ACADEMIA Tech Frontiers Journal

DOI: 10.63056

Post-Quantum Cryptography for Next-Generation Communication Networks

Daniyal Zaheer[a]
[a] *Department of Computer Science, Virtual University, Islamabad, Pakistan*
daniyalzaheer139@gmail.com

Article Info:
Received: June 16, 2025
Revised: July 11, 2025
Accepted: July 30, 2025
Corresponding Author:
Daniyal Zaheer

ABSTRACT

The potential of the swift development of quantum computing is an extreme danger to the traditional cryptographic programs, and they are the foundation of the modern communication infrastructure. RSA and ECC are classical public-key algorithms that can be successfully quantum-attacked, in particular, Shor's algorithm can easily factor large integers and calculate discrete logarithms (Bernstein et al., 2017). The Post-Quantum Cryptography (PQC) has become the key to secure the next-generation communication networks against these threats, which relies on lattice problem-based algorithms, hash-based based algorithms, multivariate polynomials-based algorithms, and code-based cryptography. The paper examines the concepts, design, and implementation issues of PQC within current network infrastructure focusing on the secure transmission of data, authentication, and key management in the upcoming 5G and 6G networks. The approach will include the survey of existing algorithms of PQC, model the integration of protocol in the communication systems and test computational efficiency, security strength, and scalability. It has been found that PQC is suitable to protect network communications against quantum attackers, and achieves reasonable performance, though trade-offs can be seen in terms of computation overhead, key size, and latency. The research offers understanding to the researcher, network engineers and policy makers in order to adopt quantum resistant cryptography protocols to secure the confidentiality, integrity and authenticity of information in the future communication networks.

Keywords:
Post-Quantum Cryptography, Quantum computing, lattice-based cryptography, hash-based signature, multivariate cryptography, code-based cryptography, 5G security, 6G networks.

INTRODUCTION

The ongoing dynamic development of communication networks, such as the ubiquitous implementation of 5G and the future installation of 6G systems, has improved the possibilities of data transmission, ultra-low latency, and high reliability in many different applications from Internet of Things (IoT) to autonomous systems and critical infrastructure (Zhang et al., 2020). With the introduction of quantum computing, however, there are whole new security concerns on the classical cryptographic tools that have kept digital communications safe throughout the decades. A quantum poly time algorithm like Shor algorithm can be used to crack most popular cryptosystems based on the principle of public-key cryptology, including RSA and elliptic-curve cryptography (ECC) by factoring large numbers and solving discrete logarithm problems, making them insecure when combined with quantum adversaries (Bernstein et al., 2017). With the development of quantum computing hardware on the side of practical implementation, the secure communication networks against quantum-enabled attacks have become an urgent concern.

Post-Quantum Cryptography (PQC) is a cryptographic algorithms that has been developed in a manner that it is resistant to quantum computers attacks. Scholarly of classical cryptography, PQC is based on mathematical problems that are hard to solutions not only to quantum machines but also to quantum machines, including lattice-

based problems, multivariate polynomial systems, hash-based constructions, and code-based cryptographic schemes (Chen et al., 2016). Lattice-based cryptography, an example is based on the hardness of such problems as the Shortest Vector Problem (SVP) and Learning With Errors (LWE), that are considered to be resistant to both classical and quantum attacks (Peikert, 2016). Hash-based signature schemes are cryptographic hash schemes that make use of cryptographic hash functions to produce one-time or few-time signature such that they offer high security guarantees against quantum adversaries along with relative simplicity in implementation (Buchmann et al., 2011). Additional variations on PQC Multivariate and code-based cryptography provide further diversity of PQC methods, providing other ways to implement public-key encryption and other digital signatures in quantum-secure systems.

Introduction of PQC in next-generation communication networks has opportunities and challenges. Fifth-generation and 6G networks are defined by large numbers of devices, high data rate, low latency, and support to new applications, including autonomous vehicles, industrial internet of things, and real-time health surveillance (Zhang et al., 2020; Li et al., 2021). The use of PQC in such contexts must be attentive to the efficiency of the computation, key sizes, overhead of bandwidth and latency. Some PQC schemes have large key sizes that can affect network performance, whereas the computationally intensive algorithms can be a challenge to resource-constrained IoT devices (Chen et al., 2016). Hence, it is important to consider trading off between the security strength and operational efficiency in order to implement it practically.

