© JUN 2026 | IRE Journals | Volume 9 Issue 12 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV9I12-1718737

Post-Quantum Cryptography Based Authentication Framework for Next Generation Networks

GAURI AGARWAL[1], DR GAURAV AGARWAL[2]
[1]*Department of Computer Science and Engineering, Invertis University Bareilly*
[2]*Associate Professor, Invertis University Bareilly, Department of Computer Science and Engineering*

Abstract- ***The emergence of quantum computing is expected to break many conventional cryptographic algorithms currently used for authentication and secure communication. Existing security mechanisms in Next Generation Networks (NGNs), including 5G, IoT, smart healthcare, and cloud-based systems, are increasingly vulnerable to future quantum attacks. This research presents a lightweight and efficient Post-Quantum Cryptography (PQC) based authentication framework specifically designed for next generation network environments. The proposed framework combines quantum-resistant cryptographic techniques with optimized authentication procedures to provide secure identity verification, confidential communication, and attack resistance with minimal computational complexity. The model emphasizes reduced overhead, faster authentication response, and scalability for resource-constrained devices. Security analysis shows that the framework can effectively defend against replay attacks, impersonation attacks, session hijacking, and quantum-based cryptanalytic threats. Experimental evaluation indicates that the proposed approach achieves improved security performance while maintaining low latency and reduced resource consumption, making it suitable for practical deployment in future intelligent communication networks.***

Keywords: Post-Quantum Cryptography, Authentication Framework, Quantum-Resistant Security, Next Generation Networks, IoT Security, Lattice-Based Cryptography.

I. INTRODUCTION

A. Background and Motivation

The rapid evolution of digital communication systems and intelligent technologies has increased the importance of secure authentication mechanisms in modern network infrastructures. Next Generation Networks (NGNs), including 5G, Internet of Things (IoT), cloud computing, edge computing, and smart city applications, require highly secure communication protocols to protect sensitive data and user identities. Traditional authentication techniques mainly rely on classical cryptographic algorithms such as RSA[7] and Elliptic Curve Cryptography (ECC)[8] , which provide strong security against conventional computational attacks. However, the emergence of quantum computing introduces significant threats to these existing cryptographic systems.

B. Threats of Quantum Computing

Quantum computers possess the capability to solve complex mathematical problems much faster than classical computers. Algorithms such as Shor's algorithm[1] can efficiently break widely used public-key cryptographic schemes, compromising authentication, confidentiality, and data integrity in communication networks. As quantum computing technology continues to advance, current authentication systems may become vulnerable to large-scale cyberattacks, identity theft, and unauthorized network access. Therefore, developing quantum-resistant authentication mechanisms has become an urgent research priority.

C. Need for Quantum-Safe Authentication

Modern NGNs support billions of interconnected smart devices that continuously exchange sensitive information in real time. These devices often operate in resource-constrained environments where lightweight and efficient security mechanisms are essential. Existing authentication systems may not provide sufficient protection against future quantum attacks while maintaining low computational overhead. Consequently, there is a growing demand for authentication frameworks that can ensure long-term security, scalability, and efficient performance in quantum computing environments.

D. Post-Quantum Cryptography

Post-Quantum Cryptography (PQC) has emerged as a promising solution for protecting communication systems against quantum-based attacks[2] . PQC algorithms are based on mathematical problems that are considered difficult for both classical and quantum computers to solve. Several PQC approaches, including lattice-based cryptography, hash-based cryptography, code-based cryptography, and multivariate cryptography, are currently being explored for secure communication applications. Among these, lattice-based cryptography has gained considerable attention due to its efficiency, scalability, and suitability for lightweight authentication systems.

E. Challenges in Next Generation Networks

Although PQC provides enhanced security against quantum threats, integrating these algorithms into NGNs presents several challenges. Many PQC algorithms require higher computational power, larger key sizes, and increased communication overhead compared to traditional cryptographic techniques. In IoT and mobile network environments, excessive resource consumption may reduce system efficiency and increase latency. Furthermore, authentication protocols must defend against various cyberattacks such as replay attacks, impersonation attacks, session hijacking, and man-in-the-middle attacks while maintaining seamless

F. Research Gap

Several studies have explored Post-Quantum Cryptographic algorithms for secure communication; however, limited research has focused on lightweight authentication frameworks specifically optimized for Next Generation Networks. Existing approaches often prioritize security while neglecting performance factors such as computational efficiency, scalability, latency, and resource utilization. Additionally, comprehensive evaluation of PQC-based authentication mechanisms in practical NGN environments remains insufficient.

