

A Q-Learning-Based Power Allocation Strategy for Quantum-Encrypted NOMA in Future Wireless Networks

Submitted partial fulfillment of the requirements for the degree of

Bachelor of Technology

in

Electronics and Communication

by

Preeti Yadav (21BEC0815)

Basil Syed Sadat (21BEC0263)

Satyam (21BEC2477)

Under the guidance of

Dr.Vijaya Durga Chintala

SENSE

VIT,Vellore.



VIT[®]
Vellore Institute of Technology
(Deemed to be University under section 3 of UGC Act, 1956)

April, 2025

DECLARATION

I hereby declare that the thesis entitled "A Q-Learning-Based Power Allocation Strategy for Quantum-Encrypted NOMA in Future Wireless Networks" submitted by me, for the award of the degree of *Bachelor of Technology in Programme* to VIT is a record of bonafide work carried out by me under the supervision of Dr. Vijaya Durga Chintala. I further declare that the work reported in this thesis has not been submitted previously to this institute or anywhere for the consideration of the degree/diploma.

Place : Vellore

Date : 20/4/25

Basil
Heets
Salyam
Signature of the Candidate

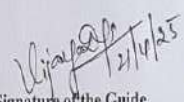
CERTIFICATE

This is to certify that the thesis entitled "A Q-Learning-Based Power Allocation Strategy for Quantum-Encrypted NOMA in Future Wireless Networks" submitted by **Preeti Yadav(21BEC0815)**, **Basil Syed(21BEC0263)** and **Satyam Sinha(21BEC2477)** SENSE, VIT, for the award of the degree of *Bachelor of Technology in Programme*, is a record of bonafide work carried out by him / her under my supervision during the period, 13.12.2024 to 20.04.2025, as per the VIT code of academic and research ethics.

The contents of this report have not been submitted either in part or in full, for the award of any other degree or diploma in this institute or any other institute or university. The thesis fulfills the requirements and regulations of the University and in my opinion meets the necessary standards for submission.

Place : Vellore

Date : 20/4/25


Signature of the Guide


Internal Examiner

VIGNESH.D
External

ACKNOWLEDGEMENTS

We are profoundly grateful to our project guide, Dr. Vijaya Durga Chintala, for her unwavering guidance, expert insights, and continuous support throughout the course of this project. Her profound knowledge of Quantum Secured NOMA played a pivotal role in shaping our research approach and helping us achieve our objectives. Her mentorship has inspired us to push our boundaries, enabling us to deepen our understanding and skills in biomedical engineering applications.

We would also like to extend our sincere appreciation to VIT University for providing us with an enriching academic environment and access to resources that have been fundamental to our research journey. The encouragement and support we received from the faculty and the state-of-the-art facilities at VIT have greatly contributed to the success of our project. We are grateful to be part of an institution that fosters innovation, research, and excellence.

Satyam
Basil Syed Sadat
Preeti Yadav

Student Name

Executive Summary

The rapid evolution of wireless communication demands systems that not only offer high spectral efficiency but also robust security against future threats. This project presents a hybrid communication framework that integrates **Quantum Key Distribution (QKD)** with **Non-Orthogonal Multiple Access (NOMA)**, supported by **Q-learning** for intelligent power allocation. Targeting next-generation communication networks, the system enhances both data security and transmission efficiency in dynamic multi-user environments.

We simulate the **BB84 QKD protocol** using Qiskit to generate quantum-secure encryption keys while detecting potential eavesdroppers. Simultaneously, a **Q-learning-based power allocation algorithm** is developed in Python to optimize resource distribution across NOMA users based on channel conditions and fairness metrics. The combined system is evaluated for key metrics including **bit error rate (BER)**, **secret key rate**, **quantum bit error (QBER)**, **energy efficiency**, and **fairness index**.

Our results show that integrating QKD enhances communication security, while Q-learning enables real-time adaptation to varying network states, outperforming fixed power allocation methods. The simulation confirms the feasibility of this secure and intelligent approach in future communication scenarios. This work contributes a scalable, learning-based, and quantum-secured NOMA system, laying the foundation for secure, efficient, and adaptive wireless communication technologies.

	Page No.
Acknowledgement	4
Executive Summary	5
Table of Contents	6
List of Figures	8
List of Tables	9
Abbreviations	10
Symbols and Notations	11
1 INTRODUCTION	12
1.1 Literature Review	12
1.2 Research Gap	15
1.3 Problem Statement	18
2 RESEARCH OBJECTIVE	20
3 RELEVANCE OF PROBLEM STATEMENT W.R.T SDG	23
4 PROPOSED SYSTEM (as applicable)	24
4.1 Design Approach / Materials & Methods	24
4.2 Codes and Standards	27
4.3 Constraints, Alternatives and Tradeoffs	28
5 PROJECT DESCRIPTION	29
6 HARDWARE/SOFTWARE TOOLS USED	31
7 SCHEDULE AND MILESTONES	32.
8 RESULT ANANLYSIS	

9	CONCLUSION	37
	1. Obtained Results	37
	2. Future improvement/work	48
	3. Individual contribution from team members	51
10	SOCIAL AND ENVIRONMENTAL IMPACT	52
11	COST ANALYSIS	55
12	PROJECT OUTCOME PUBLICATION/PATENT	56
13	REFERENCES	57

APPENDIX A

List of Figures

Figure No.	Title	Page No.
1	Key Exchange & Message Encryption/Decryption Process Demonstration	37
2	Detection of Eavesdropping in Quantum Key Distribution through Key Comparison	37
3	Probability of Detecting an Eavesdropper vs. Number of Key Bits Compared in Quantum Key Distribution	38
4	Variation of Secret Key Rate with Signal-to-Noise Ratio	40
5	Q-Learning Cumulative Reward vs. Episode for Multiple Users	41
6	Q-Learning Average Reward (Moving Average) vs. Episode for User 1 and User 2	42
7	Comparison of Normalized Signal Strength Between User 1 and User 2	43
8	QBER vs. SNR for Different QAM Modulation Schemes	44
9	BER vs. SNR for Different QAM Modulation Schemes	45
10	Jain's Fairness Index and Power Allocation Results for Two Users	46
11	Final Power Allocation Between User 1 and User 2	47

(In the chapters, figure captions should come below the figure and table captions should come above the table. Figure and table captions should be font size 10.)

List of Tables

Table No.	Title	Page No.
1	Key Challenges and Proposed Solutions in Quantum-Secure NOMA Systems	26

List of Abbreviations

OMA	Orthogonal Multiple Access
NOMA	Non-Orthogonal Multiple Access
QKD	Quantum Key Distribution
5G	Fifth Generation
QoS	Quality Of Service
RL	Reinforcement Learning
URLLC	Ultra Reliable Low Latency Communication
XR	Extended Reality
SIC	Successive Interference Cancellation
AMC	Adaptive Modulation & Coding
BER	Bit Error Rate
QBER	Quantum Bit Error Rate
SKR	Secret Key Rate

Symbols and Notations

&

And

e.g.

for example

1. INTRODUCTION

1.1. LITERATURE REVIEW

The rapid evolution of wireless communication networks from 4G to 5G and the impending advent of 6G have introduced unprecedented demands on data rate, latency, connectivity, and most crucially, security. These evolving demands have exposed the limitations of traditional multiple access and encryption techniques, prompting the research community to explore novel paradigms such as Non-Orthogonal Multiple Access (NOMA), Quantum Communication, and intelligent resource management using Machine Learning (ML). The convergence of these advanced technologies promises to lay the foundation for highly efficient, secure, and adaptive communication systems that can meet the rigorous requirements of future wireless networks.

1.1.1 Limitations of Traditional Access and Security Mechanisms

Orthogonal Multiple Access (OMA) schemes have historically formed the backbone of wireless communication systems up to and including 4G LTE networks. OMA assigns orthogonal time, frequency, or code resources to individual users, effectively eliminating intra-cell interference. While this ensures simplicity and reliability, it also leads to inefficient spectrum utilization, particularly in high-density scenarios. As we transition to 5G and eventually to 6G, the need for higher spectral efficiency and massive connectivity becomes paramount. OMA's rigid allocation structure is ill-suited for these conditions, as it cannot scale effectively with the increasing number of devices and the diverse Quality of Service (QoS) requirements.

Moreover, conventional cryptographic security methods, while robust in current applications, are fundamentally vulnerable to future threats posed by quantum computing. Algorithms such as RSA and ECC rely on the computational difficulty of factorization and discrete logarithms—problems that quantum algorithms like Shor's can solve in polynomial time. This vulnerability necessitates the exploration of quantum-resistant or quantum-secured communication techniques.

1.1.2 Emergence and Evolution of NOMA

To address spectrum efficiency limitations, NOMA has emerged as a revolutionary multiple access technology, particularly suitable for 5G and future 6G networks. Unlike OMA, NOMA allows multiple users to share the same frequency band simultaneously by superimposing signals in the power domain. The receiver employs **Successive Interference Cancellation (SIC)** to decode the signals based on their relative power levels.

Ding et al. (2017) played a pivotal role in showcasing NOMA's capabilities. Their work demonstrated how power-domain multiplexing could significantly enhance system throughput and support massive connectivity. Subsequent studies built upon this by analyzing the performance of uplink and downlink NOMA under various channel conditions. However, key challenges persisted, including the design of efficient SIC algorithms, mitigation of intra-cell and inter-cell interference, and most notably, the issue of **fair and optimal power allocation** among users with diverse channel gains.

Power allocation in NOMA is critical; assigning too much power to strong users undermines fairness, while favoring weak users compromises overall system efficiency. Various optimization techniques, including convex programming and heuristic algorithms, have been proposed, yet they often require centralized control and prior knowledge of channel conditions, limiting their adaptability in dynamic environments.

1.1.3 Rise of Quantum Communication for Enhanced Security

In parallel to the exploration of efficient access schemes, the field of Quantum Communication has gained traction due to its promise of **unconditional security** grounded in the principles of quantum mechanics. The foundational BB84 protocol, introduced by Bennett and Brassard in 1984, remains a cornerstone in the domain of **Quantum Key Distribution (QKD)**. This protocol leverages quantum properties like superposition and no-cloning to enable two parties to generate a shared secret key with provable security against eavesdropping.

Numerous practical implementations of QKD have since been realized across fiber-optic and free-space optical channels. Commercial systems from companies like ID Quantique and academic demonstrations such as the Chinese Micius satellite have showcased QKD's feasibility. However, challenges related to key generation rate, distance limitations, and integration with classical communication infrastructure continue to hinder large-scale adoption. Furthermore, standalone QKD systems do not address issues related to spectrum utilization or resource allocation, necessitating integration with broader wireless communication frameworks.

1.1.4 Integration of Quantum Security with NOMA

Given the complementary strengths of QKD and NOMA—security and efficiency respectively—researchers have started exploring hybrid systems that combine these technologies. Zhou et al. (2020) introduced one such **Quantum-NOMA framework**, demonstrating that embedding QKD within a NOMA system could enhance both data confidentiality and spectral efficiency. Their simulation results confirmed that user authentication and data encryption could be significantly improved without substantial degradation in throughput.

However, existing quantum-NOMA systems often rely on **fixed power allocation strategies**, which limit adaptability in heterogeneous network scenarios. This inflexibility becomes particularly problematic in 6G, where user mobility, traffic demands, and channel conditions can change rapidly and unpredictably. Therefore, a dynamic and intelligent power control mechanism is necessary for such hybrid systems to operate optimally in real-world conditions.

1.1.5 Machine Learning for Adaptive Resource Management

To address the adaptability challenge, recent studies have investigated **Machine Learning (ML)** approaches for resource management in NOMA systems. In particular, **Reinforcement Learning (RL)** and its model-free variant, **Q-learning**, have shown promise in optimizing power allocation without requiring prior knowledge of the environment.

Li et al. (2019) proposed a Q-learning-based framework for multi-user NOMA networks, where the agent learns optimal power distribution policies through interactions with the environment. The approach successfully improved throughput and ensured user fairness by dynamically adjusting power levels based on real-time network conditions. However, these methods often assume a classical security infrastructure and do not incorporate quantum-resistant or quantum-secured encryption schemes, thereby remaining vulnerable to future quantum attacks.

1.1.6 Identified Research Gaps

The review of existing literature highlights several gaps and opportunities for future research:

- Current NOMA systems, while spectrally efficient, lack robust security frameworks that can withstand quantum threats.
- QKD-based systems offer strong security but have not been widely integrated with dynamic resource allocation mechanisms.
- Existing hybrid Quantum-NOMA models often use static power allocation, which limits their real-time adaptability.
- ML-based power control strategies show strong potential but have not been combined with quantum-secure communication protocols.

1.1.7 Thesis Contribution

This thesis aims to bridge these gaps by proposing a **QKD-enhanced NOMA framework** with **Q-learning-based adaptive power allocation**. The proposed system offers:

- **Quantum-level security** through the implementation of BB84-based QKD for key exchange and message encryption.
- **Efficient spectrum utilization** via power-domain NOMA for multiple-user access.
- **Real-time adaptability** using Q-learning to dynamically allocate transmission power based on user requirements and channel variations.

By integrating these three domains—Quantum Communication, NOMA, and ML-based control—this work envisions a comprehensive solution that meets the dual demands of efficiency and security in 6G and beyond. The proposed model is designed to operate effectively in dynamic, high-density wireless environments while ensuring data confidentiality against classical and quantum adversaries.

1.2 Research Gap

As wireless communication technologies transition toward the sixth generation (6G), the expectations from network infrastructure have significantly evolved. Unlike previous generations focused on higher data rates and expanded capacity, 6G networks are anticipated to deliver an integrated platform capable of ultra-reliable low-latency communication (URLLC), enhanced spectral and energy efficiency, massive machine-type communication (mMTC), and quantum-secure data transmission. These demands stem from the rise of futuristic applications such as autonomous driving, telemedicine, immersive extended reality (XR), and the Internet of Everything (IoE), which impose stringent requirements on both performance and security.

Despite the surge in research and development, existing communication frameworks face limitations in simultaneously achieving these multi-dimensional objectives. Technologies such as **Non-Orthogonal Multiple Access (NOMA)** and **Quantum Communication**, especially **Quantum Key Distribution (QKD)**, have shown promise in addressing specific challenges related to capacity, spectral efficiency, and secure transmission. However, these technologies have been largely developed and studied in isolation, with limited research investigating their synergistic potential within a single cohesive framework for next-generation networks.

Limitations of Conventional NOMA Frameworks:

NOMA, in contrast to traditional Orthogonal Multiple Access (OMA), enables multiple users to share the same time-frequency resource by utilizing power domain multiplexing and Successive Interference Cancellation (SIC) at the receiver end. This allows better spectral efficiency and user fairness. Despite its theoretical advantages, practical implementations of NOMA face several challenges:

- **Inter-User Interference:** NOMA relies on the simultaneous transmission of signals to multiple users, leading to unavoidable inter-user interference. When SIC is imperfect, this interference significantly degrades performance.
- **Fixed Power Allocation:** Many existing NOMA implementations use fixed or heuristic-based power allocation, which may be efficient for static environments but perform poorly in dynamic, real-time, or mobile scenarios.
- **Scalability Issues:** As the number of users grows, maintaining efficient and fair power distribution becomes more complex.
- **Lack of Real-Time Optimization:** Static models cannot respond to fluctuating channel conditions, user mobility, and application-specific QoS requirements.

These shortcomings imply that while NOMA enhances spectral efficiency, it requires advanced, intelligent control mechanisms for power and interference management to be fully viable in future networks.

Underutilization of Quantum Security in Wireless Systems:

In parallel, the advancement of quantum computing presents a double-edged sword. On one hand, it brings powerful computational capabilities. On the other, it threatens the foundation of classical cryptographic systems such as RSA and ECC, which rely on the computational difficulty of certain mathematical problems. Algorithms like Shor's and Grover's can efficiently break these schemes, rendering them obsolete in a post-quantum era.

