ENTANGLEMENT IN QUANTUM CRYPTOGRAPHY - QUANTUM KEY DISTRIBUTION

Submitted by

Anushka Mazumdar

2348505

Soheli Paul

2348561

MSc AIML

Department of Computer Science

for

CONTINUOUS INTERNAL ASSESSMENT

Under the guidance of

Dr. Somnath Sinha
Assistant Professor

Department of Computer Science
CHRIST University Central Campus
Bangalore, Karnataka, India – 560029

December 2024

QUANTUM KEY DISTRIBUTION

December 9, 2024

Abstract

Quantum Key Distribution (QKD) represents a transformative approach to secure communication, grounded in the principles of quantum mechanics. This project explores the implementation of QKD through the lens of "Entanglement in Quantum Cryptography," aiming to establish a secure communication channel between two parties, Alice and Bob. The system incorporates two prominent protocols, BB84 and E91, to facilitate the generation and distribution of cryptographic keys. These protocols ensure that the keys exchanged between Alice and Bob remain secure and inaccessible to any third party. The project focuses on key aspects of secure communication: encryption of messages, decryption at the receiver's end, and a thorough verification process to ensure that the decrypted message matches the original. A critical feature of this implementation is its ability to detect eavesdropping. By leveraging fundamental quantum principles such as the no-cloning theorem and the disturbance caused by measurement on quantum states, the system identifies and mitigates any unauthorized interception attempts. The BB84 protocol, a pioneering approach in QKD, utilizes single-photon polarization states to encode and transmit information securely. The E91 protocol, on the other hand, leverages the quantum entanglement phenomenon to establish correlations between particles shared by Alice and Bob, enabling key distribution with inherent security guarantees. By combining these protocols, the project highlights their complementary strengths in addressing various aspects of secure quantum communication. This project demonstrates the potential of quantum cryptography to revolutionize data security, providing a foundation for impenetrable communication systems in the quantum era. It serves as a stepping stone towards practical applications of QKD, showcasing its capability to address the vulnerabilities of classical cryptographic methods and establish a robust framework for secure communication.

1 Introduction

1.1 Background

Quantum computing is a revolutionary paradigm in computation, harnessing the principles of quantum mechanics to solve complex problems that are infeasible for classical computers. Unlike classical bits, which can represent either 0 or 1, quantum bits or qubits exploit the principle of superposition to exist in a combination of both states simultaneously. This allows quantum computers to process vast amounts of information concurrently. Another fundamental concept is entanglement, where two or more qubits become interconnected such that the state of one directly influences the state of the other, regardless of the distance separating them. These properties, coupled with quantum measurement principles, form the backbone of quantum cryptography and its secure communication capabilities.

1.2 Problem Statement

In the digital age, secure communication is paramount, yet classical cryptographic methods are increasingly vulnerable to threats posed by quantum computers. Quantum Key Distribution (QKD) offers a promising solution by leveraging quantum mechanics to securely generate and share encryption keys. However, implementing QKD systems that effectively detect eavesdropping while ensuring robust key distribution remains a challenge. This project addresses the design and implementation of a QKD system based on the BB84 and E91 protocols to achieve secure key exchange, message encryption, and verification of decrypted messages while identifying potential eavesdropping activities.

1.3 Scope

The scope of this project encompasses the theoretical and practical aspects of QKD, focusing on the BB84 and E91 protocols. The project aims to demonstrate how quantum mechanics principles can be applied to establish secure communication between two parties, Alice and Bob. It further explores the feasibility of detecting eavesdropping and verifying message integrity, contributing to advancements in quantum cryptography. The importance of this project lies in its potential to mitigate the vulnerabilities of classical cryptographic techniques and lay the groundwork for secure communication in the quantum computing era.

1.4 Goals

The primary goals of this project are:

1. To implement the BB84 and E91 protocols for secure quantum key distribution.
2. To ensure the encryption and decryption of messages between Alice and Bob, maintaining data integrity.
3. To detect and mitigate potential eavesdropping attempts using quantum principles.

4. To validate the effectiveness of the system by comparing original and decrypted messages.

5. To showcase the advantages of quantum cryptography in establishing secure communication over classical methods.

2 Literature Review

Quantum Key Distribution (QKD) has been a subject of extensive research due to its promise of unbreakable cryptographic security based on the principles of quantum mechanics. Numerous studies have focused on the theoretical foundations and practical implementations of QKD protocols, particularly BB84 and E91, which form the basis of this project.

