International Journal of Advanced Scientific Research and Engineering Trends

ISSN: 2456-0774

Volume 10 Issue 1s (2026) | Pages: 139-144

Post-Quantum Public Key Infrastructure for Quantum-Resilient Banking Security

Rohit Kumar[1], Bindu Garg[2], Bishun Dev Mehta[3], Sumit Singh[4]

[1,2,3,4]Department of Computer Science & Engineering, Bharati Vidyapeeth (Deemed to be University), College of Engineering, Pune, India

Peer Review Information

Type: *Article*
Received: *02 April 2026*
Revised: *28 April 2026*
Accepted: *05 June 2026*
Published: *23 June 2026*

Abstract

The recent development in Quantum Computing is creating a potential threat to many Digital Banking Systems currently being used today. Most banking systems today use Classical Public Key Cryptography technologies like RSA and Elliptical Curve Cryptography that will be broken by a very powerful, large-scale Quantum Computer. Because financial data typically has to be kept private for an extended time period, this problem creates a major long-term risk.

This research proposes a Hybrid Post-Quantum Public Key Infrastructure (PKI) Framework for the improvement of banking security while maintaining compatibility with the existing banking systems. Rather than immediately replacing all classical cryptographic mechanisms, the Hybrid Post-Quantum Solution utilizes a combination of post-quantum algorithms along with traditional techniques. The proposed Hybrid Post-Quantum PKI model provides a reasonable and scalable path for banks to transition their systems from current quantum-vulnerable security infrastructures to new quantum-resilient security infrastructures.

Keywords: Post-Quantum Cryptography; Hybrid PKI; Banking Security; Quantum-Resilient Systems; Secure Authentication

How to Cite This Article

Kumar, R., Garg, B., Mehta, B. D., & Singh, S. (2026). Post quantum public key infrastructure for quantum resilient banking security. *International Journal of Advanced Scientific Research and Engineering Trends*, 10(1s), 139–144.

Introduction

Classical cryptographic methods like Elliptic Curve Cryptography (ECC) and RSA are being used to provide a Public Key Infrastructure system for digital banking applications that need to protect sensitive customer data and process large amounts of money. The use of ECC and RSA has provided a level of security that has been acceptable for many years but with recent advances in Quantum Computing it's now an issue whether they can be trusted long-term.

Quantum computers may be able to solve some mathematically intensive problems much quicker than classic machines. For example, Shor's algorithms have been shown to potentially break most public key encryption systems that use widely accepted public key cryptography. As a result of these threats to security in banks, and because so many types of information about bank customers need to stay secure for decades at a time, this work will develop a hybrid post-quantum Public Key Infrastructure (PKI).

To tackle the developing challenge, the research proposed in this paper investigates an alternative post-quantum PKI solution (a hybrid). The authors suggest that instead of substituting the current solutions entirely, they will use a combination of classical and post-quantum cryptography to develop their hybrid post-quantum PKI. By using this method, which is compatible with the current state of the art infrastructure and progressive, the authors propose that they can provide banks with greater security than they currently have today; as well as protect them from the potential threats resulting from the advancements of quantum computers.

Background and Related Work

Classical Public Key-infrastructure in banking

Public Key Infrastructure (PKI) is an essential part of modern banking systems because it enables secure communication methods through the use of digital signatures, user authentication, etc. The current classical PKI uses primarily RSA and ECC-based cryptography that depend upon very difficult mathematical problems to solve, e.g., factoring large integers and finding discrete logs. Although these cryptographic primitives have been built into most of today's banking architecture, there is no guarantee they will be safe when a future with "quantum" capabilities exists.

Post-Quantum cryptography

Beginning with the development of post-quantum cryptographic methods that will be resistant to a future computer being built using quantum computing, researchers have been developing new methods that will allow for encryption and decryption to continue to operate securely. The algorithms will be developed around mathematical problems related to lattice-based cryptography, code-based cryptography, hash-based cryptography, and multi-variate equation-based cryptography. Currently, organizations such as NIST are working towards selecting practical post-quantum cryptographic algorithms for use in commercial systems. At this time, there are many technical issues surrounding the potential use of these cryptographic algorithms including, but not limited to, their computational overhead, their required key sizes and how they can be implemented into existing cryptographic systems.