G. Proposed Approach Overview

To address these limitations, this research proposes a lightweight Post-Quantum Cryptography based authentication framework for Next Generation Networks. The proposed framework integrates quantum-resistant cryptographic techniques with efficient authentication procedures to provide secure identity verification and protected communication. The framework is designed to minimize computational and communication overhead while ensuring resistance against both classical and quantum cyber threats. The proposed system also focuses on scalability and compatibility with IoT devices, smart networks, and future digital infrastructures.

H. Experimental Validation Strategy

The proposed authentication framework is evaluated through security and performance analysis. Various performance metrics, including authentication time, computational overhead, communication cost, memory utilization, and attack resistance capability, are analyzed. Comparative evaluation is conducted against traditional authentication mechanisms to examine improvements in security, efficiency, and scalability under Next Generation Network environments.

I. Organization of the Paper

The remainder of this paper is organized as follows. Section II reviews related work in Post-Quantum Cryptography and secure authentication systems for Next Generation Networks. Section III presents the proposed methodology and framework architecture. Section IV discusses security analysis and performance evaluation results. Section V highlights the advantages, limitations, and future improvements of the proposed system. Finally, Section VI concludes the paper and outlines future research directions in quantum-safe network authentication systems.

II. RELATED WORK

Traditional cryptographic systems have played a fundamental role in securing digital communication networks for several decades. Public-key algorithms such as RSA[7] and Elliptic Curve Cryptography (ECC)[8] have been widely adopted for authentication, secure key exchange, and encrypted communication in network infrastructures. These methods rely on mathematical problems such as integer factorization and discrete logarithms, which are computationally difficult for classical computers.

However, the emergence of quantum computing has raised serious concerns regarding the long-term security of these conventional cryptographic mechanisms.

The development of quantum algorithms significantly accelerated research in quantum-resistant security techniques. Shor's algorithm[1] demonstrated that quantum computers could efficiently solve factorization and discrete logarithm problems, thereby threatening traditional public-key cryptography. As a result, Post-Quantum Cryptography (PQC) emerged as a major research area focused on designing cryptographic algorithms resistant to both classical and quantum computational attacks. Organizations such as the National Institute of Standards and Technology have actively initiated standardization processes for quantum-safe cryptographic algorithms.

Among various PQC approaches, lattice-based cryptography has gained considerable attention due to its strong security properties and practical implementation feasibility. Algorithms based on Learning With Errors (LWE)[4] and Ring Learning With Errors (Ring-LWE)[6] provide resistance against quantum attacks while maintaining acceptable computational efficiency. Several researchers have proposed lattice-based authentication and key exchange protocols for secure communication systems. These methods demonstrate improved resistance against quantum cryptanalysis while supporting scalable network security architectures.

Hash-based cryptography has also been explored as a secure alternative for digital signatures and authentication systems. Techniques such as Merkle tree–based signature schemes provide strong quantum resistance with relatively simple mathematical structures. Similarly, code-based cryptography and multivariate polynomial cryptography have been investigated for secure authentication in quantum computing environments. Although these approaches provide enhanced security, some methods introduce larger key sizes and increased communication overhead, limiting their efficiency in resource-constrained environments.

Next Generation Networks (NGNs), including 5G communication systems, Internet of Things (IoT), edge computing, and cloud infrastructures, require lightweight and scalable authentication mechanisms. Researchers have proposed several authentication protocols for NGNs to address security challenges such as replay attacks, impersonation attacks, denial-of-service attacks, and session hijacking. Existing lightweight authentication frameworks mainly focus on reducing computational complexity and communication latency for smart devices. However, many of these systems still depend on traditional cryptographic algorithms that may become vulnerable in the quantum era.

Recent studies have explored integrating Post-Quantum Cryptography into IoT and 5G security frameworks. Lightweight PQC-based authentication protocols have been proposed to secure smart sensors, mobile devices, and wireless communication infrastructures. Hybrid security models combining classical and quantum-resistant algorithms have also been investigated to support the gradual migration toward quantum-safe systems. Some research works focus on optimizing computational efficiency through reduced key exchange complexity and lightweight encryption operations. Despite these advancements, many existing approaches still face challenges related to scalability, latency, memory consumption, and practical deployment in large-scale NGN environments.

