TRIBHUWAN UNIVERSITY
INSTITUTE OF ENGINEERING
PURWANCHAL CAMPUS

A MINOR PROJECT
ON
BB84 QUANTUM ENCRYPTION VISUALIZER

Submitted by:

Bijaya Sharma	[PUR077BCT023]
Sulav Bhandari	[PUR077BCT084]
Yunesh Shrestha	[PUR077BCT095]
Nishant Bhattarai	[PUR077BCT096]

Department of Electronics and Computer Engineering
Purwanchal Campus, Dharan

Submission Date: Januaury, 2023

Acknowledgments

I express my sincere appreciation to the Head of the Department (HOD), Mr. Pravin Sangroula and the Deputy Head of the Department, Mr. Pukar Karki for their invaluable guidance, insightful suggestions,constructive feedback, and continuous support throughout the preparation of this proposal. I am deeply thankful to the esteemed teachers and faculty members whose valuable feedback, encouragement, and scholarly insights have enriched this proposal. Their dedication to academic excellence and commitment to fostering knowledge have been a source of inspiration. Their collective guidance have immensely contributed to the refinement and improvement of this proposal

Contents

List of Figures

List of Abbreviations

WC	Quantum Computing
QKD	Quantum key distribution
SDK	Software Development Kit
Q	Qiskit
QBER	Quantum Bit Error Rate

1. INTRODUCTION

Quantum encryption, a pioneering facet of quantum cryptography, represents a transformative paradigm in securing sensitive information. Leveraging the intricate principles of quantum mechanics, such as superposition and entanglement, quantum encryption stands as an impregnable fortress against the burgeoning threats posed by quantum computing to conventional cryptographic methods. By encoding data within the delicate quantum states of photons, this cutting-edge technology ensures unbreakable encryption, heralding a new era of unparalleled security for safeguarding critical data in an increasingly digitized world.[1]

1.1 Background

The advent of robust computational power poses a significant challenge to classical cryptography. Quantum computers, with their immense capability, threaten the once-secure foundations of traditional encryption methods. However, emerging from the intricate realms of quantum mechanics is a beacon of hope known as quantum cryptography (QC). This revolutionary approach harnesses quantum principles—such as superposition, entanglement, and the non-cloning theorem—to craft encryption keys that are inherently impervious to computational brute force.

QC diverges from conventional cryptographic practices by encoding information within the delicate quantum states of photons themselves. These polarized photons, acting as messengers of the quantum domain, hold fragments of the key, immune to interception and decryption attempts. Through the intricate dance of entangled photons, spanning distances and time, QC ensures the sanctity of the cryptographic process. While transitioning from theory to practice poses challenges—particularly in the fidelity of generating, transmitting, and detecting quantum states—the assurance of unparalleled security has galvanized a global research effort.

As QC continues to mature, it promises not just secure communication but also a fundamental shift in how we approach information security. Despite technological obstacles, the allure of absolute security has spurred rapid advancements in both theoretical exploration and experimental applications. In an era reliant on digital trust, QC stands as an unwavering fortress against the evolving landscape of computational cryptanalysis, safeguarding sensitive data in the quantum age.

1.2 Classical Cryptography

Cryptography is a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it. Classical cryptography has two major branches: secret or symmetric key cryptography and public or asymmetric key distribution.

1.3 Quantum Cryptography

Quantum cryptography is a method of secure communication that uses the principles of quantum-mechanics to protect the privacy of transmitted messages. In contrast to traditional cryptography, whichrelies on the difficulty of solving mathematical problems, quantum cryptography is based on thefundamental principles of quantum mechanics, which govern the behavior of particles at the subatomiclevel.

