59% for 64 gates, 76.25% for 32 gates. As the key size increases, the performance of the method increases. When the key size increases, the run duration increases. As can be seen from figure 4, the performance and run duration of the method increase directly proportional to the key size.

Further, this study uses the principles of quantum mechanics for the reinforcement learning and generating key. The classical XOR operation is used for encrypting and decrypting the message. Since I, X, and CNOT gates can be easily applied on classical computers, error checks can also be performed completely classically. Reinforced learning requires a quantum channel. There are many studies on quantum networking. When the quantum network is widely used, this study can be actualised. Until then, our method can be implemented using quantum network simulations.

Finally when we compare our method to other key distribution methods, we see that the other methods need to securely share the secret key for each

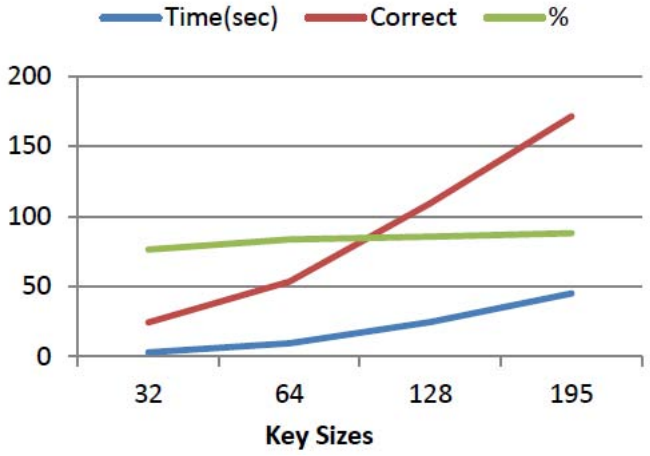

Figure 4. Simulation results. The simulation was run 10 times for each key sizes and the average was taken.

communication. However, our method prioritises safety only in the reinforcement learning phase. Instead of sending the secret key, the parties locally generate the required secret keys for each communications. The secret key should only be protected locally. As the secret key is not shared through any network, the communication cannot be interrupted by eavesdropping. This shows that the method we proposed in this study is safe. As a result, this study aims to bring a different perspective to quantum key distribution methods.

Acknowledgments

This study was produced as a part of the PhD study of Ercan ÇAĞLAR. This study is patented under contract TR 2021 019962 B.

References

[1] D. Dong, C. Chen, H. Li, and T. Z. Tarn, "Quantum reinforcement learning," *IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics)*, vol. 38, no. 5, pp. 1207–1220, 2008.

[2] Z. A. Ren, Y. P. Chen, J. Y. Liu, and Q. W. H. J. Ding, "Implementation of machine learning in quantum key distributions," *IEEE Communications Letters*, vol. 25, no. 3, pp. 940–944, 2021.

[3] S. Zhang, J. Liu, G. Zeng, C. Zhang, X. Zhou, and Q. Wang, "Machine learning-assisted measurement device-independent quantum key distribution on reference frame calibration," *Entropy*, vol. 23, no. 10, p. 1242, 2021.

[4] H. Chin, N. Jain, D. Zibar, U. Andersen, and T. Gehring, "Machine learning aided carrier recovery in continuous-variable quantum key distribution," *Quantum Information*, vol. 7, no. 20, 2021.

[5] S. Giordano and M. A. Martin-Delgado, "Reinforcement-learning generation of four-qubit entangled states," *Physical Review Research*, vol. 4, no. 4, p. 043056, 2022.

[6] K. Kashyap, Lalit, D. Shah, and L. Gautam, "From classical to quantum: A review of recent progress in reinforcement learning," presented at 2021 2nd International Conference for Emerging Technology (INCET), Belgaum, India, 2013.

[7] J. D. Martín-Guerrero and L. Lamata, "Quantum machine learning: A tutoria," *Neurocomputing*, vol. 470, pp. 457–461, 2022.

[8] N. Meyer, C. Ufrecht, M. Periyasamy, D. D. Scherer, A. Plinge, and C. Mutschler, "A survey on quantum reinforcement learning." *arXiv preprint, arXiv:2211.03464*, 2022.

[9] F. Albarrán-Arriagada, J. C. Retamal, E. Solano, and L. Lamata, "Measurement-based adaptation protocol with quantum reinforcement learning," *Phys. Rev. A*, vol. 98, no. 4, p. 042315, 2018.

[10] M. Moll and L. Kunczik, "Comparing quantum hybrid reinforcement learning to classical methods," *Human Intelligent Systems Integration*, vol. 3, pp. 15–23, 2021.

[11] M. Franz, L. Wolf, M. Periyasamy, C. Ufrecht, D. D. Scherer, A. Plinge, C. Mutschler, and W. Mauerera, "Uncovering instabilities in variational-quantum deep q-networks," *Journal of the Franklin Institute*, 2022.

[12] IBM, "Qiskit," Accessed Mar. 11, 2023. [Online]. Available: https://qiskit.org/