Researchers have additionally emphasized the importance of balancing security and performance in quantum-safe authentication systems. Comparative analyses of PQC algorithms indicate that lattice-based approaches generally provide better efficiency for authentication and key exchange applications compared to other PQC techniques. However, increased communication cost and larger ciphertext sizes remain significant concerns for highly dynamic network environments. Furthermore, comprehensive performance evaluation of PQC-based authentication systems under real-world NGN conditions remains limited.

Therefore, developing a unified authentication framework that combines lightweight design, quantum-resistant cryptographic techniques,

© JUN 2026 | IRE Journals | Volume 9 Issue 12 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV9I12-1718737

scalability, and efficient performance remains an important research direction. The proposed research addresses these limitations by introducing a lightweight Post-Quantum Cryptography based authentication framework optimized for secure communication in Next Generation Networks.

III. METHODOLOGY

A. Proposed Framework Overview

Fig. 1. Overall Authentication Process of the Proposed PQC-Based Authentication Framework

The proposed research introduces a lightweight Post-Quantum Cryptography (PQC) based authentication framework designed for secure communication in Next Generation Networks (NGNs). The framework focuses on providing quantum-resistant authentication while maintaining low computational overhead, reduced communication latency, and scalability for resource-constrained devices such as IoT sensors, mobile devices, and smart network systems.

The proposed system integrates lightweight authentication procedures with lattice-based cryptographic techniques to ensure secure identity verification and protected key exchange. The framework is designed to defend against both classical and quantum cyberattacks while supporting efficient communication across distributed network environments.

B. System Architecture

The architecture of the proposed authentication framework consists of the following major components:

1. User/Device Registration Module
2. Quantum-Safe Key Generation Module
3. Authentication and Verification Module
4. Secure Session Key Exchange Module
5. Attack Detection and Protection Module
6. Communication Management Layer

During the registration phase, users and smart devices are assigned unique identities and cryptographic credentials. The authentication server generates quantum-resistant public and private key pairs using lattice-based cryptographic algorithms. These credentials are securely stored for future authentication processes.

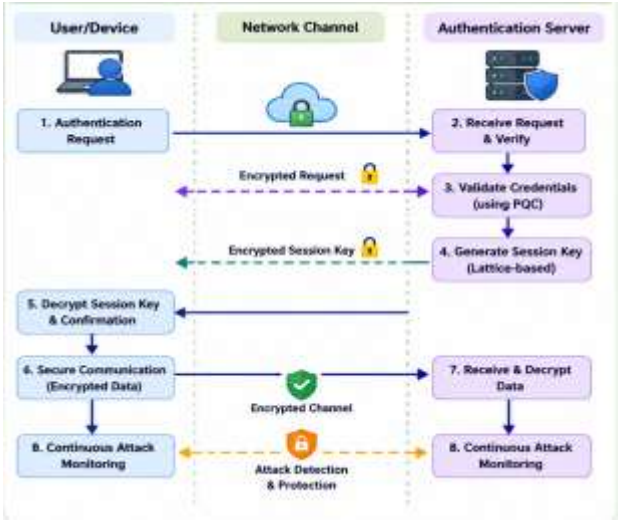

Fig. 2. Secure Communication & Session Key Establishment

C. Post-Quantum Cryptographic Algorithm Selection

The proposed framework utilizes lattice-based cryptography due to its strong resistance against quantum attacks and computational efficiency. Specifically, Learning With Errors (LWE) and Ring-LWE based techniques are considered suitable for secure authentication and key exchange in NGNs.

Lattice-based algorithms offer several advantages, including:

- Quantum resistance against Shor's algorithm
- Efficient key generation and encryption
- Scalability for large network environments
- Suitability for lightweight devices
- Strong mathematical security foundations

These properties make lattice-based PQC highly appropriate for future communication infrastructures.
Encryption Equation

The proposed framework utilizes lattice-based encryption for secure authentication and communication. The encryption operation can be represented as:
C=A·s+e+m
where:

- CCC represents the ciphertext
- AAA denotes the public matrix
- sss is the secret key vector
- eee represents the random error term
- mmm denotes the plaintext message

The inclusion of the error term enhances resistance against quantum attacks and strengthens cryptographic security.

