Securing Mobile Networks in the Quantum Era: Imperative Role of Post-Quantum Cryptography

Sogo Pierre Sanon[†] and Hans D. Schotten[*†]
[†]Intelligent Networks Research Group, DFKI, D-67663 Kaiserslautern, Email: {firstname.lastname}@dfki.de
[*]Institute for Wireless Communication and Navigation, RPTU, D-67663 Kaiserslautern, mail: {lastname}@rptu.de

Abstract

In the rapidly evolving telecommunications landscape, the advent of 6G networks promises unparalleled connectivity and transformative capabilities. However, as the potential of 6G unfolds, so too do the security challenges, particularly in the face of quantum computing advancements. Post-Quantum Cryptography (PQC) emerges as a critical safeguard against potential threats to data integrity and confidentiality in 6G networks. This paper addresses the critical role of PQC in safeguarding 6G networks against these quantum-based threats. It analyzes the potential vulnerabilities posed by quantum computing, reviews the existing landscape of quantum-safe cryptographic solutions, and assesses their implications for mobile security. The paper also outlines the necessary steps for transitioning to quantum-safe mobile networks, supported by insights from governmental and institutional recommendations.

This is a preprint of the publication which has been presented at the 2025 EuCNC & 6G Summit

Index Terms

6G, 5G, Post-Quantum Cryptography, Quantum Computing, Quantum-Safe Transition

I. Introduction

The rapid advancement of quantum computing represents one of the most profound shifts in the landscape of digital security, challenging the very foundations of contemporary cryptographic systems. Quantum computers, which operate on the principles of quantum mechanics, have the potential to solve certain complex problems exponentially faster than classical computers, a capability that poses a significant threat to current cryptographic protocols. Central to this threat is Shor's algorithm, a quantum algorithm capable of factoring large integers far more efficiently than the best-known classical algorithms. This efficiency directly undermines the security of widely used public-key cryptosystems such as RSA and Elliptic Curve Cryptography (ECC), which rely on the computational difficulty of such problems to ensure data security [1]. Moreover, the implications of quantum computing extend beyond public-key cryptography. Grover's algorithm [2], another quantum computing breakthrough, provides a quadratic speedup for unstructured search problems, which translates into a significant reduction in the time required to brute-force symmetric key cryptography systems.

The looming threat of quantum computing necessitates an urgent and proactive transition to quantum-safe cryptographic systems. While there is currently no concrete evidence that quantum computers capable of executing these algorithms at a scale necessary to break modern encryption exist, the need for migration is driven by at least two critical factors. Firstly, the "harvest now, decrypt later" strategy, in which adversaries collect encrypted data today with the intention of decrypting it once quantum computers become viable, poses an imminent risk to data confidentiality. Secondly, transitioning to new cryptographic standards is a complex and time-consuming process that involves upgrading infrastructure, software, and protocols across the entire digital ecosystem. This process requires extensive testing, standardization, and widespread adoption, making it imperative to begin the transition well before the threat fully materializes.

In particular, mobile communication systems, which serve as the backbone of global connectivity, are increasingly recognized as a critical area requiring quantum-safe migration. The deployment of 5G networks has revolutionized connectivity, enabling ultra-fast data transmission, low-latency communication, and massive device connectivity [3]. These advancements have led to innovative applications ranging from autonomous vehicles and smart cities to augmented reality and remote healthcare. As the world anticipates the advent of 6G, which promises even greater bandwidth, enhanced reliability, and new use cases such as ubiquitous Internet of Things (IoT) connectivity and seamless integration of artificial intelligence (AI), ensuring that these systems are quantum-safe is essential for the continued development and security of these technologies.

This work makes a significant contribution to quantum migration efforts in mobile communication by presenting a cryptographic inventory that identifies where cryptographic vulnerabilities exist within these systems. It also provides a comprehensive overview of the quantum threat landscape, particularly highlighting emerging threats at the intersection of AI and quantum computing. In response, it presents the latest defense mechanisms and outlines a step-by-step approach for quantum migration in 5G/6G networks. The remainder of the paper is structured as follows: Section II explores the role of cryptography in mobile communication systems. Section III examines the quantum threats and latest quantum-safe cryp-

tographic solutions. Section IV provides the necessary steps for transitioning to quantum-safe mobile networks. Finally, Section V gives a brief overview of the recommendations from governments and institutions, and VI concludes the paper.