The basic idea behind quantum cryptography is to encode a message using the properties of particles atthe quantum level, such as the polarization of photons or the spin of electrons. By using these properties,it is possible to create a secure communication channel that is protected by the laws of physics.[2]One of the key advantages of quantum cryptography is its inherent security. Because of the uncertaintyprinciple, it is impossible for an attacker to eavesdrop on a quantum communication without beingdetected. This makes quantum cryptography an attractive option for securing sensitive information, suchas military communications or financial transactions.[3]

1.3.1 BB84 Protocal

The BB84 protocol, a pioneer in quantum key distribution, orchestrates a breathtaking quantum ballet using polarized photons to forge unbreakable keys. Imagine two dancers exchanging whispers in the form of single light particles, their orientations – up, down, diagonal – encoding secret bits.[4] But the stage holds secrets of its own: eavesdropping disrupts the dance, alerting the dancers with an unmistakable tremor. This exquisite choreography, woven from superposition and entanglement, ensures privacy beyond brute computational force, leaving even the most potent quantum computers bewildered in the dark. The BB84 protocol, a masterpiece of light and logic, lays the foundation for a future where information dances in the unassailable glow of the quantum realm.[5]

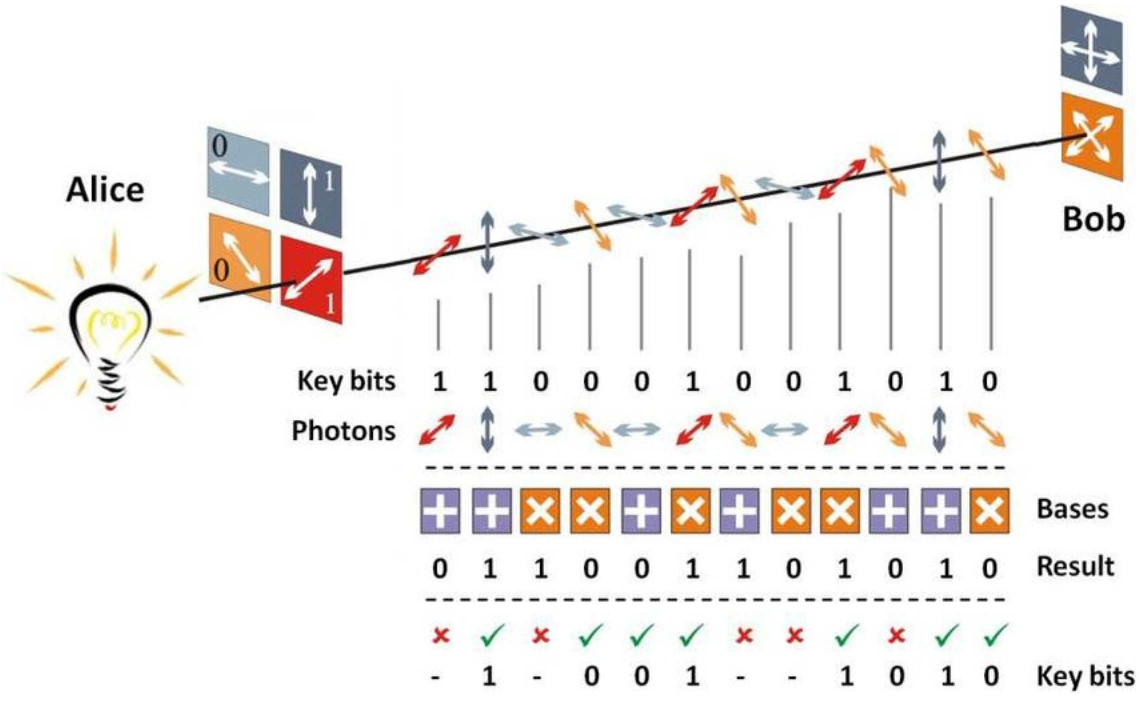

Alice
0
1
0
1
Bob
Key bits 1 1 0 0 0 1 0 0 1 0 1 0
Photons
Bases
0 1 1 0 0 1 1 0 1 0 1 0 Result
✗ ✓ ✗ ✓ ✓ ✓ ✗ ✗ ✓ ✗ ✓ ✓
- 1 - 0 0 1 - - 1 0 1 0 Key bits

Figure 1.1: BB84 protocol

In the BB84 protocol, Alice can transmit a random secret key to Bob by sending a string of photons with the private key encoded in their polarization. The no-cloning theorem guarantees that Eve cannot measure these photons and transmit them to Bob without disturbing the photon's state in a detectable way.