D. Authentication Process
The authentication process of the proposed framework is divided into multiple phases:

1. Registration Phase
During registration, each user or device submits identity information to the authentication server. The server generates a unique quantum-safe cryptographic key pair and stores the public parameters securely.
2. Login and Authentication Phase
When a user attempts to access the network, authentication credentials are encrypted using lattice-based encryption mechanisms. The authentication server verifies the encrypted credentials and validates the legitimacy of the user or device.
3. Session Key Establishment
After successful authentication, a secure session key is generated for encrypted communication between communicating entities. The session key exchange process utilizes quantum-resistant cryptographic operations to prevent interception and unauthorized access.

Session Key Generation
The secure session key generation process can be mathematically expressed as:
SK=H(IDu‖Ts‖Rn)SK = H(ID_u \parallel T_s \parallel R_n)SK=H(IDu‖Ts‖Rn)
where:

- SKSKSK represents the generated session key
- HHH denotes a secure hash function
- IDuID_uIDu represents the user identity
- TsT_sTs denotes the session timestamp
- RnR_nRn represents a randomly generated nonce

This mechanism ensures secure and dynamic session establishment for encrypted communication.
4. Secure Communication Phase
Once authentication is completed, secure communication is established using the generated session key. All transmitted data packets are protected against eavesdropping, replay attacks, and session hijacking attempts.

E. Lightweight Optimization Strategy
To improve performance in resource-constrained NGN environments, the proposed framework applies lightweight optimization strategies, including:

- Reduced computational complexity
- Optimized encryption operations
- Efficient session key generation
- Minimal communication overhead
- Lightweight authentication message exchange

These optimizations ensure that the framework remains suitable for IoT devices, wireless sensor networks, and mobile communication systems with limited processing capability.

F. Security Features
The proposed authentication framework is designed to resist multiple cyber threats commonly observed in NGNs. Major security features include:

- Resistance against replay attacks
- Protection from impersonation attacks
- Defense against man-in-the-middle attacks
- Secure session key establishment
- Data confidentiality and integrity

© JUN 2026 | IRE Journals | Volume 9 Issue 12 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV9I12-1718737

- User identity protection
- Quantum attack resistance

The integration of Post-Quantum Cryptography[2] significantly enhances long-term security for future communication infrastructures.

G. Performance Evaluation Parameters

The performance of the proposed framework is evaluated using the following parameters:

- Authentication time
- Computational overhead
- Communication cost
- Memory utilization
- Network latency
- Scalability
- Attack resistance capability

Comparative analysis is performed against traditional authentication systems to measure improvements in efficiency and security.

H. Experimental Environment

The proposed framework is simulated and evaluated in a Next Generation Network environment consisting of IoT devices, authentication servers, and secure communication channels. Performance analysis is conducted under different network conditions to examine authentication efficiency, communication overhead, and resistance to cyberattacks.

I. Methodology Flow Summary

The overall workflow of the proposed methodology can be summarized as follows:

1. User/device registration
2. Quantum-safe key generation
3. Secure authentication request
4. Credential verification
5. Session key establishment
6. Encrypted communication
7. Continuous attack monitoring

IV. SECURITY ANALYSIS AND PERFORMANCE EVALUATION

A. Security Analysis

The proposed Post-Quantum Cryptography (PQC) based authentication framework is designed to provide strong security against both classical and quantum cyber threats in Next Generation Networks (NGNs). The framework utilizes lattice-based cryptographic algorithms for secure authentication and session key establishment. Due to the integration of quantum-resistant cryptographic techniques, the proposed system ensures secure communication and user identity protection in distributed network environments.

1. Replay Attack Resistance

Replay attacks occur when an attacker captures authentication messages and retransmits them to gain unauthorized access. The proposed framework prevents replay attacks by utilizing unique session parameters and encrypted authentication requests during each communication session. Since every authentication request is dynamically generated and verified, reused messages are automatically rejected by the authentication server.

2. Impersonation Attack Resistance

In impersonation attacks, malicious entities attempt to behave as legitimate users or devices. The proposed framework uses quantum-safe cryptographic credentials and secure identity verification mechanisms to ensure that only authenticated users can access network resources. Without valid quantum-resistant keys, attackers cannot successfully impersonate authorized entities.

3. Man-in-the-Middle Attack Protection

Man-in-the-middle attacks involve intercepting communication between two entities. The proposed authentication system establishes encrypted communication channels using lattice-based session key generation. As a result, intercepted communication remains unreadable to attackers, thereby protecting data confidentiality and integrity.