Hybrid cryptographic approaches

Hybrid cryptography uses a combination of both traditional (classical) and Post-Quantum methods. Using them together provides an added layer of security through "redundancy". In other words, as long as there are at least two different encryption methods being used in combination with each other, there will always be a secure method available - even if one of those methods is eventually compromised. For this reason, hybrid cryptography is well-suited for transition periods and mission-critical environments such as finance/banking where availability and reliability are paramount.

Threat Model and Motivation

The proposed banking system's potential threats are described with reference to Figure 1 that describes the main security threats that exist in a digital banking system. It also explains how future attacks based on quantum computing may target the classical cryptography technologies currently implemented in PKI. Algorithms like RSA and ECC have been identified as being at risk from these types of attack. Because the information (data) needs to remain protected for an extended period of time for banking systems, this threat is significant.

In addition to the potential for Quantum Attacks as noted in the graph, the most common types of threats (as shown in the graph) include: Credential Theft, Phishing, Certificate Forgery, Insider Misuse of Systems and Devices and Device Compromise. These various types of threats may impact users through the means of User Authentication, Certificate Authority Operations and Banking Servers; and/or during Transaction Processing.

The reason for developing this technology is to find ways to combat both traditional (conventional) cyber threats as well as emerging quantum-based cyber threats. This hybrid Post Quantum Public Key Infrastructure will provide stronger authentication for users, better protection of digital certificates, enhance transactional security in addition to providing a seamless integration with all legacy banking systems and maintaining the integrity of the entire system.

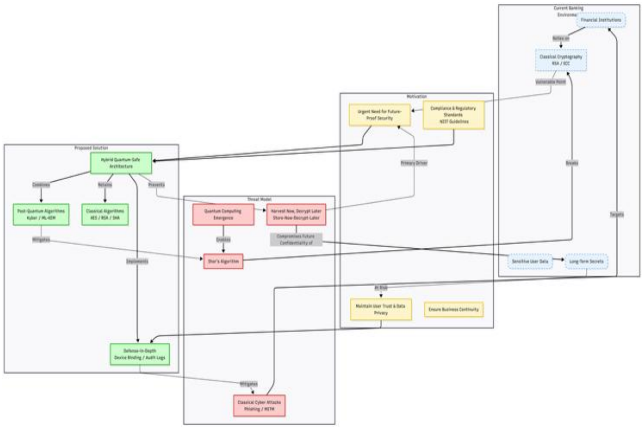

***Fig. 1**. Threat model and motivation*

Proposed Hybrid Post-Quantum PKI Architecture

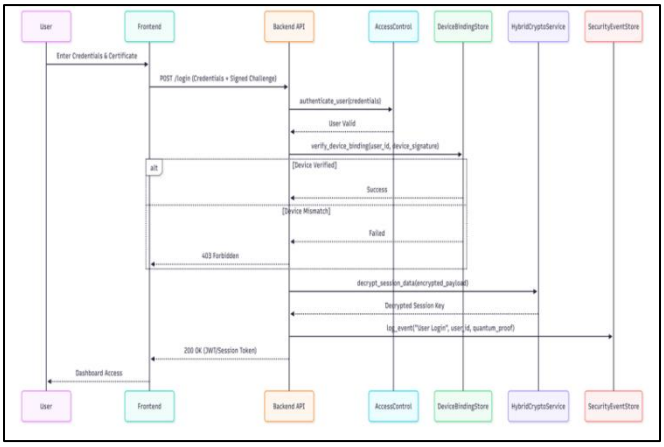

***Fig. 2**. Hybrid Post-Quantum PKI Architecture*

System Overview

Figure 2 depicts an overview of the total systems view of the proposed hybrid post-quantum PKI model for secure banking. The proposed PKI model combines two forms of cryptography – classical cryptography and post-quantum cryptography in a singular PKI framework. In this model, a central Certificate Authority (CA) will be responsible for all aspects of certificates including issuance, validation, and revocation for both end-users and Banking Servers. Hybrid Key Establishment will provide secure communications between user devices and Bank servers; Continuous Audit/Monitoring will also be implemented to ensure that there are no issues related to Accountability or Security throughout the entire System.

