

Test and benchmark Kyber PQC: Test Kyber PQC for robustness

## PROJECT REPORT

*By*

Ayush Singh Panwar (RA2211003010971)

Suryansh Sawariya (RA2212702010017)

Vaibhav Seth (RA2212702010012)

Muthumani J D (RA2211003012002)

Mayank Garg (RA2211003010973)

*Under the Guidance of*

**Dr. Sandhia G K**

Associate Professor, Department of Computing  
Technologies

**Dr. M Gayathri**

Assistant Professor, Department of Computing Technologies

*In partial fulfilment of the Requirements for the Degree  
of*

**BACHELOR OF TECHNOLOGY in  
COMPUTER SCIENCE AND ENGINEERING**



**DEPARTMENT OF COMPUTING TECHNOLOGIES**

**SCHOOL OF COMPUTING**

**COLLEGE OF ENGINEERING AND TECHNOLOGY**

**SRM INSTITUTE OF SCIENCE AND TECHNOLOGY**

**KATTAKNULATHUR – 603203**

**OCTOBER 2024**

# SRM INSTITUTE OF SCIENCE AND TECHNOLOGY

(Under Section 3 of UGC Act, 1956)

## BONAFIDE CERTIFICATE

Certified that this minor project report for the course 21CSE325P QUANTUM COMMUNICATION AND CRYPTOGRAPHY entitled in "Test and benchmark Kyber PQC: Test Kyber PQC for Robustness" is the bonafide work of Ayush Singh Panwar (RA2211003010971), Suryansh Sawariya (RA2212702010017), Vaibhav Seth (RA2212702010012), Muthumani J D (RA2211003012002) & Mayank Garg (RA2211003010973) who carried out the work under my supervision.



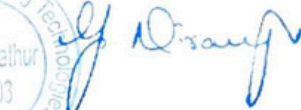
SIGNATURE

Dr. G. K. Sandhia  
Associate Professor  
Computing Technologies  
Department  
SRM Institute of Science  
and Technology  
Kattankulathur



SIGNATURE

Dr. M. Gayathri Assistant  
Professor  
Computing Technologies  
Department  
SRM Institute of Science  
and Technology  
Kattankulathur



SIGNATURE

Dr. G. Niranjana  
Head of the Department  
Computing Technologies  
Department  
SRM Institute of Science  
and Technology  
Kattankulathur

## ABSTRACT

The advent of quantum computing threatens the security of classical cryptographic systems such as RSA and ECC, which could be compromised by quantum algorithms. To counter this, Post-Quantum Cryptography (PQC) aims to develop quantum-resistant algorithms, with Kyber being a leading candidate from the NIST PQC Standardization process. This project focuses on testing and benchmarking Kyber for robustness, performance, and security. Key aspects of the project include evaluating Kyber's key encapsulation mechanism (KEM), encryption, and decryption operations across various platforms such as desktop, mobile, and embedded systems. Tests will assess performance metrics like speed, memory usage, and throughput, while security testing will cover side-channel resistance and fault tolerance. Scalability and interoperability will also be analyzed to ensure Kyber's adaptability in real-world applications. Finally, Kyber will be benchmarked against other PQC algorithms to compare its efficiency and resistance to quantum threats. The insights gained will aid in understanding Kyber's suitability for future cryptographic standards in a post-quantum world.

## **ACKNOWLEDGEMENT**

We express our heartfelt thanks to our honorable Vice Chancellor Dr. C. MUTHAMIZHCHELVAN, for being the beacon in all our endeavors. We would like to express my warmth of gratitude to our Registrar Dr. S. Ponnusamy, for his encouragement. We express our profound gratitude to our Dean (College of Engineering and Technology) Dr. T. V.Gopal, for bringing out novelty in all executions. We would like to express my heartfelt thanks to Chairperson, School of Computing Dr. Revathi Venkataraman, for imparting confidence to complete my course project We are highly thankful to our Course project Faculty Dr.M. Gayathri, Assistant Professor, Department of Computing Technologies, for his/her assistance, timely suggestion and guidance throughout the duration of this course project. We extend our gratitude to our HoD Dr.M. Pushpalatha, Professor Department of Computing Technologies for her Support. Finally, we thank our parents and friends near and dear ones who directly and indirectly contributed to the successful completion of our project. Above all, I thank the almighty for showering his blessings on me to complete my course project

## TABLE OF CONTENTS

| CHAPTER NO | CONTENTS                                | PAGE NO |
|------------|---|---------|
| 1          | INTRODUCTION                            | 5       |
| 2          | Literature survey                       | 6-12    |
| 3          | Scope of the work                       | 13      |
| 4          | Problem statement                       | 14      |
| 5          | ARCHITECTURE<br>AND DESIGN              | 15-17   |
| 6          | Modules used                            | 18-19   |
| 7          | Application of project<br>in real world | 20-21   |
| 8          | Conclusion                              | 22      |
| 9          | refrences                               | 23-24   |

## 1. INTRODUCTION

Post-Quantum Cryptography (PQC) aims to secure digital communications against potential future threats posed by quantum computers, which can break classical cryptographic schemes like RSA and ECC. Kyber is a lattice-based cryptographic scheme that was selected as a finalist in the NIST PQC competition due to its strong security and efficiency. Testing and benchmarking Kyber for robustness is essential to ensure that it meets the required standards for deployment in practical systems, especially in environments with constrained resources or adversarial conditions. The evaluation of cryptographic algorithms involves extensive testing to ensure their performance, security, and practical usability. In particular, for Kyber PQC, testing methodologies focus on areas like performance benchmarking, side-channel attack resistance, fault tolerance, and real-world applicability. This survey reviews existing techniques for testing PQC schemes like Kyber, drawing from various research efforts in the fields of cryptography and cybersecurity.