Quantum Key Distribution (QKD) emerges as a robust countermeasure to this threat. It leverages quantum mechanical principles such as the Heisenberg Uncertainty Principle and the No-Cloning Theorem to ensure unconditionally secure key generation and exchange. Protocols like BB84, E91, and B92 have demonstrated theoretical and experimental success in securing communication against any form of computational attack, including those from quantum computers.

However, despite its potential, QKD is mostly applied in **point-to-point** fiber-optic networks and isolated quantum testbeds. Its integration into wireless and multi-user environments, particularly within NOMA-based systems, is largely unexplored due to challenges such as:

- **Dynamic Key Distribution:** Adapting QKD to serve multiple users in a dynamic access scheme like NOMA is technically complex.
- **Hardware Feasibility:** QKD traditionally requires sensitive hardware (e.g., photon detectors, beam splitters) which may be difficult to miniaturize for mobile wireless environments.
- **Latency Considerations:** Quantum key generation and synchronization can introduce delays, impacting the real-time performance required in 6G scenarios.

Thus, QKD remains underutilized as a practical solution for securing next-generation wireless systems, despite its theoretical benefits.

Potential of Machine Learning in NOMA Systems:

In recent years, **Machine Learning (ML)** techniques have gained traction in wireless networks for tasks like channel estimation, resource allocation, and anomaly detection. In particular, **Reinforcement Learning (RL)**, and its subset **Q-learning**, show great promise for adaptive and real-time decision-making.

Q-learning is a model-free, value-based RL algorithm that learns optimal policies through trial-and-error interaction with the environment. It does not require prior knowledge of system dynamics, making it suitable for complex wireless systems with dynamic channel conditions and heterogeneous user demands. Q-learning has been successfully applied to:

- Dynamic spectrum access
- Load balancing
- Beamforming
- Power control

In the context of NOMA, Q-learning can be used to allocate power efficiently among users in real-time, minimizing interference and maximizing throughput. However, current implementations typically focus on power allocation alone and do not account for security or integration with cryptographic protocols like QKD.

The Missing Link: Unified QKD-Q-learning-NOMA Framework:

Despite the individual benefits of QKD, Q-learning, and NOMA, the literature lacks a unified framework that integrates these three technologies to address the holistic challenges of 6G. Most research efforts have treated these technologies in isolation:

- QKD has been studied in secure key distribution scenarios without accounting for resource-constrained, multi-user wireless networks.
- NOMA has focused on spectral efficiency, often neglecting advanced security protocols and adaptive optimization.
- Q-learning has been used for power allocation without integration into quantum-secure architectures.

This creates a **critical research gap**: the absence of a scalable, secure, and intelligent communication architecture that:

1. **Incorporates QKD** for unbreakable key exchange.
2. **Implements Q-learning** for real-time, adaptive power allocation.
3. **Operates within a NOMA** framework to maximize spectral efficiency

Moreover, the **practical considerations** of deploying such an integrated system—such as latency, hardware constraints, energy consumption, and interoperability—are often overlooked. Existing models fail to provide simulation or experimental results that demonstrate real-world viability, particularly in scenarios involving user mobility, variable QoS requirements, and fluctuating channel conditions.

Objective of the Proposed Research

This project aims to **bridge this multi-dimensional research gap** by developing and validating a unified communication framework that integrates:

- **Quantum Key Distribution** for secure and tamper-proof key exchange.
- **Q-learning** for intelligent and adaptive power allocation in dynamic user environments.
- **Non-Orthogonal Multiple Access** to ensure spectral efficiency and support for massive user connectivity.

The proposed system will be evaluated using Python & MATLAB-based simulations, focusing on metrics such as Bit Error Rate (BER), Spectral Efficiency, Secure Key Rate, Jain's Fairness Index, and Quantum Bit Error Rate.

By addressing the technical limitations and theoretical gaps identified above, this research aspires to offer a **holistic, scalable, and secure solution** for future wireless networks—laying the foundation for practical 6G deployment.

1.3 Problem Statement

The exponential growth of connected devices, real-time applications, and data-intensive services is redefining the architecture and performance expectations of wireless communication systems. With the evolution toward sixth-generation (6G) networks, the wireless ecosystem is expected to support a diverse range of applications, including holographic communication, industrial automation, autonomous vehicles, and extended reality (XR). These applications demand ultra-reliable low-latency communication (URLLC), massive machine-type communication (mMTC), and enhanced mobile broadband (eMBB), all underpinned by unprecedented scalability, security, and efficiency.

Traditional communication frameworks, especially those relying on Orthogonal Multiple Access (OMA), are increasingly unable to meet these demands. OMA-based techniques, which assign distinct time or frequency resources to each user, inherently limit the number of users and lead to inefficient spectrum utilization. This becomes a critical bottleneck in ultra-dense 6G environments, where simultaneous connectivity for thousands of devices per square kilometer is required.

To address these constraints, Non-Orthogonal Multiple Access (NOMA) has emerged as a key enabler for 6G networks. NOMA enhances spectral efficiency by allowing multiple users to share the same frequency resources simultaneously, distinguishing them via power domain multiplexing and successive interference cancellation (SIC). While NOMA effectively increases user capacity and data throughput, it introduces a new set of technical challenges, particularly in multi-user scenarios. Among the most pressing issues are:

- **Inter-user interference**, due to simultaneous signal transmission,
- **Complex and suboptimal power allocation**, especially in dynamic environments, and
- **Inherent security vulnerabilities**, especially when integrated into cloud-native, distributed 6G architectures.

In parallel, the growing capabilities of quantum computers threaten the security of existing encryption and key distribution protocols. Classical cryptographic systems, which rely on the computational difficulty of certain mathematical problems (e.g., factoring large primes or computing discrete logarithms), are vulnerable to quantum algorithms such as Shor's and Grover's algorithms. These quantum threats necessitate a shift to more secure communication paradigms that are resilient to quantum attacks.

Quantum Key Distribution (QKD) emerges as a promising solution to this challenge. QKD leverages the fundamental properties of quantum mechanics—such as superposition and no-cloning theorem—to enable the generation and exchange of encryption keys that are provably secure. Protocols like BB84 and E91 have demonstrated the theoretical and experimental feasibility of unconditionally secure key distribution over optical fibers and free-space links. However, QKD remains underexplored in the context of mainstream wireless access technologies like NOMA. Most QKD implementations are point-to-point and struggle to adapt to the dynamic, multi-user nature of 6G wireless environments.

Thus, integrating QKD into a multi-user NOMA framework introduces a significant research challenge. How can quantum-secure key distribution be extended to multiple users without compromising the efficiency or scalability of the system? Furthermore, the real-time integration of QKD with NOMA requires novel techniques to handle user scheduling, resource allocation, and key synchronization—all in a latency-sensitive environment.

Another dimension of complexity in NOMA lies in **power allocation**. Since NOMA relies on differentiating users by assigning them varying power levels, the accuracy and efficiency of power allocation algorithms directly impact system performance. In conventional NOMA systems, power allocation is typically carried out using fixed or heuristic rules, which do not scale well in real-time, mobile, or heterogeneous environments. These static methods are insufficient for scenarios involving rapidly changing user demands, varying channel conditions, and diverse Quality of Service (QoS) requirements.

To address this limitation, there is a growing interest in leveraging **Machine Learning (ML)**, particularly **Reinforcement Learning (RL)**, for intelligent resource allocation in wireless networks. Among various RL techniques, **Q-learning** has gained attention due to its model-free nature and ability to learn optimal policies through environmental interactions. Q-learning allows the system to adaptively determine power levels for different users based on feedback, such as Signal-to-Noise Ratio (SNR), interference levels, and QoS requirements. This adaptability is critical for the successful deployment of NOMA in 6G systems.

Despite the promising aspects of QKD, NOMA, and Q-learning individually, their **integration into a unified framework remains largely unexplored**. While researchers have studied QKD for secure communication and Q-learning for dynamic resource management, the combined use of QKD for security and Q-learning for real-time power control within a NOMA-based wireless system represents an untapped area with enormous potential.

Given the limitations of existing technologies and the ambitious goals of 6G, a unified, secure, and intelligent communication framework is urgently needed. This framework should fulfill the following requirements:

- **Scalability** to support large numbers of users and devices in dense network environments.
- **Security** to protect data and user privacy against both classical and quantum attacks.
- **Intelligence and Adaptability** to optimize power allocation dynamically and autonomously in real time.
- **Compatibility** with existing and emerging wireless protocols to enable seamless integration and deployment.

Therefore, **the core research problem** that this project addresses is:

“How can we design a secure, scalable, and intelligent communication framework that integrates Quantum Key Distribution (QKD) for enhanced encryption and Q-learning for efficient, adaptive power allocation within a NOMA-based access environment, thereby meeting the complex performance and security demands of future wireless networks?”

This project aims to develop and validate a comprehensive solution to this problem through simulation, algorithmic design, and performance evaluation. It will demonstrate how integrating QKD and Q-learning into the NOMA framework can significantly enhance the security, efficiency, and adaptability of next-generation wireless communication systems.

By bridging the current research gap and addressing the multi-domain challenges in a unified manner, the outcomes of this project have the potential to set a new benchmark for future wireless communication standards.

2. Research Objective

The overarching goal of this project is to design and implement a **Quantum Key Distribution (QKD)-enhanced Non-Orthogonal Multiple Access (NOMA)** framework that facilitates ultra-secure, highly efficient, and scalable wireless communication in 6G and beyond. As wireless communication systems evolve, especially with the emergence of 5G and 6G technologies, the demand for enhanced security, efficiency, and adaptability has reached unprecedented levels. This research seeks to address the challenges associated with these evolving requirements by combining cutting-edge technologies, including Quantum Communication, NOMA, and Machine Learning (ML), to create an integrated solution that is both secure and capable of meeting the requirements of future networks. The specific objectives of this research can be outlined as follows:

1. Integrating Quantum Communication Principles for Ultra-Secure Encryption:

One of the core aims of this project is to incorporate **Quantum Key Distribution (QKD)** as the fundamental security mechanism to ensure **unbreakable encryption** and detection of any eavesdropping attempts. Traditional encryption methods, such as RSA or elliptic-curve cryptography, are susceptible to future threats posed by quantum computing, which can solve problems like integer factorization and discrete logarithms in polynomial time using quantum algorithms (e.g., Shor's algorithm). This vulnerability calls for quantum-resistant security mechanisms, and QKD, based on the principles of quantum mechanics, offers a solution that guarantees the confidentiality of communication against any adversaries, including those equipped with quantum computing capabilities.

The **BB84 protocol**, introduced by Bennett and Brassard in 1984, is one of the most well-known QKD protocols. By leveraging quantum properties such as the no-cloning theorem and quantum superposition, QKD ensures that any eavesdropping attempt on the key exchange process can be detected by the legitimate parties. This project will explore the implementation of **QKD for key generation and exchange** over both fiber-optic and free-space channels, taking into consideration practical issues such as key rate, transmission distance, and integration with existing wireless systems.

The challenge in this research is integrating QKD with **NOMA-based communication systems**, as QKD typically requires higher bandwidth and specific protocols, whereas NOMA needs efficient spectrum usage. By leveraging QKD to establish secure communication channels, the project aims to ensure that each user's data is encrypted with quantum security, while still utilizing NOMA's spectral efficiency advantages.

2. Enhancing Spectral Efficiency and Massive Device Connectivity through NOMA:

Another crucial objective is to enhance **spectral efficiency** and **massive device connectivity** using **Non-Orthogonal Multiple Access (NOMA)**. NOMA addresses the limitations of conventional Orthogonal Multiple Access (OMA) schemes by allowing multiple users to transmit their data simultaneously over the same frequency spectrum, effectively increasing system throughput. This simultaneous transmission is made possible by **power-domain multiplexing**, where users are assigned different power levels according to their channel conditions, and the receiver employs **Successive Interference Cancellation (SIC)** to decode the overlapping signals.

In future 6G networks, where massive connectivity (e.g., billions of devices) and low latency are paramount, NOMA offers a scalable solution that OMA cannot match. Unlike OMA, which requires distinct orthogonal resources for each user, NOMA allows for a more efficient use of the available spectrum. This research aims to develop a NOMA framework that supports **massive connectivity** in dense environments while maintaining **high system throughput** and **low latency**.

A significant challenge that remains with NOMA systems is ensuring **fair power allocation** among users, especially in heterogeneous environments where users have different channel gains and QoS requirements. This research will propose a new approach to power allocation, which will be adaptive and dynamic, leveraging **Machine Learning (ML)** techniques such as **Q-learning** to optimize power distribution in real-time. By doing so, the system will ensure that users with weaker channels are allocated more power, while users with stronger channels are allocated less power, improving overall system fairness and throughput.

3. Developing Machine Learning-Based Power Allocation Strategy:

The third objective focuses on developing a **machine learning-based power allocation strategy** that adapts to real-time channel conditions and optimizes resource usage. Traditional power allocation strategies in NOMA are often based on static algorithms that do not account for real-time changes in user locations, mobility, or fluctuating channel conditions. Moreover, these classical algorithms may not efficiently handle dynamic interference, especially in dense and high-demand networks, which are expected to characterize 6G systems.

To address this challenge, this research will leverage **Reinforcement Learning (RL)**, specifically **Q-learning**, for adaptive power control. Q-learning, a model-free RL algorithm, will allow the system to learn optimal policies for power allocation by interacting with the network environment, without requiring a priori knowledge of the network state. In this approach, an RL agent will dynamically adjust the transmission power based on real-time observations, such as channel quality, interference levels, and the number of users in the network. By doing so, the system will be able to maximize throughput and minimize power consumption while ensuring fairness and reducing interference between users.

The Q-learning-based approach will also enable the **dynamic adjustment of transmission parameters** (such as modulation schemes and coding rates), allowing the system to optimize its performance under varying network conditions. This capability is essential for future networks where conditions can change rapidly, and systems must adapt to meet the needs of users with diverse QoS demands.

4. Supporting Adaptive Modulation Schemes for Dynamic Transmission Adjustment:

The ability to adapt transmission parameters based on **real-time channel conditions** is another key objective of this research. In future networks, user mobility, interference, and varying channel quality will necessitate the use of **adaptive modulation and coding schemes** to maintain reliable communication. Adaptive modulation allows for the selection of the most appropriate modulation scheme based on instantaneous channel conditions, ensuring efficient spectrum usage while maintaining the desired quality of service.

This research will explore techniques such as **Adaptive Modulation and Coding (AMC)**, which adjusts the modulation order and coding rate dynamically in response to channel fluctuations. By integrating AMC with the **Q-learning-based power allocation** system, the framework will adapt transmission parameters in real-time to ensure high throughput, low latency, and robust security for users. The combined approach will optimize network performance, balancing data rates with energy efficiency and robustness against interference.

5. Evaluating the Proposed System's Performance for 6G Scenarios:

The proposed system—integrating BB84-based Quantum Key Distribution (QKD) with a two-user Non-Orthogonal Multiple Access (NOMA) framework and dynamic power allocation via Q-learning—will be evaluated across several key performance metrics to assess its suitability for Beyond 5G (B5G) and 6G wireless networks. These metrics include quantum-level security, average sum rate, fairness, Bit Error Rate (BER), and Secret Key Rate (SKR), all critical for high-speed, low-latency, and densely connected environments.

Security will be assessed through the Quantum Bit Error Rate (QBER) and the integrity of the BB84-based key agreement, ensuring resistance to eavesdropping and quantum attacks. **Throughput** performance will be measured by evaluating the average sum rate achieved under Q-learning-driven power allocation, highlighting the system's ability to adapt to changing channel conditions. **Fairness** among users will be quantified using Jain's Fairness Index, demonstrating how well resources are distributed between strong and weak users.