Recent research highlights the standardization and appraisal of PQC algorithms as an important process to the prospective secure communications. A Post-Quantum Cryptography standardization project was started by the National Institute of Standards and Technology (NIST), the candidate algorithms are proposed in the areas of public-key encryption, key exchange, and digital signatures (Chen et al., 2016). Some of the candidates, including CRYSTALS-Kyber (lattice-based key encapsulation) and CRYSTALS-Dilithium (lattice-based digital signature), have good security and efficiency characteristics that can be used in communication protocols. Algorithms of PQC have been proven to run with reasonable performance overhead on existing network infrastructures, although further optimization and protocol modification are needed to make them effective in large scale (Peikert, 2016; Li et al., 2021).

Along with algorithmic deliberations, secure key management, authentication, and protocol design are all a part of the provision of quantum-resilient communication networks. Transitional schemes Hybrid cryptographic schemes based on classical and post-quantum algorithms are suggested as an intermediate to keep the security intact until infrastructures are fully upgraded (Mosca, 2018). These mixed solutions deliver short-term advantages in terms of security and enable progressive integration of PQC that do not cause major inconveniences to current systems. Moreover, at network-level, work on the integration of network-level security, such as the adaptation of transport-layer security (TLS), IPsec, and 5G security architecture to PQC is needed to provide end-to-end quantum-safe communication (Zhang et al., 2020).

PQC also has extensive implications on industry, government and regulatory systems. Finance, healthcare, energy and defense are critical infrastructures that are highly dependent on the security of communications and should go ahead to ensure data confidentiality, integrity, and authenticity against quantum attacks. Migration plans, standards of compliance, and interoperability issues are some of the considerations that policymakers and network operators have to make when switching to quantum-resilient cryptography (Mosca, 2018).

In short, the introduction creates the sense of urgency of post-quantum cryptography in the process of ensuring the next-generation communication networks are not compromised by the new threat of quantum computing. It also mentions the weakness of classical cryptography, presents the use of lattice-based, hash-based, multivariate problems, and code-based algorithms in PQC, and underlines their difficulty in integrating with 5G and 6G systems. This paper offers a basis to apply the advanced, quantum-resistant security solutions to the contemporary communication systems by considering the algorithmic performance, network limitations, and hybrid deployment practices (Bernstein et al., 2017; Chen et al., 2016; Peikert, 2016; Mosca, 2018; Zhang et al., 2020).

LITERATURE REVIEW

Quantum computing offers a serious threat to the traditional cryptography that forms the basis of modern communication networks. In classical public-key cryptosystems, like RSA, ECC, and Diffie-Hellman, the hardness of integer factorization or discrete logarithm problems, which can be effectively solved using quantum algorithms such as the Shor algorithm, is used (Bernstein et al., 2017). As a result, such common encryption and authentication techniques are deemed to be insecure in a post-quantum world, and the cryptographic primitives resistant to quantum attacks should be developed. Post-Quantum Cryptography (PQC) is a collection of algorithms that are resistant to such attacks of classical and quantum computers and targets computational problems that are thought to be resistant to quantum computers, such as lattice-based problems, multivariate polynomial systems, hash-based signatures and code-based cryptography (Chen et al., 2016).

Lattice-based cryptography has received great interest because it provides great security requirements and has been shown to be practical. Key exchange, public-key encryption and digital signature algorithms like Learning With Errors (LWE) and Ring-LWE are built on the underlying algorithms (Peikert, 2016). Even the quantum

computers can no longer solve lattice problems, and thus, it provides quantum computers with the best choice to ensure long-term secure communications. CRYSTALS-Kyber is a lattice-based key encapsulation mechanism that has been identified as one of the top candidates in the NIST PQC standardization procedure due to its trade-off of security, computational efficiency, and a sizeable key and ciphertext (Chen et al., 2016). Likewise, CRYSTALS-Dilithium offers a digital signature scheme based on lattices, which is highly resistant to both classical and quantum attacks at a cost the scheme has a high efficiency in verification and signature generation. It has been shown that lattice-based schemes may be incorporated into network protocols with controllable overhead and can therefore be deployed in 5G and future 6G networks (Zhang et al., 2020).

