Quantum Key Distribution

Tahir Sajjad Butt(22120013)
Javed Ali(22120008)
Department of Physics, School of Science, LUMS, Lahore, Pakistan

April 9, 2023

Abstract

The comparison between two QKD protocols, BB84 and B92 has been investigated. Both techniques use quantum physics to protect the communication channel and identify any possible eavesdropping attempts. An in-depth analysis of the two protocols, taking into account their advantages, disadvantages, and potential security risks has been given. Finally, a conclusion has been drawn between the two protocols that both are successful in creating safe communication channels, but the selection of protocol is determined by the particular demands of the communication scenario.

1 Introduction

Cryptography is the art of exchanging information between two parties securely. Different techniques are used to encrypt and transmit data in such a way that only the intended recipient can read and comprehend it. Cryptography can be of classical as well as quantum nature.

1.1 Classical cryptography

Our current communication system is based on classical cryptography which depends on a set of mathematical rules called algorithms. It can be of two types namely secret or symmetric key cryptography and public key cryptography. The security of classical cryptography relies on how difficult it is to factor huge numbers computationally. Hence its security is at high risk if computational power improves or some efficient algorithms to solve factorization in a polynomial amount of time are discovered [1].

1.2 Quantum cryptography

Quantum cryptography methods are based on the principles of Quantum Mechanics such as the uncertainty principle [5], no-cloning theorem[5], and quantum entanglement[5]. These concepts guarantee the security of key distribution

and provide an additional advantage of exposing any eavesdropper trying to intercept. Quantum cryptography includes various cryptography techniques such as quantum teleportation, quantum encryption quantum key distribution (QKD), etc. Let's delve into the world of quantum key distribution (QKD) and explore two of its popular protocols, BB84 and B92.

1.2.1 BB84 protocol

The BB84 protocol was proposed by Charles H. Bennett and Gilles Brassard in 1984 at an IEEE conference in India. The technique employs the quantum characteristics of subatomic particles to produce a confidential key. The key's bits are embedded in the polarization states of a sole photon. BB84 uses four polarisation states of the photon namely horizontal (0°, or H-polarisation), vertical (90° or V-polarisation), diagonal (+45°), and anti-diagonal (-45°). This approach relies on two crucial tenets of quantum mechanics, namely the uncertainty principle and the no-cloning theorem, which heighten its security and dependability. This is because the information encoded in the state of a photon cannot be accessed without detecting the state of the photon, which results in its destruction. Also according to the "no-cloning theorem", it is impossible to create identical copies of an unknown quantum state without detecting it, so any eavesdropper (called Eve) attempting to obtain access to the key in an unauthorized way will be exposed. This is due to the fact that she can not create and she has to detect the photon and if she measured it on the wrong basis, she is going to be revealed [2].

1.2.2 B92 protocol

Charles Bennett introduced the B92 protocol in his publication "Quantum Cryptography using any two non-orthogonal States" in 1992 which is a modified version of the BB84 protocol. He realized that only two non-orthogonal polarisation states of a photon are sufficient to encode information. The B92 protocol uses only two non-orthogonal states conventionally the H-polarization state from the rectilinear basis and the +45°-polarization state from the diagonal basis [2].

2 The Mathematical Formulation

2.1 Working of the Bennett-Brassard(BB-84) Protocol

To create a secret, shared key, Bob, and Alice wish to use randomness. Eve, the eavesdropper, wants to learn more about this key without being discovered. If she succeeds in doing this, she will eventually be able to decrypt an actual secret message using that key and read at least a portion of it. Considering that Alice sends quantum signals to Bob as part of the Bennett-Brassard key distribution protocol, Eve will often be unable to measure these signals without creating some disruption. By doing this, Alice and Bob hope to spot Eve's presence and prevent her scheme. There are many generalized cases of the Brennet-Barrasard

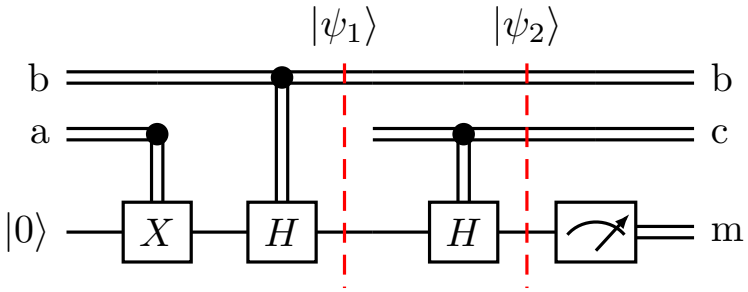

Figure 1: The systematic Diagram of QKD-BB84 protocol. [4]

a	b	$\|\psi_1\rangle$
0	0	$\|0\rangle$
0	1	$\|+\rangle$
1	0	$\|1\rangle$
1	1	$\|-\rangle$

Table 1: Alice basis after the Pauli x and Hadamard gate $|\psi_1\rangle$.

protocol but here we are demonstrating a simple example of the BB-84 protocol as shown in Figure (1) [3].

