
Post-Quantum Cryptography for Securing Banking API: A Survey

Kshitij Dhake, Atharva Dhake, Kartik Tichkule, Abhinay Dhamankar & Sachin
Pande

*Department of Information Technology, SCTR's Pune Institute of Computer Technology,
Pune, India, kdhake289@gmail.com, atharvadhake01@gmail.com,
kartik.tichkule.11@gmail.com, agdhamankar@pict.edu, sspande@pict.edu*

Abstract.

Recent strides in quantum computing have posed a challenge to conventional classical cryptographic algorithms like RSA and Elliptic Curve Cryptography (ECC). With the progression of quantum computing, there is a possibility of vulnerability to traditional cryptography in the future, leading to significant concerns from the perspective of the security of the banking industry. In this survey, we will review the adoption of Post-Quantum Cryptography (PQC), focusing on specific schemes like CRYSTALS-Kyber or CRYSTALS-Dilithium, together with an approach involving hybrid cryptosystems, ensuring seamless implementation. In addition, several challenges related to computational costs, difficulties of integration, and the growing significance of flexible deployment of cryptography will be considered. In summary, the objective of the research is to help financial institutions and scholars determine efficient quantum-safe security systems that offer protection for banking APIs.

1. INTRODUCTION

The modern banking system relies significantly on APIs and operates on a digital platform through different functions like financial transactions, payments, authentication, and interaction. At present, these interactions are protected using conventional public key cryptography techniques. Public key cryptography has been quite dependable so far because of the very complex nature of mathematical calculations that cannot be solved easily by conventional means.

Progress in quantum computing is raising significant questions about the future effectiveness of standard encryption techniques. Algorithms like Shor's have the potential to compromise traditional public-key cryptography much faster than current computers. While fully functional quantum computers have yet to be released, experts warn that sensitive financial information encrypted today could be at risk once these powerful machines become a reality.

"A delay like that makes banks more vulnerable to quantum computing algorithms down the road because banks handle confidential financial information."

The rise of quantum technology has created an urgent need to safeguard financial data. To address this, researchers and standardization bodies are working on post-quantum

cryptography (PQC) algorithms designed to protect against threats from both classical and quantum computers. This survey reviews how NIST-approved PQC algorithms are being integrated into the security systems of banking institutions and evaluates their compatibility with TLS, OAuth 2.0, JWT, and mTLS protocols.

2. RELATED WORKS

Extensive research has explored the effects of quantum computing on cryptographic systems employed in financial and banking sectors. Standard cryptographic mechanisms are widely used for securing online banking and financial communications. However, these systems are vulnerable to compromise through quantum attacks leveraging Shor's algorithm.

Bettale, Oliveira & Dottax (2022) discuss post-quantum cryptography systems specifically designed for banking systems and how quantum-resistant protocols can be integrated into banking infrastructure. Ramamoorthy & Singh (2025) examine how quantum algorithms affect classical public-key cryptography and how PQC can replace traditional schemes. Gujjala (2023) presents a new multi-factor authentication scheme for online banking that employs post-quantum cryptography.

Existing research primarily addresses architectural aspects or develops systems using PQC to improve authentication. However, little research has specifically investigated the implementation of NIST-standardized PQC algorithms in banking API protocols such as TLS, OAuth 2.0, JWT, and mTLS. This survey bridges that gap.

3. CONTRIBUTIONS

This survey makes the following contributions:

- (1) Examines quantum security risks to banking APIs that use RSA and ECC cryptosystems, providing justification for adopting quantum-safe cryptography.
- (2) Discusses primary categories of PQC, focusing on security and performance of NIST-standardized schemes: Key encapsulation using ML-KEM, digital signing through ML-DSA and hash based authentication with SLH-DSA.
- (3) Assessing the applicability of Post-Quantum Cryptography (PQC) for securing bank APIs via TLS, OAuth 2.0, JSON Web Tokens (JWT), and mTLS.
- (4) Hybrid model analysis and their potential for making an enabling easy transmission to quantum-resistant cryptography.

4. EVALUATION METHODOLOGY

This section integrates the current literature and available benchmark data. No new experimental results are presented here. The purpose is to discuss the quantum threat model, evaluate the key categories of PQC algorithms, and evaluate the viability of PQC for banking API security.

4.1. *Quantum threat model*

Shor's Algorithm: provides a quick way to factorize large integers and calculate discrete logarithms, thus rendering RSA and Elliptic Curve Cryptography encryption algorithms

insecure. The RSA-2048 algorithm is just one of many that may be considered a serious threat to security in future years.

Grover's Algorithm: is superior to brute force search, resulting in reduced security levels for symmetric algorithms. AES-256 must be used instead for quantum-resistant security.

Harvest Now, Decrypt Later: involves the interception of ciphertexts currently and decryption in the future when quantum computers are more advanced. This attack model shows the importance of implementing PQC quickly to protect critical data.

4.2. Standards for Cryptography

As per NIST, there are three standards for Post-Quantum Cryptography. This safeguards against both classical and quantum architectures for attacks:

ML-KEM (FIPS 203): A key encapsulation mechanism utilizing a lattice-based cryptography algorithm, originating from the CRYSTALS-Kyber KEM. ML-DSA (FIPS 204) and SLH-DSA (FIPS 205): A digital signature algorithm.