Another direction towards quantum-resistant security is given by hash-based cryptography (and especially hash-based digital signatures). Other schemes like XMSS (eXtended Merkle Signature Scheme) and LMS (Leighton-Micali Signature) use the one-way property of cryptographic hash functions to produce secure stateful signatures (Buchmann et al., 2011). Hash based signatures are resistant to quantum attacks as long as the underlying hash functions are resistant to quantum attacks. Such schemes are especially beneficial in the applications where it is essential to have long-term signature security like software updates, the evaluation of certificate authorities and their communications with critical infrastructure. Nonetheless, the requirement of state administration and the restriction of a number of signatures on the key pair make the implementation strategies considerate and reliable and useful.

Another type of PQC algorithms is based on solving systems of multivariate equations (polynomials) over finite fields, and is called multivariate cryptography. Multivariate public-key schemes are very efficient in generating and verifying signature but can be characterized by increased key sizes (Ding et al., 2017). The algorithms scale well to devices that have limited computational resources, e.g. IoT sensors and edge devices, and need fast authentication. Code-based cryptography, a notable example being the McEliece encryption scheme, is based on the difficulty of decoding random linear codes and has survived decades of cryptanalytic attack, and offers high security levels against classical and quantum attacks (Bernstein et al., 2017). Though in code-based schemes, large public keys are usually used, there is ongoing research to reduce the key size and computation efficiency to be feasible to use over a network.

The process of incorporating PQC into the next-generation communication networks has several challenges. New networks, such as 5G and 6G, feature ultra-low latency, massively connected devices, high-throughput and serve applications like autonomous systems, industrial Internet of Things, and telemedicine (Li et al., 2021). The PQC algorithms would have to be applied in these settings with the consideration of balance of security strength and flexibility with bandwidth constraints and device limitations. Research indicates that hybrid cryptographic methods, which are a combination of classical and post-quantum algorithms, may be used as interim measures to secure the transmission of sensitive messages but with slow PQC transition (Mosca, 2018). Hybrid protocols are backwards compatible and offer immediate security gains, and an attack by near-term quantum-capable adversaries is reduced.

Some of the researchers have studied the effect of PQC on protocol design as well as network performance. As an example, the incorporation of lattice-based key exchange protocols into Transport Layer Security (TLS) and IPsec has been demonstrated to offer quantum-resilient communication channels with no comparable latency and computation cost (Chen et al., 2016; Peikert, 2016). On the same note, post-quantum TLS simulation research on 5G networks suggests that the increment in latency can be controlled, particularly when the implementation of the post-quantum TLS is optimized and the key management strategy is efficient. PQC deployment in IoT networks focuses on the use of lightweight cryptographic functions, including multivariate schemes and hash-based signature, to support resource-constrained devices without compromising the security of the authentication and confidentiality of the system (Li et al., 2021).

It has also been pointed out in research that standardization and interoperability are essential in the adoption of post-quantum cryptography. NIST PQC standardization project gives an model of how candidate algorithms are evaluated in terms of security, efficiency and implementability. Standardized algorithms including CRYSTALS-Kyber, CRYSTALS-Dilithium, Falcon, and SPHINCS+ help to deploy and integrate across platforms and integrate with commercial and industrial network infrastructures (Chen et al., 2016). Moreover, the investigation of hybrid schemes and protocol modifications will help in developing robust migration paths of the legacy systems that will be able to maintain continuity of the safe communications in the process of passing to post-quantum-safe networks.

Besides algorithmic and protocol issues, secure key management and lifecycle practices are also important to the effective deployment of PQC. Cryptographic key management, including generation, distribution, rotation, and revocation, will need to support the special needs of quantum-resistant hash function, including more and larger key sizes and a stateful operation (Mosca, 2018). The network operators also have to address the performance trade-offs such as the computation, storage and bandwidth requirements to have scalable and secure network operations. Studies have shown that a combination of equally careful optimization of algorithm parameters and hybrid solutions can alleviate most of these issues, and PQC is becoming practical in large-scale communication networks (Zhang et al., 2020).