Architectural Components

As illustrated in figure 3, the proposed system contains the primary structural elements. The Certificate Authority (CA) functions as the central trusted element in this architecture. It employs two sets of public-private key pairs, one generated by classical cryptography and another employing post-quantum algorithms. Device binding and certificate-based login are used to establish secure user authentication. Hybrid encryption with digital signatures is employed to ensure transactional integrity. Auditing and logging mechanisms track and store information about all important transactions. These elements work together to produce an architecture that provides a scalable, secure and resilient to quantum attacks PKI solution applicable to banking systems.

Cryptographic Design

Hybrid Key Establishment

The Hybrid Key Establishment Approach (HKEA) generates both Classical Keys and Post Quantum Keys for use by the same communication protocol. Each of these types of keys generate key pairs as depicted in Figure X. For example; each type of key has its own public key and private key. In order to create secure Session Keys for communications between two parties; both Public Keys from each key generation process are utilized. If either the Classical Keys or Post Quantum Keys were compromised due to advances in cryptography or computational power; the remaining set of keys would still provide sufficient protection for continued secure communications.

Certificate Lifecycle

The Hybrid Key Generation System will use a combination of classical (RSA) and post-quantum (Kyber) methods for generating and utilizing keys. As illustrated below, each of the two types of keys will be utilized individually to generate a single, hybridized key-pair. Each type of key will be utilized individually to create a secure session-key. Session-keys will provide security as long as either of the two cryptographic schemes are still viable.

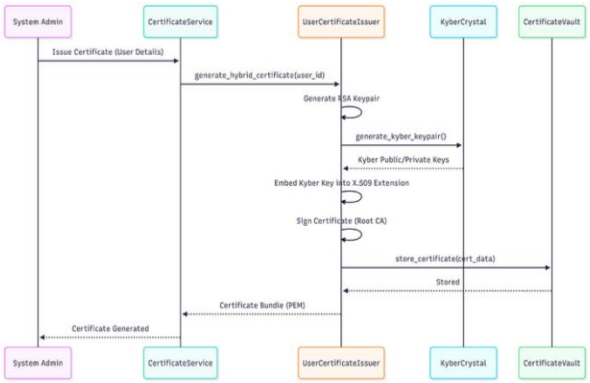

***Fig. 3**. Certificate Lifecycle*

Post Algorithms Used

Kyber lattice-based post-quantum encryption algorithm (a method of quantum-resistant key encapsulation) is used in the system because it has been recommended by standards organizations and offers stronger security than classical algorithms like RSA. Additionally, since both RSA and Kyber will be supported within the system simultaneously, this allows for an efficient transition from the use of classical algorithms to all-post-quantum algorithms.

Secure Banking Workflow

User registration

During enrollment for a new user during the registration process, the banking system will enroll the customer in their system with control. The Banking System creates a digital identity and issues an identity certificate using the Hybrid Public Key Infrastructure (PKI) Mechanism. This Certificate contains all Classical and Post Quantum credentials; therefore, the user's Identity will remain protected from future threats based on Quantum computing.

Authentication

When users want to use the System, authentication occurs via certificates and digital signatures (and then using some crypto-proofs) and credentials are checked for authenticity prior to the authorization being issued. Post-Quantum Signature Verification has been added to improve overall security by minimizing risks like impersonating a User or making a Replay Attack or Unauthorized Credential Misuse Attempt.