II. Background

Cryptography is essential for securing mobile communications. It ensures the confidentiality, integrity, and authenticity of data transmitted over wireless networks. In mobile communication systems, both symmetric and asymmetric cryptographic techniques are employed, along with a robust public key infrastructure (PKI) to safeguard against various threats.

A. Cryptography Inventory in 5G

In 5G systems, cryptographic algorithms are employed at various layers to secure data and ensure privacy.

*1) **Authentication**:* 5G employs three primary authentication protocols to establish secure communication between the UE and the network: 5G AKA (Authentication and Key Agreement), EAP-AKA (Extensible Authentication Protocol AKA), and EAP-TLS (Transport Layer Security). While 5G AKA and EAP-AKA rely on SIM cards (Subscriber Identity Modules) for pre-shared keys during authentication, EAP-TLS uses certificates and is particularly designed for IoT environments where traditional SIM-based authentication may not be suitable. The authentication is usually a tripartite scheme involving the User Equipment (UE), the Home Network (HN), which serves as the subscriber's primary service provider, and the Serving Network (SN), which manages the base station with which the UE communicates. The goal is to authenticate the user securely and establish a shared key for encrypted communication between the UE and the network. In terms of algorithms, 5G supports two main cryptographic suites for authentication: TUAK, based on the Keccak hash function, and MILENAGE, which utilizes the AES block cipher. Subscriber privacy in 5G is safeguarded through the use of the Subscription Concealed Identifier (SUCI), which masks the user's Subscription Permanent Identifier (SUPI). This is achieved through the Elliptic Curve Integrated Encryption Scheme (ECIES), based on a Diffie-Hellman key exchange between the UE and the HN. However, this protocol is vulnerable to quantum attacks, particularly the Diffie-Hellman phase, which will need to be replaced with a quantum-resistant alternative, such as a FIPS 203 (see Section III-D), as part of future security enhancements in PQC. Quantum attacks do not yet break TUAK and MILENAGE [4].

*2) **NAS, AS Encryption**:* After authentication, Non-Access Stratum (NAS) and Access Stratum (AS) signaling rely on symmetric encryption algorithms such as AES, SNOW, and ZUC to secure communication between the UE, the Access and Mobility Management Function (AMF), and the base station (gNB). To achieve a security level of 128-bit against quantum attacks, a key size of 256 is required. AES supports 256-bit key encryption, whereas SNOW and ZUC do not. To address this, the development of SNOW 5G and ZUC 256 algorithms has been proposed. SNOW 5G has undergone rigorous testing and is considered robust, while ZUC 256 is still undergoing evaluations [5].

*3) **Core Network Security**:* The security of Virtual Network Functions (VNFs) in the 5G core network is critical for ensuring secure communication and service access, both within a single Public Land Mobile Network (PLMN) and between different PLMNs. 5G employs the OAuth 2.0 framework for network services' access control. This is achieved using JSON Web Tokens (JWTs), protected by digital signatures (JSON Web Signature), which authorize secure communication between network functions. The Network Repository Function (NRF) acts as the OAuth 2.0 authorization server, while network services communicate securely via TLS, ensuring the safe transmission of credentials. Inter-PLMN communication is secured through Security Edge Protection Proxies (SEPP) connected via the N32 interface, comprising N32-c (handling mutual AKA establishment) and N32-f (securing messages using Javascript Object Signing and Encryption (JOSE)). Agreed cryptographic keys ensure secure communication between SEPPs. Currently, these interfaces rely on algorithms vulnerable to quantum attacks, including AES-128, ECDHE, RSA, and SHA-256. To safeguard against future quantum threats, standardized PQC algorithms have to be considered.

*4) **Transport Network Security**:* The security of the transport network, the communication between the Radio Access Network (RAN) and the core network, is another critical area in 5G. Security Gateways (SecGWs) are strategically placed within the network architecture to provide IPSec tunnels, which ensure authentication, data integrity, and confidentiality during data transmission between base stations and core network functions. The IPSec protocol suite, specifically the Internet Key Exchange (IKE) protocol, is used to set up secure channels for this communication. Additionally, data transmitted over these channels is protected by a Transport Layer Security (TLS) or a TLS-like protocol. However, IKE and TLS are susceptible to the "harvest now, decrypt later" style attacks that quantum computers can exploit. To authenticate the base stations and SecGWs, a PKI is employed, providing certificates in formats like X.509 that verify the identity of these network components. The management of these certificates, including renewal and revocation, is typically handled through standardized protocols such as the Certificate Management Protocol (CMP). These certificates rely on classical cryptographic algorithms like RSA and ECDHE, which are vulnerable to quantum computing.