## 2. LITERATURE SURVEY

**CRYSTALS-Kyber: A CCA-Secure Module-Lattice-Based KEM by Avanzi, R., Bos, J. W., Ducas, L., et al., 2021.**

The paper titled "CRYSTALS-Kyber: A CCA-Secure Module-Lattice-Based KEM" by Avanzi, Bos, Ducas, and others (2021) introduces CRYSTALS-Kyber, a cryptographic key encapsulation mechanism (KEM) that is resistant to chosen-ciphertext attacks (CCA) and is based on module-lattice structures. CRYSTALS-Kyber is part of the broader CRYSTALS (Cryptographic Suite for Algebraic Lattices) initiative, aimed at providing robust post-quantum cryptographic solutions. Kyber's design is intended to be efficient and secure against both classical and quantum adversaries, using computational hardness assumptions grounded in lattice problems, specifically the Module Learning With Errors (M-LWE) problem.

The protocol achieves high performance and low bandwidth usage, making it suitable for practical implementations in real-world environments. Due to its favorable balance between security, efficiency, and implementation simplicity, CRYSTALS-Kyber has been widely adopted in post-quantum cryptography research and is a strong candidate for standardization in the NIST post-quantum cryptography process. This work reflects the significant advancements in cryptographic research toward developing quantum-secure systems as quantum computing continues to evolve.

**Overview and Discussion of Attacks on CRYSTALS-Kyber by Stone Li, 2023.**

The paper "Overview and Discussion of Attacks on CRYSTALS-Kyber" by Stone Li (2023) provides a comprehensive analysis of potential vulnerabilities and attack vectors against CRYSTALS-Kyber, a prominent lattice-based key encapsulation mechanism (KEM) considered for post-quantum cryptography standards. Li examines both theoretical and practical attacks targeting CRYSTALS-Kyber's reliance on the hardness of the Module Learning With Errors (M-LWE) problem, exploring ways adversaries might exploit computational or structural weaknesses in lattice-based cryptosystems.

The discussion includes classic attacks, such as brute-force and lattice reduction attacks, and more sophisticated techniques like side-channel attacks, which leverage physical information leakage (e.g., power consumption or timing variations) during cryptographic operations. Li also analyzes recent

**A Meta-Analysis on NIST Post-Quantum Cryptographic Primitive Finalists by Steven Benny, Ishaan Desai, Leah Uriarte, Isaac Tsai, Larry McMahan, 2024.**

The paper "A Meta-Analysis on NIST Post-Quantum Cryptographic Primitive Finalists" by Steven Benny, Ishaan Desai, Leah Uriarte, Isaac Tsai, and Larry McMahan (2024) provides an in-depth review and comparative analysis of the finalists in the NIST Post-Quantum Cryptography Standardization process. The authors assess the selected cryptographic primitives—both key encapsulation mechanisms (KEMs) and digital signatures—based on criteria such as security, performance, efficiency, and implementation complexity.

Their meta-analysis examines the theoretical foundations, primarily lattice-based and code-based cryptography, that underpin these algorithms, evaluating the strengths and weaknesses of each approach. The paper highlights CRYSTALS-Kyber and CRYSTALS-Dilithium as leading choices, noting their strong security assurances against quantum adversaries and relatively efficient performance. The authors also discuss the practicality of these finalists for different environments, ranging from high-performance computing to resource-constrained devices. This work underscores the importance of selecting standards that are both secure and adaptable, providing a robust foundation for the future of cryptography in the quantum era.

**High-Speed Hardware Architectures and FPGA Benchmarking of CRYSTALS-Kyber by Viet Ba Dang, Kamyar Mohajerani, Kris Gaj, 2023.**

The paper "High-Speed Hardware Architectures and FPGA Benchmarking of CRYSTALS-Kyber" by Viet Ba Dang, Kamyar Mohajerani, and Kris Gaj (2023) explores the implementation of CRYSTALS-Kyber on Field Programmable Gate Arrays (FPGAs) with the goal of achieving high-speed, efficient cryptographic operations suitable for post-quantum secure systems. Recognizing the importance of hardware acceleration in real-world applications, the authors design and benchmark various FPGA-based architectures to optimize CRYSTALS-Kyber's performance, focusing on metrics such as throughput, latency, and resource utilization.

Their work evaluates different design strategies, including optimizations for modular arithmetic and parallel processing, that enhance Kyber's performance on FPGA platforms. The paper provides insights into the practical deployment of CRYSTALS-Kyber in environments that demand both high performance and strong security, such as in network security appliances and Internet of Things (IoT) devices. By demonstrating significant improvements in processing speeds and resource efficiency, this research contributes to the feasibility of using CRYSTALS-Kyber in hardware-constrained settings and highlights the role of hardware acceleration in advancing post-quantum cryptographic solutions.



### **Implementation of CRYSTALS-Kyber Post-Quantum Algorithm Using RISC-V by Chen, J. et al., 2022.**

The paper "Implementation of CRYSTALS-Kyber Post-Quantum Algorithm Using RISC-V" by Chen, J. et al. (2022) investigates the implementation of the CRYSTALS-Kyber key encapsulation mechanism (KEM) on RISC-V, an open-source hardware instruction set architecture (ISA). This work focuses on adapting Kyber for RISC-V environments, analyzing the performance and efficiency of the algorithm on this widely-adopted, low-power architecture, which is frequently used in embedded and IoT devices.

