Mukesh Patel School of Technology Management & Engineering, Mumbai

Cybersecurity Department

Project Synopsis

Title of Project: **:** AI For Post Quantum Cryptography Era

Team Members:

Avani Bhat | Prathamesh Shetty | Shruti Bhandare

Under the Supervision of

Ashwini Rao

Table Of Contents

1. Title of the Project: AI For Post Quantum Cryptography Era

2. Team Members:

1. Avani Bhat (K016)
2. Prathamesh Shetty (K054)
3. Shruti Bhandare (K065)

3. Introduction

In the wake of unprecedented advancements in quantum computing, the global cybersecurity environment is experiencing a significant transformation—one that raises particular alarm for essential sectors like banking and financial services. Quantum computers, using algorithms such as Shor's and Grover's, pose a risk to disassemble widely used cryptographic systems including RSA, ECC, and ECDSA. Once deemed secure, these algorithms are now at risk from prospective quantum adversaries. As financial infrastructures grow increasingly reliant on secure digital communications, this threat is not merely hypothetical—it is practical and imminent.

In response, the financial sector, particularly central banks and essential infrastructure providers, has started to take action. The U.S. National Institute of Standards and Technology **(NIST)** has completed the first set of quantum-resistant algorithms, including **CRYSTALS-Kyber** and **Dilithium**, to serve as the next cryptographic standard for public key encryption and digital signatures. Global financial organizations like **SWIFT** have also released evaluations indicating how quantum computing might disrupt financial messaging and payment systems. Leading firms such as **McKinsey** and **Accenture** have collaborated with central banks, including the **Reserve Bank of India (RBI)**, to explore how new technologies—e**ncompassing AI** and **quantum-safe security**—can be integrated into future-proof banking infrastructures. The pathway is evident: future financial systems need to be crypto-agile, upgradeable, and prepared for a post-quantum future.

Although cryptographic agility has often been considered in software systems, achieving it in hardware and hybrid systems adds another layer of complexity. Hardware-based cryptographic engines and embedded security modules typically exhibit rigidity, possessing fixed algorithm implementations that are not easily updated. To bridge this gap, we introduce a modular, AI/ML-augmented cryptographic agility framework that merges cryptography throughout both the hardware and software layers while facilitating runtime adaptability, secure algorithm transitions, and policy-driven cryptographic governance. Instead of tightly integrating cryptographic functionalities into monolithic designs, our framework advocates for a layered, pluggable cryptographic abstraction that can adapt in response to threats, performance criteria, or compliance necessities.

The proposed solution presents a versatile cryptographic infrastructure that fuses dynamic algorithm selection with secure, modular hardware elements. Cryptographic functions are carried out through specialized hardware units capable of supporting various post-quantum algorithms, while AI/ML logic aids in choosing suitable ciphers according to performance, risk, and compliance parameters. Hardware accelerators work in conjunction with configurable software logic, enabling updates, policy adjustments, or algorithm changes without necessitating a complete redesign of the underlying framework. Additionally, the system includes secure key management, modular arithmetic units, and standardized communication protocols to uphold robust security across all operational layers.

This design is specifically crafted for large-scale financial systems—such as national online banking platforms—where enduring cryptographic sustainability, adaptiveness, and adherence to emerging standards like **NIST PQC** and **FIPS 140-3** are vital. The primary objective is to ensure that the established cryptographic infrastructure remains resilient, capable of being upgraded, and in line with both present and future security demands within a swiftly changing threat landscape.

4. Literature Review

With the looming threat of large-scale quantum computers, there is growing urgency to transition from classical cryptographic algorithms like RSA and ECC to quantum-safe alternatives. In critical sectors such as banking and fintech, this migration is not only a technological imperative but also a regulatory one, shaped by data protection and financial security standards like **PCI-DSS**, **GDPR**, and the **NIST post-quantum cryptography standardization project**. However, migrating encryption infrastructure in such regulated environments poses deep architectural and operational challenges. This has led researchers to explore the concept of **crypto-agility**—the ability of a system to adapt cryptographic algorithms and protocols dynamically, without major system redesign.