Quantum security challenges extend beyond traditional network traffic, affecting Machine-to-Machine (M2M) and IoT communications as well. The Internet Engineering Task Force (IETF) is actively working on hybrid schemes for protocols like TLS, IKEv2, and X.509 to combine classical cryptography with post-quantum algorithms.

III. Quantum Threats

For decades, the bedrock of public key cryptography has been the difficulty of factoring large numbers and solving discrete logarithm problems. These complex mathematical

tasks have ensured the inability to break many cryptographic systems with classical computers. However, the advent of quantum computing poses a significant threat to this paradigm [6].

A. Shor's and Grover's Algorithms

Two prominent quantum algorithms, Shor's algorithm, and Grover's algorithm, can significantly impact classic cryptographic systems:

- Shor's algorithm, developed by Peter Shor in 1994, for period finding, can factor large numbers and solve discrete logarithm problems in polynomial time. This capability undermines the security of RSA and discrete logarithm-based cryptography like ECC.
- Grover's algorithm allows for inverting functions in $O(\sqrt{n})$ time, impacting symmetric key cryptography by reducing its security by a factor of the square root. For instance, while AES-128 currently offers 128 bits of security, Grover's algorithm could reduce this to only 64 bits. It can also make brute-force attacks on hash functions more feasible; a 256-bit hash is still considered secure against classical attacks, but it is theoretically as secure as a 128-bit hash against quantum attacks.

Fortunately, increasing the key size in symmetric cryptography can mitigate the impact of Grover's algorithm. However, this solution is not readily applicable to asymmetric systems and therefore, the emergence of quantum computing necessitates the development of quantum-resistant schemes for those systems.

B. Post Quantum Impact Assessment on Mobile Networks

As discussed above, cryptography is widely utilized in mobile networks, making various components potentially vulnerable to quantum threats. The advent of a cryptographically relevant quantum machine would critically undermine mobile communication systems by exploiting weaknesses in current cryptographic protocols. Confidentiality would be severely compromised as quantum algorithms could decrypt encrypted communications, exposing sensitive user data and secure communications. Authentication systems based on current cryptographic mechanisms would be vulnerable, potentially allowing unauthorized access and impersonation. Quantum computing could further erode the integrity of systems by enabling the alteration of critical software, SIM card data, and network configurations, leading to potential manipulation of system operations and data integrity. Non-repudiation would also be jeopardized, allowing for falsification of emergency calls, billing records, and inter-operator transactions, facilitating fraud and service denials. Additionally, financial records, cloud workloads, and sensitive business data could be tampered with, resulting in a loss of trust and stability across sectors dependent on cryptographic security, necessitating an urgent shift to quantum-resistant solutions.

C. Threat from combining AI and Quantum Computing

The rapid advancement of hybrid quantum-classical computing, alongside AI, Machine Learning (ML), and Deep Learning (DL), poses a significant threat to encryption systems, potentially impacting the transition timelines PQC [7]. These technologies, both individually and in combination, introduce new vulnerabilities that require attention and research.

Grover's Adaptive Search (GAS) [8], is one such concern, as it enhances Grover's Algorithm with adaptive techniques, making it more effective for breaking encryption. Similarly, the quantum-accelerated Harrow-Hassidim-Lloyd (HHL) Algorithm [9], which solves linear equations faster than classical methods, could compromise lattice-based encryption, a key component of PQC [7].

Hybrid Quantum-Classical Computing (HQCC) exploits the strengths of both quantum and classical systems. It allows quantum systems to handle complex computations while classical computers manage tasks like data processing and system control. Additionally, Quantum Artificial Intelligence (QAI), Quantum Machine Learning (QML), and Quantum Deep Learning (QDL) are being developed to harness quantum computing's capabilities for improving AI algorithms, speeding up calculations, and accelerating neural network training [9]. However, these technological advancements also introduce serious risks to encryption and digital security. According to [7], co-authored by Whitfield Diffie, Quantum-accelerated AI/ML could reveal previously unknown weaknesses in encryption algorithms, potentially leading to breakthroughs in cryptanalysis. This could enable quantum-enhanced AI to execute brute-force attacks much faster, compromising even the strongest encryption keys. Additionally, quantum-powered AI might amplify side-channel attacks by exploiting minor leaks from cryptographic devices and bypassing traditional security protocols through optimized techniques. Furthermore, the security of cryptographic hash functions and PKI is at risk, as quantum-improved algorithms could more easily discover collisions and weaken the foundational security of algorithms. To address these emerging vulnerabilities, some solutions are explored in [7], offering potential strategies to mitigate the risks associated with this rapidly evolving field.