Lastly, the literature focuses on the larger implication of PQC in achieving critical infrastructures and sensitive communications. Secure data exchanges are of great importance to finance, healthcare, energy, and defense spheres, and they are specifically susceptible to quantum-enabled attacks. To prepare these sectors to a post-quantum environment, it is necessary to actively evaluate the cryptographic resources, detect the components that are sensitive to quantum, and deploy quantum-resistant protocols gradually (Mosca, 2018). The literature is categorical in pointing out that concerted action amongst the researchers, industry players, and policymakers is urgently needed to enable the seamless adoption of next-generation communication networks.

Overall, the literature shows that post-quantum cryptography offers the necessary means of protecting the next-generation communication network against the current menace of quantum computing. There are lattice-based, hash-based, multivariate and code-based algorithms that provide different methods of key exchange, encryption and digital signatures with their own benefits and implementation issues. Integration of PQC in 5G, 6G and IoT networks poses challenges concerning computational efficiency, key management, protocol adaptation and hybrid deployment which is the way forward however ongoing research and standardization efforts offer potential solutions to adoption. Future research will aim at maximizing the performance of PQC, enabling interoperability, and coming up with a strong migration plan to attain secure and quantum resistant communication infrastructures (Bernstein et al., 2017; Chen et al., 2016; Peikert, 2016; Mosca, 2018; Li et al., 2021; Zhang et al., 2020).

METHODOLOGY

This study methodology aimed at assessing the viability, functionality and integration issues of post-quantum cryptographic (PQC) algorithms in the next-generation communications systems, such as 5G and future 6G communication systems. Multi-phase approach was used, which involved analysis of algorithms, testing which was conducted by simulation, and protocol analysis. First of all, an overview of the existing PQC algorithms has been provided, with the emphasis on lattice-based schemes (e.g., CRYSTALS-Kyber, CRYSTALS-Dilithium), hash-based signatures (e.g., XMSS, SPHINCS+), multivariate-based public-key schemes, and code-based encryption methods (Chen et al., 2016; Peikert, 2016). This review influenced the choice of algorithms that compromise security strength, computational efficiency, key size, and is appropriate to use in the current communication infrastructures.

Next, the datasets that depict network communication situations were created in order to emulate real-life operations. These covered transport-layer security (TLS) and Internet Protocol security (IPsec) message exchanges, as well as protocols that are specific to IoT, and covered a wide variety of traffic patterns, device constraints, and latency requirements (Zhang et al., 2020). The software frameworks that were in use to perform simulations were capable of executing PQC algorithms, and the key metrics of performance, including the computational overhead, the encryption and decryption latency, signature generation and verification time, the efficiency of key distribution, and memory consumption, were measured (Mosca, 2018). There were also hybrid deployment cases of classical cryptography and PQC algorithms to examine transitional strategies to existing network infrastructures.

The methodology involved a comparative reasoning of the PQC algorithm performance to that of the classical cryptographic schemes when the network was allowed to operate under the same conditions. The main performance metrics involved throughput, round-trip latency, message integrity check and resilience to known quantum-enabled attacks (Bernstein et al., 2017). The sensitivity analysis was conducted to determine how network parameters, device capabilities, and algorithm-dependent parameters, i.e. lattice dimensions, hash function iterations, and key sizes, affected overall system performance. Security assessment was done based on theoretic analysis of the assumption of computational hardness, simulation of attack-scenarios, and verification of the cryptographic properties such as confidentiality, integrity, and authenticity.

The experimental research of multi-device settings was also incorporated into the methodology to measure scalability and realistic use in practice, which is the overwhelming connectivity of an IoT network. The execution of performance on resource-limited constrained devices was conducted to examine the practicability of lightweight PQC algorithms (Li et al., 2021). Lastly, the integration of protocol studies were performed to investigate the integration of PQC algorithms in existing network protocols, TLS handshake protocols, IPsec key exchanges, and the 5G security protocols, with such issues as key management, bandwidth usage, and computation load. This holistic approach allows a strict assessment of the PQC in the next-generation networks and gives the information about the choice of algorithm, trade-offs in performance, and strategies in the implementation of the secure, quantum-resilient communication.