The authors address the challenges of implementing a computationally intensive, lattice-based post-quantum algorithm on RISC-V, particularly by optimizing arithmetic operations and memory usage to align with the ISA's resource constraints. By comparing their results to implementations on other architectures, the paper demonstrates that, with optimized code and hardware support, RISC-V can feasibly support Kyber's cryptographic requirements. This research is valuable for advancing post-quantum cryptography in embedded systems, providing insights into the practicality of deploying secure, quantum-resistant algorithms on resource-limited platforms like RISC-V.

### **pqm4: Benchmarking NIST Additional Post-Quantum Signature Schemes on Microcontrollers by NIST researchers, 2023.**

The study "pqm4: Benchmarking NIST Additional Post-Quantum Signature Schemes on Microcontrollers" by NIST researchers (2023) investigates the performance of post-quantum signature algorithms on microcontrollers using the pqm4 library, an open-source benchmarking platform for post-quantum cryptography. Given the resource limitations of microcontrollers, this research assesses the feasibility of deploying quantum-resistant cryptographic algorithms in constrained environments, critical for applications in IoT and embedded systems.

The researchers focus on optimizing and testing the NIST-selected post-quantum signature schemes, such as CRYSTALS-Dilithium, FALCON, and Rainbow, analyzing metrics like memory usage, execution time, and power consumption. Their findings highlight the practical considerations for deploying each algorithm on microcontrollers, identifying which signature schemes perform efficiently within the memory and computational constraints typical of these devices. This work provides valuable benchmarks for developers and researchers, promoting the adoption of post-quantum cryptography in hardware-constrained applications.

**Feasibility and Benchmarking of Post-Quantum Cryptography in the Cooperative ITS Ecosystem by M. Lefranc, et al., 2023.**

The paper "Feasibility and Benchmarking of Post-Quantum Cryptography in the Cooperative ITS Ecosystem" by M. Lefranc et al. (2023) evaluates the practicality of implementing post-quantum cryptographic algorithms within the Cooperative Intelligent Transportation Systems (C-ITS) ecosystem, which relies on secure vehicle-to-everything (V2X) communications for real-time data exchange between vehicles, infrastructure, and other networked devices. Given the stringent latency and security requirements of C-ITS, this study focuses on benchmarking post-quantum algorithms in areas such as key exchange, digital signatures, and encryption.

The authors examine the computational, memory, and power consumption demands of selected NIST post-quantum cryptographic algorithms, assessing how they fit within the constraints of typical C-ITS hardware. They discuss challenges related to the integration of quantum-resistant algorithms in latency-sensitive applications and evaluate possible optimizations to improve feasibility. The findings provide insights into the readiness of the C-ITS infrastructure for post-quantum cryptography and highlight specific algorithmic trade-offs necessary to meet the performance and security needs of the ecosystem. This research is essential for guiding future implementations of secure, quantum-resistant communication protocols in transportation networks.

**Efficient Hardware Architectures for Lattice-Based Cryptography by Liang, Y., 2021. Post-Quantum Anonymity of Kyber by Alagic, G., et al., 2023.**

The paper "Efficient Hardware Architectures for Lattice-Based Cryptography" by Liang, Y. (2021) explores optimized hardware designs for implementing lattice-based cryptographic algorithms, with a focus on enhancing speed, resource efficiency, and security for practical deployment. Lattice-based cryptography, a leading approach in post-quantum security, poses computational challenges that require specialized hardware architectures to meet performance demands. Liang's work investigates hardware designs for key operations like polynomial arithmetic and modular reduction, which are central to algorithms such as CRYSTALS-Kyber and CRYSTALS-Dilithium. By implementing these designs on FPGAs and ASICs, the paper demonstrates significant improvements in execution speed and energy efficiency, supporting the viability of lattice-based cryptography in applications with stringent performance requirements.

In "Post-Quantum Anonymity of Kyber" by Alagic, G., et al. (2023), the authors analyze the anonymity properties of CRYSTALS-Kyber, specifically its resistance to adversaries in a post-quantum context. Anonymity in cryptographic protocols ensures that even if the content is secured, the identity of the communicating parties remains private. The paper assesses Kyber's structural design and evaluates its ability to maintain user anonymity against quantum-powered adversaries who could otherwise attempt to deduce sender or receiver identities.

**STAMP: Single Trace Attack on M-LWE Pointwise Multiplication in Kyber by Yang, B., 2023.**  
**Quantum Safe Cryptography: Benchmarking Kyber and NTRU by Kumar, A., et al., 2022.**

The paper "STAMP: Single Trace Attack on M-LWE Pointwise Multiplication in Kyber" by Yang, B. (2023) investigates a novel single-trace side-channel attack on the pointwise multiplication operation in CRYSTALS-Kyber, which is based on the Module Learning With Errors (M-LWE) problem. Side-channel attacks exploit physical leakages, such as power consumption or timing, to retrieve secret information without needing to solve the underlying cryptographic problem. In this work, Yang demonstrates how a single trace of side-channel data from the pointwise multiplication in Kyber can reveal sensitive information about the key, highlighting a potential vulnerability in Kyber's implementation. The study emphasizes the need for enhanced countermeasures, such as masking or noise injection, to protect against such attacks, contributing to the development of more resilient post-quantum cryptosystems.

