Eavesdropping detection in Quantum Communication Channel for secure message transmission using Qiskit

Razwan Ahmed Tanvir & Swapnil Saha

August 11, 2022

1 Overview:

We aim to detect eavesdropping in a quantum communication channel using BB84 protocol [1] for secure message exchange. The basic idea is that the state of the qubit changes with any measurement, and this change can be detected. For instance, a message sender A wants to transmit a message to receiver B using the quantum communication channel provided by C. Now, if A sends a qubit to B, we want to ensure that C cannot intercept the qubit's state. We do this by using a fundamental property of qubits: The state of a qubit changes if someone measures that qubit. We detect this change in states and thus make the channel secure for message transmission.

2 Motivation

This project coagulates the knowledge from the theories of quantum computing and also focuses on the implementation style using modern frameworks. This project contributes to the fact that the classic encryption is assumed to fail with the rise of quantum computing and to transmit messages from sender to receiver, we need a proven mechanism to secure the transmission. The arrival of quantum computing may put banks, servers, and online transactions at risk. This approach tackles these issues and promises privacy and secure exchange of secret messages.

3 Protocol Description

This protocol is based upon a core concept of qubits. We know that measurement will change the state of a qubit. We can identify if a qubit was measured in the quantum channel at the time of transmission. This alteration in the state while measurement, is the core idea of this eavesdropping detection mechanism.

4 Methodology

For the sake of explanation, we take three parties namely Alice (Sender), Bob (Receiver) & Eve (Eavesdropper). Now, assume that Alice prepares a qubit in $|+\rangle$ state in the X-basis.

$$\text{We know, } |+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

If Alice sends this qubit to Bob, and Bob measures this qubit on X-basis, it will be measured 0. However, if Eve measures the qubit on Z-basis before the qubit reaches Bob, Bob will not be sure to measure the qubit as 0 every time because the state will be changed.

If Eve tries to measure the qubit through the channel, Bob now has a 50% chance of measuring 1 instead of 0 every time. In this way, we detect eavesdropping.

In this experiment, in the first phase, we will observe how Alice and Bob establish a secret key using Eve's channel without interception of Eve. Later we will experiment with the interception by Eve and ensure that the interception has been detected.

Now, we will describe our circuits and their implementations. For the implementation of these circuits, we used Qiskit framework in python. The following circuits show that the measurement will cause the qubit to change its state.

1. Alice prepares a qubit for Bob and Bob measures that qubit.

```
qc = QuantumCircuit(1,1)
qc.h(0)
qc.barrier()
qc.h(0)
qc.measure(0,0)
display(qc.draw())
```

Figure-1 illustrates the above circuit implemented in Qiskits.

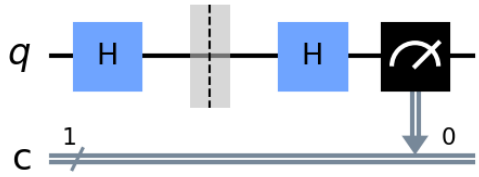

Figure 1: No measurement in between

2. If Alice's qubit is measured before it reaches Bob, then Bob may not measure Alice's bit certainly. Bob will measure 0 or 1 as if they were in a superposition.

```
qc = QuantumCircuit(1,1)
qc.h(0)
qc.measure(0, 0)
qc.barrier()
qc.h(0)
qc.measure(0,0)
display(qc.draw())
```

Figure-2 illustrates the above circuit implemented in Qiskit.

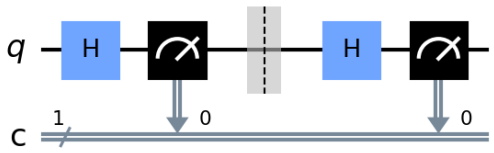

Figure 2: Eve measures the qubit before Bob

The following histogram shows that Bob has around a 50% chance of measuring 1 if a measurement is performed on the qubit Alice sent.