Transaction Processing

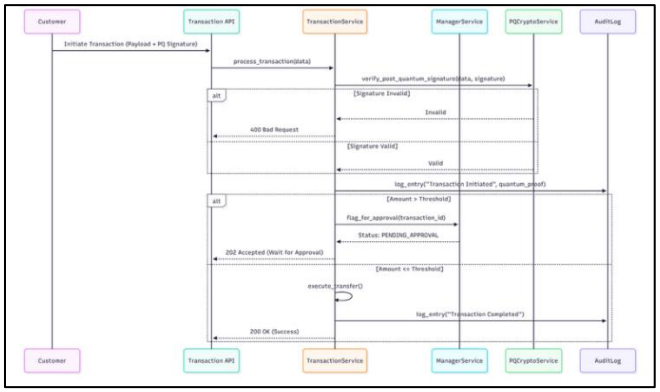

***Fig. 4.** Secure Banking Transaction Flow*

Beginning during User Registration, an account holder is added as a user in the Bank's System with a controlled enrollment method. A Digital Identity is established for the account holder and a Hybrid PKI Certificate is issued that contains both classical and Post Quantum

Credentials (PQC). The Hybrid PKI Certificate provides assurance that the Account Holder ID will remain protected from future quantum attacks.

Secure Banking Flow

The Hybrid Post-Quantum Public Key Infrastructure (PKI) System for Banking will improve banking security by combining Classical Cryptography with Quantum-Resistant Algorithms. The Hybrid Post-Quantum PKI System will protect Sensitive Data from both Current Cyber Threats as well as Future Attacks using Quantum Computing. The use of Certificates for Authentication and Post-Quantum Signature Verification will assist to eliminate Impersonation Attacks, Replay Attacks and Transaction Forgery. Device Binding and Role-Based Access Control will also reduce the risks associated with Unauthorized Access and Insider Misuse. Audit Logs that are secure and tamper-resistant will be used to increase Accountability and Traceability in Banking Systems as well as comply with Regulatory Requirements.

Performance Evaluation

The hybrid Post Quantum (PQ) Public Key Infrastructure (PKI) system's performance has been evaluated with respect to both the computation expense of performing the system's tasks as well as its usability. The additional computation required by PQ cryptographic processes increases the overall computation load over traditional (classical) methods; but the increase in computation time for banking applications is considered tolerable. All hybrid key pair generation and signature verification functions were performed at sufficient speed so that they did not produce significant delay in either the user authentication process or transaction processing. Overall, the results demonstrate that the PQ PKI system provides an appropriate balance between increased security and operational efficiency to support practical use in commercial banking environments.

Conclusion And Future Work

This paper introduces a hybrid PKI (Public Key Infrastructure) system which is based on post-quantum cryptography. This was developed as an improvement over traditional approaches to protecting banking application data due to possible threats from new and emerging quantum computing technologies. By providing both pre-quantum and post-quantum encryption capabilities in one single solution, this hybrid approach allows for high levels of security to be provided at the same time that it maintains compatibility with currently installed banking hardware.

In addition to providing stronger security for the authenticity of transactions and auditing of transactions within a banking environment, this system does so without requiring excessive overhead to achieve such enhanced security.

The next phase of development of this project will include integration of other applicable post-quantum digital signature schemes into the current hybrid system. Additionally, further optimization of performance may occur to allow for deployment of these systems at very large scale. Lastly, a goal for future testing includes deploying and using these systems in a production banking environment.

Further studies could involve complete migration strategy design to move from hybrid use of both pre-quantum and post-quantum methods of public key cryptography to complete use of post-quantum public key cryptography.

Acknowledgments

I appreciate the opportunity to express my gratitude to my project advisor for the help and guidance they have given me during the time I was working on this project. The continued guidance and encouragement they gave me were invaluable as they helped me shape and complete this project. Additionally, I would like to thank all researchers and writers who contributed to the body of knowledge of cryptography and post-quantum security.

Conflict of Interest Statement

The authors declare that they have no conflict of interest.

References

1. P. W. Shor, “Algorithms for quantum computation: Discrete logarithms and factoring,” *Proc. 35th Annual Symposium on Foundations of Computer Science*, Santa Fe, NM, USA, 1994, pp. 124–134.
2. M. Mosca, “Cybersecurity in an era with quantum computers: Will we be ready?” *IEEE Security & Privacy*, vol. 16, no. 5, pp. 38–41, Sep.–Oct. 2018.
3. NIST, *Post-quantum cryptography standardization*, National Institute of Standards and Technology, Gaithersburg, MD, USA, 2024.
4. D. J. Bernstein, J. Buchmann, and E. Dahmen, *Post-quantum cryptography*, Berlin, Germany: Springer, 2009.