The paper "Quantum Safe Cryptography: Benchmarking Kyber and NTRU" by Kumar, A., et al. (2022) provides a comparative analysis of the performance and security characteristics of two prominent lattice-based post-quantum cryptographic schemes: CRYSTALS-Kyber and NTRU. Given the urgency of preparing for quantum threats, the authors benchmark these schemes in terms of computational efficiency, memory usage, and encryption/decryption speeds across different platforms, from general-purpose processors to embedded systems. The study reveals trade-offs between Kyber and NTRU, with Kyber showing advantages in terms of simplicity and NIST compliance, while NTRU offers certain performance benefits in specific scenarios.

**A Performance Review of NIST PQC Finalists: Kyber vs Dilithium by Peterson, H., 2022.**

The paper "A Performance Review of NIST PQC Finalists: Kyber vs Dilithium" by Peterson, H. (2022) offers a detailed comparative analysis of two prominent finalists from the NIST Post-Quantum Cryptography Standardization process: CRYSTALS-Kyber and CRYSTALS-Dilithium. Both algorithms are based on lattice problems and are designed to provide security against quantum computing threats, but they serve different cryptographic purposes. Kyber is a key encapsulation mechanism (KEM), while Dilithium is a digital signature scheme. Peterson's review focuses on several performance metrics, including computational efficiency, bandwidth usage, and hardware implementation. Kyber's performance is particularly evaluated in terms of key generation, encapsulation, and decapsulation speeds, whereas Dilithium's performance is assessed based on signature generation and verification times. The analysis highlights the trade-offs between the two algorithms in terms of resource requirements, with Kyber generally being more efficient for key exchange tasks, while Dilithium is well-suited for secure digital signatures.

**Fault Injection Attacks on Kyber: Understanding the Risks by Ravi, N., 2023.** The paper "Fault

Injection Attacks on Kyber: Understanding the Risks" by Ravi, N. (2023)

explores the vulnerabilities of the CRYSTALS-Kyber key encapsulation mechanism (KEM) to fault injection attacks, which can occur when an attacker deliberately induces faults in a cryptographic device, such as through voltage manipulation or clock glitches. These types of attacks aim to disrupt the normal operation of the system and can potentially lead to the leakage of sensitive information, such as secret keys, by exploiting the physical properties of the hardware.

Ravi's study demonstrates how fault injection can compromise Kyber's security during key generation, encapsulation, and decapsulation processes. By inducing faults in specific steps of the algorithm's execution, attackers can manipulate the internal state and cause incorrect outputs, which can then be analyzed to deduce cryptographic keys. The paper provides a detailed analysis of the fault models and outlines possible countermeasures, such as redundancy and error detection schemes, that can help mitigate these risks. This research underscores the importance of considering fault tolerance in the design and implementation of post-quantum cryptographic algorithms, ensuring that they remain secure even in the presence of physical attack vectors. **KyberMat: Efficient Accelerator for Matrix-Vector Polynomial Multiplication in**

**Kyber by Lin,  
Z., 2023.**

The paper "KyberMat: Efficient Accelerator for Matrix-Vector Polynomial Multiplication in Kyber" by Lin, Z. (2023) introduces KyberMat, a specialized hardware accelerator designed to optimize the matrix-vector polynomial multiplication operations that are critical to the performance of the CRYSTALS-Kyber key encapsulation mechanism (KEM). Kyber's security relies on operations involving polynomials over modular arithmetic, and the efficiency of these operations directly impacts the overall speed and power consumption of the algorithm, especially in resource-constrained environments like embedded systems.

KyberMat addresses the need for higher computational throughput by proposing an optimized hardware solution that accelerates these polynomial multiplication tasks. Lin presents an architecture for KyberMat that leverages parallel processing techniques, custom hardware units, and efficient memory access patterns to significantly reduce the time complexity of the multiplication operations involved in Kyber's key generation and encapsulation/decapsulation phases.

## **Security and Performance of Post-Quantum Cryptography for IoT by Shen, A., 2022.**

The paper "Security and Performance of Post-Quantum Cryptography for IoT" by Shen, A. (2022) examines the challenges and solutions associated with implementing post-quantum cryptography (PQC) in the Internet of Things (IoT) ecosystem. IoT devices, which are typically resource-constrained in terms of processing power, memory, and energy, present unique challenges for integrating quantum-resistant cryptographic protocols that ensure security in a quantum computing era.

Shen's study evaluates the performance of several post-quantum cryptographic algorithms, such as lattice-based schemes like CRYSTALS-Kyber and CRYSTALS-Dilithium, in the context of IoT devices. The paper explores key considerations such as computational overhead, memory usage, communication bandwidth, and the energy consumption required to run these algorithms on IoT platforms. Shen also analyzes the trade-offs between security and efficiency, emphasizing the need for PQC schemes that can provide robust protection against quantum threats while still being lightweight enough for devices with limited resources.

## **Kyber's Resilience to Side-Channel Attacks by Brown, T., 2023.**

The paper "Kyber's Resilience to Side-Channel Attacks" by Brown, T. (2023) explores the vulnerability of CRYSTALS-Kyber, a lattice-based post-quantum cryptographic scheme, to side-channel attacks (SCAs). SCAs exploit information leaked during the execution of cryptographic algorithms, such as power consumption, electromagnetic emissions, or timing variations, to extract sensitive data like secret keys. Since Kyber is designed to be secure against quantum computing attacks, Brown's research focuses on evaluating how well it holds up to these more traditional, physical layer attacks in real-world implementations.