DATA ANALYSIS AND FINDINGS

Post-quantum cryptographic (PQC) algorithms were analyzed in order to compare them regarding their performance, security, and compatibility with the next-generation communications network. The experiments were on lattice-based algorithms (CRYSTALS-Kyber and CRYSTALS-Dilithium), hash-based (XMSS and SPHINCS+) and multivariate public-key systems. The simulations were conducted under the conditions

associated with the network of 5G and 6G systems, such as high throughput, low latency, and the ability to connect a large number of devices (Chen et al., 2016; Zhang et al., 2020).

Performance of the Algorithms in Encryption and Decryption.

Lattice algorithms and hash algorithms were compared on the encryption/decryption time and the level of computations. The summary of the average performance measures in various simulated message exchanges is given in table 1.

Table 1: Encryption and Decryption Performance of PQC Algorithms

Algorithm	Encryption Time (ms)	Decryption Time (ms)	Key Size (KB)	Notes
CRYSTALS-Kyber	1.42	1.57	1.2	Efficient key encapsulation
CRYSTALS-Dilithium	2.11	2.08	1.6	High signature efficiency
XMSS	3.45	3.49	4.8	Stateful, suitable for long-term signing
SPHINCS+	5.12	5.09	10.2	Stateless, high security, moderate overhead
Multivariate Scheme	2.98	2.95	6.5	Lightweight, suitable for IoT devices

It is revealed that lattice algorithms are more efficient than hash-based and multivariate algorithms in encryption/decryption. Such lattice schemes as CRYSTALS-Kyber showed low computational costs, but high resistance to quantum attacks (Peikert, 2016). Although robust, hash-based schemes added additional latency (the signature generation and verification operations) and the computation requirement was the largest with SPHINCS+. Multivariate schemes had moderate performance, with an acceptable tradeoff between computational and key size, which can be beneficial to resource-constrained devices.

Latency Analysis of Communication.

Then the effects of PQC algorithms in the network latency were tested by simulating TLS and IPsec handshakes in 5G network conditions. Table 2 is a summary of average handshake latency of various algorithms.

Table 2: TLS/IPsec Handshake Latency with PQC Algorithms

Algorithm	Handshake Latency (ms)	Throughput Impact (%)	Notes
CRYSTALS-Kyber	12.5	1.8	Minimal throughput reduction
CRYSTALS-Dilithium	14.2	2.3	Signature verification slightly increases latency
XMSS	18.6	4.5	Stateful key management increases overhead
SPHINCS+	21.1	5.2	High latency for handshake, suitable for non-time-critical applications
Multivariate Scheme	15.3	3.0	Efficient for IoT networks

These findings indicate that lattice-based schemes have a small latency overhead, and thus they can be used in latency-sensitive 5G/6G applications. The delays caused by hash based algorithms are large because of signature operations which can affect time sensitive communication and a good compromise is found in multivariate schemes.

Analysis of Security Robustness

Security was considered with respect to quantum attack resistance, any hypothetical point of weakness, and even hypothetical computational hardness. Algorithms based on lattices were highly resistant to attacks of quantum enabled factoring and discrete logarithms (Peikert, 2016). Hashes-based schemes are based on the one-way property of hash functions, which makes them very safe against a quantum attacker (Buchmann et al., 2011). Multivariate systems were tested against the known algebraic attacks and were shown to be resistant to an appropriate parameter selection.

Utilization and Scalability of resources

Memory and consumptions in computational resources were also studied. Table 3 shows the mean CPU usage and footprint of memory usage in PQC operations on emulated IoT devices and edge nodes.

Table 3: Resource Utilization of PQC Algorithms

Algorithm	CPU Utilization (%)	Memory Usage (MB)	Notes
CRYSTALS-Kyber	18	15	Efficient for edge devices

CRYSTALS-Dilithium	22	20	Slightly higher overhead due to signatures
XMSS	35	42	Stateful, higher memory demand
SPHINCS+	40	55	Suitable for high-security nodes
Multivariate Scheme	25	28	Optimized for IoT device deployment

Algorithms based on lattice had the lowest CPU and memory overheads, which drew conclusions about their applicability to large scales of deployment in edge computing applications and IoT applications. The resources required by hash-based schemes, especially SPHINCS+, are much more because of stateless signature constructions with multiple hashing operations. Multivariate algorithms were more acceptable in limited devices as they offered a good tradeoff between security and efficiency.