D. NIST Standardization Efforts in PQC

The concern regarding advancements in quantum computing has prompted the National Institute of Standards and Technology (NIST) to take proactive measures. In 2016, it initiated a call for the development and standardization of PQC algorithms that could withstand the potential threats posed by quantum computers.

These new PQC approaches diverge from traditional cryptographic methods by exploring alternative mathematical foundations. Notably, they focus on areas such as code-based, lattice-based, hash-based, and isogeny-based cryptography. Each of these areas offers unique mechanisms for securing information, ensuring that even with the advent of quantum computing, data remains protected.

By July 2022, after rigorous evaluation and analysis, NIST made an announcement by selecting four algorithms for standardization: CRYSTALS-KYBER, CRYSTALS-Dilithium, FALCON, and SPHINCS+ [10]. These algorithms were chosen based on their robustness, efficiency, and potential to secure communications in a post-quantum world. Additionally, NIST identified four other algorithms; BIKE, HQC, Classic McEliece, and SIKE; for further study and evaluation, recognizing their potential but requiring additional scrutiny before standardization.

However, the path to post-quantum cryptography has not been without challenges. In August 2022, a significant setback occurred when Castryck and Decru published a paper that presented an efficient classical key recovery attack against the SIKE algorithm. This discovery exposed vulnerabilities in SIKE, leading to its removal from further consideration in NIST's standardization process. This incident underscored the critical importance of thoroughly vetting cryptographic algorithms before they are widely adopted.

In August 2023, NIST released draft standards for three of the four algorithms selected in 2022. These drafts marked a crucial step forward in the formalization of post-quantum cryptographic standards. However, the standardization of FALCON was deferred to a later date.

NIST's efforts in PQC standardization also emphasized the importance of cryptographic diversity. The majority of PQC algorithms under consideration, including the ones selected for standardization, rely on lattice-based cryptography. While lattice-based methods are currently among the most promising candidates for post-quantum security, over-reliance on a single mathematical foundation could introduce systemic risks. To mitigate this, NIST issued a call for additional digital signature submissions by July 2023 and after over a year of evaluation, NIST has selected 14 algorithms for the second round. The goal is to encourage the development of a broader array of PQC algorithms based on different mathematical problems, thus reducing the risk of a single point of failure in the cryptographic ecosystem.

In August 2024, NIST officially published three new Federal Information Processing Standards (FIPS) for post-quantum cryptography. These standards, which were also approved by the Secretary of Commerce, represent a significant milestone in the transition to quantum-resistant cryptographic systems [11]:

- **FIPS** 203 **- ML-KEM:** Based on the CRYSTALS-KYBER submission, this standard addresses key encapsulation mechanisms, offering a quantum-safe method for securing data exchange.
- **FIPS** 204 **- ML-DSA:** Derived from the CRYSTALS-Dilithium submission, this standard focuses on digital signatures, ensuring authenticity and integrity in a post-quantum environment.
- **FIPS** 205 **- SLH-DSA:** Based on the SPHINCS+ submission, this standard also addresses digital signatures.

FIPS 203 and 204 are the primary chosen quantum-resistant algorithms and can be used instead of the currently used public-key algorithms like RSA and ECC.

These FIPS publications mark a crucial step forward in securing the digital infrastructure against future quantum threats, ensuring that organizations have the tools and standards necessary to protect sensitive information in the coming quantum era.

E. Approaches for Post-Quantum Cryptosystems

NIST recommends using multiple approaches for PQC to enhance security in the quantum era and among the promising methods, lattice-based cryptography stands out. Recently, a potential quantum attack on was proposed by Yilei Chen in April 2024, threatening many lattice-based systems [12]. However, a critical error was found in the attack, rendering it ineffective. This incident highlights the need for crypto-agile systems that can quickly adapt by swapping out cryptographic algorithms as new vulnerabilities are discovered. NIST also advocates for the use of multiple algorithms based on different approaches. Approaches to PQC include:

1) ***Lattice-Based Cryptography****:* Known for its robust security based on problems like the Shortest Vector Problem (SVP) and Ring Learning With Errors (RLWE). It enables the creation of schemes like Fully Homomorphic Encryption (FHE). CRYSTALS-KYBER, CRYSTALS-Dilithium, and FALCON are lattice-based algorithms.