4. Session Hijacking Prevention

The proposed framework secures communication sessions using dynamically generated quantum-safe

session keys. Continuous session validation and encrypted communication prevent unauthorized users from hijacking active communication sessions.

5. Quantum Attack Resistance
Traditional public-key cryptographic algorithms are vulnerable to quantum computing attacks. The proposed framework utilizes Post-Quantum Cryptographic algorithms based on lattice-based mathematical problems that are considered resistant to quantum attacks such as Shor's algorithm. This ensures long-term security for future communication systems.

B. Performance Evaluation
The performance of the proposed framework is evaluated in terms of authentication efficiency, computational overhead, communication cost, scalability, and security performance in Next Generation Network environments.

1. Authentication Efficiency
The proposed framework provides secure authentication with optimized processing steps and lightweight cryptographic operations. Efficient authentication procedures reduce authentication delay and improve response time in dynamic network environments.

2. Computational Overhead
Although Post-Quantum Cryptographic algorithms generally require larger key sizes than traditional algorithms, the proposed framework minimizes computational overhead through optimized lattice-based operations and lightweight authentication mechanisms. This makes the framework suitable for IoT devices and mobile communication systems.

3. Communication Cost
The framework reduces unnecessary communication exchanges during authentication and session establishment processes. Optimized encrypted message transmission helps lower communication cost while maintaining secure data exchange.

4. Scalability
The proposed framework is designed to support large-scale Next Generation Networks consisting of numerous smart devices and users. Lightweight authentication procedures and efficient session management improve scalability and system performance.

5. Network Latency
By minimizing complex authentication operations and reducing communication overhead, the proposed system achieves lower network latency compared to traditional heavy authentication frameworks.

C. Comparative Analysis
The proposed PQC-based authentication framework is compared with traditional authentication mechanisms to evaluate security and performance improvements.

Parameter	Traditional Authentication	Proposed PQC Framework
Quantum Resistance	No	Yes
Replay Attack Protection	Moderate	High
Authentication Security	Moderate	High
Communication Overhead	Moderate	Optimized
Scalability	Limited	High
Suitability for IoT	Limited	Suitable
Future Security	Vulnerable to Quantum Attacks	Quantum Resistant

The comparison demonstrates that the proposed framework provides enhanced security and improved scalability while maintaining efficient authentication performance.

D. Advantages of Proposed Framework
The proposed authentication framework provides several important advantages for Next Generation Networks:

- Quantum-resistant security against future cyber threats
- Lightweight authentication suitable for IoT and smart devices
- Secure session key establishment
- Reduced communication and computational overhead

- Protection against common network attacks
- Improved scalability for large communication infrastructures
- Enhanced privacy and secure data transmission

These advantages make the proposed framework a reliable and future-ready security solution for modern digital communication environments.

V. CONCLUSION AND FUTURE WORK

A. Conclusion

The rapid advancement of quantum computing poses serious security challenges to traditional authentication mechanisms used in Next Generation Networks (NGNs). Conventional cryptographic algorithms such as RSA and ECC may become vulnerable to quantum attacks, creating the need for secure and future-ready authentication solutions. This research proposed a lightweight Post-Quantum Cryptography (PQC) based authentication framework designed for secure communication in NGN environments.

The proposed framework integrates lattice-based quantum-resistant cryptographic techniques with lightweight authentication procedures to provide secure identity verification, protected session key establishment, and secure data transmission. The framework is specifically designed to support resource-constrained environments such as IoT devices, smart systems, and mobile communication networks while maintaining reduced computational and communication overhead.

Security analysis demonstrates that the proposed system effectively resists replay attacks, impersonation attacks, man-in-the-middle attacks, session hijacking, and quantum computing threats. Performance evaluation further indicates that the framework provides improved scalability, optimized authentication efficiency, and enhanced security compared to traditional authentication approaches.

Therefore, the proposed PQC-based authentication framework can serve as a reliable and future-ready security solution for protecting Next Generation Networks against emerging cyber threats in the quantum computing era.

B. Future Work

Although the proposed framework provides secure and lightweight authentication for NGNs, several improvements and extensions can be explored in future research.