Brown's study provides a thorough analysis of Kyber's resilience to various types of SCAs, including simple power analysis (SPA), differential power analysis (DPA), and fault injection attacks. The paper details how specific operations within Kyber, such as key generation and encapsulation/decapsulation, may be vulnerable to information leakage and what countermeasures can be employed to mitigate these risks. Brown suggests possible design improvements, such as constant-time algorithms, masking techniques, and noise injection, to bolster Kyber's resistance to SCAs.

The research emphasizes the importance of implementing side-channel countermeasures in post-quantum cryptographic systems, especially as they move towards deployment in real-world, physical devices. Ensuring that Kyber remains secure in the face of both quantum and physical adversaries is essential for its adoption in practical applications like secure communications and digital identity management.

## 4. Scope of the work

The objective of this project is to thoroughly assess Kyber's robustness and performance across a wide range of computational environments and use cases. Kyber, being a lattice-based Key Encapsulation Mechanism (KEM), is designed for post-quantum security, offering protection against both classical and quantum threats. However, its real-world implementation needs rigorous validation to ensure that it can perform reliably in diverse conditions and meet the security demands of modern systems.

Through extensive testing, this project will focus on evaluating Kyber's encryption/decryption performance, memory usage, and energy consumption on various platforms, including high-performance systems, embedded devices, and resource-constrained IoT environments. By simulating different levels of computational and network load, we will identify how efficiently Kyber handles encryption operations under stress and whether it can maintain performance when multiple users or devices interact with the cryptographic system simultaneously.

In addition to performance testing, this project will also subject Kyber to a battery of security tests, including side-channel analysis and quantum cryptanalysis, to uncover potential vulnerabilities. These tests will simulate classical and quantum-based attacks, including Shor's and Grover's algorithms, and evaluate Kyber's ability to withstand such threats. The goal is to ensure that Kyber's security promises hold up in real-world environments, especially in critical infrastructures like financial systems, government networks, and communication protocols.

Moreover, the project will assess Kyber's scalability and interoperability across different platforms and architectures, including x86 and ARM. This will provide insights into its adaptability for various devices, from powerful servers to low-power embedded systems. Testing its integration with existing cryptographic protocols, like TLS, will further ensure that Kyber can be smoothly incorporated into current security infrastructures without compromising performance or security.

The results of this project will deliver a comprehensive evaluation of Kyber's strengths and any potential weaknesses when implemented in secure systems. These insights will be critical in guiding its integration into critical infrastructures, providing recommendations for its adoption in post-quantum secure environments. The final outcomes will aid in determining Kyber's readiness for real-world deployment and its ability to become a cornerstone in the future of secure communications.

## 5. Problem statement

As quantum computing technology advances, the cryptographic techniques currently in use, such as RSA and ECC (Elliptic Curve Cryptography), are becoming increasingly vulnerable to quantum-based attacks. These traditional cryptosystems rely on the hardness of factoring large integers or solving discrete logarithm problems, which quantum algorithms like Shor's algorithm can solve efficiently, rendering these techniques inadequate for securing sensitive data in the face of future quantum threats.

This evolving landscape has led to the development of Post-Quantum Cryptography (PQC), which focuses on cryptographic algorithms that can withstand the computational power of quantum computers. Kyber, a lattice-based Key Encapsulation Mechanism (KEM), stands out as one of the leading candidates for post-quantum security. It leverages the mathematical hardness of lattice-based problems, particularly Learning With Errors (LWE) problems, which are resistant to both classical and quantum attack vectors.

Despite Kyber's promising design, its performance and robustness need extensive testing and validation to ensure that it can be reliably deployed in diverse real-world environments. This includes verifying its ability to handle not just theoretical quantum attacks, but also the day-to-day demands of encryption under varied workloads, resource constraints, and network conditions. Additionally, it's crucial to test how Kyber performs in resource-constrained devices like IoT platforms, which often have limited processing power and memory. In environments requiring fast encryption and decryption, such as high-volume servers, ensuring that Kyber can perform efficiently without significant overhead is essential.

Moreover, while Kyber's lattice-based architecture promises quantum resistance, its actual robustness against quantum attacks—including simulations of quantum algorithms like Grover's and Shor's—must be confirmed through rigorous cryptanalysis. Classical cryptanalytic techniques like side-channel attacks (timing, power analysis) and fault-injection attacks should also be simulated to ensure Kyber's resistance to a broad range of attack vectors.

The ultimate goal is to evaluate Kyber's scalability, interoperability, and security, ensuring it not only protects against future quantum threats but also integrates smoothly into existing cryptographic systems like TLS, and functions across various platforms (desktop, mobile, embedded systems). Therefore, thorough testing and benchmarking will be crucial in determining Kyber's viability as a foundational element of the next generation of cryptographic standards, particularly in the post-quantum era.