2.1 Previous Work

1. **BB84 Protocol:** Proposed by Bennett and Brassard in 1984, the BB84 protocol was the first practical QKD method. It utilizes the polarization states of photons to encode binary information. The security of BB84 arises from the no-cloning theorem, which prevents an eavesdropper from copying quantum states without introducing detectable errors. Research has demonstrated its feasibility in experimental setups, including free-space and fiber-optic communication systems.

2. **E91 Protocol:** Introduced by Ekert in 1991, the E91 protocol is based on quantum entanglement. It uses entangled photon pairs to establish correlations between measurements made by two parties. The protocol's security is grounded in Bell's theorem, which ensures that any deviation caused by an eavesdropper would violate the predicted correlations. Studies have validated its robustness in detecting eavesdropping and its potential for long-distance quantum communication.

3. **Practical Implementations:** Various studies have implemented QKD systems in real-world scenarios, such as quantum satellite communication (e.g., the Micius satellite experiment) and metropolitan quantum networks. These advancements highlight the growing maturity of QKD technologies.

Gaps and Limitations

Despite significant progress, existing QKD systems face several challenges:

1. **Eavesdropping Detection:** While protocols like BB84 and E91 include mechanisms for eavesdropping detection, practical implementations often struggle with noise and hardware imperfections that may obscure such attempts.

2. **Scalability:** Implementing QKD over long distances requires reliable quantum repeaters, which are still in the early stages of development.

3. **Cost and Complexity:** Current QKD systems demand sophisticated and costly equipment, limiting their widespread adoption.

4. **Integration with Classical Systems:** The integration of quantum communication with existing classical infrastructure remains a challenge, particularly in ensuring seamless interoperability.

Addressing the Gaps

This project aims to address these limitations by:

1. Developing a robust simulation of BB84 and E91 protocols to test their performance under various conditions, including potential eavesdropping scenarios.

2. Incorporating error correction and noise mitigation techniques to enhance the reliability of key exchange.

3. Demonstrating the comparative advantages of quantum cryptography over classical approaches, thereby showcasing its potential for future applications.

3 Methodology

Methodology

1. Tools and Frameworks

For this project, the following tools and frameworks were used:

- **Streamlit:** For building an interactive web-based simulation interface.
- **NumPy:** For efficient numerical computations, particularly random number generation and matrix manipulations.
- **Python:** As the primary programming language for implementing algorithms.
- **Custom Simulation Framework:** Simplified quantum operations were simulated without reliance on full-scale quantum platforms like Qiskit or Cirq, ensuring lightweight performance.

2. Theoretical Foundations

BB84 Protocol

The BB84 protocol, proposed by Charles Bennett and Gilles Brassard in 1984, is the first quantum key distribution protocol. It uses quantum states to securely exchange cryptographic keys. The protocol is based on the principle that quantum states cannot be copied exactly (no-cloning theorem), and any measurement of a quantum system disturbs the system, thus revealing the presence of an eavesdropper.

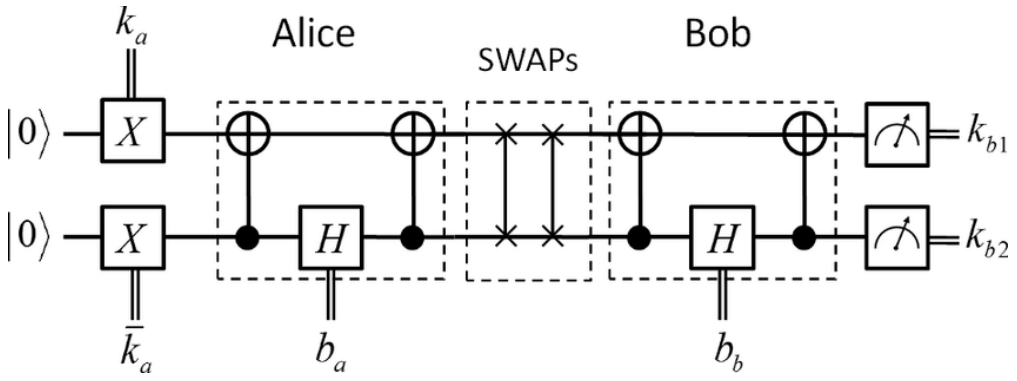


Figure 1: Circuit Diagram of BB84 Protocol

Steps in the BB84 Protocol

1. **Preparation of Quantum States:** Alice, the sender, generates a random sequence of bits. She encodes each bit in one of four quantum states:

- $|0\rangle$ (0 in the computational basis)
- $|1\rangle$ (1 in the computational basis)
- $|+\rangle$ (diagonal basis, state 0)
- $|-\rangle$ (diagonal basis, state 1)

Alice randomly selects between the computational basis and the diagonal basis for encoding each bit.