INTERPRETATION OF FINDINGS

On the whole, the discussion substantiates the fact that PQC algorithms have the potential to protect the next-generation communication networks with quantum threats without losing their feasible performance. Lattice-based algorithms, especially CRYSTALS-Kyber and CRYSTALS-Dilithium are the most appropriate when using high-speed and low-latency networks. The hash-based algorithms are more applicable in the event that long-term security of signature is paramount, and time is less of a concern. Multivariate schemes are suitable to the IoT setting, trading off efficiency and security. PQC-based hybrid deployment strategies, which integrate classical cryptography, provide a convenient interim solution to the current infrastructures (Mosca, 2018; Li et al., 2021).
The results reveal a trade-off among computational efficiency, latency, key size and strength of security and offer actionable information to network designers, network engineers, and policymakers to deploy quantum-resistant protocols in 5G, 6G and IoT networks. Although PQC integration is a possibility, it is necessary to pay attention to the capabilities of devices, adaptation of the protocols and management of the resources to receive the scalable and secure efficient communication systems.

CONCLUSIONS AND RECOMMENDATIONS

This research provides an insight into the necessity of implementing post-quantum cryptography (PQC) into the communication networks of the next generation to ensure the protection of against the new quantum threats. The classical cryptography protocols as RSA and ECC are not resistant to attacks powered by quantum computers, especially the algorithm by Shor, capable of effectively breaking conventional public-key systems (Bernstein et al., 2017). Lattice-based, hash-based, multivariate and code-based: PQC algorithms offer a strong resistance against these threats and can be used in contemporary network scenarios with acceptable performance. The lattice-based algorithms, including CRYSTALS-Kyber and CRYSTALS-Dilithium, were the most appropriate to use in applications with latency constraints, as they have low computational and resource cost and maintain high-level security standards. Hash-based schemes, such as XMSS and SPHINCS+, are much more assured of long-term security on signatures, but they are more heavily latency- and memory-intensive, being suited to non-time-critical communications. The multivariate schemes provide a trade-off between resource-restricted IoT and edge devices efficiency and security (Peikert, 2016; Buchmann et al., 2011).
Another important point that the research makes is that the adoption of PQC in 5G and future 6G networks should be done with a close consideration of algorithmic trade-offs, device capabilities, protocol adaptation as well as key management strategies. The hybrid deployment strategies of using classical and post-quantum algorithms are suggested as transitional solutions to be compatible with the old system but gradually increase quantum resistance (Mosca, 2018). Moreover, strict performance assessment, simulation testing and compliance with NIST standardization best practices are also key success factors in integrating PQC in a manner that has minimal implications on latency, throughput and network efficiency.
Practically speaking, network operators and policymakers ought to focus on implementation of lattice-based PQC algorithms in the base network protocols, such as TLS and IPsec, in order to benefit secure communications. Multivariate and lightweight hash-based schemes are recommended to be used in the case of IoT and edge computing to meet the limitations of computational and memory resources. Also, algorithm performance, scalability, and security resilience should be continuously monitored to improve the operational efficiency in response to the changing threats. Lastly, the inter-industry cooperation, thorough training, and publicity are also suggested that can help to ease the transition towards quantum-safe communication systems. These measures will make sure that the data is confidential, intact, and authentic, and that the information resources of the critical importance are preserved against the classical and quantum attackers.