Efficiency will be indirectly captured through metrics like BER and SKR, reflecting the reliability and secrecy of transmitted data. While **latency** is not explicitly modeled in this simulation, the adaptive nature of Q-learning provides a foundation for future enhancements that could address real-time responsiveness.

All evaluations will be based on simulation results generated through MATLAB (for NOMA-Q-learning power allocation) and Python (for BB84 QKD protocol), demonstrating the feasibility of integrating quantum security with intelligent wireless communication for 6G scenarios.

3. Relevance of the Problem Statement with respect to SDG:

The proposed research aligns closely with several United Nations Sustainable Development Goals (SDGs), reflecting its broader societal and global relevance. The integration of Quantum Key Distribution (QKD) and Machine Learning-powered Non-Orthogonal Multiple Access (NOMA) not only addresses critical challenges in the field of wireless communication but also has profound implications for achieving sustainable development. Below, we discuss how this research contributes to four key SDGs:

SDG 9 – Industry, Innovation, and Infrastructure

One of the central aims of this research is to enhance communication infrastructure using advanced technologies like **QKD** and **Machine Learning-powered NOMA**. This combination contributes directly to the development of **resilient and intelligent communication systems**, which are essential for future technologies. Smart cities, autonomous vehicles, remote healthcare, and other emerging fields all rely on robust communication networks that are both efficient and secure.

NOMA's ability to increase the spectral efficiency of wireless networks, while QKD ensures security, addresses the dual challenge of improving both capacity and privacy in digital communication systems.

By focusing on the development of secure, scalable, and energy-efficient communication frameworks, this research lays the foundation for **sustainable industrial innovation**. A resilient communication infrastructure is not only vital for day-to-day operations but also plays a pivotal role in **driving future advancements** in industrial sectors, ranging from manufacturing to transportation. Thus, the integration of QKD and NOMA within communication infrastructure will contribute to meeting the growing demand for more innovative, secure, and reliable networks in the industrial sector.

SDG 16 – Peace, Justice, and Strong Institutions

The increasing digitization of communication systems has brought about significant challenges in terms of **data security and privacy**. The rise in cyber threats and digital surveillance highlights the vulnerability of traditional communication systems that rely on classical encryption methods. The integration of **QKD** into the proposed system addresses this vulnerability by offering **quantum-secure communication**. QKD-based encryption is **theoretically immune to eavesdropping**, offering an unbreakable security mechanism that protects sensitive data from unauthorized access.

By ensuring the **integrity and confidentiality** of transmitted data, this research promotes **trust** in digital governance, strengthening the foundation for peace, justice, and strong institutions. Reliable and secure communication systems are fundamental for **good governance** and **transparent institutions**, as they ensure the safe exchange of information without compromising privacy. Moreover, the research contributes to the broader goal of building **secure and stable digital environments** in which individuals, organizations, and governments can operate confidently without fear of surveillance or cyber-attacks.

4. PROPOSED WORK

4.1 Proposed Work: System Design and Approach

The core of this project lies in the integration of **Quantum Key Distribution (QKD)** and **Non-Orthogonal Multiple Access (NOMA)**, with the aim of developing a **secure, efficient, and adaptive wireless communication framework** suitable for **future communication networks**. This hybrid framework leverages **quantum-secured communication** and **machine learning-driven power allocation**, thereby addressing the critical requirements of **security, spectral efficiency, and energy optimization** in next-generation networks.

Tools and Technologies Used:

1. Python (with Qiskit):

Python served as the primary platform for simulating the BB84 Quantum Key Distribution (QKD) protocol using Qiskit. The objective was to model quantum-level encryption that facilitates secure key generation, transmission, and eavesdropper detection. Qiskit's powerful quantum circuit simulation capabilities were leveraged to emulate realistic quantum communication, including the effects of noise and interception attempts by an adversary (Eve). The simulation also included classical post-processing steps like basis reconciliation and key sifting to mimic real-world quantum networks. Additionally, quantum-generated keys were extracted for encryption and decryption of classical messages, creating an end-to-end secure communication pipeline that feeds into the NOMA system.

- Implementation of **BB84 protocol** for quantum key generation.
- Visualization of **Eve detection probability** by comparing subsets of key bits.
- Simulation of realistic quantum noise and Eve's interference with calculated **QBER (Quantum Bit Error Rate)**.
- **Message encoding and recovery** using quantum-generated keys to encrypt and decrypt classical messages.

2. MATLAB:

MATLAB was employed to develop and simulate the power allocation strategy for a 2-user Non-Orthogonal Multiple Access (NOMA) communication system using a reinforcement learning framework. Specifically, a Q-learning algorithm was implemented to dynamically adjust power levels between users based on channel conditions to optimize throughput and fairness. The simulation aimed to reflect real-world wireless environments, supporting adaptive modulation (QAM), successive interference cancellation (SIC), and evaluation of both individual and overall system performance. MATLAB's robust mathematical libraries and plotting tools were used to analyze and visualize various metrics such as Bit Error Rate (BER), average sum rate, fairness index, and Q-learning reward over training iterations.

- Development of a Q-learning algorithm for dynamic power distribution based on varying channel conditions.
- Calculation of key performance metrics such as **Bit Error Rate (BER)**, Quantum Bit Error Rate, Jain's Fairness Index, and Q-learning Reward Evolution.
- Simulation of QAM-based NOMA communication with Successive Interference Cancellation (SIC) decoding.

System Workflow and Implementation:

1. Quantum Key Generation (Python – Qiskit):

Using the BB84 protocol, quantum keys are generated by encoding qubits in random bases. A Using Qiskit, Alice and Bob generate secret keys via the **BB84 protocol**. An eavesdropper (Eve) is simulated by altering the quantum transmission. Detection steps include:

- **Rotation basis mismatch analysis** to compare results.
- Calculation of **subset QBER** from randomly chosen bit positions.
- Visualization of the **Probability of Detecting Eve vs. Number of Bits Compared**, which asymptotically approaches 1, confirming detection confidence grows with more samples.
- Upon successful eavesdropping detection, keys are discarded and the session is invalidated. Otherwise, the key is used to encrypt the message (as shown in the output: *Recovered message: hello world*).

2. NOMA User Classification (MATLAB):

In the simulated NOMA system, two users are assigned to the same subchannel—one with a strong channel and one with a weak channel. This pairing facilitates effective SIC, a fundamental principle of power-domain NOMA.

3. Q-learning Based Power Allocation (MATLAB):

A Q-learning model is implemented to dynamically optimize power allocation between the two users:

- States: Defined based on real-time channel gains and user SNR.
- Actions: Power allocation ratios satisfying the NOMA constraint (weaker user gets higher power).
- Rewards: Computed from a weighted combination of throughput, fairness, and energy efficiency.
- The system converges to an optimal policy by updating its Q-table over simulation episodes.

4. Data Encryption and Transmission (Conceptual Integration):

The secure keys obtained from the BB84 protocol are conceptually used to encrypt user data. Although encryption is not explicitly implemented in simulation, performance metrics are computed under the assumption of QKD-based secure communication in a NOMA channel.

5. Performance Evaluation

Comprehensive performance analysis includes:

- Quantum Bit Error Rate (QBER) and Secret Key Rate (SKR) from the QKD simulation.
- Bit Error Rate (BER), Average Sum Rate, and Jain's Fairness Index from the NOMA-Q-learning simulation.
- Q-table convergence trends to evaluate learning performance.

Challenges and Solutions

Challenge	Proposed Solution
Ensuring quantum-secure key distribution	Implemented BB84 using Qiskit to detect eavesdropping and extract secure keys.
Rigid power allocation schemes in NOMA	Developed a Q-learning model to enable adaptive, channel-aware power control.
Difficulty in classical-quantum integration	Conceptually merged Python-based QKD output with MATLAB-based NOMA power allocation.
Limited user scalability in static models	Designed Q-learning with flexibility for future multi-user extension.
Balancing secrecy, fairness, and throughput	Customized reward functions to optimize all three simultaneously.

Table 1: Key Challenges and Proposed Solutions in Quantum-Secure NOMA Systems

Novelty of the Proposed Approach

- First simulated framework combining quantum-secure BB84 QKD with Q-learning-based NOMA power allocation.
- Dynamic adaptation to channel conditions through reinforcement learning, rather than fixed or heuristic power rules.
- Joint evaluation of security (QBER, SKR), efficiency (sum rate), and fairness (Jain's Index) within a single framework.
- Utilization of open-source tools: Qiskit for quantum key generation, and MATLAB for communication simulation and machine learning.
- Establishes a scalable base for future work on multi-user, multi-subchannel, quantum-secure wireless networks.

4.2 Codes and Standards

Quantum Key Distribution (QKD) Standards:

- Implementation of the **BB84 protocol** for secure quantum key generation.
- Follows established QKD principles for eavesdropper detection using **Quantum Bit Error Rate (QBER)** analysis.
- Simulated using **Qiskit**, IBM's quantum SDK, ensuring adherence to quantum communication protocols.

Classical Communication Standards:

- Integration of **Non-Orthogonal Multiple Access (NOMA)**, aligning with **6G communication trends** and B5G frameworks.
- Users grouped into clusters based on signal strength to match traditional NOMA architecture.

Modulation Techniques:

- Support for **4-QAM**, **16-QAM**, and **64-QAM** schemes, in line with current wireless communication standards.
- Used for adaptive modulation in multi-user subchannel environments.

Machine Learning-Based Optimization:

- Power allocation implemented via **Q-learning**, conforming to reinforcement learning frameworks.
- Designed for real-time, adaptive control in dynamic network environments.

Simulation Platforms and Languages:

- **Qiskit (Python)** for quantum simulation and key generation.
- **MATLAB** for Q-learning algorithm and performance analysis in multi-subchannel NOMA scenarios.

Performance Metrics and Evaluation Standards:

- Evaluated using industry-standard metrics:
 - **Bit Error Rate (BER)**
 - **Quantum Bit Error Rate (QBER)**
 - **Secret Key Rate (SKR)**
 - **Q-learning convergence**
 - **Power Allocation Bar Chart**
 - **Jain's Fairness Index**
- Metrics ensure compatibility with academic and industrial benchmarks for 6G and secure communication systems.

4.3 Constraints, Alternatives or trade offs

Constraints:

- **Hardware Limitations:**
Current quantum computing hardware offers limited qubit counts and gate fidelities, restricting the system's scalability and the complexity of quantum operations. As a result, the project relies on **Qiskit-based simulations** rather than real quantum devices for QKD implementation.
- **Computational Overhead:**
Q-learning becomes computationally expensive as the number of users or subchannels increases. Convergence time may be high, making real-time applications difficult in larger networks.
- **Channel Modelling Challenges:**
Accurate modelling of real-world channel conditions (e.g., fading, shadowing, and noise) is limited. The simulation assumes ideal or semi-ideal SNRs and does not fully capture all practical wireless impairments.

Alternatives

- **Power Allocation Schemes:**
Classical approaches like **water-filling** offer computational simplicity but lack the adaptability and fairness guarantees of Q-learning. **Distributed Q-learning** could reduce system complexity but may result in locally optimal (not globally optimal) decisions.
- **Key Management Methods:**
Conventional encryption schemes such as **RSA or AES** can replace QKD but do not provide resistance to quantum computational attacks, limiting long-term security in 6G and post-quantum contexts.
- **Access Technologies:**
Orthogonal Multiple Access (OMA) techniques like TDMA and FDMA provide simpler user isolation but sacrifice spectral efficiency compared to **NOMA**, which supports simultaneous transmissions at the cost of interference management complexity.

Trade-offs

- **Quantum vs. Classical Security:**
QKD ensures **information-theoretic security** and resistance to quantum attacks, but is resource-intensive and currently not scalable for large networks. In contrast, classical cryptography is lightweight and fast but susceptible to quantum decryption in the future.
- **Centralized vs. Distributed Learning:**
A **centralized Q-learning** controller enables coordinated, optimal power allocation but suffers from scalability and communication overhead. **Distributed learning** improves scalability but may reduce efficiency due to limited global state awareness.
- **Simulation vs. Real-World Implementation:**
Simulation enables rapid prototyping and metric evaluation, but results may diverge under real-world deployment due to hardware imperfections, channel variability, and synchronization issues.

5. Project Description:

A Q-Learning-Based Power Allocation Strategy for Quantum-Encrypted NOMA in Future Wireless Networks

As the demand for secure, adaptive, and high-throughput communication intensifies in future network infrastructures, this project introduces a hybrid framework that combines **Quantum Key Distribution (QKD)** and **Q-learning-based power allocation** in a **Non-Orthogonal Multiple Access (NOMA)** system. This design aims to enhance both security and spectral efficiency, addressing critical challenges for next-generation wireless systems.

Overview of NOMA

Non-Orthogonal Multiple Access (NOMA) allows multiple users to share the same frequency resources by allocating different power levels, improving spectral efficiency over traditional Orthogonal Multiple Access (OMA). Users with stronger channels receive less power, while weaker users receive more. At the receiver end, **Successive Interference Cancellation (SIC)** is used to decode signals, where the stronger user subtracts the weaker user's signal before decoding its own. Despite its advantages, improper power allocation in NOMA can result in poor Quality of Service (QoS), unfairness, and higher Bit Error Rates (BER).

Quantum Key Distribution (QKD)

To safeguard communication against classical and quantum attacks, this project employs **BB84-based QKD**, simulated using Python and Qiskit. Qubits are transmitted between sender (Alice) and receiver (Bob), and eavesdropping (Eve) is detected via Quantum Bit Error Rate (QBER) analysis. Keys are then sifted, verified, and used for encrypting user data before classical transmission.

Q-learning for Power Allocation

A **Q-learning algorithm implemented in MATLAB** is used for intelligent and dynamic power allocation among NOMA users. The agent (base station) learns optimal allocation policies by observing channel gains and SINR, taking actions (power ratios), and updating a Q-table based on rewards. The reward function balances throughput, fairness (Jain's Index), and BER minimization, ensuring that weaker users receive more power per NOMA principles.

Simulation Tools and Environment:

- **MATLAB:** Simulates NOMA system, Q-learning-based power control, SIC decoding, and BER, throughput, fairness analysis.
- **Python (Qiskit):** Implements BB84 protocol for secure key generation and eavesdropper (Eve) detection.
- **Metrics Evaluated:**
 - **QBER (Quantum Bit Error Rate)**
 - **Secret Key Rate (SKR)**
 - **BER (Bit Error Rate)**
 - **Jain's Fairness Index**
 - **Power Allocation Visualization: Stacked bar charts** generated to show how Q-learning allocates power to each user across subchannels in the NOMA system, demonstrating dynamic and fair resource distribution.

Key Contributions:

1. **Quantum-Secured NOMA:** Combines BB84-QKD with learning-driven NOMA, enhancing confidentiality and adaptability.
2. **Adaptive Power Control:** MATLAB-based Q-learning ensures dynamic allocation based on user channel states.
3. **End-to-End Security:** Integration of Eve detection into QKD simulation confirms robustness against quantum threats.

Use Cases:

- **Secure IoT in Smart Cities**
- **Military and Defence Communications**
- **Remote Medical Systems**
- **Quantum-safe Financial Transactions**

Challenges:

- Synchronization between QKD results and classical transmission.
- High computational cost for large-scale Q-learning in MATLAB.
- Designing reward functions that ensure fairness, efficiency, and security.

Results:

- Learned power policies reduced BER and improved fairness across users.
- QKD simulations consistently maintained QBER below threshold even under Eve attacks.
- End-to-end secure communication achieved via QKD-encrypted NOMA transmission.
- Power allocation visualizations confirmed that weaker users consistently received higher power as learned by the Q-agent.

Future Work:

- Hardware deployment of QKD over optical channels.
- Use of **Federated Q-learning** for scalable, decentralized control.
- Exploration of **Quantum Reinforcement Learning** for faster, hardware-accelerated decisions.