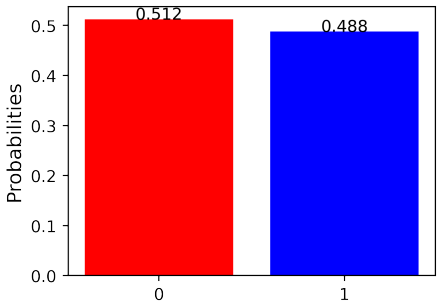

Figure 3: Interception impacts Bob's measurement

We will describe the protocol in five steps and mention who possesses what information.

Step 1. Alice generates a string of random bits, let us say-1000101011010100, and randomly assigns a basis for each of the bits of the prepared string. Assume that the bases are $ZZXZXXXZXZXXXXXX$.

bits	1	0	0	0	1	0	1	0	1	1	0	1	0	1	0	0
bases	Z	Z	X	Z	X	X	X	Z	X	Z	X	X	X	X	X	X

Figure 4: Bits and Bases prepared by Alice

This information is private to Alice. Bob and Eve do not know about these bits and their basis.

Step 2. In this step, Alice randomly picks a basis for each bit and encodes that bit with the chosen basis. There are four possible states for each qubit. These are- $|0\rangle, |1\rangle, |+\rangle,$ and $|-\rangle$.

The encoded message Alice sent to Bob is the following-

$$|1\rangle|0\rangle|+\rangle|0\rangle|-\rangle|+\rangle|-\rangle|0\rangle|-\rangle|1\rangle|+\rangle|-\rangle|+\rangle|-\rangle|+\rangle|+\rangle$$

Step 3. After receiving the qubits from Alice through Eve's channel, Bob measures each qubit on a randomly chosen basis. For example, Bob might choose bases in the following sequence- $XZZZXZXZXZXZZZXZ$. Bob keeps his measurements secret.

Step 4. In this step, Alice and Bob both publicly share the sequence of their previously chosen basis. Bob then keeps the bits that are measured on the same basis as Alice's and discard the mismatched measurements.

Step 5. Finally, they exchange a random sample of their secret key. If the sample matches, then they are certain that the transmission was successful within a small margin of error.

However, in the case of interception, Bob will not measure the qubits as intended, and their sample will not match. In this way, the interception from Eve can be detected.

5 Risk Analysis

The probability of an undetected interception depends on the number of bits Alice and Bob compare. If they compare 1 bit, then the probability of the undetected interception-

$$P(\text{Undetected interception}) = 0.75^1 = 0.75$$

For 2 bits,

$$P(\text{Undetected interception}) = 0.75^2 = 0.5625$$

Therefore, the generalized formula,

$$P(\text{Undetected interception}) = 0.75^n, \text{ where n is the number of bits}$$

In our experiment, we used 15 bits. So, the probability that the interception will go undetected would be,

$$P(\text{Undetected interception}) = 0.75^{15} = 0.013$$

However, if we want to increase the detection probability, we can increase the number of bits compared by Alice and Bob. For 64 bits comparison, the detection rate will be-

$$P(\text{Detection}) = 1 - (0.75^{64}) = 0.9999999899$$

Therefore we can conclude that this protocol ensures the detection of eavesdropping with a high probability.

6 Conclusion

The impact of the invention of quantum computing will be ubiquitous. Cryptography and encryption to ensure security will be affected directly by the emergence of the quantum computer. In this study, we have implemented a protocol that can detect the interception of any third party in a quantum channel connecting a message sender and a receiver. This protocol utilizes the fundamental properties of a qubit. Detecting a measurement on a qubit is the core idea of this protocol. Our experiment shows that this protocol can detect an interception of eavesdropping with a high probability. However, the limitation of this study is that it assumes a quantum channel connects both the receiver and the sender.

References

[1] Davide Rusca, Alberto Boaron, Marcos Curty, Anthony Martin, and Hugo Zbinden. Security proof for a simplified bennett-brassard 1984 quantum-key-distribution protocol. *Physical Review A*, 98(5), nov 2018.