5. L. Chen, S. Jordan, Y. Liu, D. Moody, R. Peralta, and D. Smith-Tone, "Report on post-quantum cryptography," NIST Internal Report 8105, 2016.
6. J. Hoffstein, J. Pipher, and J. H. Silverman, *An introduction to mathematical cryptography*, 2nd ed., New York, NY, USA: Springer, 2014.
7. E. Alkim, L. Ducas, T. Pöppelmann, and P. Schwabe, "Post-quantum key exchange—A new hope," *25th USENIX Security Symposium*, Austin, TX, USA, 2016, pp. 327–343.
8. R. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, vol. 21, no. 2, pp. 120–126, Feb. 1978.
9. V. Miller, "Use of elliptic curves in cryptography," *Advances in Cryptology—CRYPTO '85*, LNCS, vol. 218, Springer, 1986, pp. 417–426.
10. N. Koblitz, "Elliptic curve cryptosystems," *Mathematics of Computation*, vol. 48, no. 177, pp. 203–209, Jan. 1987.
11. D. Moody, "The transition to post-quantum cryptography," *IEEE Security & Privacy*, vol. 17, no. 3, pp. 60–63, May–Jun. 2019.
12. C. Peikert, "Lattice cryptography for the internet," *Post-Quantum Cryptography*, LNCS, vol. 8772, Springer, 2014, pp. 197–219.
13. ETSI, *Quantum-safe cryptography and security*, ETSI White Paper No. 8, 2015.
14. A. Bindel, J. Buchmann, M. Krämer, and A. McLauchlan, "Transitioning to a quantum-resistant public key infrastructure," *Proc. 2017 IEEE International Conference on Cyber Security and Cloud Computing*, New York, NY, USA, 2017, pp. 1–8.
15. S. Fluhrer, "Cryptographic agility and its role in transitioning to post-quantum cryptography," *IEEE Communications Magazine*, vol. 56, no. 8, pp. 26–31, Aug. 2018.
16. H. Krawczyk, "SIGMA: The 'SIGn-and-MAc' approach to authenticated Diffie-Hellman," *Advances in Cryptology—CRYPTO 2003*, LNCS, vol. 2729, Springer, 2003, pp. 400–425.
17. ISO/IEC 9594-8, *Information technology—Open systems interconnection—The directory: Public-key and attribute certificate frameworks*, ISO, Geneva, Switzerland, 2019.
18. A. Langley et al., "Experimenting with post-quantum cryptography," *Google Security Blog*, 2016.
19. M. Green and M. Smith, "Cryptopals crypto challenges," 2013, unpublished.
20. S. Gueron and V. Krasnov, "Fast prime field elliptic-curve cryptography with 256-bit primes," *IEEE Transactions on Computers*, vol. 64, no. 1, pp. 217–229, Jan. 2015.
21. P. Schwabe, R. Avanzi, and B. Smith, "Post-quantum TLS without handshake signatures," *ACM CCS Workshop on Post-Quantum Cryptography*, 2015.
22. A. Hülsing, D. Butin, S. Gazdag, J. Rijneveld, and A. Mohaisen, "XMSS: Extended hash-based signatures," RFC 8391, IETF, May 2018.
23. B. Schneier, *Applied cryptography: Protocols, algorithms, and source code in C*, 2nd ed., New York, NY, USA: Wiley, 1996.
24. R. Canetti, "Universally composable security: A new paradigm for cryptographic protocols," *Proc. 42nd IEEE Symposium on Foundations of Computer Science*, Las Vegas, NV, USA, 2001, pp. 136–145.
25. K. Lauter, "Post-quantum cryptography," *Notices of the American Mathematical Society*, vol. 66, no. 3, pp. 397–400, Mar.