Quantum Key Distribution

Tahir Sajjad Butt(22120013)
Email: 22120013@lums.edu.pk

Javed Ali(22120008)
Email: 22120008@lums.edu.pk
School of Science and Engineering(SSE),LUMS, Pakistan.

May 8, 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.

Keywords
QKD protocols BB84 and B92, Classical and Quantum Cryptography.

Contents

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 BB-84 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 B-92 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 Implementation Methodology

The rectilinear bases can be represented by the symbol Z, while the horizontal and vertical states of a photon can be represented by $|0\rangle$ and $|1\rangle$, respectively. Similarly, the diagonal bases can be represented by the symbol X, with the diagonal and anti-diagonal states of a photon represented by $|+\rangle$ and $|-\rangle$, respectively. Here, $|+\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}$, and $|-\rangle = \frac{|0\rangle-|1\rangle}{\sqrt{2}}$.

2.1 Implementation of the QKD BB-84 protocol

The implementation of the BB-84 protocol can be generalized in the following steps:

1. Alice generates two random binary strings: A = $(a_1, ..., a_n)$ and S = $(s_1, ..., s_n)$. The entries a_i are zeros and ones, and a portion of these entries will eventually be utilized to generate a shared secret key. The entries s_i are picked from the binary set "Z and X."

2. Alice sends a sequence of n photons to Bob, and the polarization of the ith photon is determined as follows: If $|\psi\rangle$ = Z, the photon's polarization will be selected from the rectilinear basis ($|0\rangle$,$|1\rangle$). On the other hand, if $|\psi\rangle$ = X, the photon's polarization will be chosen from the diagonal basis ($|+\rangle$,$|-\rangle$). Alice will use the first or second element of the basis depending on whether a_i equals 0 or 1. The bit Alice intends to send to Bob is represented by a_i, while s_i determines how she will encode the bit[3].

3. Bob generates a random string R of length n before receiving any photons. Each entry in R is chosen from the set Z, X. When he receives the ith photon, he measures its polarization in the basis labeled by r_i and records the outcome as either 0 or 1, depending on which of the two possible outcomes he obtains. Thus, Bob obtains a sequence B of length n, consisting of zeros and ones that represent the results of his measurements. It is important to note that Alice and Bob may not have used the same basis for a given photon i, and therefore s_i may not be equal to r_i. However, if they used

the same basis, and the photon was not disturbed during transmission, then a_i should be equal to b_i. For instance, if Alice sent a photon in the state $|1\rangle$ using the basis ($|0\rangle$,$|1\rangle$) and Bob measured it in the same basis, he should obtain the outcome $|1\rangle$ and record the bit 0. On the other hand, if they used different bases, then there should be no correlation between Alice's bit a_i and Bob's bit b_i.

4. Alice and Bob communicate by sending photons and then use a public channel to exchange their sequences of bases S and R. They compare the two sequences and identify the index values i where there are differences. At this stage, they are not comparing any values from their bit strings A and B, only the bases. Alice and Bob then remove the bits in their respective bit strings that correspond to the identified index values. The resulting shorter strings are labeled $A^{'}$ and $B^{'}$. Assuming that there was no interference, $A^{'}$ and $B^{'}$ should be identical and have an expected length of n/2, as there is a 50% chance that Alice and Bob used the same basis for each photon transmitted.

5. Even if there is no eavesdropper, there will still be transmission mistakes. Now that there are errors or bits in $B^{'}$ that are not equal to their counterparts in $A^{'}$, Alice and Bob want to estimate how many errors there are. To accomplish this, Alice sends Bob a small random sample of her actual bits from $A^{'}$ over a public channel, which Bob then compares to the corresponding bits in $B^{'}$. After the comparison, Alice and Bob ignore these details because Eve might be aware of them. They now want to fix these remaining problems, presuming that the remaining bits have roughly the same percentage of errors as the ones they checked. To see how they will do this without giving everything away, refer to the example in the Mathematical Formulation section (error correction and privacy amplification). Upon completion of this stage, Alice and Bob are expected to have acquired shorter strings $A^{''}$ and $B^{''}$, which are highly likely to be identical.

6. Alice and Bob estimate the maximum information an eavesdropper may have obtained about the remaining bits in step 5, based on the errors they have identified. They use this estimate to create shorter strings $A^{'''}$ and $B^{'''}$ to replace $A^{''}$ and $B^{''}$, respectively. These new strings are almost entirely unknown to the eavesdropper and can be used to generate a secret key, which in turn can be used to encode and send information securely[3].