These PQC standards will be implemented through the OQS initiative in transport layer security and application programming interface.

The Kyber and Dilithium cryptosystem standards provide authentication to protect OAuth 2.0, JSON Web Tokens (JWT), and mTLs.

4.3. Analysis of PQC algorithms and comparison

Table 1 gives a comparative study of major post quantum cryptographic algorithms with respect to security foundation, key size, performance and suitability for banking applications.

Property	ML-KEM-768	ML-DSA-65	FALCON-1024	SLH-DSA (L3)
Purpose	KEM	Signature	Signature	Signature
Cryptography Type	Lattice (MLWE)	Lattice (MLWE)	NTRU Lattice	Hash-Based
Public Key size	1.2 KB	1.9 KB	1.8 KB	48 B
Ciphertext size	1.1 KB	3.3 KB	1.2 KB	16 KB
Operation time	60–90 μ s	60–100 μ s	100 μ s	5–10 ms
Fit for Bank API	Excellent	Excellent	Moderate	Backup

TABLE 1. COMPARATIVE ANALYSIS OF PQC ALGORITHMS FOR BANKING APPLICATIONS.

Table 2 summarizes recommended PQC algorithm usage across various banking and financial applications based on performance and security characteristics.

Application	Main Algorithm Used	Backup / Alternative
TLS & Payment Gateways	ML-KEM-768 for secure key exchange	—
API Authentication	ML-DSA-65 for verifying identities	—
Digital Signatures	ML-DSA-65 as the primary signing method	SLH-DSA as a fallback option
Blockchain & High-Frequency Trading	FALCON-1024 for fast and secure signatures	ML-DSA-65 as backup
IoT & Embedded Devices	ML-DSA-44 optimized for lightweight devices	ML-KEM-512 as an alternative

TABLE 2. RECOMMENDED PQC ALGORITHM USAGE ACROSS BANKING APPLICATIONS.

4.4. PQC implementations in banking APIs

Hybrid methods combine Kyber and Dilithium with traditional cryptography for quantum resistance and backward compatibility. Hybrid protocols such as ECDHE + Kyber and ECDSA + Dilithium support secure API migration. PQC integration must address larger keys, computational overhead, and infrastructure compatibility. OQS and OpenSSL-OQS provide open-source tools for PQC and hybrid TLS integration.

5. DISCUSSIONS

Lattice-based schemes offer a good balance of security and efficiency for banking APIs. Classic McEliece provides strong security but has large keys, while SLH-DSA and FALCON suit specific requirements. Hybrid RSA/ECC + ML-KEM/ML-DSA approaches enable practical migration while supporting existing TLS, OAuth 2.0, JWT, and mTLS protocols.

6. CONCLUSION

Quantum computing threatens RSA and ECC, making PQC essential for banking API security. Lattice-based schemes are promising, while hybrid approaches support interoperability with existing systems. Future work should evaluate side-channel security, HSM performance, and low-latency financial applications.

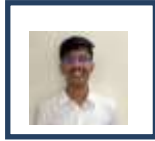
7. REFERENCES

- [1] Bettale, L., De Oliveira, M. & Dottax, E. 2022. Post-quantum protocols for banking applications. *In 4th PQC conference Proceeding*.
- [2] Gujjala, P.K.R. 2023. Quantum-enhanced multi-factor authentication framework for digital banking systems: a post-quantum cryptographic approach. *(IJMR)* 5(6).
- [3] National Institute of Standards and Technology (NIST). 2024. *Module-Lattice-Based Key-Encapsulation Mechanism Standard (ML-KEM), FIPS 203; Module-Lattice-Based Digital Signature Standard (ML-DSA), FIPS 204; Stateless Hash-Based Digital Signature Standard (SLH-DSA), FIPS 205*. Gaithersburg, MD: NIST.
- [4] Oleti, C.S. 2024. Post-quantum cryptographic architecture for secure banking: lattice-based implementation with blockchain integration. *(IJMR)* 6(2).
- [5] Pasupuleti, M.K. 2025. Post-quantum cryptography: algorithms and implementation challenges. *International Journal of Academic and Industrial Research Innovations* 5(6).
- [6] Ramamoorthy, U. & Singh, S. 2025. Post-quantum cryptography to secure future IT and financial systems. *IJARIE* 11(4): 3788–3792.
- [7] Rane, S.R., Shelake, V., Katte, T.B., Patil, S.V., Patil, D.V. & Musale, V. 2025. Quantum-resistant cryptographic algorithms: a comparative analysis for securing next-generation communication networks. *Journal of Information Systems Engineering and Management* 10(13s).

Biographies



Kshitij Dhake. Student, Department of Information Technology, SCTR's Pune Institute of Computer Technology, Pune, India



Atharva Dhake. Student, Department of Information Technology, SCTR's Pune Institute of Computer Technology, Pune, India



Kartik Tichkule. Student, Department of Information Technology, SCTR's Pune Institute of Computer Technology, Pune, India



Abhinay Dhamankar. Assistant Professor, Department of Information Technology, SCTR's Pune Institute of Computer Technology, Pune, India



Sachin Pande. Assistant Professor, Department of Information Technology, SCTR's Pune Institute of Computer Technology, Pune, India