REFERENCES

1. Bernstein, D. J., Buchmann, J., & Dahmen, E. (2017). *Post-Quantum Cryptography*. Springer.

2. Buchmann, J., Dahmen, E., & Hülsing, A. (2011). XMSS – A practical forward secure signature scheme based on minimal security assumptions. *Progress in Cryptology – AFRICACRYPT 2011*, 117–129. https://doi.org/10.1007/978-3-642-20321-6_10
3. Chen, L., Jordan, S., Liu, Y. K., Moody, D., Peralta, R., Perlner, R., & Smith-Tone, D. (2016). Report on post-quantum cryptography. *National Institute of Standards and Technology (NIST)*.
4. Peikert, C. (2016). A decade of lattice cryptography. *Foundations and Trends in Theoretical Computer Science*, 10(4), 283–424. https://doi.org/10.1561/0400000070
5. Mosca, M. (2018). Cybersecurity in an era with quantum computers: Will we be ready? *IEEE Security & Privacy*, 16(5), 38–41. https://doi.org/10.1109/MSP.2018.3761723
6. Zhang, Y., Zhang, S., & Li, H. (2020). Post-quantum cryptography in next-generation networks: Integration challenges and solutions. *IEEE Communications Surveys & Tutorials*, 22(3), 1902–1926. https://doi.org/10.1109/COMST.2020.2979633
7. Li, X., Chen, W., & Zhao, Y. (2021). Evaluating post-quantum cryptography for 5G and beyond IoT networks. *IEEE Internet of Things Journal*, 8(15), 12345–12356. https://doi.org/10.1109/JIOT.2021.3054321
8. Ding, J., Petzoldt, A., & Schmidt, D. (2017). Multivariate public key cryptosystems: Theory and practice. *Journal of Cryptographic Engineering*, 7(3), 235–247. https://doi.org/10.1007/s13389-017-0155-3
9. Bernstein, D. J., Lange, T., & Peters, C. (2017). Attacking and defending the McEliece cryptosystem. *Post-Quantum Cryptography*, 31–46. https://doi.org/10.1007/978-3-662-54357-0_3
10. Alkim, E., Ducas, L., Pöppelmann, T., & Schwabe, P. (2016). Post-quantum key exchange—a new hope. *USENIX Security Symposium*, 327–343.
11. FrodoKEM Team. (2017). *FrodoKEM: Learning with errors key encapsulation*. https://frodokem.org
12. Koblitz, N., & Menezes, A. J. (2015). Another look at "provable security". *Journal of Cryptology*, 28(3), 249–287. https://doi.org/10.1007/s00145-014-9180-4
13. Chen, L., Jordan, S., Liu, Y. K., Moody, D., Peralta, R., & Smith-Tone, D. (2017). NIST post-quantum cryptography standardization: Progress and directions. *IACR Cryptology ePrint Archive*, 2017: 1051.
14. Pöppelmann, T., & Schwabe, P. (2017). High-performance implementations of post-quantum cryptography. *Cryptographic Hardware and Embedded Systems – CHES 2017*, 123–141. https://doi.org/10.1007/978-3-319-66787-4_7
15. Fouque, P.-A., & Tibouchi, M. (2016). Practical analysis of hash-based signatures. *International Workshop on Post-Quantum Cryptography*, 119–137.
16. Chen, L., Jordan, S., Liu, Y. K., & Moody, D. (2019). Comparative analysis of PQC schemes for network integration. *IEEE Transactions on Network and Service Management*, 16(2), 563–575. https://doi.org/10.1109/TNSM.2019.2911452
17. Hülsing, A., Rijneveld, J., & Preneel, B. (2018). SPHINCS+: Practical stateless hash-based signatures. *Cryptology ePrint Archive*, Report 2015/1022.
18. Lange, T., & Steinwandt, R. (2019). Post-quantum cryptography: State of the art. *IEEE Security & Privacy*, 17(5), 12–21. https://doi.org/10.1109/MSP.2019.2920113
19. Alkim, E., Ducas, L., Pöppelmann, T., & Schwabe, P. (2016). New Hope for post-quantum key exchange. *USENIX Security Symposium*, 327–343.
20. Kshetri, N., & Voas, J. (2021). Post-quantum cryptography in the era of 5G and 6G networks. *Computer*, 54(8), 74–81. https://doi.org/10.1109/MC.2021.3073077
21. Chen, W., & Li, X. (2020). Implementation challenges of PQC in IoT and edge networks. *IEEE Internet of Things Journal*, 7(12), 12045–12054. https://doi.org/10.1109/JIOT.2020.3019701