Let us elaborate on how Alice and Bob can detect errors in their communication and how an eavesdropper's interference can cause errors. In the communication process, each photon is associated with a basis, and if Eve knows the basis of a given photon, she can learn Alice's bit without disrupting the signal. However, the protocol used in step 2 prevents Eve from knowing which basis Alice uses to encode each bit. Therefore, Eve may guess the basis and measure the photon accordingly. If her guess is correct, she will obtain the bit as intended. However, if she guesses incorrectly, errors may occur. To be specific, let's assume Alice is using the Z basis ($|0\rangle$,$|1\rangle$) and is sending the bit 0, which is represented by the state $|1\rangle$. However, Eve measures the photon using the wrong X basis ($|+\rangle$,$|-\rangle$). There are two equally likely outcomes of her measurement, but neither outcome reveals what state Alice actually sent. Therefore, Eve has not gained any information about Alice's bit a_i. Moreover, Eve is unaware that she used the wrong basis, so she prepares and sends a new photon to Bob with the diagonal polarization corresponding to her measurement outcome[3].

What occurs on Bob's end now? If Bob is using the diagonal basis X, then it's irrelevant because, according to step 4, the associated bits of this photon will eventually be disregarded. Therefore, we can focus on the case where Bob uses the same basis as Alice, which is the rectilinear basis Z in our example. Bob measures a diagonally polarized photon in a rectilinear basis, and the two outcomes have an equal likelihood. If Bob receives the vertical outcome, it's lucky for Eve because she records the bit $b_i = 0$, which matches Alice's bit a_i. Consequently, this photon doesn't offer any evidence of Eve's interference to Alice and Bob. At this point, "lucky" for Eve refers only to minimizing the damage. It's already been established that she hasn't learned anything about Alice's bit. However, she can hope that her attempt won't be detected. If Bob receives the horizontal outcome, he'll record the bit $b_i = 1$, which is not equal to a_i. This disparity will exist in the strings A' and B' and could be discovered in step 5. If this occurs, Alice and Bob will have learned something about Eve's behavior through her attempt to learn the details of the key that she and Bob exchanged[3].

To calculate the relevant probabilities, let's consider a scenario where Eve decides whether to measure each photon probabilistically, and the probability of measuring a photon is p. Now, let's analyze the probability of Eve causing an error in a photon whose bit will be part of the strings A and B. The probability of error in such a bit is p/4. This means that there's a p chance that Eve will measure the photon, a 1/2 probability that she will select the wrong basis, and if she does so, there's a 1/2 chance of her causing an error. We can also determine the probability of Eve learning the value of the bit, which is p/2 since she can learn the value only when she chooses the correct basis. Thus, in the long term, for every two bits that Eve learns, she is likely to cause one error[3].

Eve can employ a variety of strategies, but one that works well for her is to extract as much information as she can from a photon with the least chance of making an observable error. While the likelihood of an error can be calculated, it is more difficult to estimate how much information Eve will learn. Since Eve either learned the value of a bit or didn't, the calculation in the previous example was fairly simple. With other methods, though, the information she gathers might be hazy or probabilistic. For instance, without being positive, she might believe that the value 0 is more likely than 1. The Renyi entropy is a valuable mathematical tool to quantify the amount of information Eve gains in such circumstances.

Eve's chances of getting either a bit value of 0 or 1 are initially equal, making both outcomes equally likely for her. So, p_0 and p_1 are both equal to half.

However, Eve hopes that after measuring the photon and learning about Alice and Bob's open communication, her probabilities will be more biassed towards one of the two bit values. She might anticipate that, for instance, $p_0 = 3/4$ and $p_1 = 1/4$. The "Renyi entropy" of order 2, denoted by H_R, is a measure of the uncertainty that Alice has about the bit, whether before or after she takes a measurement. It is defined as