In this example, Alice is creating the classical random bits which are denoted by "a" and "b". Alice is using Pauli x gate on a classical bit "a" and a controlled Hadamard gate is applied on a classical bit "b" which creates the X and Z bases. A single qubit is used in the state $|0\rangle$. If both random bits a and b are zero, then no transformation occurs on $|0\rangle$ but when a=0,b=1, the Hadamard gate applies on it and converts the state from $|0\rangle$ to $|+\rangle$ as shown in table (1). For a=1,b=0, and a=1,b=1, we get $|1\rangle$ and $|-\rangle$ respectively. Alice then sends this to Bob and Bob on the other hand creates a random classical bit and applies the controlled Hadamard on the incoming qubits as shown in

a	b	c	$\|\psi_2\rangle$
0	0	0	$\|0\rangle$
0	0	1	$\|+\rangle$
0	1	0	$\|+\rangle$
0	1	1	$\|0\rangle$
1	0	0	$\|1\rangle$
1	0	1	$\|-\rangle$
1	1	0	$\|-\rangle$
1	1	1	$\|1\rangle$

Table 2: Final output $|\psi_2\rangle$.

Figure (1). This increases the number of possibilities as shown in Table (2). Bob performed a measurement and compares the results of his and Alice's classical bit b. Bob can publically declare that the b=c or b≠c. An interesting pattern is observed here when b=c, the output of $|\psi_2\rangle$ is the same as the classical bit "a" as shown in Table (2). Bob and Alice decide that they need to just save the outputs of b=c and discard the other. They discard the other bits and perform this experiment many times which gives them a Quantum key.
What if an eavesdropper called Eve decides to intercept their message? Eve cannot read the message without collapsing the states which makes QKD secure. When Eve decided to measure the state, Eve needs the X and Z bases, which already reduces the chances up to 50-50 probability. If Eve can extract a lot of information from a photon while reducing the likelihood that she will make a mistake that can be detected, she has a successful technique. How can we calculate the quantity of information she gains? We know how to calculate the probability of an error. We can use error correction methods and privacy application techniques but we also need to find a way to check how much information Eve obtained. We use Renyi entropy for this, The Renyi entropy, which we will define as a measure of the amount of information Eve lacks about the bit, turns out to be a valuable mathematical tool for determining Eve's information in such a case.

$$H_R = -log_2(P_0^2 + P_1^2), \tag{1}$$

Even though Renyi entropy is a pure integer that does not require units, it is frequently mentioned as being measured in "bits" [3].

2.2 Working of B92 protocol

- Since in this protocol only two polarization states are used, Alice can choose to use the H-polarization state from the rectilinear basis to represent zeros, and the +45°-polarization state from the diagonal basis to represent ones.

- Bob also has the freedom to randomly chose either of the two basis to measure the photon he receives. Now if Bob measures the photon in a rectilinear basis then there are two possible outcomes. If the incident photon was in the H-state then Bob will measure it in the H-state with probability 1. But if the incident photon was in the +45°-state then he will measure it with probability 1/2. As he can either get an H-state or a V-state.

- Similarly if Alice sends a +45°-state photon then Bob has two options: measure in the H-state or the +45°-state. If Bob measures in the H-state, he can measure the H-state or the V-state with equal probability 1/2. But if his measurement outcome results in the V-state then he will realize that he has selected the wrong basis and Alice must have used the +45° state, since neither Alice nor Bob use the V-state.

- The same is true if Bob measures in a diagonal basis. If he detects the -45°-state, he will infer that the polarization state of the photon was 'H' and he has used the wrong basis.
- After transmission of the photon sequence, Bob records each time where the measurement result was either a 'V-state' or a '-45°-state', and both discard the remaining outcomes. And using these results, Alice and Bob can generate a secret Key.
- Alice and Bob make a piece of the created random bit string out to the public in order to prevent eavesdropping. The protocol ends if the error rate of the exposed bits exceeds a predefined threshold. They can utilize the extra bits to create a safe and symmetric key that links them assuming the error rate is tolerable [2].

References

[1] Classical Cryptography and Quantum Cryptography. (2019, April 29). GeeksforGeeks. https://www.geeksforgeeks.org/classical-cryptography-and-quantum-cryptography/

[2] Roorkee, Q. C. G., IIT. (2021, September 6). Fundamentals of Quantum Key Distribution BB84, B92 E91 protocols. Medium. https://medium.com/@qcgiitr/fundamentals ofquantum key distribution-bb84-b92-e91-protocols-e1373b683ead

[3] Loepp, S., Wootters, W. K. (2006). Protecting Information. Cambridge University Press.

[4] 28. Quantum key distribution I: BB84 protocol. (n.d.). Www.youtube.com. Retrieved April 8, 2023, from https://youtu.be/uK9jPBrOwA

[5] Haitjema, M. (n.d.). A Survey of the Prominent Quantum Key Distribution Protocols. Retrieved April 9, 2023, from https://www.cse.wustl.edu/ jain/cse571-07/ftp/quantum.pdf