Alnahawi et al. (2023), in their paper *On the State of Crypto-Agility*, present a detailed landscape of existing efforts toward achieving cryptographic flexibility. They emphasize that current enterprise systems often lack standardized methods for algorithm switching, resulting in lengthy and error-prone migrations. The authors call for more modular, policy-driven architectures that enable on-demand updates to cryptographic primitives without interrupting service availability or violating compliance constraints.

In response to these limitations, the *Enterprise-Level Cryptographic Agility (ELCA)* framework introduces a policy-controlled cryptographic abstraction layer that decouples encryption logic from application logic. This design enables centralized management of cryptographic policies and allows enterprises to transition between algorithms like RSA, ECC, and NIST-standard post-quantum schemes (e.g., Kyber, Dilithium) without modifying the consuming applications. However, ELCA is primarily built for monolithic or enterprise systems and does not directly address decentralized architectures such as microservices, which are becoming the de facto standard in fintech.

Other works, such as *A Scalable Framework for Post-Quantum Authentication in PKI*, focus on the extension of public key infrastructures (PKIs) to support post-quantum digital signatures. These papers propose the use of hybrid certificates that contain both classical and post-quantum signatures to facilitate smoother algorithm transitions. While effective for certificate management, such solutions do not address the challenges of encryption agility within transaction-based service environments like Unified Payments Interface (UPI) or mobile banking systems.

At the same time, the growing adoption of **microservice architectures** in the financial sector offers an opportunity to integrate crypto-agility at the service level. Microservices inherently promote **modular isolation**, allowing each component (such as authentication, transaction signing, or key management) to independently enforce its own encryption policies. Leading security standards such as **PCI-DSS v4.0** mandate that sensitive data (e.g., PAN, CVV, UPI handles) must be encrypted during transmission and at rest using strong cryptography—an objective more easily met with decentralized, containerized service deployments. Similarly, **GDPR** and **PSD2** regulations impose strict data protection and consent management obligations that can benefit from service-level crypto flexibility. While regulatory guidelines like **NIST SP 800-208**, **PCI-DSS**, and **GDPR Article 32** recommend cryptographic agility and regular key rotation, few current implementations support runtime algorithm switching, secrets isolation, or per-service key policies in a production setting. Existing banking systems often remain monolithic or semi-modular, embedding encryption logic within application code. This limits their ability to adapt quickly to new algorithms—especially quantum-resistant ones—as they become standardized.

The framework proposed in this research addresses this gap by introducing a **plug-and-play, containerized microservice architecture** that is inherently crypto-agile and compliant with evolving global standards. A core innovation is the integration of **AI-driven decision logic**, which dynamically selects the most appropriate encryption algorithm for each microservice, based on contextual parameters such as data sensitivity, latency constraints, available hardware security modules (HSMs), and channel trust level.

For instance, lightweight models such as decision trees or neural nets can automatically recommend **Dilithium3** for highly sensitive financial transactions over untrusted networks, or fallback to **AES-128 + ECC** for internal traffic where latency is critical. This adaptive behavior not only improves performance and compliance but also accelerates transitions to **NIST-approved PQC algorithms** without disrupting service availability.

In summary, this work contributes a novel fusion of post-quantum cryptography, microservices, compliance enforcement, and intelligent policy automation into a unified proof-of-concept architecture. It demonstrates that the future of secure financial systems lies in **modular, standards-aligned**, and **AI-augmented crypto frameworks**, capable of withstanding both classical and quantum threats.