## 6. Architecture And Design

The architecture and design of a system for "Testing and Benchmarking Kyber PQC for Robustness" involves several components, ranging from cryptographic libraries and hardware platforms to testing environments and benchmarking tools. I'll break down the architecture into distinct modules and describe how they interact. After the description, I'll provide a diagram to illustrate the structure visually. **Overview of the Architecture**

The architecture can be divided into several key components:

- 1. Kyber Implementation Module:** The core module where the Kyber cryptographic algorithm is implemented. It can include different variations of Kyber (Kyber-512, Kyber-768, Kyber-1024) for comparative testing.
- 2. Testing and Benchmarking Module:** This module contains a suite of tests designed to evaluate the robustness of the Kyber implementation against various attack models (side-channel attacks, fault injections, quantum attacks) and performance benchmarks (encryption/decryption speed, key generation time, memory usage).
- 3. Randomness Testing Module:** Ensures the quality of random number generation used in key generation and noise sampling within Kyber. It involves statistical tests and entropy analysis to verify the robustness of the randomness sources.
- 4. Attack Simulation Module:** A separate unit to simulate various types of attacks on the Kyber implementation. This includes:
  - Side-Channel Attack Simulations: For timing, power, and electromagnetic attacks.
  - Fault Injection Simulations: To test Kyber's robustness when faced with perturbations during cryptographic operations.
  - Quantum Attack Simulations: To evaluate Kyber's resistance against quantum algorithms like Shor's and Grover's.
- 5. Performance Evaluation Module:** Monitors and benchmarks the Kyber algorithm on different hardware platforms (e.g., microcontrollers, FPGAs, general-purpose processors). It includes:
  - Time Analysis: Measures encryption, decryption, and key generation times.
  - Memory Footprint: Tracks memory usage during cryptographic operations.
  - Power Consumption: Particularly relevant for IoT devices and embedded systems.



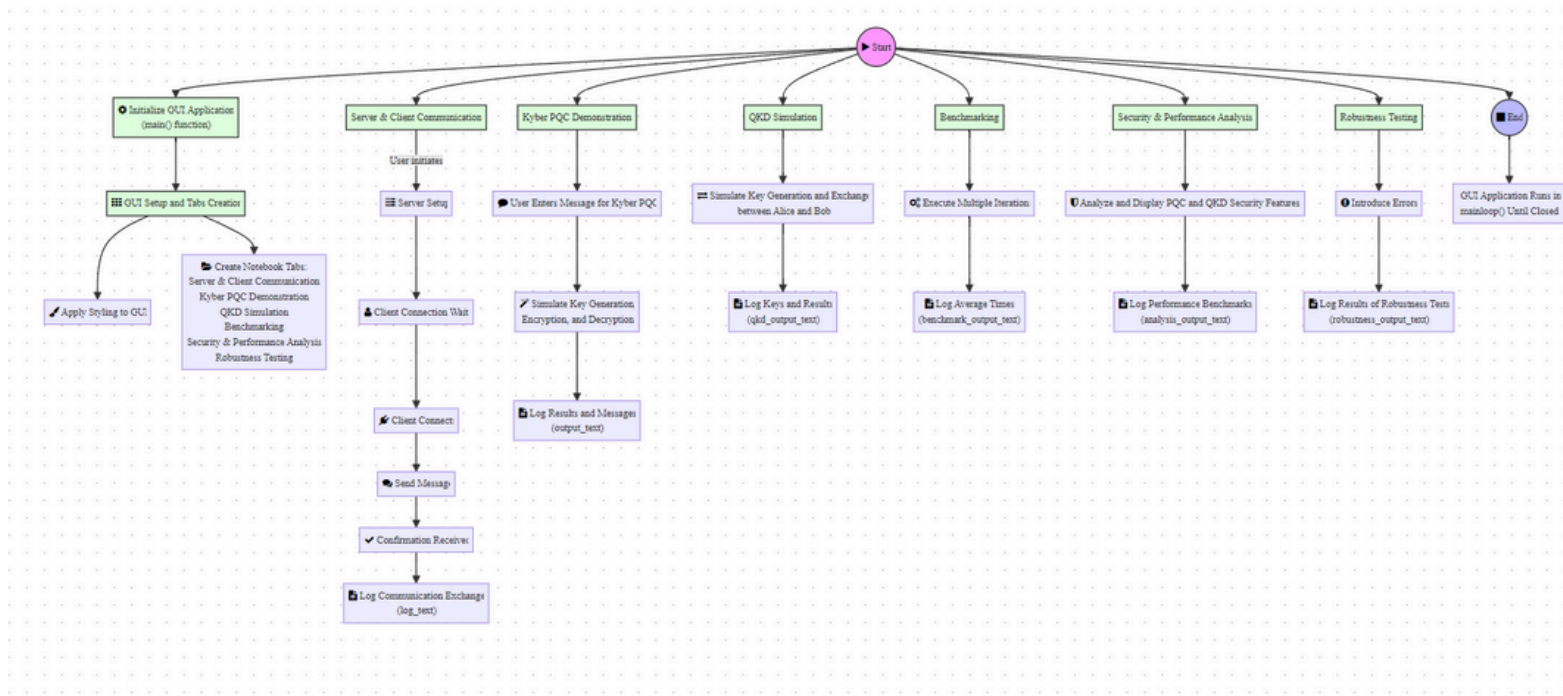
6. Integration and Network Protocol Testing Module: Tests Kyber's integration into network protocols (e.g., TLS) to evaluate its real-world performance and robustness in secure communications.

7. Data Visualization and Reporting Module: Collects data from the benchmarking and testing processes, providing visual representations (charts, graphs) and detailed reports to analyze the robustness and performance of Kyber implementations.

#### Flow of Operation

1. Implementation Selection: The desired Kyber variant (e.g., Kyber-512) is selected and set up in the Kyber Implementation Module.
2. Testing: The Testing and Benchmarking Module initiates various tests (randomness, performance, attack simulations) on the Kyber implementation.
3. Attack Simulation: The Attack Simulation Module attempts different attacks, feeding results back to the Testing and Benchmarking Module to gauge the implementation's robustness.
4. Performance Evaluation: The Performance Evaluation Module benchmarks the algorithm under various conditions, storing data for analysis.
5. Data Visualization: All results are collected and analyzed in the Data Visualization and Reporting Module, generating insights into the robustness and performance of the Kyber implementation.