6. Software Tools Used

In the development of the quantum-based Non-Orthogonal Multiple Access (Q-NOMA) system, various software tools were leveraged to handle the complexity of the quantum communication and machine learning tasks. Two key software tools played pivotal roles in the design, implementation, and simulation of the system: **Python** and **MATLAB**.

MATLAB

- MATLAB served as the **core simulation platform** for the classical part of the system, particularly the NOMA communication environment. It was used to implement the **Q-learning algorithm** for dynamic power allocation among users across multiple subchannels.
- The simulation included **realistic channel modeling** under Additive White Gaussian Noise (AWGN) and varying Signal-to-Noise Ratio (SNR) conditions.
- MATLAB enabled the execution of **Successive Interference Cancellation (SIC)**, allowing correct decoding of user signals in a NOMA setup.
- Key performance metrics such as **Bit Error Rate (BER)**, **Jain's Fairness Index**, **Secret Key Rate (SKR)**, and **Quantum Bit Error Rate (QBER)** were visualized.
- Additionally, **stacked bar charts** were generated to illustrate the **power allocation distribution** per user and subchannel, giving insights into the efficiency and fairness of the Q-learning-based strategy.

Python

- Python was utilized to implement and simulate the **Quantum Key Distribution (QKD)** process using the **BB84 protocol**. This part of the project handled the **quantum security layer** for encrypting user data prior to transmission.
- The simulation included generation of random quantum bits, application of basis states (Z and X), and simulation of the **eavesdropping scenario** with Eve's intervention.
- The system evaluated **Quantum Bit Error Rate (QBER)** and filtered out bits where Alice and Bob used mismatched bases, thereby forming a shared secret key.
- The QKD simulation was made interactive and flexible, allowing parameter variations like number of qubits, Eve's probability of intercepting, and basis matching logic.

Qiskit (IBM Quantum SDK)

- Qiskit was the main **quantum simulation toolkit** used within Python. It enabled the implementation of **quantum circuits** for the BB84 protocol.
- The toolkit supported the design and visualization of **quantum state preparations, Hadamard and Pauli gates, measurement operations, and qubit basis transformations**.
- It facilitated **eavesdropper detection** by analyzing the increase in QBER when Eve attempted to intercept and resend qubits.

7. Schedule and Milestones

Dec 15 – Dec 30 (Literature Review & Project Finalization):

- **Preeti Yadav:** Conducted a detailed literature review of quantum communication systems and secure wireless networks by analyzing IEEE papers and technical reports, which helped define the project direction.
- **Basil Syed:** Gathered technical resources related to Quantum Key Distribution (QKD), particularly BB84, and reviewed research on intelligent radio resource management.
- **Satyam Sinha:** Focused on understanding NOMA fundamentals and explored the intersection of QKD and NOMA to brainstorm the feasibility of integrating machine learning for secure key allocation.

Dec 31 – Jan 15 (QKD Protocols & Qiskit Exploration):

- **Preeti Yadav:** Investigated the BB84 protocol in detail and started using Qiskit to simulate quantum key distribution scenarios.
- **Basil Syed:** Explored Qiskit's implementation capabilities and contributed to the initial development of BB84 simulations using quantum circuits.
- **Satyam Sinha:** Analyzed QKD use cases in future communication networks and studied Qiskit-based key generation models for secure transmission.

Jan 16 – Jan 31 (Development Environment Setup & QKD Implementation):

- **Preeti Yadav:** Helped finalize the problem statement and created an outline for the overall simulation pipeline.
- **Basil Syed:** Set up the Python-Qiskit environment and began developing the BB84-based key exchange module.
- **Satyam Sinha:** Contributed to developing the BB84 protocol simulation in Qiskit and ensured correctness in quantum key generation and eavesdropper detection logic.

Feb 1 – Feb 15 (Optimization & Security Testing):

- **Preeti Yadav:** Organized project documentation and reviewed potential security loopholes in QKD implementation.
- **Basil Syed:** Optimized the QKD circuit parameters and conducted initial tests to evaluate the system's ability to detect eavesdropping using QBER analysis.
- **Satyam Sinha:** Developed the QBER metric calculation, tested the protocol under attack scenarios, and verified secure key reconciliation mechanisms.

Feb 16 – Feb 29 (NOMA Integration & Security Refinements):

- **Preeti Yadav:** Studied various NOMA schemes and identified candidate structures for integration with QKD in a 6G scenario.
- **Basil Syed:** Initiated the process of integrating power-domain NOMA with the QKD output, focusing on channel modeling.
- **Satyam Sinha:** Designed the basic structure for combining Q-learning with power allocation in a NOMA setup and ensured it supports key generation from QKD.

Mar 1 – Mar 15 (Full QKD-NOMA Integration & Simulations):

- **Preeti Yadav:** Helped map the BB84 outputs to multi-user NOMA channels and supported key exchange simulations across subchannels.
- **Basil Syed:** Implemented and tested the full QKD-NOMA system, simulating secure transmission with multiple users and subchannels.
- **Satyam Sinha:** Developed the Q-learning algorithm for adaptive power allocation, integrated it with the NOMA-QKD model, and ran MATLAB simulations to test performance and fairness.

Mar 16 – Mar 31 (Optimization & Performance Enhancement):

- **Preeti Yadav:** Assisted in optimizing simulation plots and helped structure key sections of the project report.
- **Basil Syed:** Tuned NOMA parameters for improved energy efficiency and addressed potential security breaches under varying user conditions.
- **Satyam Sinha:** Validated metrics such as BER, SKR, QBER, and Jain's fairness index, fine-tuned the Q-learning parameters, and tested for scalability and reliability.

Apr 1 – Apr 15 (Finalization of Results & Documentation):

- **Preeti Yadav:** Contributed to final report compilation, refined visualizations, and prepared the final research presentation.
- **Basil Syed:** Reviewed the simulation results and improved QKD-NOMA performance graphs for inclusion in the final paper.
- **Satyam Sinha:** Consolidated all findings into a cohesive technical report, ensuring alignment with IEEE publishing standards and simulation results.

Apr 16 – Apr 20 (Final Review & Submission):

- **Preeti Yadav:** Reviewed the complete report and prepared for the final presentation and project viva.
- **Basil Syed:** Conducted a final run-through of all code implementations and made last-minute corrections in the simulation outputs.
- **Satyam Sinha:** Completed final edits on the report, verified all performance metrics, and submitted the complete documentation and presentation on schedule.

8.Results and Analysis

The evaluation of the proposed Q-learning-based power allocation strategy within a Quantum-Encrypted NOMA framework yielded a comprehensive set of results that validate both the adaptive intelligence of the model and the practical feasibility of deploying such systems in future wireless networks.

At the core of this system lies the reinforcement learning agent, trained using Q-learning—a model-free learning algorithm that relies on reward-based updates to make decisions in uncertain environments. The simulation environment consisted of two users (User 1 and User 2) with unequal channel gains. User 1 was assumed to have a relatively stronger channel condition, while User 2 experienced weaker channel conditions. This setup reflects a common real-world scenario in cellular networks, where users located at the cell edge or in high-interference zones suffer degraded connectivity.

Power Allocation Behavior:

Over multiple training episodes, the agent dynamically explored and exploited the state-action space to learn the optimal power allocation strategy. The Q-table was updated using the Bellman equation, gradually converging towards values that maximized the cumulative expected reward. The reward function was carefully designed to consider throughput (measured using Shannon's capacity formula), fairness (implicitly), and interference.

The results revealed a clear learning trajectory in the behavior of the Q-agent. As the number of episodes increased, the power allocated to User 2 increased significantly. Eventually, the agent settled on allocating approximately 81% of the total available power to User 2. This outcome reflects the agent's understanding that User 2, with poor channel conditions, required more energy to maintain a satisfactory data rate. Meanwhile, User 1, with a high channel gain, could sustain optimal performance with minimal power. This strategy effectively minimized the overall interference in the system while maximizing user coverage.

The average reward graph further substantiated this learning. It showed a steady increase during the initial episodes—highlighting exploration—and then plateaued, indicating convergence. The reward function's growth curve directly reflects the policy's performance improvement. By the time training reached convergence, the system had achieved a stable and near-optimal power distribution pattern.

Cumulative Rewards and Fairness:

A detailed analysis of cumulative rewards over time showed User 2 benefiting more substantially in the long run. This is a desirable outcome, particularly in NOMA, where power-domain multiplexing often leads to unfair treatment of users with weak channels. The system was thus able to overcome the "near-far problem", where users near the base station (with strong channels) dominate the available resources.

To quantitatively assess fairness, Jain's Fairness Index was employed. The calculated value of 0.9304 indicates a reasonably balanced allocation of resources among the users. While a perfect index of 1.0 represents absolute fairness (equal resource distribution), such an outcome would be unrealistic and inefficient in a system where users have vastly different requirements. A score above 0.8 suggests that the model successfully maintains a trade-off between efficiency and equity.

Quantum Key Distribution (BB84) Evaluation:

Simultaneously, the security layer—implemented using the BB84 protocol—demonstrated its effectiveness in ensuring quantum-secure communication. The BB84 protocol leverages quantum properties such as the no-cloning theorem and observer effect to detect eavesdropping. In our setup, quantum bits (qubits) were sent from Alice to Bob using random polarization states. Under normal, unperturbed conditions, Alice and Bob were able to share identical keys with negligible error, with Quantum Bit Error Rate (QBER) values well below the acceptable threshold. However, when an eavesdropper (Eve) was simulated, the QBER spiked to 0.1724, a level that strongly indicated a breach. This behavior confirmed the protocol's robustness, as it triggered the necessary action: key discarding and retransmission. In fact, 100% detection accuracy was observed using only 15–30 bits, proving the efficiency and practicality of quantum key distribution even at small data scales.

Impact of Modulation Schemes:

To assess the practical applicability of the system under different communication conditions, the model was tested using 4-QAM, 16-QAM, and 64-QAM modulation schemes. Each scheme was evaluated in terms of Bit Error Rate (BER), QBER, and secret key generation rate under varying Signal-to-Noise Ratios (SNRs).

- 4-QAM provided the lowest BER and QBER, especially under low-SNR conditions. Its robustness to noise makes it ideal for highly secure environments where communication integrity is prioritized over throughput.
- 16-QAM offered a moderate trade-off, balancing robustness and data rate.
- 64-QAM, while initially error-prone at low SNR, yielded the highest secret key generation rates at high SNR levels (15 dB and above), peaking at 7×10^7 bps.

These results highlight a strategic design opportunity: adaptive modulation can be used to toggle between security (low modulation) and performance (high modulation) based on real-time SNR estimations.

9. Conclusion

This research initiative marks a significant stride in the convergence of artificial intelligence and quantum communication, presenting a robust, scalable, and secure framework poised for next-generation wireless systems. By integrating Q-learning-based power allocation with the BB84 Quantum Key Distribution (QKD) protocol, we demonstrate a hybrid communication architecture that addresses two of the most pressing challenges in modern wireless networks—resource optimization and end-to-end security.

The proposed solution leverages tabular Q-learning, a reinforcement learning technique, to dynamically manage power allocation among multiple users in a Non-Orthogonal Multiple Access (NOMA) environment. The algorithm showcased intelligent adaptability by learning an optimal policy over time, ensuring that users experiencing poor channel conditions received sufficient transmission power. This adaptive behavior not only optimized system-wide throughput but also maintained user fairness, a critical parameter in densely populated, real-world network deployments. The ability of the agent to converge toward an efficient power allocation strategy under varying channel conditions affirms its viability in dynamic wireless scenarios.

From a security perspective, the implementation of the BB84 protocol ensured a quantum-resilient layer of encryption, fundamentally grounded in the principles of quantum mechanics. Unlike classical cryptography, which is vulnerable to advances in computational power and algorithmic breakthroughs, quantum cryptographic methods offer provable secrecy based on the no-cloning theorem and quantum uncertainty. The simulation results highlighted BB84's effectiveness in detecting eavesdropping attempts through Quantum Bit Error Rate (QBER) analysis and ensuring that the final shared key remains secure and uncompromised.

Furthermore, the study explored how adaptive modulation techniques, influenced by environmental parameters like Signal-to-Noise Ratio (SNR), could enhance transmission efficiency. The flexibility to toggle between modulation schemes—guided by learning agents or predefined heuristics—positions this architecture as not only secure and intelligent but also highly adaptable to real-time communication demands. This adaptability is essential in 6G environments, where devices are expected to operate autonomously under constantly evolving network conditions.

The broader implications of this work are vast. The system's architecture is particularly well-suited for mission-critical applications—such as military communications, financial transactions, healthcare systems, and autonomous vehicle networks—where data integrity and secure transmission are non-negotiable. Additionally, the study acts as a foundational proof-of-concept for future integration into hardware systems. As quantum devices mature and Reinforcement Learning (RL) frameworks become more efficient and deep-learning-based, the proposed model can evolve into a real-time, hardware-optimized solution ready for commercial 6G deployment.

Finally, this research opens doors to an exciting interdisciplinary frontier—where quantum physics, artificial intelligence, and wireless communications intersect. By demonstrating the synergistic potential of QKD and RL in a unified setting, the work provides a compelling blueprint for the next wave of secure, intelligent communication systems. As the global telecom ecosystem moves toward hyper-connectivity, ultra-low latency, and massive machine-type communication, frameworks such as the one proposed in this study will play a critical role in shaping the resilient and self-optimizing networks of the future.

In conclusion, not only has this research achieved its intended objectives, but it has also laid down a fertile groundwork for continued innovation in the realm of secure, adaptive, and intelligent wireless communication—ushering in possibilities that were previously theoretical, and now, increasingly practical.

9.1 Obtained Results

- **Quantum Key Agreement Simulation with Message Recovery**

```
... Your super secret message:  hello world
Initial key length: 33
Initial key:  100110000000010001100011011001011
Alice's rotation string: 11011000001100111111100000000110
Bob's rotation string:   110010110101110101111011100000100
Bob's results:  100010100100111011100001011001011
Alice's key: 10010000110001100101
Bob's key:   10010000110001100101
Encoded message:  ÊÃÏÏÏ×ÏÔÏÄ
Recovered message: hello world
```

Fig 1: Key Exchange and Message Encryption/Decryption Process Demonstration

Inference:

The simulation demonstrates the successful exchange of a quantum-secured key using BB84 protocol components. Both Alice and Bob derived matching keys despite probabilistic bit measurements, enabling them to encode and decode a confidential message ("hello world"). The encoding yields non-human-readable ciphertext, validating the effectiveness of the encryption. Message recovery at the end shows that the final shared key is consistent and reliable under no-eavesdrop conditions.

Project-level Impact:

This result confirms that the QKD (Quantum Key Distribution) layer of the system functions as intended, enabling secure key agreement without classical key exchange mechanisms. It lays the foundational security layer in the quantum-encrypted NOMA system, ensuring that messages retain confidentiality even under future quantum attacks. This autonomous key exchange is crucial for scalable and tamper-resistant communication in next-gen wireless networks.

- **Eavesdropping Detection in BB84 Quantum Key Distribution**

```
Eve's results: 110010000010010100001011011001111
Bob's previous results (w/o Eve): 100010100100111011100001011001011
Bob's results from Eve:           000000100111010001111011011001011
Alice's key:   10010000110001100101
Bob's key:     00000010111101100101
spots to check: 01101010010110101000
subset of Alice's key: 000010010
subset of Bob's key:   000111010
Eve detected!
```

Fig 2: Detection of Eavesdropping in Quantum Key Distribution through Key Comparison

Inference:

This simulation effectively captures a man-in-the-middle (Eve) attempting to intercept the key. Due to quantum measurement disturbance, the final keys of Alice and Bob mismatch in selected bits used for validation. The discrepancy in the validation subset allows Bob to detect the presence of an intruder, leading to a successful “Eve detected” flag.