5. Why This Topic was Chosen

The choice of this topic is driven by the rapid progress in quantum computing and its significant implications for the security of cryptography. As quantum threats have the potential to make classical encryption methods ineffective, there has been a global shift towards post-quantum cryptography (PQC) as a crucial future step in protecting digital systems. Simultaneously, we have noted the urgent actions being taken by national financial institutions, such as the Reserve Bank of India (RBI), which are seeking partnerships with companies like McKinsey and Accenture to enhance cybersecurity in banking. Given that banks are major targets in the landscape of quantum threats due to their reliance on public-key infrastructure, we recognized a distinct need for a resilient, adaptable solution for the future. Our concept is to implement AI/ML-driven, plug-and-play adaptability within cryptographic systems, enabling banking infrastructure to adjust in real-time to new threats and algorithmic changes. This approach is in line with global initiatives from organizations like SWIFT and NIST, which stress the importance of agility and resilience during the transition to post-quantum systems. Thus, this project is not only technically pertinent but also strategically well-timed, providing a research-based, scalable framework that addresses an urgent real-world challenge in a vital sector.

6. Objective & Scope of the Project

The goal of this project is to design and propose a secure, AI-enhanced, crypto-agile framework specifically tailored for modern online banking infrastructure, such as those operated by central financial institutions. As advancements in quantum computing pose increasing threats to traditional public-key cryptography, there is a pressing need to integrate post-quantum cryptographic (PQC) readiness into real-world systems. This project focuses on creating a robust architecture that supports dynamic switching between cryptographic algorithms at runtime, ensuring adaptability to evolving security threats without any system downtime. By incorporating hardware acceleration technologies, such as FPGAs (Field-Programmable Gate Arrays), and a modular design, the solution provides high performance and flexibility.An AI and machine learning-driven control mechanism will facilitate intelligent decision-making for selecting ciphers based on performance, threat levels, and policy compliance. The system addresses critical aspects such as secure key management, polynomial arithmetic for PQC schemes, and real-time handling of cryptographic operations. It ensures compliance with widely accepted cryptographic standards while remaining scalable and deployable within critical, latency-sensitive environments like digital banking.This unified architecture is intended to serve as a future-ready foundation for cryptographic modernization efforts, offering security, agility, and operational continuity as the financial sector transitions into a quantum-resilient era.

7. Hardware & Software Requirements

7.1 Hardware

- 8GB RAM
- 64GB Storage
- Ubuntu OS
- Nvidia GeForce RTX 3050

7.2 Software

- Open Quantum Safe
- SP 800-22-tests-master
- Visual Studio Code
- TLS 1.3
- JWT
- PKCS#11
- OpenSC Project
- NetHSM

7.3 Frontend

- HTML
- CSS
- JS

7.4 Backend

- Python
- JWT

8. Final Deliverables

- An AI model that is compliant to regulations like PCI-DSS/NIST/GDPR
- A script that can automatically identify the best suited cryptographic algorithm according to the **sensitivity**, **medium of transport** & **system setup** of the bank
- A detailed report explaining how the selected encryption algorithm is best considering all the factors
- An detailed comparison between all the encryption algos with their advantage and disadvantage
- A microservice based approach which will help in cryptographic agility
- Design software and show how particular hardware setup will help in incorporating multiple cryptographic algorithms

9. References

1. https://www.researchgate.net/publication/367101711_Post-quantum_cryptographic_algorithm_identification_using_machine_learning
2. https://github.com/open-quantum-safe
3. https://docs.oasis-open.org/pkcs11/pkcs11-base/v2.40/os/pkcs11-base-v2.40-os.html
4. https://www.microsoft.com/en-us/research/project/post-quantum-tls/
5. https://github.com/OpenSC/OpenSC
6. https://www.consultancy.in/news/4020/reserve-bank-of-india-selects-mckinsey-and-accenture-for-ai-project
7. https://blogs.cisco.com/developer/how-post-quantum-cryptography-affects-security-and-encryption-algorithms?utm_source=chatgpt.com
8. https://www.nccoe.nist.gov/crypto-agility-considerations-migrating-post-quantum-cryptographic-algorithms?utm_source=chatgpt.com

Mentor Signature
2025-2026
Dr. Ashwini Rao