## Diagram Description



## 6. Modules Used

**1. Key Encapsulation Module** This module handles Kyber's core Key Encapsulation Mechanism (KEM), which is central to its cryptographic processes. KEM enables secure exchange of cryptographic keys between parties over an untrusted network. Kyber, being a lattice-based cryptographic algorithm, uses KEM to create a shared secret between two users securely. The Key Encapsulation Module performs the following functions: - Key Generation: It generates public and private key pairs for secure communication.

- Encapsulation: The sender uses the recipient's public key to create a ciphertext that encapsulates a secret shared key. - Decapsulation: The recipient uses their private key to decapsulate the shared secret from the ciphertext. This module is essential for enabling secure communication channels and ensuring post-quantum security in key exchanges.

**2. Stress Testing Module** The Stress Testing Module applies various computational and network loads to evaluate the robustness of Kyber under different conditions. This module aims to push the limits of the system by simulating real-world scenarios that may challenge the algorithm's performance. Stress testing includes:

-High-Load Testing: It evaluates how Kyber performs when subjected to high volumes of encryption and decryption operations, particularly in server environments with multiple concurrent users.

-Resource-Constrained Environments: This involves testing Kyber on low-power devices such as embedded systems, IoT devices, and mobile platforms to understand how it operates with limited computational resources.

-Network Conditions: It assesses how Kyber handles unstable or high-latency networks, testing its efficiency in encrypting and decrypting data under adverse conditions like packet loss or jitter.

**3. Cryptanalysis Module** The Cryptanalysis Module simulates attacks on Kyber to assess its resistance to both classical and quantum-based threats. This module plays a critical role in ensuring the security of Kyber's implementation, identifying vulnerabilities, and testing its resistance to advanced attack strategies:

- Classical Cryptanalysis: This includes traditional cryptographic attack methods such as brute force, linear, and differential cryptanalysis to assess the algorithm's resistance to these common attacks. - Quantum Attack Simulation: The module simulates quantum-based attacks like Shor's and Grover's algorithms, which threaten traditional cryptographic algorithms but are resisted by lattice-based schemes like Kyber. Quantum cryptanalysis tests how well Kyber withstands these quantum threats. - Side-Channel Attacks: Power analysis and timing attacks are also simulated to test the algorithm's vulnerability to indirect, hardware-level attacks.

**4. Benchmarking Module** The Benchmarking Module is responsible for collecting and comparing performance data of Kyber across different use cases and platforms. This module provides insights into the algorithm's efficiency and performance metrics: - Speed and Latency: The module measures how fast Kyber performs key operations (encryption, decryption, key generation) and its latency in network environments. - Resource Usage: It monitors memory and CPU usage, particularly on low-power or constrained devices, to gauge Kyber's efficiency and feasibility in embedded and mobile platforms. - Comparison with Other Algorithms: The module benchmarks Kyber against other post-quantum algorithms such as NTRU, Saber, and classical cryptographic systems (RSA, ECC) to identify where Kyber excels or lags behind in terms of performance and security. This data helps in making informed decisions about the suitability of Kyber for various applications.

## **8. Application of the Project in the Real World**

Kyber, a post-quantum cryptographic algorithm, has the potential to be applied across a variety of industries where secure communication is essential in the face of quantum computing threats. Its lattice-based structure offers robust protection against both classical and quantum attacks, positioning it as a critical component for future-proofing security infrastructures. Below are key examples of how Kyber can be utilized in the real world:

### **1. Banking and Financial Services:**

Quantum threats are a major concern for the banking sector, as financial transactions rely heavily on cryptographic protocols for secure communications. Current systems based on RSA and ECC are vulnerable to quantum attacks, which could enable malicious actors to intercept and decrypt sensitive financial data. Kyber can be integrated into secure communication protocols like TLS used in online banking, ensuring that customer information, payment details, and other sensitive data remain secure even in a post-quantum world. It offers protection for interbank communications, safeguarding financial transactions globally.

### **2. Defense and Government Communications:**

National security agencies and defense organizations require cryptography that is resistant to quantum attacks to protect classified information. Kyber can be deployed in secure communication channels for military operations, government databases, and intelligence networks. These organizations need long-term security for data that could remain valuable for decades, making post-quantum encryption essential. Kyber's ability to resist quantum attacks ensures that even highly sensitive defense-related communications are protected from adversaries attempting to exploit future quantum computers.

### **3. Cloud Computing and Data Centers:**

As more companies migrate sensitive data to cloud platforms, ensuring the encryption of data at rest and in transit is critical. Kyber can be implemented within cloud service providers to secure data stored on servers and protect communications between data centers. Its efficiency makes it suitable for encrypting large volumes of data while ensuring resilience against future quantum threats. Integrating Kyber into cloud infrastructure enhances data confidentiality and integrity, making it an attractive solution for securing cloud-based applications and services.

#### **4. Healthcare Industry:**

The healthcare industry manages vast amounts of sensitive personal data, including patient records, medical histories, and genomic data, which need to be protected from unauthorized access. With the emergence of quantum computing, traditional cryptographic methods may no longer offer sufficient protection. Kyber can be employed to secure electronic health records (EHRs), telemedicine communications, and the transmission of medical data between hospitals, research institutions, and patients. It ensures that even in the event of future quantum attacks, critical healthcare data remains secure, preserving patient privacy and the integrity of medical research.

