A New Look on Quantum Key Distribution

Michael Coffey

August 10, 2021

Abstract

The quantum key distribution protocol is a subcategory of quantum cryptography that allows entities to create and transmit a shared key between each other to help secure a private communication channel. In this paper quantum cryptography and the quantum key distribution protocol are defined. Then a new approach to this protocol is proposed to emphasize the security of this protocol and experiments are conducted with this new approach to show its validity.

1 Introduction

As mentioned in [3] cryptography is defined as the "art of hiding information in a string of bits meaningless to any unauthorized party." However, due to the imperfections presented in classical cryptography, malicious actors can intercept and decrypt these hidden messages if given the right amount of time and resources. For a long time, this crack in the security of classical cryptography has ignored, due to the shear amount of time and resource previously needed by these malicious actors. As time progresses, these attackers get more skilled, new technologies lead to less of a need in time and resources, and these flaws in classical cryptography begin to grow more and more vast. This is why a need for a more secure type of cryptography is ever growing stronger. One proposed solution is found in quantum cryptography. Quantum cryptography is the use of quantum mechanics to encrypt data and send it in an unhackable form [1]. The core principle used in this cryptography is that you cannot copy a quantum photon without changing the data stored within it. Due to this, a malicious actor cannot intercept a message and remain unknown. The problem then becomes, how do we ensure the non-repudiation of senders and receivers in this system? This problem is solved my the use of a secret key, which is created and transmitted with the quantum key distribution protocol.

The quantum key distribution protocol is used to create and transmit secret keys between two parties with the goal that a malicious actor cannot intercept this key without the other parties knowing. It is able to do this by using the principle of quantum mechanics that measuring a photon changes the information of said photon. In this paper, we will discuss how the quantum key

distribution protocol works, we propose a new approach to this protocol to ensure non-repudiation is maintained, and provide an experiment done to solidify our hypothesis.

The remainder of this paper is structured as follows; in section 2 we will discuss the methods used in the quantum key distribution protocol, propose a modification to this protocol, and describe the experiments used to evaluate this improvement. Section 3 elaborates on the results found in the conducted experiments and section 4 concludes the paper by describing the value of the experiments conducted.

2 Methods

The quantum key distribution protocol is a simplistic protocol that takes advantage of principles found in quantum mechanics to produce and transmit a secret key between two entities [2]. To describe this protocol lets assume that we have two entities, Alice and Bob, where Alice is trying to send a secret key to Bob so that they can communicate over a public channel without worrying about an attacker obtaining their message. For the quantum key distribution protocol, Alice will begin by choosing a string of random bits and a string of random basis, from the X and Z basis, used for these bits. These two strings are to remain private for Alice only. Alice will then encode the string of random bits with the string of random basis, which will result in a random string of qbits from the X and Z basis. Alice then sends this encoded string to Bob. Upon receiving this encoded string, Bob measures each qbit with either the X or Z basis at random and keeps the results of this measurement private. Bob and Alice then make the basis that they used public and they use the qbits measured with the same basis to form the secret key. The parts of the shared basis that do not match up are thrown out of consideration. After the secret key is established, Bob and Alice share with each other a random sample of their secret keys to prove that they match. Once the keys are considered to be identical, the parts of the secret key that were shared are thrown out and Bob and Alice are left with a shared secret key.

This key distribution works even if a malicious actor intercepts the key. To show this let's add another actor to the mix, Eve, where Eve is trying to acquire the secret key and start stealing messages between Alice and Bob. Because Alice and Bob are using a public channel to conduct the quantum key distribution protocol, Eve can intercept messages passed between the two actors. Let's assume that when Alice sends Bob the original encrypted message for Bob to decrypt it, Eve intercepts the message before it can get to Bob. Eve then decrypts the message with a random set of basis between the X and Z basis, stores the result, and passes the encrypted message along to Bob. The remainder of the protocol remains the same, until the parts of the secret key are shared between Bob and Alice at the end. Because Eve intercepted the message before it could get to Bob and measured it before passing it along, the message the Bob got was different from the message that Alice sent, causing differences

to be found in the finalized secret keys. This change in the encrypted message is due to the principle of quantum mechanics where taking the measurement of a photon changes the information of that photon. Upon measuring a difference in their secret keys, Alice and Bob will delete the flawed secret key and repeat the protocol until their secret keys match at the end.

A problem may arise when Alice and Bob measure their resulting secret keys at the end of the protocol. Due to Alice and Bob selecting a random section from their secret keys and comparing this section, there is a chance that Alice and Bob are measuring parts of the secret key that were not corrupted by Eve's interception. This allows Eve to have a chance of getting away with stealing the secret key without being noticed. In order to lessen the occurrence of this flaw, I propose that instead of only encrypting the message with the X and Z basis, we instead use the X, Y, and Z basis. The thought behind this is that the keys will become more random, causing the interception difference to become more noticeable.

I conducted several experiments to prove the results of the hypothesis that adding the Y basis to the quantum key distribution protocol helps to ensure the interception state of the secret key. I first ran a control experiment to show that the quantum key distribution protocol works with only the X and Z basis both with and without interception. After the control experiment was run, I ran an experiment while using the X, Y, and Z basis to determine if the correctness of the protocol is kept without interception. Finally, I ran an experiment to display the difference in secret keys after interception has occurred. The results of these experiments are shown in section 3.

3 Results

From the control experiments discussed in section 2, I was able to determine that the quantum key distribution protocol works as designed while using the X and Z basis. When a malicious actor intercepts the message the protocol is successful at determining the presence of this actor due to the difference in the selected secret keys as shown in Figure 1. Continuing with the experiments, I tested the protocol with the use of the X, Y, and Z basis and without interception in order to determine its correctness. The results of this experiment showed that the protocol was successfully able to perform with the added basis. With these previous experiments run to show the ability to add the Y basis to the protocol, I ran final experiment to see how the protocol reacted to interception while using the X, Y, and Z basis. The results of this experiment are shown in Figure 2. Upon comparing the results shown in Figure 1 and Figure 2, we can conclude that the addition of the Y basis to the quantum key distribution protocol increases the ability of us to determine if the secret key has been intercepted by a malicious actor. This is due to the additional variety available while using a third basis to encrypt the message at the beginning of the protocol.

Figure 1: Difference between Alice and Bob's secret keys with base protocol

```
  bob_sample = [1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1]
alice_sample = [1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1]
```

Figure 2: Difference between Alice and Bob's secret keys with new protocol

```
  bob_sample = [1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1]
alice_sample = [0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1]
```

4 Discussion

The quantum key distribution protocol is used to create and transmit a shared secret key between two entities that wish to engage in private communication. Upon examining this protocol, it was hypothesised that the use of the Y basis along with the X and Z basis to encrypt the message building of the secret key between the entities would increase the uniqueness of the secret key, amplifying the errors displayed if a malicious actor attempted to intercept the key. This hypothesis was then proven by conducting experiments to show this change to the protocol. After these experiments have been conducted it can be said that the quantum key distribution protocol is made more secure by involving the Y basis along with the X and Z basis in the processes used by this protocol.

References

[1] Quantum cryptography, explained, Jan 2020.

[2] The Qiskit Team. Quantum key distribution, Aug 2021.

[3] H. Zbinden, H. Bechmann-Pasquinucci, N. Gisin, and G. Ribordy. Quantum cryptography. In *Applied Physics B: Lasers and Optics*, number 67, pages 743–748, May 1998.