2) ***Code-Based Cryptography****:* Relies on the complexity of problems from coding theory, such as Syndrome Decoding (SD) and Learning Parity with Noise (LPN). These systems use error-correcting codes to create secure one-way functions. The McEliece encryption scheme, a well-known code-based method, is a Fourth Round Candidate Algorithm to be standardized by NIST.

3) ***Hash-Based Cryptography****:* Utilizes hash functions to create digital signatures, offering security with fewer assumptions compared to traditional schemes like RSA. The SPHINCS+ scheme, standardized by NIST, is a hash-based signature.

4) ***Isogeny-Based Cryptography****:* Utilizes mappings between elliptic curves (or abelian varieties), offering compact key sizes and complex structures for secure communications. The SIKE scheme, previously considered by NIST but later broken is isogeny-based. Additional systems using isogenies that are not broken include [13].

5) ***Other Approaches****:* Additional methods include multivariate signatures, Multi-Party Computation (MPC), and symmetric-based encryption. These approaches provide quantum resistance with various trade-offs in key sizes, signature sizes, and computational complexity [14].

This diversity of approaches ensures that the cryptographic community remains prepared for the wide-ranging challenges posed by quantum computing.

IV. 6G Cryptographic Migration to Quantum Safe

6G technology is set to transform industries by providing unprecedented speed, low latency, and vast connectivity, enabling real-time, personalized experiences. By leveraging

ultra-high frequencies, 6G will achieve data transfer rates far beyond 5G, benefiting sectors like healthcare, public safety, and entertainment. However, this technological leap faces significant cryptographic challenges due to the advent of quantum computing. Integrating PQC into 6G networks can be complex and require time and effort. A systematic and strategic approach to PQC migration must be explored to address these challenges effectively. It is crucial to embed crypto-agility into strategies and execution methods to ensure adaptability and resilience against future cryptographic threats. The migration process can be effectively managed by breaking it down into three key phases: Preparation, Planning, and Execution.

A. Preparation Phase

The preparation phase of 6G quantum migration involves recognizing the unique cryptographic challenges that PQC presents in the context of 6G networks. Unlike traditional systems, PQC algorithms must balance the need for small key sizes and efficient processes; such as key generation, encryption, decryption, signing, and verification; while ensuring the operational efficiency required by 6G's high-speed communication environments. A key aspect of preparation is understanding that the performance of different PQC algorithms can vary significantly in terms of memory and CPU usage, which is particularly challenging for resource-constrained edge nodes. To address this, organizations must design 6G architectures that support multiple PQC algorithms within the same interface. This approach allows for the concurrent use of various algorithms tailored to specific applications or use cases, ensuring that the cryptographic needs of all network layers are met. Furthermore, network slicing in 6G must incorporate these cryptographic requirements to maintain robust security across the entire network.

B. Planning Phase

The planning phase is critical for establishing a comprehensive 6G quantum migration strategy. First, it is important to evaluate the migration criteria and identify diverse 6G use cases that reflect different security needs across multiple domains. These domains include network access, network architecture, user-specific needs, and service-based architecture (SBA). For example, the network access domain might involve scenarios like extremely reliable and low-latency communication (eURLLC) and massive machine-type communication (umMTC), while the user domain focuses on secure boot processes and biometric authentication. Once the use cases are identified, the next step is to define specific security requirements for each domain. These requirements should address confidentiality, integrity, authenticity, non-repudiation, and performance metrics such as latency, throughput, and energy efficiency. With these requirements in mind, the evaluation and comparison of security solutions can begin. This involves selecting quantum-resistant security options tailored to the specific needs of each domain. Hybrid solutions that combine PQC with traditional cryptographic algorithms can also be considered to meet the unique demands of different use cases. To ensure that these solutions are viable, it is essential to develop test environments that accurately reflect each security domain. These environments should incorporate relevant 6G use cases, network components, protocols, and applications. Through these test settings, organizations can assess the effectiveness of PQC solutions, evaluating factors such as latency, throughput, energy consumption, and cryptographic key establishment times. A thorough security analysis, including both theoretical and practical simulations, should be conducted to gauge the resilience of each solution against quantum and traditional cryptanalytic attacks.