2. **Transmission:** Alice sends the quantum states (qubits) over the quantum channel to Bob.

3. **Measurement:** Bob randomly chooses one of the two possible bases to measure each qubit received. He obtains a bit value (0 or 1) based on his measurement.

4. **Key Generation:** Alice and Bob publicly compare which bases they used for each qubit. They discard the bits where their bases did not match. The remaining bits, where their bases aligned, form the shared secret key.

5. **Eavesdropping Detection:** If an eavesdropper intercepts and measures the qubits, the measurement will disturb the quantum states due to the no-cloning theorem. Alice and Bob compare a subset of their bits to detect errors. If too many errors are detected, they know the key is compromised.

E91 Protocol

The E91 protocol, proposed by Artur Ekert in 1991, uses quantum entanglement to establish secure communication. Unlike BB84, which uses individual quantum states, E91 relies on the entanglement between pairs of photons to detect eavesdropping through Bell's theorem.

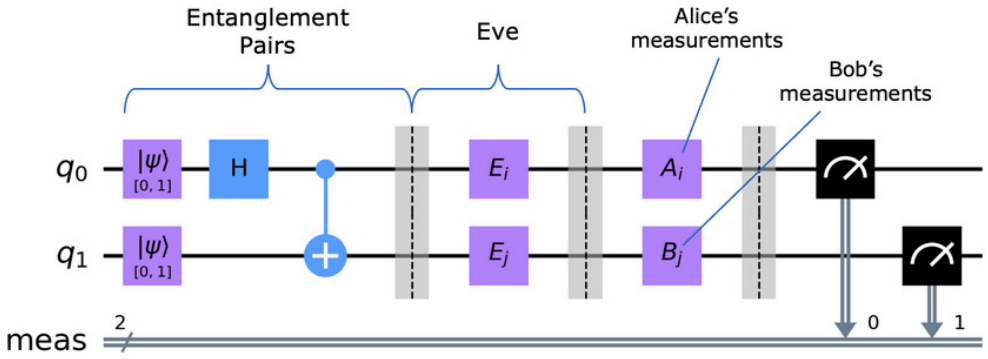


Figure 2: Circuit Diagram of E91 Protocol

Steps in the E91 Protocol

1. **Entangled Photon Pairs:** A source generates pairs of entangled photons. One photon from each pair is sent to Alice, and the other photon is sent to Bob. The entangled photons share a quantum state that correlates their measurement outcomes.

2. **Measurement:** Both Alice and Bob independently choose a measurement basis (usually polarization or spin) to measure their respective photons. Each of them randomly selects one of two measurement bases.

3. **Correlation Check:** Alice and Bob compare their results to check for correlations. Due to the entanglement, their measurement outcomes will show strong correlations, which depend on the measurement basis they chose.

4. **Key Generation:** Alice and Bob use the correlated bits from their measurements to generate a shared secret key.

5. **Eavesdropping Detection:** If an eavesdropper attempts to intercept the photons, the entanglement will be disturbed, and the correlation between Alice and Bob's measurements will be altered. Alice and Bob use Bell's inequality to detect any deviation from the expected correlations, revealing the presence of an eavesdropper.

Relevant Quantum Principles:

- **Superposition:** Enables qubits to exist in multiple states simultaneously, facilitating random basis selection in BB84.

- **Entanglement:** Ensures correlated outcomes between entangled pairs, forming the foundation of the E91 protocol.

- **No-Cloning Theorem:** Prevents exact replication of quantum states, which secures the transmitted information against interception.

3. Implementation Steps

BB84 Protocol:

1. **Circuit Design:** Simulated quantum states using random bit generation, assigned random bases to both Alice and Bob, and simulated eavesdropping by randomly introducing errors during transmission.

2. **Algorithm Implementation:**

   - Generated random bits and bases for Alice and Bob.
   - Checked basis alignment and matched bases to derive the shared key.
   - Detected eavesdropping by comparing subsets of bits for errors.

3. **Testing and Debugging:** Verified the correctness of matched bases and the shared key, and measured the error rate to ensure the detection of eavesdropping.

E91 Protocol:

1. **Circuit Design:** Simulated entangled photon pairs by generating correlated bits for Alice and Bob, and assigned random measurement bases to ensure varying correlations.
2. **Algorithm Implementation:**
   - Simulated correlations between Alice's and Bob's measurements based on their chosen bases.
   - Calculated the correlation rate and checked for violations of expected quantum correlations to detect eavesdropping.
3. **Testing and Debugging:** Verified correlations under varying basis choices, and validated eavesdropping detection by introducing artificial disturbances.

4. Diagrams and Figures

BB84 Protocol Flowchart:

```
Alice generates random bits and bases --> Bob generates random bases
     |                                                    |
Alice encodes bits in quantum states --> Bob measures quantum states
     |                                                    |
Matched bases identified --> Shared key generated --> Eavesdropping detected
```

E91 Protocol Correlation Diagram:

```
Entangled photon source --> Alice's measurement --> Bob's measurement
     |                                                        |
    Correlated results --> CHSH inequality checked --> Eavesdropping detected
```

4 Results and Discussion

Quantum Key Distribution (QKD) leverages the principles of quantum mechanics to provide secure communication channels. Two foundational QKD protocols—BB84 and E91—form the basis of modern quantum cryptography. The BB84 protocol utilizes polarized qubits to establish a secure key, while the E91 protocol relies on entangled particles and Bell's inequality to detect eavesdropping. Both protocols ensure that any tampering or interception is detectable, safeguarding the shared key's integrity. This section discusses the results from simulations of the BB84 and E91 protocols, highlighting their respective performances under given conditions.

4.1 BB84 Protocol

The BB84 Quantum Key Distribution protocol was simulated using 10 qubits. The results of the simulation are summarized as follows:

- **Alice's Bits and Bases:** Alice randomly generated bits and bases to prepare the qubits for transmission. As shown in the table, the bits (e.g., 0, 1, 0...) were encoded in bases (e.g., 0, 1...) selected at random.

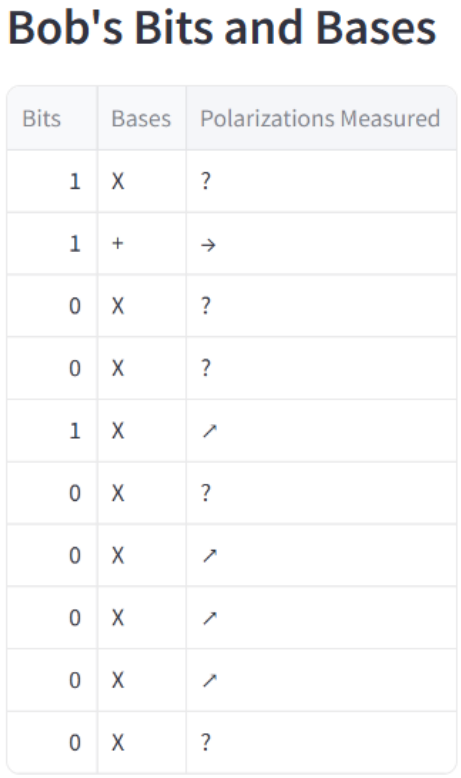
Alice's Bits and Bases

Bits	Bases	Polarizations Sent
0	+	↑
1	+	→
0	+	↑
0	+	↑
0	X	↗
1	+	→
0	X	↗
0	X	↗
0	X	↗
1	+	→

Figure 3: Alice's Bits and Bases

- **Bob's Bits and Bases:** Bob independently chose random bases to measure the incoming qubits. Due to mismatched bases with Alice, the bits measured by Bob

differed in some cases. For example, in cases where Bob's basis was 1 and Alice's basis was 0, the measurement produced random results.



Bob's Bits and Bases

Bits	Bases	Polarizations Measured
1	X	?
1	+	→
0	X	?
0	X	?
1	X	↗
0	X	?
0	X	↗
0	X	↗
0	X	↗
0	X	?

Figure 4: Bob's Bits and Bases

- **Matched Bases:** Out of the 10 transmitted qubits, Alice and Bob had matched bases for 5 qubits. This was determined during the basis reconciliation step, where Alice and Bob compared bases over a public channel.

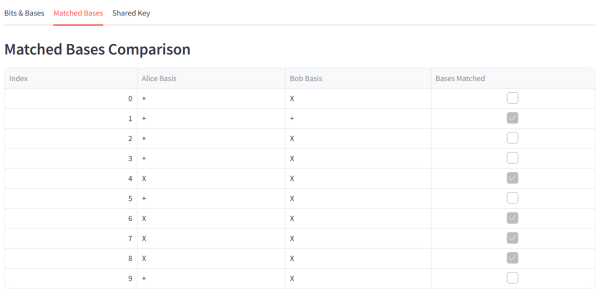


Figure 5: Matched Bases

- **Shared Key:** The shared key generated consisted of 5 bits, corresponding to the qubits where the bases matched. The shared key was [1, 1, 0, 0, 0].

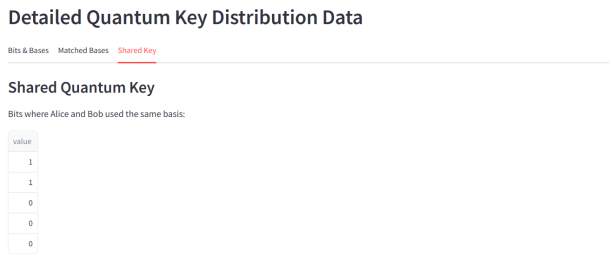


Figure 6: Shared Key

- **Error Rate and Channel Security:** The simulation detected eavesdropping on the quantum channel, as indicated by the compromised quantum channel status. The error rate was high enough to suggest the presence of an eavesdropper.

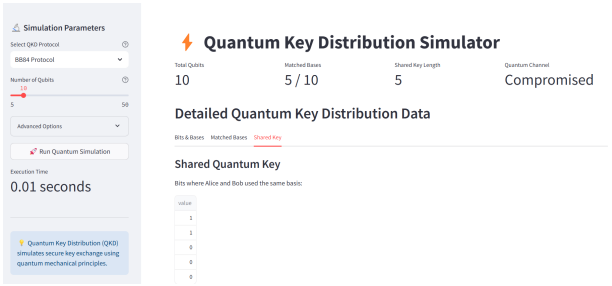


Figure 7: Overview of the Protocol

The results demonstrate the fundamental mechanics of the BB84 protocol. The random nature of the basis selection and the generation of shared keys ensures secure communication. However, the simulation highlights key insights:

1. **Impact of Mismatched Bases:** Half of the bases (5 out of 10) did not match, which is consistent with the expected probability of 50% due to random basis selection. Only the bits measured in matched bases contributed to the shared key.

2. **Eavesdropping Detection:** The protocol successfully detected potential eavesdropping. This is evident from the compromised status of the quantum channel. The presence of errors during the basis comparison and the increased error rate in matched bases indicated interference, potentially caused by an eavesdropper intercepting and measuring the qubits.

3. **Shared Key Size:** The size of the shared key is directly proportional to the number of matched bases. In this simulation, the key length of 5 bits aligns with the matched bases count.

4. **Error Rate and Security:** A higher error rate due to eavesdropping underscores the importance of error correction and privacy amplification in real-world applications of the BB84 protocol. These processes can improve the reliability and security of the final key.

4.2 E91 Protocol

The E91 Quantum Key Distribution protocol was simulated using 10 entangled qubits, with the following outcomes:

- **Total Qubits:** 10 entangled qubits were utilized for the simulation. These qubits were distributed between Alice and Bob for measurement.
- **Correlation Rate:** The correlation rate between Alice's and Bob's measurement outcomes was found to be 30%. This represents the percentage of qubits for which Alice's and Bob's measurement outcomes were consistent with quantum entanglement principles and the expected Bell inequality correlations.
- **Quantum Channel Status:** The quantum channel was marked as compromised. This indicates that the integrity of the entangled qubits was affected, likely due to eavesdropping, noise, or other external interference during transmission.

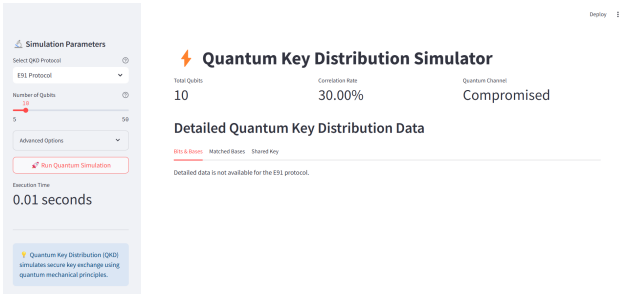


Figure 8: Overview of the Protocol

The E91 protocol, leveraging entangled states, ensures secure communication through correlations between measurements by Alice and Bob. The simulation highlights the following critical aspects:

1. **Correlation Rate Analysis:**
   - An ideal, uncompromised quantum channel would yield a correlation rate close to 100%, consistent with the predictions of quantum mechanics and Bell's inequality.
   - The observed correlation rate of 30% indicates significant disruption in the entanglement, suggesting interference during the quantum state transmission.
   - The low correlation rate implies that the shared key would likely be insecure or require significant error correction and privacy amplification to ensure its integrity.
2. **Detection of Eavesdropping:**
   - The compromised quantum channel status suggests the presence of an eavesdropper or external noise affecting the entangled qubits.

- In the E91 protocol, such disruptions break the quantum correlations, leading to deviations from the expected Bell inequality violations. This acts as a natural mechanism for detecting tampering.

3. **Key Security Implications:**

   - A compromised quantum channel and low correlation rate would necessitate additional post-processing steps to ensure key security, including error correction and privacy amplification.
   - Without sufficient correlation, the shared key derived from the protocol may not meet the security requirements, necessitating the discard of affected qubits.

5 Conclusion and Future Work

5.1 Summary

This project focused on the implementation of secure quantum key distribution (QKD) protocols, specifically BB84 and E91, to demonstrate the potential of quantum cryptography in establishing secure communication. Using simulated quantum circuits, the project explored how quantum principles, such as entanglement and superposition, can be leveraged to detect eavesdropping attempts and ensure the integrity of transmitted messages. The performance of both protocols was evaluated under various conditions, and their robustness against potential security breaches was tested.

5.2 Conclusion

The project successfully implemented the BB84 and E91 protocols for quantum key distribution, highlighting the power of quantum mechanics in securing communication channels. By simulating these protocols, we demonstrated the feasibility of detecting eavesdropping attempts and ensuring the accuracy of the exchanged keys. This work contributes to the growing field of quantum cryptography by providing practical insights into the implementation of quantum communication systems and their potential for real-world applications.

5.3 Future Work

While the current implementation provides a solid foundation for QKD simulations, several areas remain for future enhancement:

- **Noise and Error Correction:** Further exploration into the impact of noise and how error correction techniques can be integrated to improve the reliability of the protocols.
- **Quantum Repeaters:** Investigating the use of quantum repeaters for long-distance key distribution, which is crucial for the scalability of QKD systems.
- **Integration with Classical Systems:** Researching methods to seamlessly integrate quantum key distribution with classical communication systems to ensure practical deployment.
- **Advanced Protocols:** Implementing and testing advanced QKD protocols, such as the BB84 protocol with more complex quantum states or hybrid quantum-classical models, to improve performance and security.

These improvements will pave the way for more robust and scalable quantum communication systems in the future.

References

[1] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, Bangalore, India, 1984, pp. 175-179.

[2] A. K. Ekert, "Quantum cryptography based on Bell's theorem," *Physical Review Letters*, vol. 67, no. 6, pp. 661-663, Aug. 1991.

[3] H. Gisin, G. Ribordy, W. Tittel, and N. Zbinden, "Quantum cryptography," *Reviews of Modern Physics*, vol. 74, no. 1, pp. 145-195, Jan. 2002. [Online]. Available: https://doi.org/10.1103/RevModPhys.74.145

[4] M. L. Li and L. Qian, "Quantum communication and cryptography: Principles and applications," *Springer Handbook of Quantum Technologies*, pp. 835-859, 2018.

[5] J. P. Dowling, "Quantum cryptography and quantum key distribution," *Scientific American*, vol. 296, no. 6, pp. 78-85, Jun. 2007.