1.4 Problem Statements

Current challenges limit the real-world implementation and evaluation of secure quantum communication based on the BB84 protocol:

- Lack of accessible simulation tools: Researchers and developers require user-friendly software tools to analyze and optimize the BB84 protocol under various conditions.
- Limited understanding of vulnerability: Analyzing the protocol's susceptibility to different attack strategies and vulnerabilities in realistic scenarios is crucial for robust implementation.

- Optimizing key generation: Exploring parameters and techniques to maximize secure key generation rate while minimizing errors and noise impact is essential for practical applications.

1.5 Objectives

- Develop a software simulation of the BB84 protocol: This involves modeling the generation, transmission, and measurement of qubits, incorporating realistic noise and channel imperfections.
- Investigate the influence of various parameters: Explore how factors like channel length, noise levels, and error correction techniques affect the secure key generation rate.
- Provide a user-friendly interface: Design a clear and interactive interface for user input, visualization of key generation process, and analysis of results.

1.6 Feasibility Study

1.6.1 Technical Feasibility

- Simulation Methods: Various methods exist for simulating quantum states and QKD protocols like BB84, including density matrix formalism, Monte Carlo simulations, and circuit-based simulators.
- Web Platform Development: Existing web technologies like JavaScript and WebAssembly can be used to build the online simulator, ensuring accessibility and ease of use.
- Security Considerations: Implementing robust security mechanisms is crucial to prevent unauthorized access and ensure the integrity of the simulation results.

1.6.2 Market Feasibility

- Target Audience: The simulator can cater to various audiences, including academic researchers, students, cybersecurity professionals, and individuals interested in quantum technologies.

- Competitive Landscape: While a few online QKD simulators exist, there's potential for a differentiated offering with advanced features, user-friendly interface, and educational resources.
- Market Demand: Growing interest in quantum technologies and cybersecurity creates a market for educational and research tools like this simulator.

1.6.3 Financial Feasibility

- Development Costs: Development costs depend on the complexity of features, platform choice, and security measures implemented. Open-source tools and libraries can help reduce costs.
- Revenue Model: Different models like Freemium (basic features free, premium features paid), subscription-based access, or institutional licensing can be explored.
- Funding Opportunities: Research grants and collaborations with academic institutions or private companies can be pursued to support development.

1.7 Technical Requirements

1.7.1 Core Functionalities

- Simulate qubits with various polarization states.
- Model realistic channel noise and decoherence.
- Simulate BB84 protocol with configurable basis sets.
- Calculate key generation rate and QBER.
- Offer attack simulation and analysis options.
- Design a user-friendly interface with interactive elements and visualizations.

1.7.2 Technical Infrastructure

- Web application accessible through standard browsers.
- Consider frameworks like JavaScript, FlutterWeb.
- Programming languages and libraries like Python, NumPy, SciPy, QuTiPy, Qiskit, Matplotlib.

1.7.3 Performance and Scalability

- Smooth functionality on various devices and internet connections.

2. LITRATURE REVIEW

Plesa, M. I., Mihai, T. (2018). explored quantum computation's evolution presenting a new encryption scheme aimed at replacing RSA in public key infrastructures. Their research delves intothe scheme's security, implementation using IBM Q SDK, qiskit, and practical validation through experimental applications to see how secure and practical it could be.By probing the scheme's operational facets and conducting rigorous experiments, the authors provided a thorough examination of its potential to revolutionize encryption methodologies.[6]

Sharbaf, Mehrdad S.(2009) showcased quantum cryptography's revolutionary approach to information security, highlighting its superiority over classical encryption methods in securing network communications emphasizing the reliance on quantum laws and underscored the vulnerabilities of traditional cryptographic approaches.his comprehensive analysis not only establishes the criticality of quantum cryptography but also serves as a foundational reference in understanding its paramount importance in modern network security paradigms.[7]

Bayerstadler A., Becquin G., Binder J., Botter T., Ehm H., Ehmer T. & Winter F. (2021) explores practical applications of quantum encryption beyond theoretical frameworks.Their comprehensive exploration extends into various sectors, including finance, healthcare, and government, offering invaluable insights into the deployment of quantum encryption in real-world scenarios. Through meticulous examination and analysis, the research elucidates the transformative potential of quantum encryption in safeguarding sensitive data across diverse industries. This pioneering work not only bridges the gap between theory and practice but also establishes a roadmap for the integration of quantum encryption in critical sectors, paving the way for enhanced data security and privacy[8]