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

Where p_0 and p_1 are the probabilities of the bit being 0 or 1, respectively. This entropy quantifies the information that Alice is missing about the bit. The term "entropy" can be used interchangeably with "uncertainty." This can be a helpful way to understand what entropy means in this context. Although Renyi entropy is dimensionless, it is commonly described in "bits." For instance, if Eve's probabilities were $p_0 = 1$ and $p_1 = 0$, her Renyi entropy would be H_R = - $log_2(1^2 + 0^2) = 0$ bits, which indicates that she has no missing information. In contrast, when the two probabilities are equal, as they are before Eve makes her measurement, her Renyi entropy equals H_R = - $log_2(1/2^2 + 1/2^2) = 1$ bit, which is the highest possible value. Thus, if you have no prior knowledge about the bit's value, you are missing one bit of information. Suppose that after measuring, Eve's probabilities of obtaining outcomes 0 and 1 are $p_0 = 3/4$ and $p_1 = 1/4$, respectively. In this case, her Renyi entropy is given by the formula

$$H_R = -log_2(\frac{3}{4})^2 + (\frac{1}{4})^2 = 0.678 \; bits, \tag{2}$$

which is less than the maximum value it could be. We can refer to the difference between Eve's Renyi entropy and its maximum value as her "Renyi information" for convenience. Thus,

$$Renyi \; information = 1 - (Renyi \; entropy) = 1 - H_R[3]. \tag{3}$$

2.2 Implementation of the QKD B-92 protocol

The implementation of the B-92 protocol is similar to that of the BB-84 protocol, with the main difference being that the former utilizes only two non-orthogonal polarization states of a photon. However, the implementation of the B-92 protocol can be generalized in the following steps:

1. Alice can choose to represent zeros using the H-polarization state (i.e, $|0\rangle$) from the rectilinear basis and ones using the +45°-polarization state (i.e, $|+\rangle$ from the diagonal basis, as only two polarization states can be used.

2. Bob also has the freedom to randomly choose either of the two bases to measure the photon he receives. If Bob measures the photon in a rectilinear basis, there are two possible outcomes. If the incident photon was in $|0\rangle$, then Bob will measure it in $|0\rangle$ with a probability of 1. However, if the incident photon was in the $|+\rangle$, he will measure it with a probability of 1/2, as he can either get an $|0\rangle$ state or a $|1\rangle$

3. Similarly if Alice sends a $|+\rangle$ photon then Bob has two options: measure in the $|0\rangle$ or the $|+\rangle$. If Bob measures in the$|0\rangle$, he can measure the $|0\rangle$ or the $|1\rangle$ with equal probability 1/2. But if his measurement outcome results in the $|1\rangle$ then he will realize that he has selected the wrong basis and Alice must have used the $|+\rangle$ since neither Alice nor Bob uses the $|1\rangle$.

4. The same is true if Bob measures in a diagonal basis. If he detects the $|+\rangle$, he will infer that the polarization state of the photon was $|0\rangle$ and he has used the wrong basis.

5. After transmission of the photon sequence, Bob records each time where the measurement result was either a '$|1\rangle$' or a '$|-\rangle$', and both discard the remaining outcomes. And using these results, Alice and Bob can generate a secret Key.

6. Alice and Bob generate a random bit string and share a portion of it publicly to prevent unauthorized access. If the number of incorrect bits in the shared portion exceeds a certain limit, the protocol ends. They can use the remaining bits to create a secure and mutually agreed-upon key, as long as the number of errors is within an acceptable range[2].

3 The Mathematical Formulation of 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 protocol but here we are demonstrating a simple example of the BB-84 protocol as shown in Figure (1) [4].

Table 1: Alice basis after the Pauli x and Hadamard gate $|\psi_1\rangle$[4].

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

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

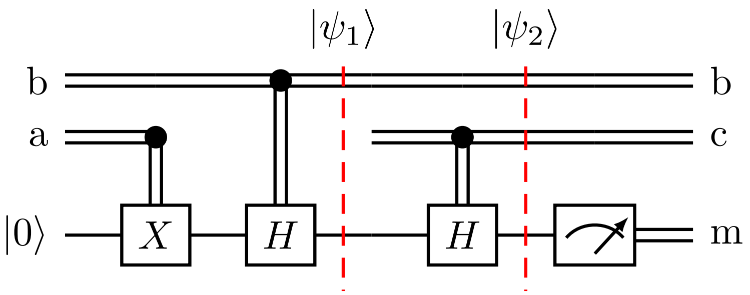


Figure 1: The systematic Diagram of QKD-BB84 protocol. [4]

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 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[4].

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

Table 2: Final output $|\psi_2\rangle$[4].

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	$\|1\rangle$

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.

$$H_R = -log_2(P_0^2 + P_1^2), \tag{4}$$

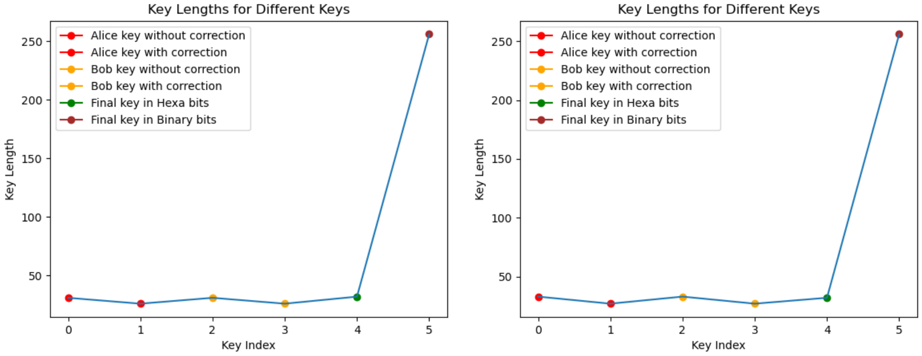
Even though Renyi entropy is a pure integer that does not require units, it is frequently mentioned as being measured in "bits" [3].

4 Results and Disscusion

The experiment was conducted using the BB84 and B92 protocols for quantum key distribution. In the BB84 protocol, Alice and Bob exchanged a total of 100 bits, of which 31 bits were successfully exchanged between them. The error correction is applied to the obtained Alice's key and Bob's key using the parity check[6][7][8] and hamming code[9][10]. The length of the keys was reduced to 26 bits. Privacy amplification code was implemented on the obtained Alice's key and Bob's key by using a hash function which enhanced the security of the secret key. The hash function first stored the bits in hexa bits and then converted the bits into binary form. The length of hexa bits and binary bits are shown in Figure (2a). The error rate from the samples was found to be 33.3% while the total error was found to be 35% and 15 errors were found in the keys. The accuracy before the error correction was 64.5 % while the accuracy after the error correction was found to be 100%.

In the B92 protocol, Alice and Bob exchanged a total of 100 bits, of which 33 bits were successfully exchanged between them. The error correction is applied to the obtained Alice's key and Bob's key using the parity check and hamming code. The length of the keys was reduced to 27 bits. Privacy amplification code was implemented on the obtained Alice's key and Bob's key by using a hash function which enhanced the security of the secret key. The has function first stored the bits in hexa bits and then converted the bits into binary form. The length of hexa bits and binary bits are shown in Figure (2b). The error rate from the sample was found to be 50.0% while the total error was found to be 51.5% and 15 errors were found in the keys. The accuracy before the error correction was 48.4 % while the accuracy after the error correction was found to be 100%.

The results show that the BB84 protocol is more efficient and secure than the B92 protocol. The higher percentage of bits that were successfully exchanged without errors in the BB84 protocol indicates that it has a higher transmission rate and is less vulnerable to errors. In contrast, the B92 protocol has a higher error rate and is less efficient than the BB84 protocol. Overall, the results suggest that the BB84 protocol is a more robust and reliable method for quantum



(a) This figure shows Alice's and Bob's bits without and after correction and also represents the hexa bits and final secret key in binary form for BB84 protocol

(b) This figure shows Alice's and Bob's bits without and after correction and also represents the hexa bits and final secret key in binary form for B92 protocol

Figure 2: The Plots of the QKD BB84 and B92 protocols

key distribution but it costs a lot, and it requires four states while B92 does the transmission into two states.

5 Conclusion

we can conclude that the BB84 and B92 protocols each have different advantages and disadvantages. The best protocol to adopt will depend on the particulars of the communication as well as the resources available. Although the B92 protocol is easier to use and uses fewer resources, it is less secure than the BB84 protocol and has a higher error rate. Therefore, choosing the right protocol for a given application requires finding a balance between security, resource needs, and error tolerance. It is likely that as quantum cryptography continues to develop, new protocols that combine the positive aspects of both BB84 and B92 will emerge, further enhancing the security and effectiveness of quantum key distribution.

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 and 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

[6] What is Parity? (n.d.). Www.youtube.com. Retrieved April 30, 2023, from https://www.youtube.com/watch?v=DdMcAUlxh1M

[7] 4-Bit Even Parity Generator. (n.d.). Www.youtube.com. https://www.youtube.com/watch?v=RfTGvpY2Z5Y

[8] Hamming Code — Error detection. (n.d.). Www.youtube.com. https://www.youtube.com/watch?$v = 1A_NcXxdoCc$

[9] How to send a self-correcting message. (n.d.). Www.youtube.com. https://www.youtube.com/watch?$v = X8jsijhllIA$

[10] 3Blue1Brown. (2020). Hamming codes part 2, the elegance of it all. In YouTube. https://www.youtube.com/watch?$v = b3NxrZOu_CE$