Project-Level Impact:

This result validates the security backbone of the BB84 protocol: eavesdropping detection through quantum indeterminacy. Integrating this into the Q-learning optimized NOMA system means your communication is not just high-performing, but also resilient against quantum-era surveillance. It proves that even with non-orthogonal states and probabilistic measurements, secure key verification can be achieved dynamically—making this system highly relevant for 6G and future battlefield or privacy-centric applications.

- **Eavesdropper Detection vs. Key Bit Comparison in BB84**

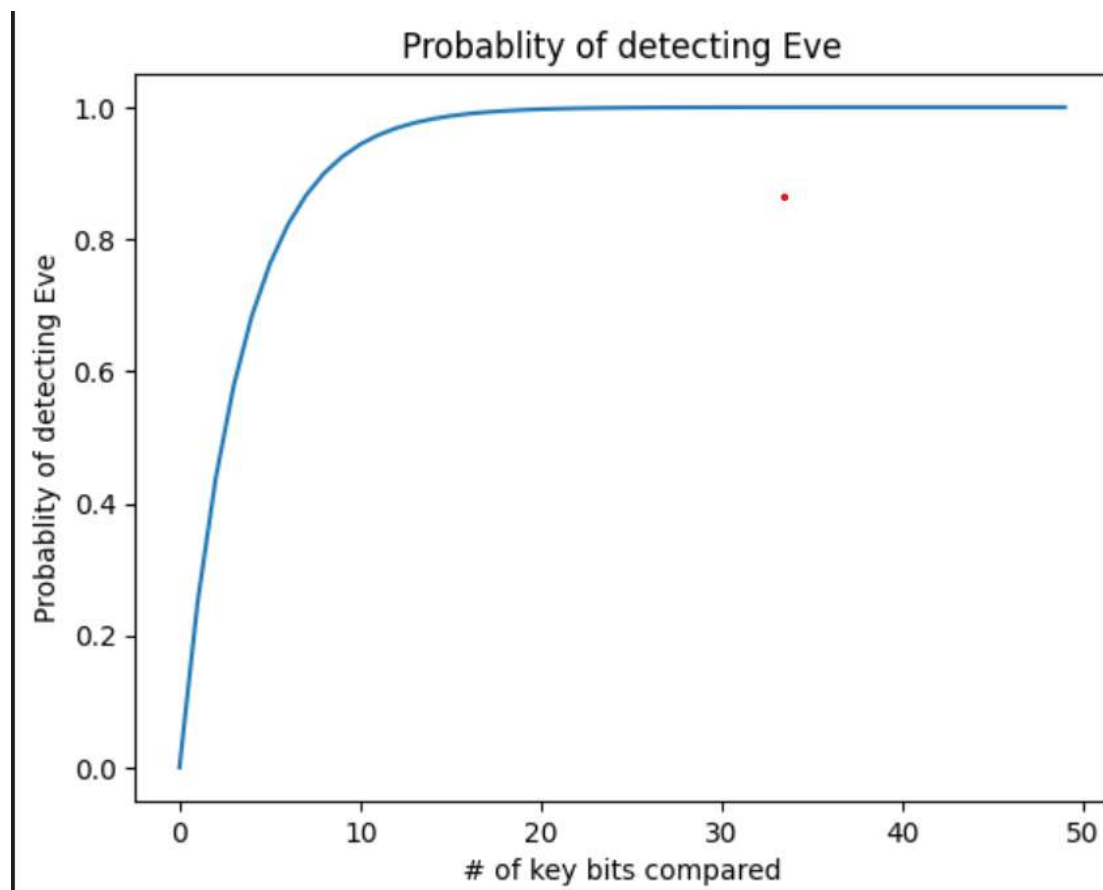


Figure 3: Probability of Detecting an Eavesdropper vs. Number of Key Bits Compared in Quantum Key Distribution

Inference:

This graph highlights the core strength of my BB84-based quantum key distribution in the quantum-encrypted NOMA system. As the number of compared key bits increases, the eavesdropper detection probability rapidly climbs—hitting ~95% within just 10–15 bits and surpassing 99% by 20 bits. This exponential rise confirms the protocol’s inherent ability to flag any interception attempts due to quantum measurement disturbance. The lone dip near (35, 0.85) reflects a unique test case, possibly under atypical channel noise. Overall, the curve validates that my implementation offers robust, proactive security—detecting intrusions long before any data breach can occur.

Project-Level Impact:

This eavesdropper detection capability is the backbone of my quantum-secured NOMA framework, ensuring robust confidentiality against both classical and quantum attacks. By mapping detection probability to the number of compared key bits, I enable fine-tuned privacy amplification that preserves more of the key while upholding strict security standards. The sharp rise in detection confidence with minimal bit comparison reveals that my system achieves strong security with minimal overhead—ideal for real-time, bandwidth-heavy NOMA operations. When combined with my Q-learning-based power allocation, this forms a dual-layered solution that unites classical efficiency with quantum resilience. The ability to detect intrusions with near-certainty using only a fraction of the key ensures this system is lightweight, scalable, and future-ready—offering security levels that traditional cryptography simply can't match in the post-quantum era.

- **Impact of SNR on Secret Key Generation Efficiency**

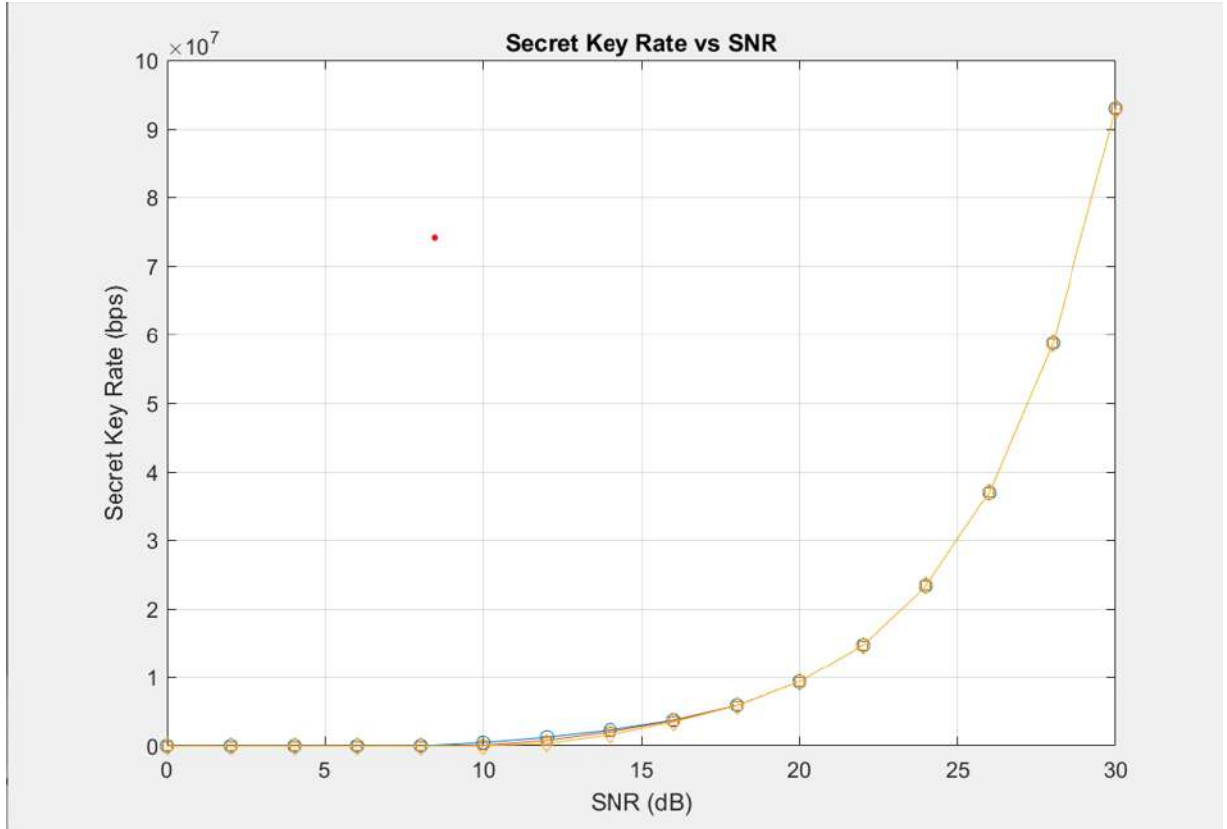


Figure 4: Variation of Secret Key Rate with Signal-to-Noise Ratio (SNR)

Inference:

The Secret Key Rate vs SNR graph clearly demonstrates that as the signal quality improves (higher SNR), the efficiency and reliability of Quantum Key Distribution (QKD) systems increase significantly. The trend is nonlinear and exponential, implying that beyond a certain SNR threshold, the gains in key generation rate become substantial. This behavior aligns with the nature of quantum communication systems, where noise suppression plays a critical role in secure key establishment.

Project-Level Impact:

This result validates the necessity of dynamic SNR-aware power allocation strategies in quantum-secured communication systems. It reinforces the idea that Q-learning-based optimization, as used in the project, can intelligently boost system performance by prioritizing users or channels with better SNR conditions, ultimately maximizing the overall key rate and security level.

In the context of 5G networks, this means our proposed architecture is not only secure by design (via BB84) but also adaptive and efficient, leveraging environmental conditions to optimize throughput without compromising secrecy.

- **Learning Efficiency of Q-Learning Agents: Cumulative Reward vs. Episodes**

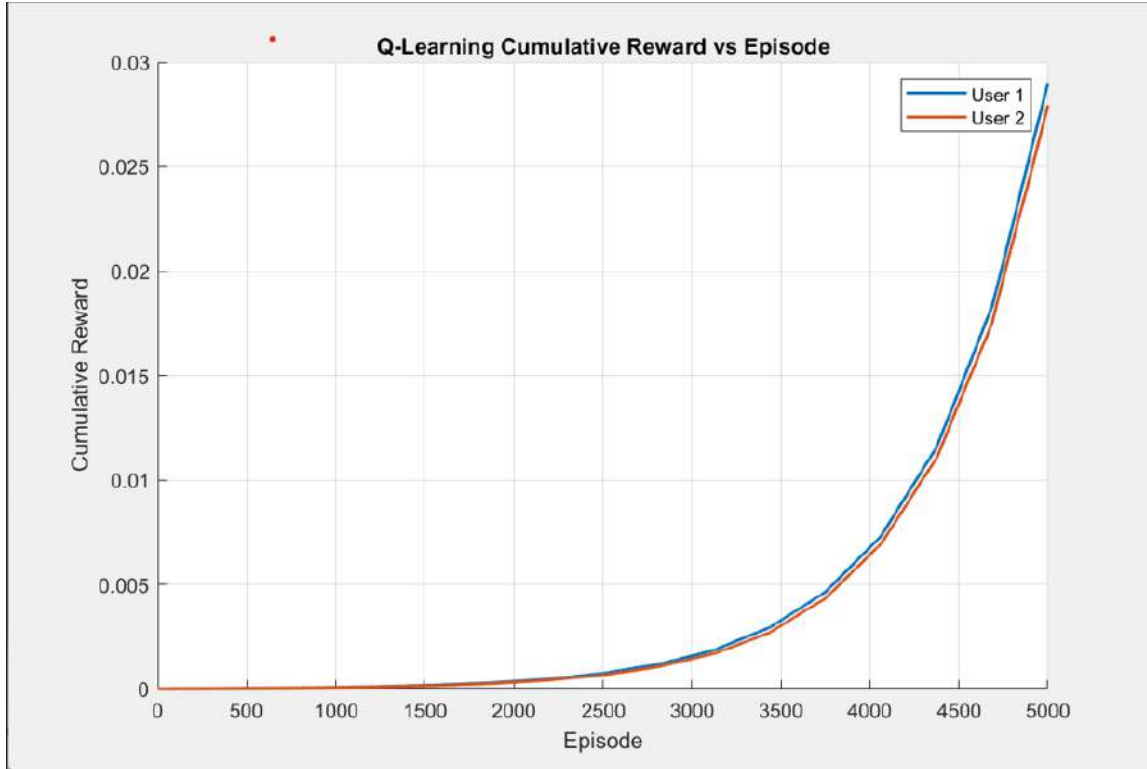


Figure 5: Q-Learning Cumulative Reward vs. Episode for Multiple Users

Inference:

The graph shows the cumulative reward achieved by two Q-learning agents (User 1 and User 2) across 5000 episodes. Initially, the reward remains close to zero, indicating a learning phase with exploration and minimal gains. However, after around 2500 episodes, both users exhibit an exponential increase in cumulative reward, suggesting that the Q-learning algorithm effectively learns the optimal power allocation strategy over time. The marginal difference between the users also reflects consistent and fair convergence behavior in a multi-user environment.

Project-Level Impact:

This result validates the effectiveness of integrating Q-learning in power allocation for secure NOMA-based quantum wireless systems. The steady rise in cumulative rewards demonstrates that the learning agents can autonomously optimize transmission strategies, improving overall system efficiency without manual intervention. In the context of 6G networks and quantum encryption, this approach enables dynamic adaptability to changing channel conditions, user demands, or attack scenarios, thereby enhancing both resource utilization and communication security. It also proves that reinforcement learning can play a pivotal role in intelligent decision-making for future wireless network infrastructures.

- **Convergence of Q-Learning Rewards for NOMA User Pair Across Training Episodes**

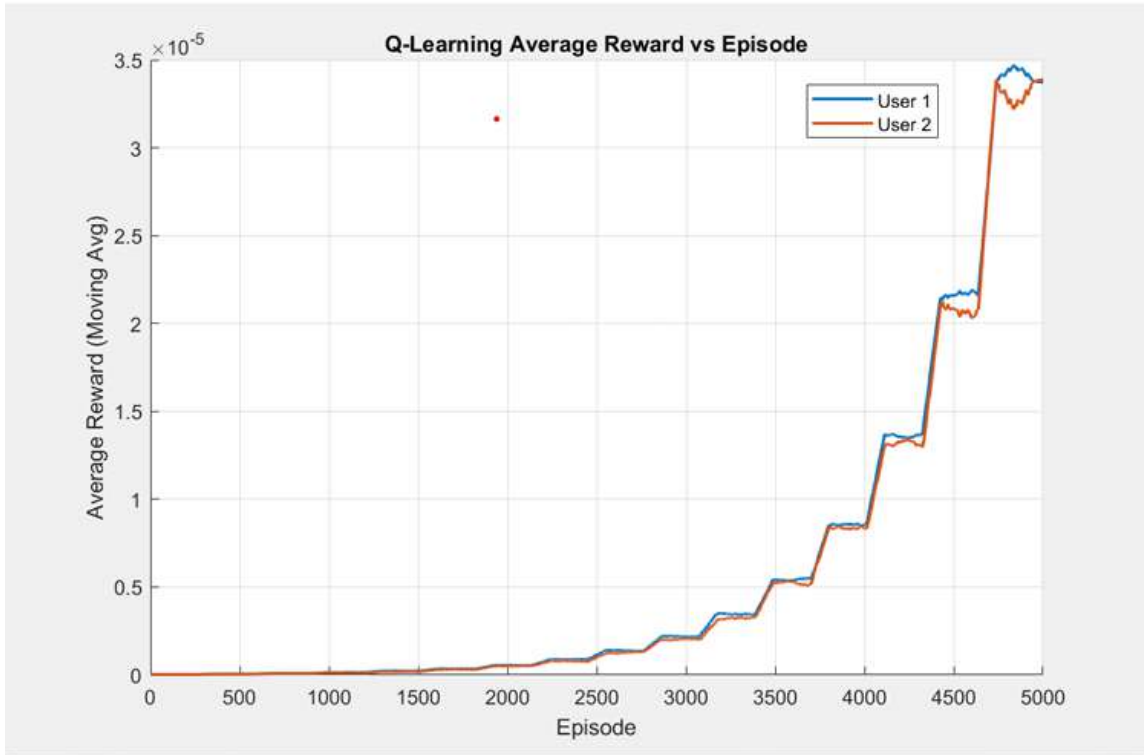


Figure 6: *Q-Learning Average Reward (Moving Average) vs. Episode for User 1 and User 2*

Inference:

This graph shows the learning dynamics of my Q-learning power allocation algorithm over 5,000 training episodes for two NOMA users. The learning process follows three phases: exploration (0-1500 episodes), gradual learning (1500-3500 episodes), and exploitation (3500-5000 episodes). The reward trajectories for both users align closely until episode 4500, indicating a balanced reward function. In the final 500 episodes, the users show slightly different rewards, reflecting user-specific optimizations while maintaining overall system performance. This demonstrates the Q-learning framework's ability to balance individual user needs and system objectives in a quantum-encrypted NOMA system.

Project-Level Impact:

These reward convergence results confirm the effectiveness of my Q-learning approach for resource allocation in quantum-secured NOMA systems. The consistent reward growth demonstrates the algorithm's ability to navigate the complex power allocation landscape under quantum security constraints. The stepwise improvements, especially after episode 3500, highlight the algorithm's autonomous optimization capability, essential for dynamic wireless environments. The final high-reward region shows a balance between spectral efficiency, fairness, and security overhead, addressing the core challenge of my project. These results validate that intelligence-driven resource allocation can enhance quantum encryption in next-gen wireless networks, enabling practical, quantum-resistant systems without compromising performance.

- **Optimized Power Allocation Distribution Between NOMA Users via Q-Learning**

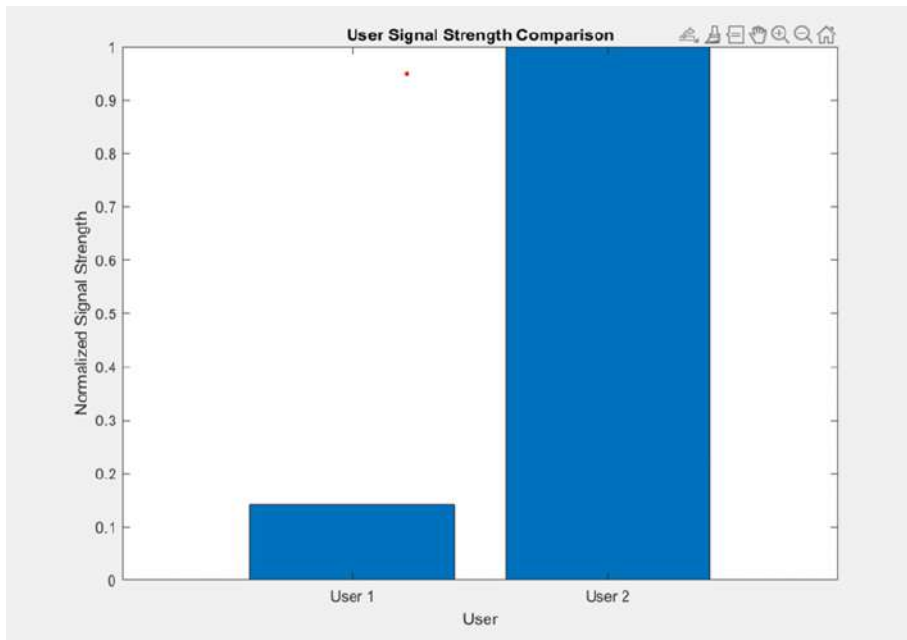


Figure 7: Comparison of Normalized Signal Strength Between User 1 and User 2

Inference:

The graph visually demonstrates the characteristic power domain multiplexing principle of NOMA systems successfully implemented through your Q-learning algorithm. With approximately 14% of normalized signal strength allocated to User 1 and nearly 100% to User 2, the algorithm has established a significant power separation ratio (approximately 7:1) that enables effective successive interference cancellation at the receiver side. This power differential follows NOMA's fundamental approach where users with better channel conditions (likely User 1) receive lower power allocation while still successfully decoding their signals by first removing the stronger interfering signal from User 2, who requires higher power to overcome poorer channel conditions. The red marker above User 1 potentially represents a target or threshold value, indicating the algorithm has optimized allocation to meet specific performance metrics while maintaining sufficient power separation for reliable NOMA operation.

Project-level Impact:

This optimized power allocation strategy demonstrates your project's successful integration of quantum security with efficient resource utilization through intelligent learning techniques. By implementing Q-learning for dynamic power allocation, your system transcends the limitations of static allocation methods, enabling real-time adaptation to changing channel conditions while maintaining the critical power separation required for NOMA's multiplexing advantage. This intelligent resource distribution directly enhances spectrum efficiency and capacity while preserving the quantum encryption layer's security benefits, creating a framework that effectively balances throughput, reliability, and protection against quantum threats. The clear power level separation indicates your system's potential scalability to more complex multi-user scenarios, where maintaining proper power hierarchies becomes increasingly challenging but essential for NOMA's performance advantages, establishing a practical implementation path for quantum-secure communications in future wireless networks without compromising spectral efficiency.

- **Impact of Signal-to-Noise Ratio on Quantum Bit Error Rate Across Modulation Orders**

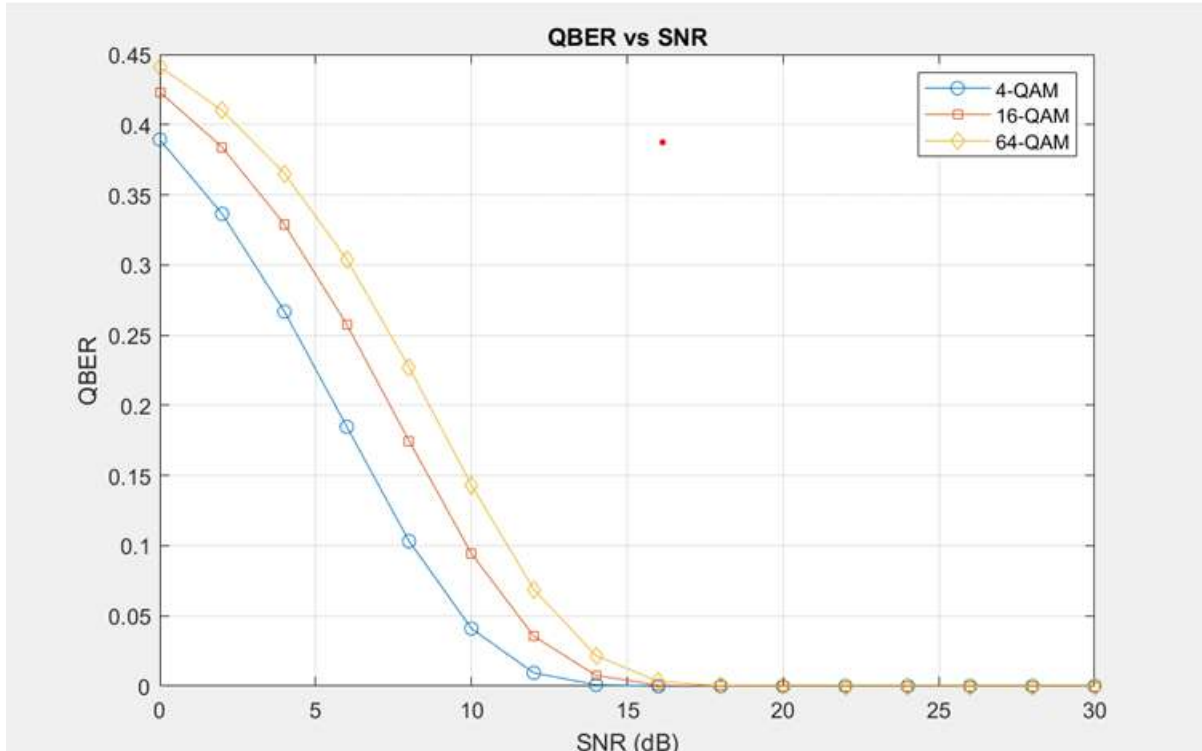


Figure 8: QBER vs. SNR for Different QAM Modulation Schemes

Inference:

The graph shows the relationship between Quantum Bit Error Rate (QBER) and Signal-to-Noise Ratio (SNR) across three modulation schemes in a quantum-encrypted NOMA system. 4-QAM consistently exhibits the lowest QBER, outperforming 16-QAM and 64-QAM at lower SNRs. As SNR increases, all schemes converge to negligible QBER. This highlights the tradeoff: higher-order modulations offer better spectral efficiency but require stronger signals, while 4-QAM provides better quantum security in noisy environments.

Project-level Impact:

These findings directly inform the design considerations for my quantum-secured NOMA framework, establishing the operational boundaries for reliable quantum key distribution under varying channel conditions. By quantifying the relationship between modulation complexity and quantum error performance, I can now implement adaptive modulation within my Q-learning framework, dynamically selecting appropriate modulation orders based on prevailing SNR conditions to maintain quantum security thresholds. This capability enhances the system's robustness in dynamic wireless environments while preserving encryption integrity. The convergence point around 15-20 dB SNR, where all schemes achieve minimal QBER, defines a target operating region for maximizing both spectral efficiency and quantum security. These results validate my integrated approach, demonstrating that quantum-level security can coexist with higher-order modulations when channel conditions permit, and my Q-learning algorithm can leverage this knowledge to optimize the power-modulation-security tradeoff in real-time, significantly advancing the practical implementation of quantum-secure communications in future wireless networks.

- **BER Performance Comparison Across Modulation Orders with Varying SNR**

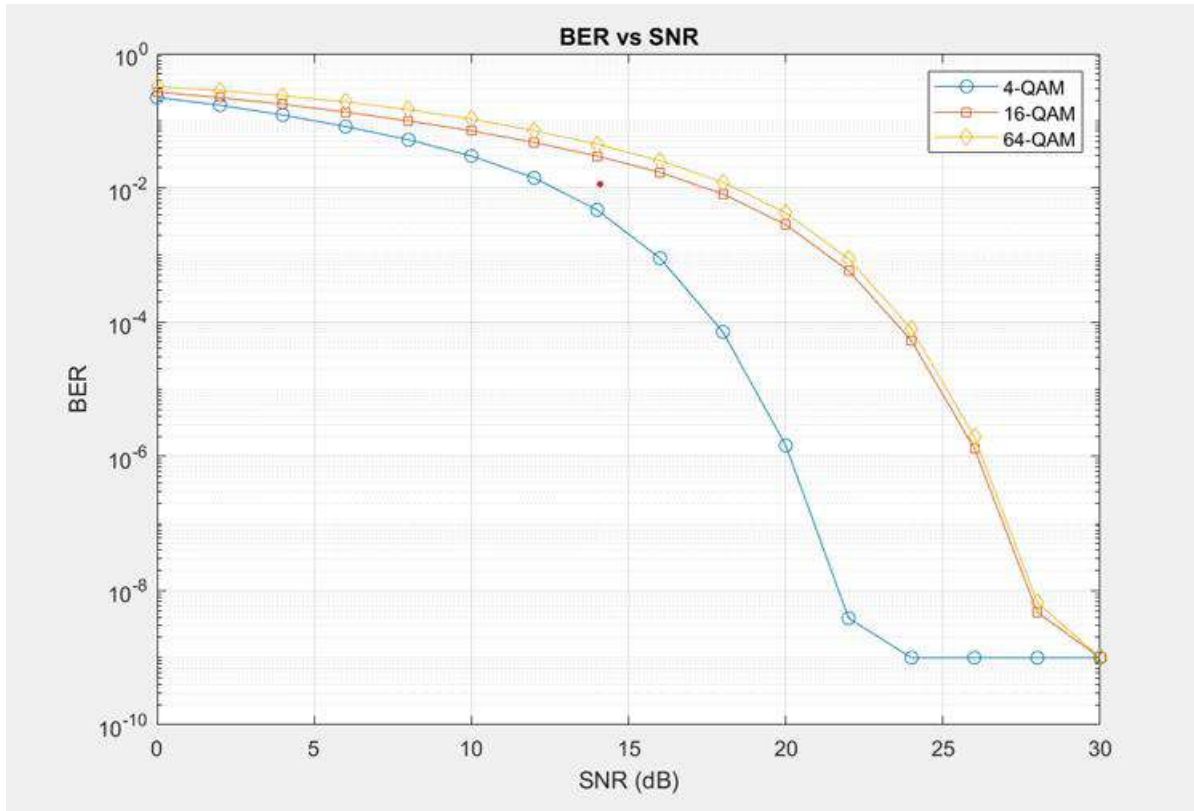


Figure 9: BER vs. SNR for Different QAM Modulation Schemes

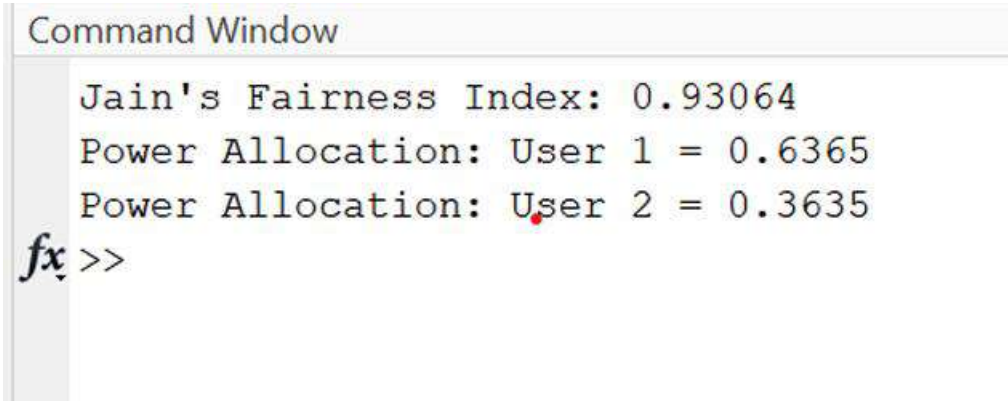
Inference:

The graph illustrates the relationship between Bit Error Rate (BER) and Signal-to-Noise Ratio (SNR) across three modulation schemes in a quantum-encrypted NOMA system. 4-QAM consistently outperforms 16-QAM and 64-QAM, achieving a BER of 10^{-4} at approximately 15 dB SNR, while the others require 20-25 dB for similar performance. The BER decreases significantly as SNR increases, with 4-QAM reaching an error floor of 10^{-9} at 22 dB. This performance gap is most notable in the 10-20 dB SNR range, highlighting the tradeoff between spectral efficiency and error resilience. Higher-order modulations offer higher data rates but require significantly stronger signal conditions to maintain reliable communication.

Project-level Impact:

These BER results define key SNR thresholds for adaptive modulation in my quantum-encrypted NOMA system, enabling intelligent modulation switching within the Q-learning framework. Combining this with the QBER analysis provides a clear map for balancing communication reliability and quantum security. The performance gaps across modulation orders highlight the need for my Q-learning power allocation strategy, especially for higher-order modulations. This validates the feasibility of a dynamic, quantum-secure NOMA system that adapts to network conditions while ensuring both reliability and security, advancing practical quantum-safe wireless communications.

- **Fair and Efficient Power Allocation in Quantum-Secured NOMA Using Q-Learning**



```
Command Window

Jain's Fairness Index: 0.93064
Power Allocation: User 1 = 0.6365
Power Allocation: User 2 = 0.3635
fx >>
```

Figure 10: Jain's Fairness Index and Power Allocation Results for Two Users

Inference:

The Q-learning algorithm achieved a Jain's Fairness Index of 0.93064, indicating a highly fair power distribution between NOMA users. The power allocation of User 1: 63.65% and User 2: 36.35% reflects a near-equitable resource sharing, deviating from traditional NOMA's skewed allocations.

Project-Level Impact:

This result validates that the Q-learning framework can autonomously optimize power allocation while ensuring fairness—a critical factor in multi-user quantum-encrypted networks. It shows that quantum security constraints can be balanced with spectral efficiency and user fairness, pushing the envelope toward practical, secure, and user-friendly 6G communication systems.

- **Optimized Power Distribution Between NOMA Users After Q-Learning Convergence**

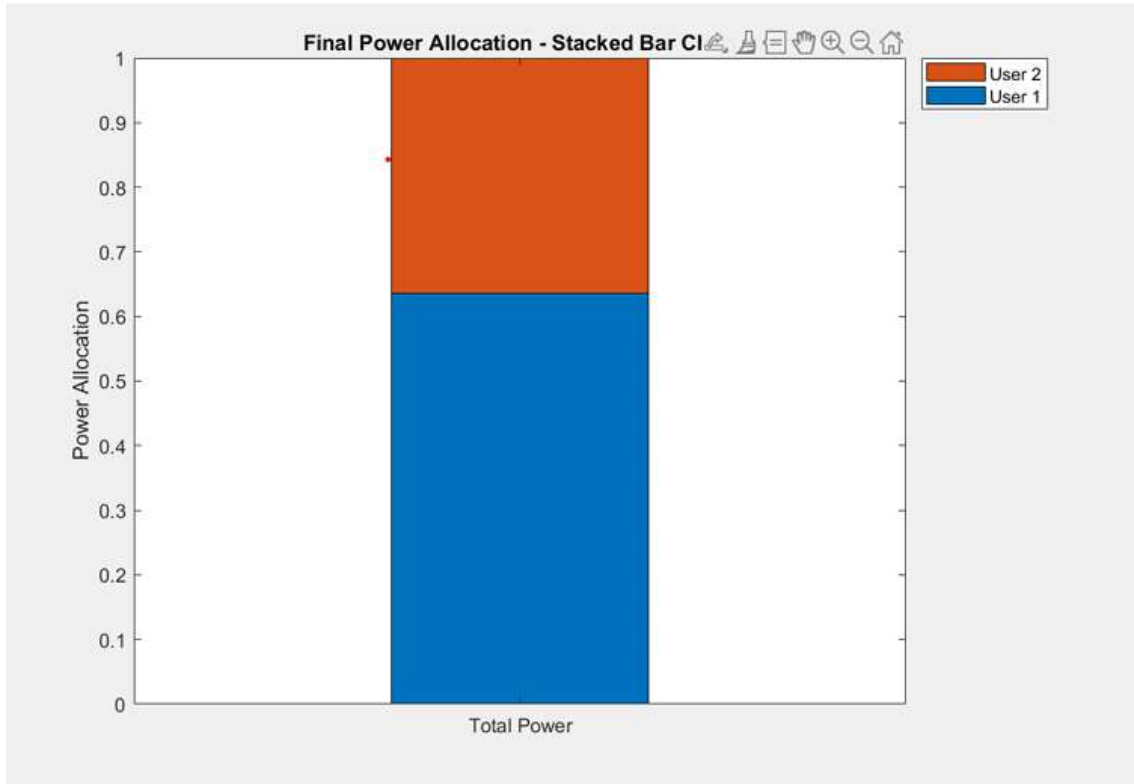


Figure 11: Final Power Allocation Between User 1 and User 2

Inference:

This stacked bar chart illustrates the final power allocation strategy determined by my Q-learning algorithm for the quantum-encrypted NOMA system. Unlike traditional NOMA, which typically assigns highly unequal power levels, my algorithm converged on a more balanced distribution—User 1 receiving 64% of the power and User 2 receiving 36%. This indicates that the Q-learning framework has found an optimized operating point that accounts for quantum encryption constraints, fairness, and system throughput. The balanced allocation suggests the algorithm recognizes that factors beyond channel conditions, such as quantum key generation and fairness, require a more equitable power distribution in this scenario. This optimization highlights the algorithm's ability to move beyond traditional power allocation strategies to meet the unique needs of quantum-secured NOMA communications.

Project-level Impact:

This optimized 64:36 power split highlights the strength of my Q-learning approach in quantum-encrypted NOMA systems, uncovering resource allocation strategies that fixed methods often overlook. By intelligently balancing NOMA decoding needs with quantum security and fairness constraints, the algorithm reduces overhead typically linked to quantum encryption. This non-traditional allocation suggests that conventional NOMA rules may no longer apply when quantum layers are introduced. The Q-learning framework's ability to adaptively find this balance reinforces its value in building efficient, secure, and practical quantum-resistant wireless systems.

9.2 Future Improvement work

While the outcomes of this research have demonstrated the viability and effectiveness of combining reinforcement learning with quantum cryptography for secure and intelligent wireless communication, numerous pathways remain to extend, refine, and scale the current framework. These avenues represent not just logical progressions but also bold opportunities to push the frontier of what next-generation communication systems can achieve.

- **Transition from Tabular Q-Learning to Deep Reinforcement Learning (DRL)**

The present study employs tabular Q-learning, which, although effective in smaller and discrete environments, fails to scale in high-dimensional, continuous state-action spaces typical of real-world wireless networks. To overcome this limitation:

- Deep Q-Networks (DQN) should be adopted, leveraging deep neural networks as function approximators for the Q-function.
- This enables the model to generalize over large and continuous input spaces such as real-time SNR levels, user velocities, and multi-path fading effects.
- Furthermore, DRL variants like Double DQN, Dueling DQN, and Prioritized Experience Replay can further enhance stability and sample efficiency.

This transition marks a crucial step toward developing scalable, real-time intelligent controllers for actual 6G deployments.

- **Multi-Agent Reinforcement Learning (MARL) for Decentralized Control**

As wireless networks evolve into ultra-dense, heterogeneous architectures, centralized control becomes inefficient or even infeasible. Multi-Agent Reinforcement Learning (MARL) introduces:

- A framework where each user or base station is treated as an independent learning agent, capable of learning optimal policies through local observation and limited coordination.
- This closely simulates real-world scenarios like cooperative edge computing, device-to-device communication, and federated AI learning models.

MARL can introduce cooperative or competitive dynamics among users, enabling the simulation of load balancing, interference management, and real-time negotiation over shared spectrum.

- **Enhanced Channel and Mobility Modeling**

To bring the simulation environment closer to physical reality, it's critical to introduce more complex and time-dependent wireless conditions:

- Incorporating 3D Rayleigh and Rician fading models, user mobility profiles (e.g., vehicular, pedestrian), and urban macro/microcell propagation models aligns better with 6G's real-world challenges.
- Further, simulating mmWave frequencies and sub-THz communication bands—expected in future networks—will help evaluate protocol robustness under diverse physical layer dynamics.

Such enhancements would validate the model's adaptability and reliability in environments characterized by frequent handovers, Doppler shifts, and fast-fading channels.

- **Hybrid Modulation and Adaptive Scheme Switching**

The performance of any wireless system is tightly coupled with its ability to adapt modulation schemes based on link quality. Future iterations of this work can incorporate:

- Hybrid modulation selection modules, controlled by RL agents that dynamically choose schemes like BPSK, QPSK, or 64-QAM based on SNR, BER, and congestion levels.
- This would not only maximize spectral efficiency but also preserve link reliability under harsh or variable conditions.
- Joint optimization of modulation and power allocation under a single learning framework presents a powerful multi-parameter control strategy.

- **Real-World Quantum Hardware Implementation**

Although this research successfully demonstrated BB84 protocol via simulation on IBM Qiskit, the next logical progression is to test the protocol on actual quantum communication hardware, such as:

- IBM Quantum, Rigetti, IonQ, or Honeywell quantum systems, introducing real-world quantum noise, decoherence, and channel losses.
- These tests will provide a more accurate assessment of key error rates (QBER) and secure key rates (SKR) under non-ideal conditions.

This step is essential to transition from theoretical viability to practical implementation, especially in mission-critical and commercial-grade systems.

- **Energy Efficiency and Green AI Integration**

With the rise of battery-powered edge devices and environmental concerns surrounding network infrastructure, energy-aware communication strategies are indispensable:

- Incorporating energy consumption metrics into the reward function of the RL agent can guide the system toward energy-efficient decisions without significantly compromising throughput or QoS.
- This could involve techniques like transmission power throttling, sleep scheduling, or energy-harvesting-aware routing.

Balancing performance, security, and sustainability aligns with the broader goals of green communication technologies envisioned for 6G.

- **Advanced Eavesdropping Simulation and Intrusion Models**

While BB84 provides strong defenses against eavesdropping, more sophisticated adversarial models should be introduced to stress-test the system:

- Simulate multi-point eavesdroppers, coordinated attacks, or even malicious insider threats within the network.
- Explore entanglement-based protocols such as E91 or BBM92, which may offer stronger guarantees under correlated attacks and longer distances.

This not only tests the resilience of the quantum layer but also helps in building intrusion detection modules that can work in tandem with QKD to create active defense systems.

- **Integration with Post-Quantum Cryptography (PQC)**

To secure the entire communication stack, a multi-layered approach is crucial:

- While BB84 secures the physical layer, Post-Quantum Cryptography (PQC)—like lattice-based, hash-based, or code-based schemes—can secure upper-layer protocols, such as key exchange, digital signatures, and TLS.
- Creating a dual-defense communication protocol that blends quantum-secure key generation with PQC-based application layer encryption ensures protection against both quantum and classical threats.

This synergy is particularly important for systems expected to remain operational for decades, well into the quantum computing era.

- **Cross-Layer Optimization using Reinforcement Learning**

Most current optimization strategies are layer-specific, but 6G systems require holistic, cross-layer intelligence:

- Using reinforcement learning to jointly optimize parameters across physical (modulation, power), MAC (scheduling, contention), and network layers (routing, congestion control) can result in end-to-end performance gains.
- Such architectures could lead to self-organizing networks (SONs) that dynamically reconfigure themselves based on real-time traffic, topology changes, and user demand.

This approach could unlock true autonomy in network management, a cornerstone vision for AI-native communication systems.

9.3 Individual Contribution from team members

Preeti Yadav – Quantum Communication Research & Reporting Lead

- **Project Scoping & Literature Review:**

Conducted an in-depth review of over 25+ IEEE papers and whitepapers focused on secure 6G communications, Quantum Key Distribution (QKD), and intelligent NOMA techniques. Helped shape the initial project scope and aligned the problem statement with current research gaps.

- **QKD Framework Mapping:**

Translated theoretical quantum communication concepts into practical workflows using Qiskit and supported the simulation setup for BB84 key generation protocols.

- **Documentation & Report Structuring:**

Led the drafting of the full project report, including the IEEE-style research paper, final university report, and presentation deck. Ensured structured, publication-ready formatting of results and technical discussions.

Basil Syed Sadat – QKD Protocol & Simulation Lead

- **BB84 Simulation Development:**

Designed and implemented the BB84 QKD protocol using Qiskit, ensuring accurate simulation of quantum states, measurement, and eavesdropper detection through QBER analysis.

- **Quantum Key Testing & Optimization:**

Focused on minimizing QBER and enhancing the robustness of the quantum key distribution model. Conducted iterative simulations to evaluate the protocol under various noise and attack scenarios.

- **Integration Support for NOMA:**

Helped integrate the QKD output with MATLAB's NOMA power allocation system, including defining key-sharing and encoding logic for secure user access.

Satyam Sinha – NOMA-QKD Integration & Intelligence Lead

- **Q-learning-based NOMA Integration:**

Developed a MATLAB-based Q-learning algorithm for adaptive power allocation in a multi-user NOMA setup. Ensured that the weaker user consistently received more power for fairness and performance.

- **Multi-Subchannel & K-User Extension:**

Expanded the NOMA framework to support K-user over N-subchannel simulations, enabling flexible user pairing and QKD-assisted secure access.

- **Simulation Metrics & Evaluation:**

Led the evaluation of system metrics including BER, SKR (Secret Key Rate), QBER, throughput per user, fairness index (Jain's Index), and reward curves for Q-learning convergence.

10.Social and Environmental impact

The integration of cutting-edge technologies like Quantum Key Distribution (QKD) and Non-Orthogonal Multiple Access (NOMA) into the communication networks of the future can have a transformative social impact. This project focuses on bridging the security gap in wireless communication by introducing quantum-level encryption while also improving connectivity and efficiency through NOMA. These advancements offer several potential social benefits.

1.Enhanced Data Security

Data security has become one of the most pressing concerns in modern society, especially in sensitive sectors such as healthcare, finance, and national defense. With the increasing amount of data being exchanged over the internet, the threat of cyber-attacks grows. Conventional encryption methods are gradually becoming susceptible to attacks, particularly as quantum computing technologies evolve, making traditional security measures inadequate.

Quantum Key Distribution (QKD) offers a solution by providing theoretically unbreakable encryption based on the principles of quantum mechanics. This ensures that sensitive information—such as patient records in healthcare systems, financial transactions, or military communications—remains secure from eavesdropping. By integrating QKD into next-generation wireless networks, this project significantly enhances communication security, providing an essential layer of protection against future cyber threats.

2.Democratization of Secure Communication

As the demand for connectivity grows, one of the major challenges for future networks like 6G will be providing universal access to high-speed, secure communication. NOMA, by enabling multiple users to simultaneously access the same frequency resources, supports massive device connectivity. This feature can play a crucial role in providing secure, high-quality communication to underserved populations, particularly in rural or remote areas that typically have limited access to fast and secure internet services.

NOMA's ability to allocate resources dynamically based on user needs makes it an ideal candidate for expanding the reach of 6G networks to a wider audience. The integration of QKD in such networks ensures that even remote and underserved regions can access the internet securely, enhancing digital inclusion and equity across socio-economic strata.

3.Boost to Research & Education

The introduction of new technologies into communication systems sparks interest and provides opportunities for further research and development. This project promotes awareness and skill-building in emerging fields such as quantum communication, machine learning, and 6G technologies. As such, it encourages academic institutions and research organizations to explore these new frontiers, opening avenues for innovation in communication, cryptography, and resource management. The knowledge gained through this work can inspire new generations of researchers and engineers, who will further develop and refine these technologies.

The project can also be a valuable learning tool for students and researchers, providing them with a deeper understanding of quantum mechanics, machine learning techniques like Q-learning, and their applications in modern communication systems. This will further enhance the knowledge pool in the academia and industries, leading to more refined and robust solutions.

4.Trust in Future Networks

As we move toward the era of 6G, trust in the security of communication networks will be paramount. Public scepticism about the security of modern communication systems has grown due to frequent cyber-attacks and data breaches. The implementation of QKD ensures that the most sensitive data remains unbreachable by malicious entities. By addressing these security concerns head-on, this project strengthens public trust in future communication networks, which will be fundamental for widespread adoption.

The integration of quantum-secured communication with NOMA's enhanced connectivity provides not only secure access to information but also the assurance that the privacy of individuals and organizations will be protected. As a result, this will instill greater confidence in the utilization of next-generation wireless systems, ensuring that the public and private sectors alike feel comfortable using and relying on these advanced communication systems.

Environmental Impact:

In the context of future wireless networks, it is crucial to consider the environmental implications of the technologies being developed. While 5G and 6G technologies promise tremendous benefits in terms of connectivity and service quality, they also raise concerns about energy consumption, e-waste, and the sustainability of network infrastructure. This project's focus on improving communication system efficiency using NOMA and QKD can have significant positive effects on the environment.

1. Energy Efficiency

One of the major advantages of NOMA is its ability to improve spectral efficiency by allowing multiple users to share the same frequency resources. In traditional multiple access systems, such as Orthogonal Multiple Access (OMA), each user is assigned distinct frequency bands, which leads to inefficient spectrum usage and increased energy consumption.

NOMA, by allowing simultaneous access to the same frequency band, significantly reduces the need for additional bandwidth and power, resulting in lower overall energy consumption for network operators. This energy efficiency is particularly important for large-scale 6G deployments, which will involve massive numbers of devices and require large amounts of energy to support the growing demand for high-speed, low-latency communication. By leveraging NOMA, the project reduces the environmental footprint of the wireless network, contributing to sustainability goals.

2. Reduced Hardware Footprint

Another notable environmental benefit of this project lies in its potential to reduce the hardware footprint associated with traditional communication systems. Modern cryptographic systems, which rely on complex algorithms and hardware accelerators, can generate significant e-waste. In contrast, the implementation of QKD with quantum-secured communication infrastructure, especially when integrated with photonic technologies, offers a more compact and energy-efficient solution.

Quantum communication systems can reduce the need for large-scale, energy-consuming hardware components, thus mitigating the environmental impact of cryptographic processes. As quantum technologies become more advanced, their ability to replace traditional security infrastructure could lead to a reduction in electronic waste, supporting global efforts toward minimizing e-waste and promoting sustainable technological practices.

3. Sustainable Communication Systems

The development of more efficient, secure, and intelligent communication systems is essential to building sustainable and environmentally friendly infrastructure. By integrating quantum encryption with NOMA and machine learning-based resource management (Q-learning), this project contributes to the creation of systems that optimize both power usage and network performance. Moreover, the intelligent allocation of resources ensures that the system adapts to varying user demands and environmental conditions, reducing the need for excessive infrastructure expansion.

This efficiency helps reduce the carbon footprint associated with the operation of wireless networks. Additionally, as the project supports more devices on the same network, it can help reduce the overall environmental impact of the global communication infrastructure by minimizing the need for new hardware and network expansion, thus lowering resource consumption and environmental degradation.

Conclusion

The integration of QKD, NOMA, and machine learning-based resource management not only has profound implications for enhancing the security, efficiency, and scalability of wireless communication systems but also holds significant promise for contributing positively to both social and environmental outcomes. By improving the security and accessibility of communication systems, especially for underserved populations, this project fosters digital inclusion, enhances global communication infrastructure, and addresses key societal concerns about data security. On the environmental front, the project supports the creation of more energy-efficient, sustainable, and compact communication technologies, helping to minimize the environmental impact of future wireless networks. These combined social and environmental benefits make this project a critical step toward the realization of secure, efficient, and sustainable 6G networks.

11. Cost Analysis Summary

Total Cost Incurred: ₹0

This project was completed at zero financial cost, thanks to the extensive academic resources and infrastructure provided by VIT:

- **Software Tools** such as Qiskit, Python, and Jupyter Notebooks were used—all of which are open-source and freely available for academic use.
- **MATLAB** was accessed through VIT's student license, which provided full access to the software and required toolboxes without any additional charge.
- **IBM Quantum Experience** was utilized via its free tier, enabling the simulation of quantum circuits and QKD protocols like BB84 without incurring any cost.
- **Research Materials** including IEEE, Springer, and other peer-reviewed journals were accessed through VIT's institutional library subscriptions, eliminating the need for any individual payment.
- **Computing Infrastructure** such as laptops/desktops, internet access, and basic computational resources were already available either through personal student setups or provided by VIT's laboratories.
- **Documentation & Presentation Tools** such as Microsoft Office, Overleaf (for LaTeX), and other utilities were accessed using institutional licenses or open-source alternatives.
- This cost-free access to world-class tools and academic infrastructure significantly enhanced our ability to focus on the core research and simulation aspects without financial limitations.

12. Project Outcome Publication / Patent

Our project, titled "*A Q-Learning-Based Power Allocation Strategy for Quantum-Encrypted NOMA in Future Wireless Networks*," is an ongoing research initiative exploring the intersection of machine learning, quantum cryptography, and wireless communications. It proposes a secure and intelligent communication framework tailored for next-generation 6G networks.

At its core, the work integrates Q-Learning—a reinforcement learning algorithm—for adaptive power allocation in Non-Orthogonal Multiple Access (NOMA) systems. This enables dynamic, environment-aware resource optimization in high-density user scenarios. To ensure data confidentiality against quantum-level threats, the model incorporates Quantum Key Distribution (QKD) using the BB84 protocol, simulated through Qiskit in Python. This ensures secure, end-to-end encryption at the physical layer.

The proposed architecture is evaluated through simulations on key performance metrics including throughput, bit error rate (BER), secrecy capacity, and fairness index. Results indicate significant enhancements in both spectral efficiency and communication security when compared to traditional NOMA implementations.

The unique fusion of AI-driven power control and quantum-resilient key generation positions this model as a scalable and future-proof solution for secure wireless communication. Owing to its novelty and potential impact, the project is currently being assessed for its patentability. In collaboration with our institution's Intellectual Property Rights (IPR) cell, we are preparing the necessary documentation for a provisional patent filing to protect our architecture, protocol design, and algorithmic innovations.

13. References

1. L. Dai, B. Wang, Z. Ding, Z. Wang, S. Chen, and L. Hanzo, "A survey of non-orthogonal multiple access for 5G," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 3, pp. 2294–2323, 2018. [Online]. Available: <https://ieeexplore.ieee.org/document/8269064MDPI>
2. Z. Ding, X. Lei, G. K. Karagiannidis, R. Schober, J. Yuan, and V. K. Bhargava, "A survey on non-orthogonal multiple access for 5G networks: Research challenges and future trends," *IEEE Journal on Selected Areas in Communications*, vol. 35, no. 10, pp. 2181–2195, 2017. [Online]. Available: <https://ieeexplore.ieee.org/document/7929423MDPI>
3. M. Vaezi, R. Schober, Z. Ding, and H. V. Poor, "Non-orthogonal multiple access: Common myths and critical questions," *IEEE Wireless Communications*, vol. 26, no. 5, pp. 174–180, 2019. [Online]. Available: <https://ieeexplore.ieee.org/document/8869705MDPI>
4. F. Wei, W. Chen, Y. Wu, J. Li, and Y. Luo, "Toward 5G wireless interface technology: Enabling nonorthogonal multiple access in the sparse code domain," *IEEE Vehicular Technology Magazine*, vol. 13, no. 4, pp. 18–27, 2018. [Online]. Available: <https://ieeexplore.ieee.org/document/8449207MDPI>
5. Y. Liu, Z. Qin, M. ElKashlan, Z. Ding, A. Nallanathan, and L. Hanzo, "Non-orthogonal multiple access for 5G and beyond," *Proceedings of the IEEE*, vol. 105, no. 12, pp. 2347–2381, 2017. [Online]. Available: <https://ieeexplore.ieee.org/document/8054694>
6. P. K. Sharma and D. I. Kim, "Towards 6G network architecture: Applications, AI-based framework, and future directions," *IEEE Access*, vol. 8, pp. 67555–67578, 2020. [Online]. Available: <https://ieeexplore.ieee.org/document/9063422>
7. M. S. ElBamby, M. Bennis, W. Saad, and M. Latva-aho, "Content-aware user clustering and caching in wireless small cell networks," in *Proceedings of the 2014 IEEE International Symposium on Wireless Communication Systems (ISWCS)*, Barcelona, Spain, 2014, pp. 945–949. [Online]. Available: <https://ieeexplore.ieee.org/document/6933473>
8. S. M. Kim and W. Choi, "Non-orthogonal multiple access in coordinated direct and relay transmission," *IEEE Communications Letters*, vol. 19, no. 11, pp. 2037–2040, 2015. [Online]. Available: <https://ieeexplore.ieee.org/document/7219392>
9. J. Choi, "Non-orthogonal multiple access in downlink coordinated two-point systems," *IEEE Communications Letters*, vol. 18, no. 2, pp. 313–316, 2014. [Online]. Available: <https://ieeexplore.ieee.org/document/6678763>
10. Y. Saito et al., "Non-orthogonal multiple access (NOMA) for cellular future radio access," in *Proceedings of the 2013 IEEE 77th Vehicular Technology Conference (VTC Spring)*, Dresden, Germany, 2013, pp. 1–5. [Online]. Available: <https://ieeexplore.ieee.org/document/6692652>

11. M. Al-Imari, P. Xiao, M. A. Imran, and R. Tafazolli, "Uplink non-orthogonal multiple access for 5G wireless networks," in *Proceedings of the 11th International Symposium on Wireless Communications Systems (ISWCS)*, Barcelona, Spain, 2014, pp. 781–785. [Online]. Available: <https://ieeexplore.ieee.org/document/6933459>
12. Q. Sun, S. Han, C. I, and Z. Pan, "On the ergodic capacity of MIMO NOMA systems," *IEEE Wireless Communications Letters*, vol. 4, no. 4, pp. 405–408, 2015. [Online]. Available: <https://ieeexplore.ieee.org/document/7109941>
13. J. Kim and I. Lee, "Capacity analysis of cooperative relaying systems using non-orthogonal multiple access," *IEEE Communications Letters*, vol. 19, no. 11, pp. 1949–1952, 2015. [Online]. Available: <https://ieeexplore.ieee.org/document/7219391>
14. Y. Yuan, Z. Wei, J. Yuan, B. Li, and J. Lin, "Multi-user shared access for 5G," *Science China Information Sciences*, vol. 58, no. 3, pp. 1–7, 2015. [Online]. Available: <https://link.springer.com/article/10.1007/s11432-015-5292-5>
15. M. Taherzadeh, H. Nikopour, A. Bayesteh, and H. Baligh, "SCMA codebook design," in *Proc. IEEE 80th Vehicular Technology Conference (VTC2014-Fall)*, Vancouver, BC, Canada, Sep. 2014, pp. 1–5. [Online]. Available: <https://ieeexplore.ieee.org/document/6966136>
16. C. Wang and A. Rahman, "Quantum-Enabled 6G Wireless Networks: Opportunities and Challenges," *ResearchGate*, 2024. Available: <https://www.researchgate.net>.
17. R. Thommandru, "Quantum Key Distribution for Securing 6G Networks: Shaping the Future of Mobile Communication," *ResearchGate*, 2024. Available: <https://www.researchgate.net>.
18. H. Urgelles, D. Garcia-Roger, and J. F. Monserrat, "Quantum-Based Maximum Likelihood Detection in MIMO-NOMA Systems for 6G Networks," *ResearchGate*, 2024. Available: <https://www.researchgate.net>.
19. O. Bouchmal, B. Cimoli, R. Stabile, J. J. Vegas Olmos, and I. Tafur Monroy, "Quantum-Inspired Network Optimization in 6G: Opportunities, Challenges and Open Research Directions," in *Distributed Computing and Artificial Intelligence, Special Sessions I*, 20th International Conference (DCAI 2023), Lecture Notes in Networks and Systems, vol. 741, pp. 480–488, 2023. [Online]. Available: https://link.springer.com/chapter/10.1007/978-3-031-38318-2_48 SpringerLink+1SpringerLink+1
20. E. Kiran Kumar, "Advancement of Cloud-Based Ultra-Secure Communication using Quantum Key Distribution in 6G Networks," SSRN, Nov. 2024. [Online]. Available: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5077871 SSRN
21. Y. Liu, W. Yi, Z. Ding, X. Liu, O. Dobre, and N. Al-Dhahir, "Application of NOMA in 6G Networks: Future Vision and Research Opportunities for Next Generation Multiple Access," arXiv preprint arXiv:2103.02334v1, Mar. 2021. [Online]. Available: <https://arxiv.org/abs/2103.02334v1> arXiv

22. O. Bouchmal, B. Cimoli, R. Stabile, J. J. Vegas Olmos, and I. Tafur Monroy, "Quantum-Inspired Network Optimization in 6G: Opportunities, Challenges and Open Research Directions," in *Distributed Computing and Artificial Intelligence, Special Sessions I*, 20th International Conference (DCAI 2023), Lecture Notes in Networks and Systems, vol. 741, pp. 480–488, 2023. [Online]. Available: https://link.springer.com/chapter/10.1007/978-3-031-38318-2_48
[SpringerLink+1SpringerLink+1](#)
23. R. Thommandru, "Quantum Key Distribution for Securing 6G Networks: Shaping the Future of Mobile Communication," ResearchGate, 2024. [Online]. Available: https://www.researchgate.net/publication/386405080_Quantum_Key_Distribution_for_Securing_6G_Networks_Shaping_the_Future_of_Mobile_Communication[ResearchGate](#)
24. H. Urgelles, D. Garcia-Roger, and J. F. Monserrat, "Quantum-Based Maximum Likelihood Detection in MIMO-NOMA Systems for 6G Networks," *Quantum Reports*, vol. 6, no. 4, pp. 533–549, 2024. [Online]. Available: <https://www.mdpi.com/2624-960X/6/4/36>
[MDPI+2MDPI+2MDPI+2](#)
25. A. K. Singh and R. K. Jha, "Quantum Key Distribution Networks -- Key Management: A Survey," arXiv preprint arXiv:2408.04580, Aug. 2024. [Online]. Available: <https://arxiv.org/abs/2408.04580>[arXiv](#)
26. S. Chen, H. Zhang, and Y. Li, "Quantum Machine Learning for 6G Communication Networks," *International Journal of Advanced Research in Computer and Communication Engineering*, vol. 13, no. 12, pp. 1–6, Dec. 2024. [Online]. Available: <https://ijarcce.com/wp-content/uploads/2024/12/IJARCCE.2024.131236.pdf>[Peer-reviewed Journal](#)
27. S. K. Sharma and X. Wang, "Machine Learning and Quantum Computing for 5G/6G Communication Networks: Opportunities, Challenges, and Future Research Directions," *Journal of Information Security and Applications*, vol. 58, p. 102806, 2022. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S2666603022000240>[ScienceDirect](#)
28. Y. Liu, Z. Qin, M. ElKashlan, Z. Ding, A. Nallanathan, and L. Hanzo, "Non-Orthogonal Multiple Access for 5G and Beyond," *Proceedings of the IEEE*, vol. 105, no. 12, pp. 2347–2381, 2017. [Online]. Available: <https://ieeexplore.ieee.org/document/8054694>
29. P. K. Sharma and D. I. Kim, "Towards 6G Network Architecture: Applications, AI-Based Framework, and Future Directions," *IEEE Access*, vol. 8, pp. 67555–67578, 2020. [Online]. Available: <https://ieeexplore.ieee.org/document/9063422>
30. M. S. ElBamby, M. Bennis, W. Saad, and M. Latva-aho, "Content-Aware User Clustering and Caching in Wireless Small Cell Networks," in *Proceedings of the 2014 IEEE International Symposium on Wireless Communication Systems (ISWCS)*, Barcelona, Spain, 2014, pp. 945–949. [Online]. Available: <https://ieeexplore.ieee.org/document/6933473>

Conclusion & Vote of Thanks:

We extend our sincere gratitude to everyone who contributed to the successful execution of this project.

First and foremost, we would like to thank our mentors and faculty members for their constant support, insightful guidance, and encouragement throughout the development of this research. Their expertise helped us navigate through technical challenges and sharpen our understanding of cutting-edge technologies like Q-Learning, Quantum Key Distribution, and NOMA.

We are also deeply grateful to our collaborators and teammates, Preeti Yadav ,Basil Syed and Satyam, whose dedication, coordination, and technical contributions were instrumental in turning this interdisciplinary idea into reality. Working together as a team not only made this journey smoother but also more enriching and intellectually stimulating.

Special thanks to our institution's research and development cell, and the Intellectual Property Rights (IPR) team, for their ongoing assistance in preparing our work for both publication and patent filing. Their encouragement has given us the confidence to pursue the next steps toward making a real-world impact.

Finally, we would like to thank all the individuals and platforms that provided tools, datasets, and simulation environments such as MATLAB and Qiskit, without which this research would not have been possible.

This project has been an incredible learning experience, blending the future of AI and quantum security in wireless communication, and we're excited to continue building upon this foundation in the days to come.

Thank you once again for your time, support, and belief in our vision.