3. PROPOSED METHODOLOGY

3.1 System Design and Block Diagram

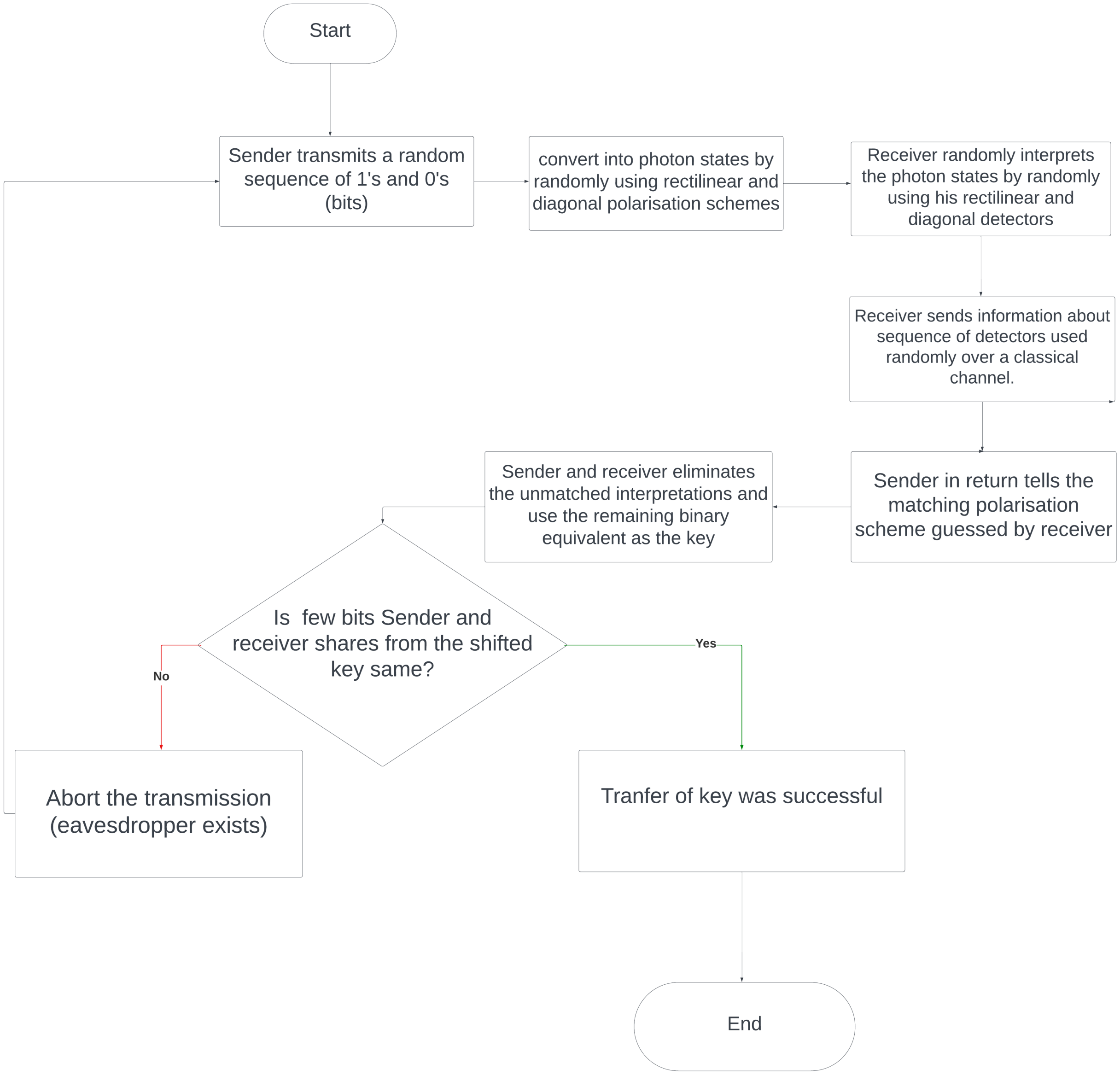

Start
Sender transmits a random sequence of 1's and 0's (bits)
convert into photon states by randomly using rectilinear and diagonal polarisation schemes
Receiver randomly interprets the photon states by randomly using his rectilinear and diagonal detectors
Receiver sends information about sequence of detectors used randomly over a classical channel.
Sender in return tells the matching polarisation scheme guessed by receiver
Sender and receiver eliminates the unmatched interpretations and use the remaining binary equivalent as the key
Is few bits Sender and receiver shares from the shifted key same?
No
Yes
Abort the transmission (eavesdropper exists)
Tranfer of key was successful
End

Figure 3.1: Block Diagram of BB84 Visualizer

3.2 Software Development Model

Waterfall Model

The Waterfall model in the Quantum Encryption Visualizer for BB8-4 protocol ensures a systematic and step-by-step approach, essential for the complex development process. This methodology is particularly beneficial in managing uncertainties and enhancing traceability. In this context, it is imperative to first study details about circuits and display them. The systematic nature of the Waterfall model aligns with the need to comprehensively understand the intricacies of circuits before progressing further in the development process. This approach facilitates a clear and structured exploration of circuit-related details, contributing to the overall effectiveness of the Quantum Encryption Visualizer for the BB8-4 protocol.

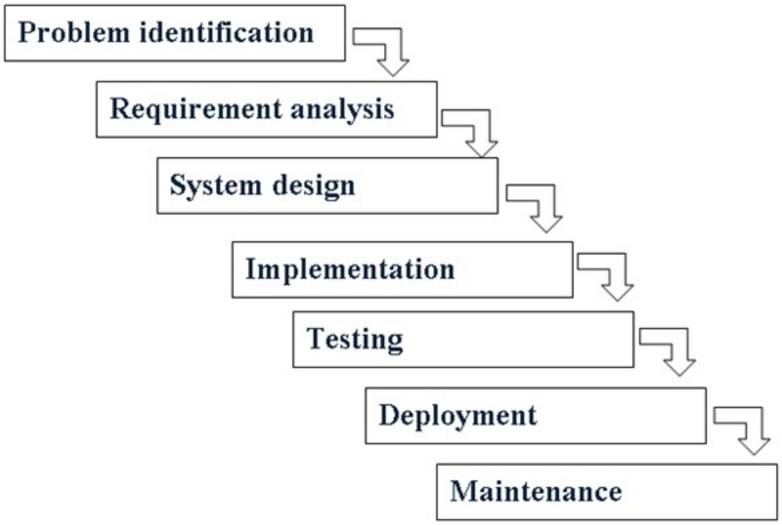
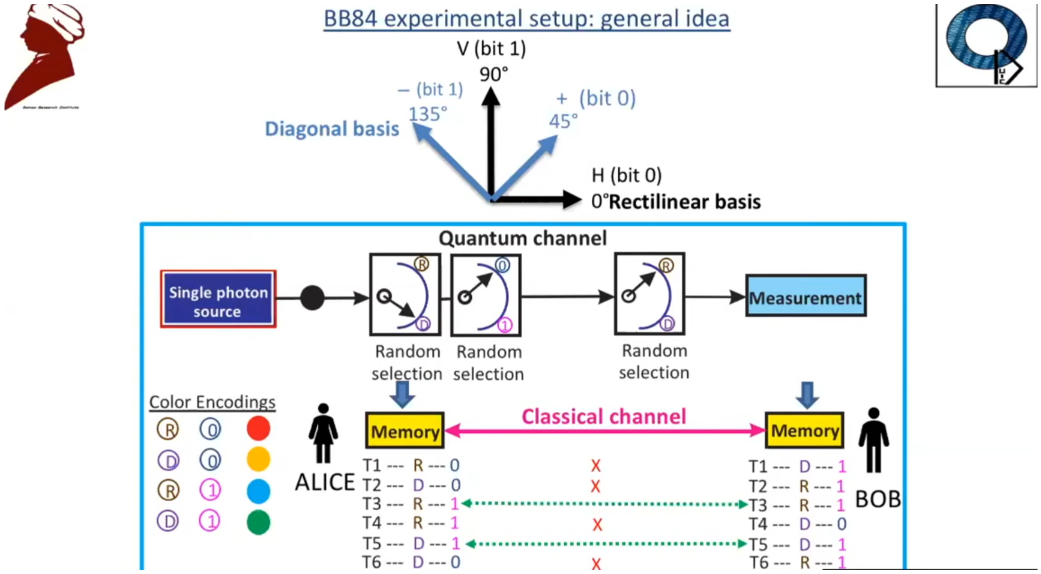


Figure 3.2: Waterfall Model

3.3 Experimental Setup



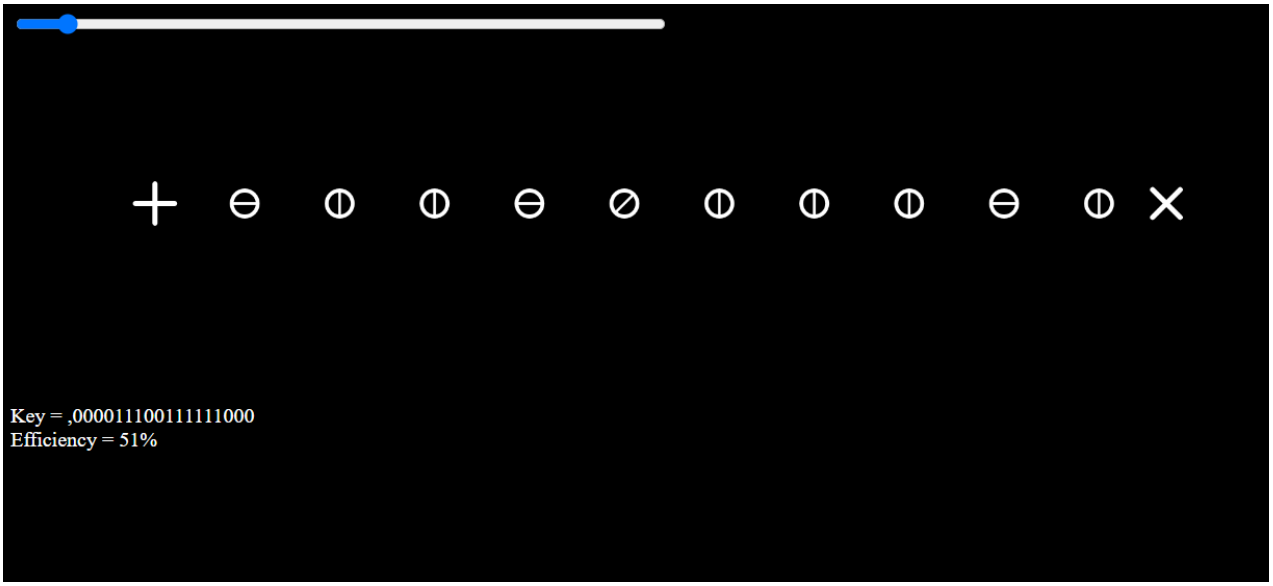
BB84 experimental setup: general idea

T1 --- R --- 0   X   T1 --- D --- 1
T2 --- D --- 0   X   T2 --- R --- 1
T3 --- R --- 1 ↔ T3 --- R --- 1
T4 --- R --- 1   X   T4 --- D --- 0
T5 --- D --- 1 ↔ T5 --- D --- 1
T6 --- D --- 0   X   T6 --- R --- 1

Figure 3.3: BB84 Experimental Setup

4. RESULT AND DISCUSSION

4.1 Expected Output



```
Key = ,000011100111111000
Efficiency = 51%
```

Figure 4.1: Expected Output

- Provides a platform to simulate and comprehend the functioning of the BB84 protocol for secure data encryption within a controlled environment.
- Allows users to adjust and regulate the speed of data transfer.
- Provides a platform to mimic the process of both sending and receiving data for evaluation.
- Provides quantitative data on the exact number of bits successfully transmitted for analysis and comparison purposes.

4.2 Budget Analysis

The project can be completed using free tools and resources. However, if additional assets or resources are required, the budget may need to be adjusted.

4.3 Timeline

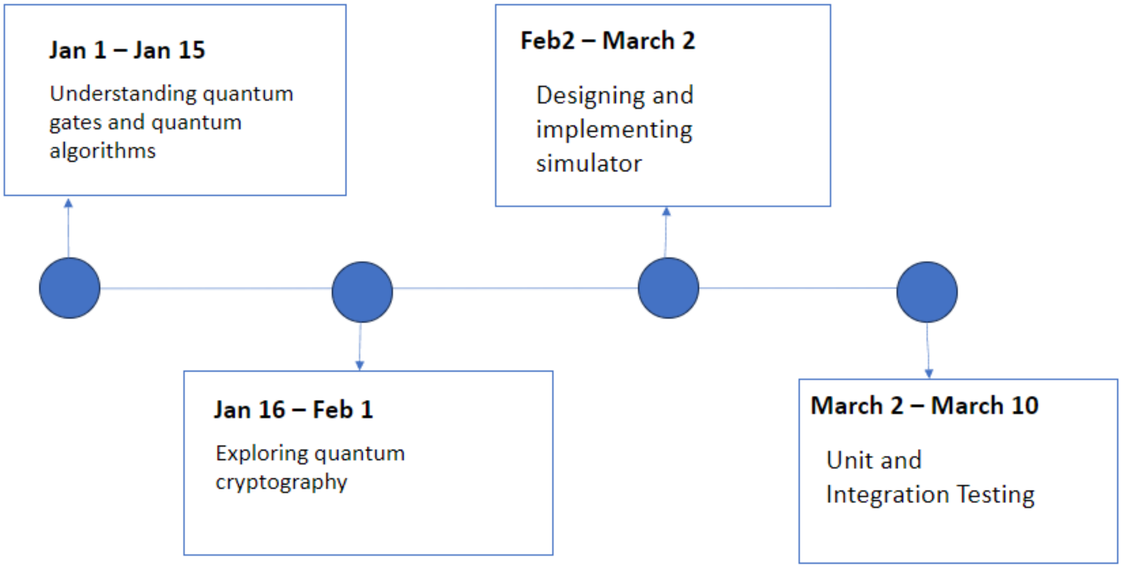

Jan 1 – Jan 15
Understanding quantum gates and quantum algorithms
Feb2 – March 2
Designing and implementing simulator
Jan 16 – Feb 1
Exploring quantum cryptography
March 2 – March 10
Unit and Integration Testing

Figure 4.2: Timeline of Project

References

[1] R. Overbeck and N. Sendrier, "Code-based cryptography," in *Post-quantum cryptography*. Springer, 2009, pp. 95–145.

[2] D. Bruss, G. Erdélyi, T. Meyer, T. Riege, and J. Rothe, "Quantum cryptography: A survey," *ACM Computing Surveys (CSUR)*, vol. 39, no. 2, pp. 6–es, 2007.

[3] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," *Theoretical computer science*, vol. 560, pp. 7–11, 2014.

[4] A. K. Ekert, "Quantum cryptography based on bell's theorem," *Physical review letters*, vol. 67, no. 6, p. 661, 1991.

[5] B. Muruganantham, P. Shamili, S. Ganesh Kumar, and A. Murugan, "Quantum cryptography for secured communication networks." *International Journal of Electrical & Computer Engineering (2088-8708)*, vol. 10, no. 1, 2020.

[6] M.-I. Plesa and T. Mihai, "A new quantum encryption scheme," *Advanced Journal of Graduate Research*, vol. 4, no. 1, pp. 59–67, 2018.

[7] M. S. Sharbaf, "Quantum cryptography: a new generation of information technology security system," in *2009 Sixth International Conference on Information Technology: New Generations*. IEEE, 2009, pp. 1644–1648.

[8] A. Bayerstadler, G. Becquin, J. Binder, T. Botter, H. Ehm, T. Ehmer, M. Erdmann, N. Gaus, P. Harbach, M. Hess *et al.*, "Industry quantum computing applications," *EPJ Quantum Technology*, vol. 8, no. 1, p. 25, 2021.