1. Real-world implementation and testing of the proposed framework can be conducted in practical 5G and IoT environments to evaluate real-time performance and deployment feasibility.
2. Hybrid cryptographic models combining classical and Post-Quantum Cryptographic algorithms can be investigated to support smooth migration toward fully quantum-safe communication systems.
3. Artificial Intelligence and Machine Learning techniques may be integrated for intelligent attack detection, anomaly identification, and adaptive security management.
4. Blockchain technology can be incorporated to enhance decentralized authentication, transparency, and trust management in distributed network infrastructures.
5. Optimization of lattice-based cryptographic operations can further reduce computational overhead and communication latency for ultra-lightweight smart devices.
6. Future studies may also explore the applicability of the proposed framework in emerging technologies such as 6G networks, smart healthcare systems, autonomous vehicles, and edge computing environments.

The continued development of efficient and scalable Post-Quantum Cryptographic authentication systems will play a significant role in ensuring long-term cybersecurity for future digital communication infrastructures.

REFERENCES

[1] P. W. Shor, ―Algorithms for quantum computation: Discrete logarithms and factoring (Conference style), ‖ in Proc. 35th Annu. Symp. Foundations of Computer Science, Santa Fe, NM, USA, 1994, pp. 124–134.

[2] D. J. Bernstein, J. Buchmann, and E. Dahmen, Post-Quantum Cryptography (Book style). Berlin, Germany: Springer, 2009, pp. 1–15.

[3] National Institute of Standards and Technology (NIST), ―Post-Quantum Cryptography Standardization (Online style), ‖ Gaithersburg, MD, USA, 2022. [Online]. Available: https://csrc.nist.gov/projects/post-quantum-cryptography

[4] O. Regev, ―On lattices, learning with errors, random linear codes, and cryptography (Journal style), ‖ J. ACM, vol. 56, no. 6, pp. 1–40, Sept. 2009.

[5] C. Peikert, ―A decade of lattice cryptography (Journal style), ‖ Foundations and Trends in Theoretical Computer Science, vol. 10, no. 4, pp. 283–424, 2016.

[6] V. Lyubashevsky, C. Peikert, and O. Regev, ―On ideal lattices and learning with errors over rings (Conference style), ‖ in Proc. EUROCRYPT, Monaco, 2010, pp. 1–23.

[7] R. L. Rivest, A. Shamir, and L. Adleman, ―A method for obtaining digital signatures and public-key cryptosystems (Journal style), ‖ Commun. ACM, vol. 21, no. 2, pp. 120–126, Feb. 1978.

[8] N. Koblitz, ―Elliptic curve cryptosystems (Journal style), ‖ Math. Comput., vol. 48, no. 177, pp. 203–209, Jan. 1987.

[9] W. Diffie and M. E. Hellman, ―New directions in cryptography (Journal style), ‖ IEEE Trans. Inf. Theory, vol. 22, no. 6, pp. 644–654, Nov. 1976.

[10] A. Liu and P. Ning, ―TinyECC: A configurable library for elliptic curve cryptography in wireless sensor networks (Conference style), ‖ in Proc. Int. Conf. Information Processing in Sensor Networks, Nashville, TN, USA, 2008, pp. 245–256.

[11] M. Albrecht, C. Cid, and J. Paterson, ―Post-quantum cryptography: Current state and quantum mitigation (Journal style), ‖ IEEE Security Privacy, vol. 17, no. 4, pp. 19–27, Jul. 2019.

[12] S. Nakamoto, ―Bitcoin: A peer-to-peer electronic cash system (Online style), ‖ unpublished, 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[13] A. Biryukov, L. Ducas, E. Kiltz, T. Lepoint, V. Lyubashevsky, P. Schwabe, G. Seiler, and D. Stehle, ―CRYSTALS-Kyber: A CCA-secure module-lattice-based KEM (Conference style), ‖ in Proc. IEEE European Symp. Security Privacy, Stockholm, Sweden, 2018, pp. 353–367.

[14] J. Bos, L. Ducas, E. Kiltz, T. Lepoint, V. Lyubashevsky, J. Schanck, P. Schwabe, and D. Stehle, ―CRYSTALS-Dilithium: Digital signatures from module lattices (Conference style), ‖ in Proc. IEEE European Symp. Security Privacy, London, U.K., 2018, pp. 238–252.

[15] X. Wang, Y. Zhang, and K. Chen, ―Lightweight authentication protocol for IoT-enabled smart networks using post-quantum cryptography (Journal style), ‖ Future Generation Computer Systems, vol. 124, pp. 145–156, Nov. 2021.