C. Execution Phase

The execution phase focuses on the practical implementation of the selected quantum-safe solutions within the 6G network. Given the complexity of migrating to PQC, it is challenging to replace all components at once; hence, prioritization is essential. Typically, infrastructure components with critical priority, such as PKI, are targeted first, as these must be quantum-safe before any certificate-based application can be updated. During execution, solutions should be ranked and prioritized based on their ability to facilitate efficient updates of keys and algorithms with minimal system disruption. The selected solutions should offer modular designs that allow for the easy replacement of cryptographic components as new PQC algorithms emerge. Additionally, it is crucial to ensure that the solutions support flexible deployment methods—such as full PQC, hybrid, and gradual migration—to suit different domains within the network. To minimize impacts on performance and security, the migration process must be carefully managed, with ongoing monitoring of quantum computer technology advancements and the PQC readiness of the systems involved. Continuous research and adaptation are necessary to address emerging security threats and to maintain the network's resilience against quantum computing risks.

V. Recommendation from Governments and Institutions

Quantum Key Distribution (QKD) and PQC represent two distinct approaches to securing data against the anticipated threats posed by quantum computing. However, most institutions and governments recommend adopting PQC over QKD due to several critical factors. QKD, while innovative, does not support digital signatures and requires specialized hardware, making it expensive and less versatile for widespread adoption. Conversely, PQC is viewed as more promising and practical by many organizations.

The U.S. government released a comprehensive report emphasizing the need to transition its information systems to PQC to protect against future quantum threats. The report outlines a strategic plan that involves creating an inventory of existing cryptographic systems, prioritizing critical systems for migration, and identifying those incompatible with PQC. NIST is leading the development and standardization of PQC algorithms to secure federal systems. The report emphasizes

the necessity of immediate action and proper funding to safeguard national data from quantum-enabled "harvest now, decrypt late" attacks, reflecting the government's proactive approach to this emerging challenge.

Similarly, GSMA issued guidelines urging telecom operators to prepare for the quantum computing era by transitioning to PQC [15]. The guidelines address the significant risks that quantum computers pose to current cryptographic systems used in telecommunication networks, customer data, and devices. They offer best practices for migrating to PQC, tailored to specific telecom use cases, and emphasize the importance of planning, risk analysis, and phased implementation. The GSMA also highlights the global momentum towards PQC adoption and the need for alignment and cooperation among stakeholders to ensure secure communications in a post-quantum world.

On the European front, the ETSI Technical Report (TR 103 619 V1.1.1) offers a structured framework for transitioning to Quantum-Safe Cryptography (QSC), advocating for a systematic three-stage migration process that includes practical resources like a migration checklist [16]. Additionally, the German Federal Office for Information Security (BSI) has highlighted the specific threats quantum computing poses to current cryptographic systems [17]. BSI emphasizes the importance of proactive migration to PQC, advocating for "crypto agility" to allow flexibility in cryptographic mechanisms and the integration of hybrid solutions combining classical and quantum-resistant methods. Furthermore, the 3GPP has recommended the incorporation of PQC into 5G and future network architectures, stressing the need for global coordination to ensure a harmonized transition to quantum-resistant systems. Other relevant standards, such as ITU-T [18], ISO/IEC 27001, and IETF, are also crucial in guiding the shift to PQC across various industries.

These various reports and guidelines converge on a critical consensus: the necessity to act now to secure digital infrastructures against quantum threats and the urgent need for collaboration and interoperability among global stakeholders to ensure a seamless transition to quantum-safe cryptography.

VI. Conclusion and Outlook

In conclusion, as 6G networks bring unprecedented connectivity and capabilities, they also face new security challenges posed by quantum computing. This paper has highlighted the crucial role of PQC in protecting these networks against potential quantum threats. Given the lengthy process of updating cryptographic systems, it is essential to adopt quantum-resistant solutions now, even before powerful quantum computers are fully realized. By examining the various PQC techniques and strategies recommended by leading institutions, this research emphasizes the need for proactive measures to ensure the security and resilience of 6G networks. The integration of PQC is not just a forward-thinking strategy but a necessary step to safeguard the future of telecommunications. