Institute of Business Administration

Department of Computer Science

# Quantum Key Distribution Using the BB84 Protocol: A Simulation-Based Approach

*Milestone 1 – Theoretical Report*

MOHAMMAD KAMIL (29464)

*Supervisor:*

Dr. Jibran Rashid

# Contents

**List of Figures** **ii**

**List of Tables** **iii**

**1 Introduction** **2**

**2 Literature Review** **4**
2.1 Background and Literature Review . . . . . . . . . . . . . . . . . . . . . . . 4

**3 Key Quantum Principles Behind QKD** **5**
3.1 Key Quantum Principles Behind QKD . . . . . . . . . . . . . . . . . . . . . 5
3.1.1 Superposition . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 5
3.1.2 Entanglement . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 5
3.1.3 The Uncertainty Principle . . . . . . . . . . . . . . . . . . . . . . 7

**4 Key Concepts Used in BB84** **8**
4.1 Key Concepts Used in BB84 . . . . . . . . . . . . . . . . . . . . . . . . . . 8
4.1.1 Photons and Polarization . . . . . . . . . . . . . . . . . . . . . . 8
4.1.2 Rectilinear and Diagonal Bases . . . . . . . . . . . . . . . . . . . 8
4.1.3 Measurement and Basis Matching . . . . . . . . . . . . . . . . . . 9

**5 BB84 Protocol** **10**
5.1 BB84 Protocol . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 10
5.2 Applications of the BB84 Protocol . . . . . . . . . . . . . . . . . . . . . . 12
5.3 Limitations of the BB84 Protocol . . . . . . . . . . . . . . . . . . . . . . . 12

**6 Conclusion** **13**
6.1 Conclusion . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 13

**References** **14**

# List of Figures

1.1 Illustration of classical and quantum communication channels, highlighting the involvement of third party entities in the key exchange process . . . . . . . . 3

3.1 Quantum Superposition . . . . . . . . . . . . . . . . . . . . . . . . . . . . 6
3.2 Quantum Entanglement . . . . . . . . . . . . . . . . . . . . . . . . . . . . 6
3.3 Uncertainty Principle . . . . . . . . . . . . . . . . . . . . . . . . . . . . 7

4.1 Photon Polarization . . . . . . . . . . . . . . . . . . . . . . . . . . . . 9

# List of Tables

4.1 Example of basis matching in BB84 protocol . . . . . . . . . . . . . . . . . . 9

5.1 Transmission between Alice and Bob (no eavesdropper) . . . . . . . . . . . . 11

# Abstract

In the modern digital world, the security of data and communication has become a critical concern. People exchange personal, financial, and sensitive information over the internet every day. Today's encryption systems mostly rely on mathematical algorithms that are believed to be hard to break. However, with the rise of quantum computing, these systems could become vulnerable, as quantum computers may eventually solve these problems much faster than classical computers. In order to deal with this risk, scientists tried to find a new way to protect data called Quantum Key Distribution (QKD). QKD does not rely on complex math but uses the laws of quantum mechanics. One of the most popular and widely studied QKD protocols is BB84, which was introduced by Charles Bennett and Gilles Brassard in 1984. BB84 uses quantum bits (qubits) to generate a shared key between two parties to detect any eavesdropping. So in this milestone, I have clearly explained how the BB84 protocol works, how it is considered secure, and how it can be applied in real-world scenarios. The main goal of this milestone is to build a strong theoretical understanding of the protocol before moving to the implementation phase, as understanding theoretical concepts is essential for implementation milestones.

# Chapter 1

# Introduction

In today's modern world, we do nearly everything with digital communication, like sending a message to a friend, paying online, or accessing a bank account. All this data passes over networks and must be secure from hackers or unauthorized use. Our data is kept secure by using encryption techniques that render readable data into unreadable code. These encryption schemes rely on knotty mathematical problems that regular computers have difficulty solving. For instance, most systems utilize algorithms such as RSA or ECC, which rely on problems such as factoring large numbers or solving elliptic curve equations. These are hard problems to solve with current computing capabilities, so they've been relied upon for decades. But as technology advances, especially with the development of quantum computers there's increased fear that the current systems may no longer work. That is why there is a need to investigate new and more secure methods, and this is where quantum cryptography and algorithms such as BB84 step in. One widespread technique is public key cryptography that utilizes two keys, one for public use and the other for private use, to secure information. Although this system is effective now, most consider that it might not stay secure.

This issue arises due to the quick progress of quantum computing. Unlike conventional computers, which operate using either 0 or 1 bits, quantum computers operate using qubits, which can be 0 and 1 simultaneously, also referred to as superposition. Due to this, quantum computers are capable of performing certain kinds of calculations much quicker than classical computers. This involves the type of problems that current encryption is based on. If an adequate quantum computer is developed, it would have the ability to break current encryption techniques quickly.

Scientists have begun researching new mechanisms to secure digital communication to combat this future challenge. Quantum Key Distribution (QKD) holds much promise as a solution. Rather than relying on difficult-to-break equations, QKD relies upon the principles of quantum physics to protect information. It operates in a way that any effort to eavesdrop or interfere with the communication will naturally disrupt the system, leaving traces of tampering. This will enable the sender and receiver to realize whether someone is attempting to spy and respond before anything leaks out. QKD, particularly the BB84 protocol, is a strong candidate for protecting future networks against quantum threats. It offers a method that doesn't just make spying hard, it makes it physically impossible without being noticed.

The BB84 protocol is the first and one of the most famous QKD methods. It was introduced by Charles Bennett and Gilles Brassard in 1984, so it's named BB84 Shor and Preskill (2000). In this protocol, two people (Alice and Bob) exchange a secret key by sending qubits to each other. What makes BB84 special is that if anyone tries to intercept or measure the qubits during transmission, their presence is automatically revealed due to the nature of quantum measurement. I have added a diagram related to classical and quantum channels where third parties are involved in the communication channel as shown in F*igure 1.1*.

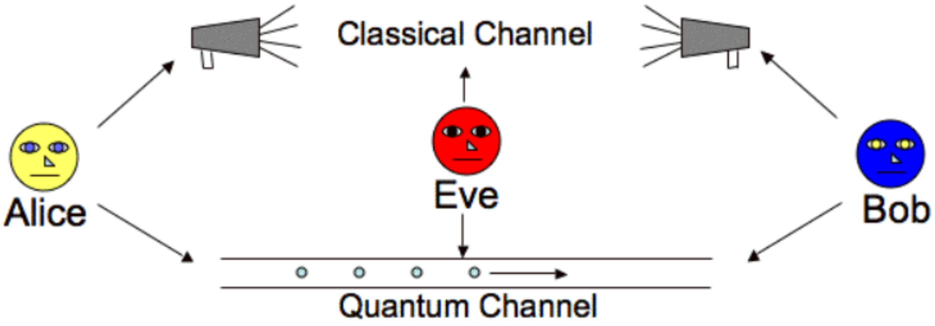

Figure 1.1: Illustration of classical and quantum communication channels, highlighting the involvement of third party entities in the key exchange process

This report is written as part of the first milestone of a quantum computing project. The goal of this milestone is to build a strong understanding of the BB84 protocol from a theoretical point of view before diving into its implementation and simulation. Instead of starting directly with coding, it's important to first study how the protocol works, what makes it secure, and why it differs from traditional encryption methods.

In this report, I have tried to explain all the core ideas behind BB84 and clearly. From how qubits are used to how photons are polarized and measured, each section focuses on breaking down the process step by step. The report also highlights how the protocol performs when there is no eavesdropper, how the sifted key is formed, and what real-world situations it can be applied to.

By completing this milestone, the goal is to develop a strong foundation that will make the upcoming stages, such as writing the code, testing the protocol, and handling cases like eavesdropping, more straightforward to understand and implement

# Chapter 2

# Literature Review

## 2.1 Background and Literature Review

Quantum cryptography is a new area in the field of secure communication. Unlike classical cryptography, which depends on mathematical assumptions and complex algorithms, quantum cryptography uses the laws of quantum mechanics to protect information Gisin et al. (2002). These laws are part of physics and are believed to be unbreakable, even by the most powerful computers in the future.

The main goal of quantum cryptography is to allow two parties to share a secret key in a way that ensures no one else can know it, not even if someone is listening. The most well-known method of achieving this is through QKD. In QKD, the secret key is not sent directly. Instead, it is created between the two parties during communication using qubits. These qubits are special because they behave differently from regular bits and cannot be copied without leaving evidence of tampering. This characteristic property renders QKD an effective means of secure data exchange. The BB84 protocol is the first and most well-known instance of quantum key distribution. It was introduced in 1984 by Charles H. Bennett and Gilles Brassard Shor and Preskill (2000). In BB84, the key idea is that any attempt to observe or measure a quantum particle, such as a qubit, changes its state. This makes it possible to detect if someone (eavesdropper) is trying to intercept the key.They showed using two different measurement bases (rectilinear and diagonal bases). I'll discuss in detail in the next sections. Since the BB84 protocol was introduced, many researchers have worked on improving, testing, and applying it in real-world systems. According to Scarani et al. (2009), BB84 remains one of the most practical and widely used QKD protocols due to its simplicity and clear theoretical basis. It has been tested over optical fiber, in free space, and even between satellites and ground stations, proving its potential for real-world use.

Another key work is by Korzh et al. (2015) who reviewed the security of QKD protocols and confirmed that BB84 provides unconditional security under ideal conditions. That means no matter how powerful the attacker is, even if they have a quantum computer. They still cannot break the BB84 protocol without being detected. Furthermore, recent research Chen et al. (2021) discusses successful implementation of a satellite-based QKD system using BB84, showing that it's now being applied beyond the lab and into actual communication infrastructure.

Even after many years, the BB84 protocol is still being taught, studied, and tested worldwide. One reason for this is that it combines a simple idea with a compelling result: secure communication that cannot be secretly intercepted. Many later QKD protocols are based on the same ideas introduced in BB84, and it continues to serve as the standard protocol for learning and experimenting with quantum communication systems.

# Chapter 3

# Key Quantum Principles Behind QKD

## 3.1 Key Quantum Principles Behind QKD

Before going into how the BB84 protocol works, it's important to understand the three core ideas from quantum mechanics that make QKD possible. These are not just technical terms but they are real phenomena observed in physics that behave very differently from anything in the classical world. The three concepts most relevant to QKD are superposition, quantum entanglement, and the uncertainty principle. Each of these plays an important role in how information is encoded, transmitted, and protected in a quantum communication system.

### 3.1.1 Superposition

Superposition refers to the idea that a quantum bit (or qubit) can exist in multiple states at once, not just as a 0 or a 1, like a regular bit, but as a combination of both simultaneously as show in *Figure 3.1*. This may sound strange, but it's a well-proven part of quantum physics. In the context of QKD, superposition allows us to encode information in impossible ways with classical systems.

When Alice sends qubits to Bob, she prepares each qubit in one of two possible bases: the rectilinear (Z) basis or the diagonal (X) basis. Because of superposition, if Bob chooses the same basis as Alice, he gets the correct bit with full accuracy. But if he chooses the wrong basis, the qubit "collapses" into a random state when measured. This collapse happens because superposition only lasts until the qubit is observed. The fact that a measurement forces the qubit into one clear state is a critical part of what makes the BB84 protocol secure.

Superposition introduces the idea that information in a quantum state cannot be perfectly known unless the person measuring it knows how it was prepared. This is what prevents anyone from secretly copying or intercepting the qubits without being noticed.

### 3.1.2 Entanglement

Quantum entanglement is another fundamental concept in quantum physics. It describes a situation where two particles become connected in such a way that the state of one directly affects the state of the other, even if a large distance separates them. While the BB84 protocol itself does not use entanglement directly, understanding this concept helps us appreciate the broader potential of quantum communication.

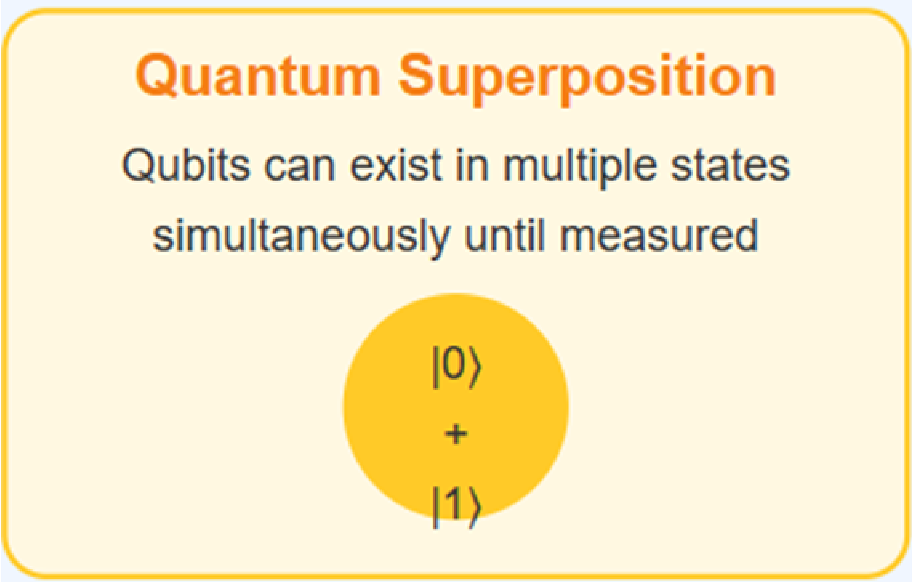
Quantum Superposition
Qubits can exist in multiple states simultaneously until measured
|0⟩
+
|1⟩

Figure 3.1: Quantum Superposition

In more advanced QKD protocols such as the E91 protocol, entangled particles are used to create shared randomness between two distant parties as shown in *figure 3.2*. In those cases, measuring one particle instantly reveals the state of the other, and any tampering with the entangled state is easy to detect. Although BB84 doesn't rely on entanglement, it still builds on the broader framework of quantum theory that includes it. Entanglement demonstrates that quantum particles can be strongly correlated in ways that defy classical logic, and this opens doors to communication methods that are fundamentally unhackable.

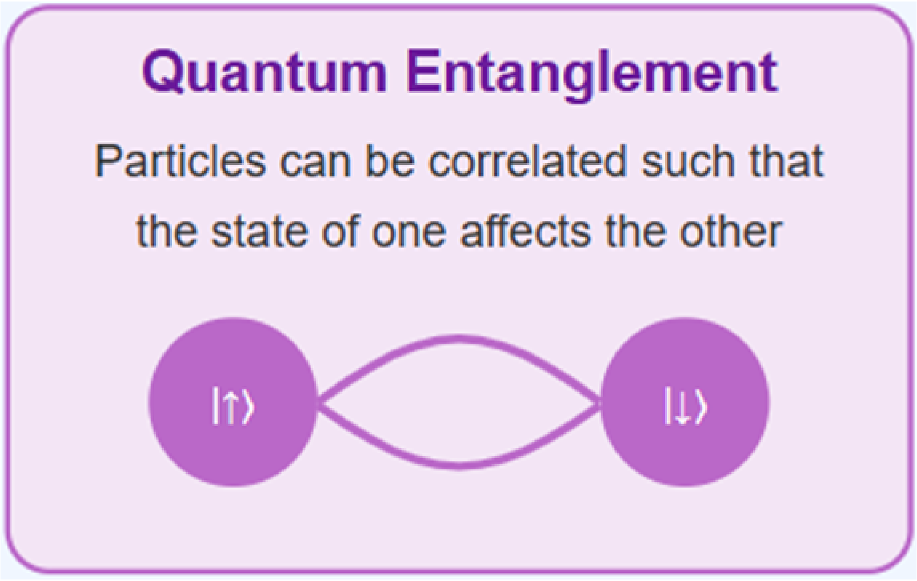
Quantum Entanglement
Particles can be correlated such that the state of one affects the other
|↑⟩
|↓⟩

Figure 3.2: Quantum Entanglement

### 3.1.3 The Uncertainty Principle

The uncertainty principle, initially proposed by Werner Heisenberg, states that certain pairs of properties in a quantum system cannot be known exactly simultaneously. The more precisely one is known, the less precisely the other can be known. In the case of QKD, this principle is reflected in how qubits behave when measured in the wrong basis as shown in F*igure 3.3*.

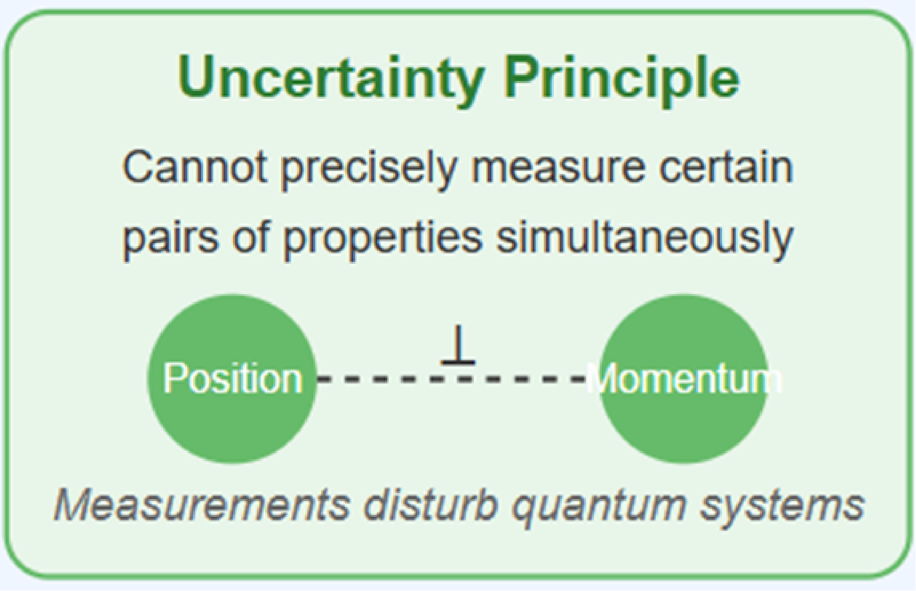
Uncertainty Principle
Cannot precisely measure certain pairs of properties simultaneously
Position
⊥
Momentum
Measurements disturb quantum systems

Figure 3.3: Uncertainty Principle

For example, if Alice sends a qubit prepared in the diagonal basis, but Bob measures it in the rectilinear basis, his result is no longer reliable. He may get a 0 or a 1, but there is a 50% chance of error. This is not due to technical faults, but because the laws of physics do not allow both types of information (X and Z bases) to be observed simultaneously without interfering with the system.

This principle plays a key role in the security of BB84. If an Eve tries to intercept the qubits sent from Alice to Bob, she has to choose a measurement basis, but since she doesn't know which basis Alice used, she will guess incorrectly half the time. This creates detectable errors in the final key, and these errors reveal that someone has been spying.

Chapter 4

# Key Concepts Used in BB84

## 4.1 Key Concepts Used in BB84

Before going into the steps of the BB84 protocol, it's important to understand a few basic concepts from quantum physics. These ideas help explain how information is carried, measured, and secured using quantum particles. Without understanding these terms, the understanding of the BB84 process will be complex. This section introduces photons, polarization, and the two types of bases used in the protocol, all of which play a central role in achieving secure communication.

### 4.1.1 Photons and Polarization

In BB84 information is sent using tiny particles of light called photons. These are the smallest units of light energy and behave according to the rules of quantum physics. Each photon can carry a bit of information, either 0 or 1, depending on its polarization.

Polarization means the direction in which the light wave vibrates. You can think of it like shaking a rope — you can shake it up and down (vertical), side to side (horizontal), or at an angle. Photons can also be polarized in similar directions. In BB84, we use four types of polarization to represent 0s and 1s as shown in Figure 4.1:

- **Vertical (|)**: Represents 0 in the *rectilinear basis*
- **Horizontal (—)**: Represents 1 in the *rectilinear basis*
- **+45° (/)**: Represents 0 in the *diagonal basis*
- **45° (\)**: Represents 1 in the *diagonal basis*

When a photon is sent with a certain polarization, it can only be properly measured if the receiver uses the correct matching direction (basis). If the direction is wrong, the measurement becomes uncertain or random. This is where quantum security comes in.

### 4.1.2 Rectilinear and Diagonal Bases

The BB84 protocol uses two measurement bases, each with its own way of representing 0s and 1s using photon polarization:

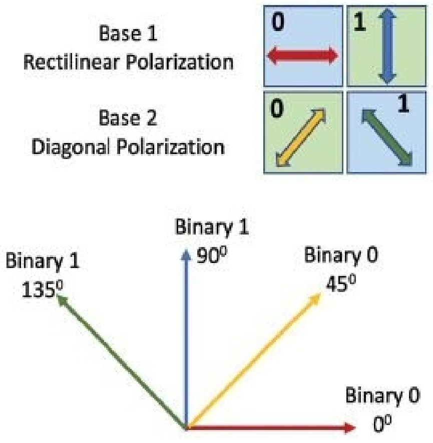

Figure 4.1: Photon Polarization

### Rectilinear Basis (Z Basis)

- 0 is sent as a vertically polarized photon
- 1 is sent as a horizontally polarized photon

### Diagonal Basis (X Basis)

- 0 is sent as a photon polarized at $+45^\circ$
- 1 is sent as a photon polarized at $-45^\circ$

## 4.1.3 Measurement and Basis Matching

The idea of matching bases is central to how BB84 works. Bob does not know which basis Alice used, so he guesses each time. After the photon transmission is complete, Alice and Bob compare which bases they used. They only keep the results where their basis choices matched. They know those bits are accurate and can be trusted.

The bits from matching bases become part of their shared secret key. The rest are thrown away. This method helps ensure that the final key is built only from reliable data. *Table 4.1* shows how Alice and Bob exchange bits using randomly chosen bases. When their bases match, Bob receives the correct bit, and the bit is kept. When the bases differ, the result is random, and the bit is discarded.

Table 4.1: Example of basis matching in BB84 protocol

| Bit # | Alice Bit | Alice Basis | Bob Basis | Bob Result | Keep? |
|---|---|---|---|---|---|
| 1 | 1 | Z | X | Random | NO |
| 2 | 0 | X | X | 0 | YES |
| 3 | 1 | Z | Z | 1 | YES |
| 4 | 0 | X | Z | Random | NO |

# Chapter 5

# BB84 Protocol

## 5.1 BB84 Protocol

As I already discussed, BB84 helps to exchange a secret key by sending qubits to each other. The main goal of the protocol is for two people(Alice and Bob), to share a secret key that only they know. This key can later be used to encrypt and decrypt messages securely.The BB84 protocol involves sending and measuring qubits, comparing measurement bases, and building a final key from the bits that were calculated correctly.The BB84 protocol mainly uses four different qubits that are randomly generated by the sender and receiver, who are Alice and Bob, respectively.

- 0 in Z basis → Vertical polarization
- 1 in Z basis → Horizontal polarization
- $+$ in X basis → $+45^\circ$ polarization
- $-$ in X basis → $-45^\circ$ polarization

I have presented the transmission between Alice(A) and Bob(B) in *Table 5.1*, which shows how Alice and Bob communicate using the BB84 protocol without any interference from an eavesdropper. Alice randomly chooses bit values and encoding bases (Z or X), and sends each bit as a polarized photon. Bob also randomly chooses a basis to measure each photon. Whenever both use the same basis, Bob successfully measures the correct bit, and they agree to keep it. If their bases differ, the result is random, and the bit is discarded. This process helps them gradually build a shared key using only the bits they can trust.

Table 5.1: Transmission between Alice and Bob (no eavesdropper)

| Bit # | A Bit | A Basis | Polarization | State | B Basis | B Result | Keep? |
|---|---|---|---|---|---|---|---|
| 1 | 0 | Z | ↕ | 0 | Z | 0 | ✓ |
| 2 | 1 | Z | ↔ | 1 | X | Random | ✗ |
| 3 | 0 | X | / | + | X | 0 | ✓ |
| 4 | 1 | X | \ | − | Z | Random | ✗ |
| 5 | 1 | Z | ↔ | 1 | Z | 1 | ✓ |
| 6 | 0 | X | / | + | X | 0 | ✓ |
| 7 | 0 | Z | ↕ | 0 | X | Random | ✗ |
| 8 | 1 | X | \ | − | X | 1 | ✓ |

As we've seen how Alice and Bob communicate using polarization and basis matching, we can see the entire BB84 process in straightforward steps.

These steps combine everything explained earlier—from how bits are prepared and sent to how they are filtered and turned into a secure key.

1. Alice creates a random list of bits (0s and 1s)
2. She randomly chooses a basis (Z or X) for each bit and encodes the bit into a polarized photon
3. Alice sends the photons to Bob using a quantum channel
4. Bob receives the photons and randomly picks a basis (Z or X) to measure each one
5. After measurement, Alice and Bob communicate over a public channel to compare the bases they used, not the bit values
6. They keep only the bits where their bases matched. This filtered list is called the *sifted key*
7. To check for spying or noise, they compare a small part of the sifted key. If the error rate is too high, the key is discarded
8. If the error rate is acceptable, they apply error correction to fix mismatches and use privacy amplification to remove any leaked information
9. The final result is a secure shared key that only Alice and Bob know

After following all these steps, Alice and Bob end up with a list of bits where their basis choices matched which is called the sifted key. These bits are the most reliable because they come from measurements in the correct basis. For example, in the table 5.1, out of 8 bits, 5 were discarded due to mismatched bases, and only 3 were kept. This means that on average, around 50% of the bits are kept after sifting.

If there's no interference or eavesdropping, and the channel is ideal, the kept bits will match 100% accurately between Alice and Bob. This is how BB84 builds security: any attempt to spy on the qubits changes them, and that creates errors in the sifted key. If too many errors appear, Alice and Bob will know something is wrong and throw away the key.

Even though only about half of the original bits survive, they are the safest ones—and that's what makes BB84 a secure protocol.

## 5.2 Applications of the BB84 Protocol

As the threat of quantum computers grows, traditional encryption methods may no longer be enough to protect sensitive information. The BB84 protocol, being one of the first practical quantum key distribution methods, offers a new level of security based on the laws of physics. Due to this, it is being researched and tested in various significant fields. One of the biggest applications of BB84 is in secure government or defense agency communication, where confidentiality is paramount. Since any effort to intercept the key can be identified, BB84 is a strong means of protecting national security data. Another significant use is in banking and financial institutions. Some banks have already tested quantum key distribution to safeguard transactions and customer information from prospective cyberattacks.

BB84 is also being utilized in constructing the quantum internet, where quantum signals will be used to transmit information. People are trying to connect cities and even nations across quantum networks, and BB84 is most commonly employed as the primary protocol in these experiments.

## 5.3 Limitations of the BB84 Protocol

Although the BB84 protocol is a significant advance in secure communication, it has a few practical issues. These are not weaknesses that make the protocol insecure, but they impact the ease with which it can be implemented in practical systems. One of the most significant problems is BB84 needs a quantum channel, typically through fiber-optic cables or free-space optics. These configurations are costly and are susceptible to distance, light loss, and environmental interference. Therefore, BB84 is now only applicable for short or medium distances, typically less than a few hundred kilometers, unless repeaters or satellites are employed. A second challenge is the precision required to generate and detect photons. BB84 relies on sending and measuring single photons, but controlling them perfectly in practice is difficult. If multiple photons are accidentally sent, it creates a security risk. Photon detectors can be slow or noise sensitive, affecting performance.

The key generation rate is also lower than classical methods. The final shared key is shorter since only about half the bits are kept after basis matching. And if error correction and privacy amplification are added, the usable key gets even smaller. While BB84 can detect if someone tries to eavesdrop, it doesn't stop them from trying. It only works if Alice and Bob can verify and react to errors which means some trust in the classical communication channel is still needed.

# Chapter 6

# Conclusion

## 6.1 Conclusion

BB84 protocol is an excellent example of applying quantum principles to solve modern security issues. In contrast to conventional encryption techniques based on mathematical complexity, BB84 provides a new type of protection based on the laws of nature. By utilizing aspects such as superposition and principle uncertainty, it provides a means whereby any attempt at intercepting a secret key can be detected and prevented.

I have explored the BB84 protocol from a theoretical perspective in this milestone. I explained the fundamental quantum concepts that enable it to function, including qubits, polarization, and basis selections. I also noted how Alice and Bob share information securely, and how a common key is established by retaining only the measured bits in corresponding bases. Key concepts such as the sifted key, precision, and basis mismatch effect were described with examples and tables. Although BB84 is limited in some ways, such as distance problems and the requirement for sophisticated hardware, it is one of the most critical milestones toward secure communication in the quantum age. It not only solidifies our knowledge of quantum cryptography but also provides us with a means of securely safeguarding data in the future.

This milestone paves the way for future work, in which I will model the protocol and investigate how BB84 reacts when an eavesdropper attempts to interfere.

# References

Chen, Y.-A., Zhang, Q., Chen, T.-Y., Cai, W.-Q., Liao, S.-K., Zhang, J., Chen, K., Yin, J., Ren, J.-G., Chen, Z. et al. (2021), 'An integrated space-to-ground quantum communication network over 4,600 kilometres', *Nature* **589**(7841), 214–219.

Gisin, N., Ribordy, G., Tittel, W. and Zbinden, H. (2002), 'Quantum cryptography', *Reviews of modern physics* **74**(1), 145.

Korzh, B., Lim, C. C. W., Houlmann, R., Gisin, N., Li, M. J., Nolan, D., Sanguinetti, B., Thew, R. and Zbinden, H. (2015), 'Provably secure and practical quantum key distribution over 307 km of optical fibre', *Nature Photonics* **9**(3), 163–168.

Scarani, V., Bechmann-Pasquinucci, H., Cerf, N. J., Dušek, M., Lütkenhaus, N. and Peev, M. (2009), 'The security of practical quantum key distribution', *Reviews of modern physics* **81**(3), 1301–1350.

Shor, P. W. and Preskill, J. (2000), 'Simple proof of security of the bb84 quantum key distribution protocol', *Physical review letters* **85**(2), 441.