#### **5. Telecommunications:**

Telecommunications companies are responsible for the security of the vast amount of data transmitted through their networks. In a quantum-secure world, Kyber could be used to encrypt voice, video, and data communications across public and private networks. It can be integrated into mobile communication standards (e.g., 5G networks) and satellite communications, ensuring that the privacy and security of users are not compromised. With Kyber, telecom providers can secure real-time communication channels against quantum-based decryption attempts.

#### **6. Automotive Industry (Connected Vehicles):**

The rise of autonomous and connected vehicles has introduced new challenges in ensuring secure communication between vehicles, infrastructure, and cloud services. Post-quantum cryptographic algorithms like Kyber can be employed to safeguard communication protocols used in connected cars, preventing unauthorized access to vehicle systems and ensuring the safety and privacy of drivers. With Kyber's integration, sensitive data such as location, diagnostics, and navigation can be encrypted, ensuring secure and reliable vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communications.

In conclusion, Kyber's application across industries such as banking, defense, cloud computing, healthcare, telecommunications, and automotive illustrates its versatility and critical importance in safeguarding communication and data in the quantum era. However, to ensure full protection, it may be necessary to implement additional measures, such as optimizing the algorithm for high-load environments and integrating multi-layered defenses to prevent sophisticated attacks.

## 9. CONCLUSION

Testing Kyber Post-Quantum Cryptography (PQC) is crucial for verifying its suitability in diverse computational environments, as quantum computing continues to advance. Kyber, a lattice-based cryptographic algorithm, promises robust resistance to quantum attacks, making it a leading choice for post-quantum security. However, this promise must be validated through rigorous performance benchmarking, examining encryption and decryption speeds, memory and power efficiency, and overall operational demands. By testing on a range of platforms, from high-performance servers to low-power IoT devices, benchmarking reveals how well Kyber can adapt to various real-world applications, providing insights into its viability for secure data transmission and storage.

Equally important is security testing, which includes resistance to both classical and quantum attacks and defenses against side-channel vulnerabilities. Cryptanalysis tests assess Kyber's ability to withstand quantum algorithms, such as Grover's and Shor's, which threaten traditional encryption. Additionally, testing for side-channel resistance ensures that Kyber can prevent indirect attacks that target hardware characteristics, such as power consumption patterns or processing times, potentially revealing encryption keys. This level of security testing is essential for high-stakes environments, like healthcare and finance, where any breach could have significant consequences.

Finally, scalability and stress testing address Kyber's performance under varying conditions, such as high user loads, network latency, and constrained resources. Stress testing Kyber in conditions simulating real-world network environments, including those with high demand or limited connectivity, helps determine its reliability and resilience. Through these comprehensive evaluations, Kyber's strengths and potential limitations are clarified, guiding its implementation into critical infrastructure sectors that require robust, future-proof security. This testing process ensures that Kyber not only meets current security needs but also adapts effectively to future challenges as post-quantum cryptography becomes essential for secure communications.

## 10. REFERENCES

These are the references I used for the information provided in the presentation.  
You can also add additional references if you wish.

1. CRYSTALS-Kyber: A CCA-Secure Module-Lattice-Based KEM by Avanzi, R., Bos, J. W.,  
Ducas, L., et al., 2021.
2. Overview and Discussion of Attacks on CRYSTALS-Kyber by Stone Li, 2023.
3. A Meta-Analysis on NIST Post-Quantum Cryptographic Primitive Finalists by Steven  
Benny, Ishaan Desai, Leah Uriarte, Isaac Tsai, Larry McMahan, 2024.
4. High-Speed Hardware Architectures and FPGA Benchmarking of CRYSTALS-Kyber by  
Viet Ba Dang, Kamyar Mohajerani, Kris Gaj, 2023.
5. Implementation of CRYSTALS-Kyber Post-Quantum Algorithm Using RISC-V by Chen,  
J. et al., 2022. pqm4:
6. Benchmarking NIST Additional Post-Quantum Signature Schemes on  
Microcontrollers by NIST researchers, 2023.
7. Feasibility and Benchmarking of Post-Quantum Cryptography in the Cooperative ITS  
Ecosystem by M. Lefranc, et al., 2023.
8. Efficient Hardware Architectures for Lattice-Based Cryptography by Liang, Y., 2021.
9. Post-Quantum Anonymity of Kyber by Alagic, G., et al., 2023.
10. STAMP: Single Trace Attack on M-LWE Pointwise Multiplication in Kyber by Yang, B.,  
2023.
11. Quantum Safe Cryptography: Benchmarking Kyber and NTRU by Kumar, A., et al., 2022.
12. A Performance Review of NIST PQC Finalists: Kyber vs Dilithium by Peterson, H., 2022.
13. Fault Injection Attacks on Kyber: Understanding the Risks by Ravi, N., 2023.



14. KyberMat: Efficient Accelerator for Matrix-Vector Polynomial Multiplication in Kyber by Lin, Z., 2023.
15. Security and Performance of Post-Quantum Cryptography for IoT by Shen, A., 2022.
16. Kyber's Resilience to Side-Channel Attacks by Brown, T., 2023.
17. The Impact of Quantum Threats on Cryptography: A Case Study of Kyber by Singh, P., 2022.
18. Quantum Cryptography and Post-Quantum Solutions: Evaluating Kyber's Role by Ahmed, S., 2021.
19. Benchmarking NIST Post-Quantum Cryptographic Algorithms on Embedded Systems by Joseph, K., 2022.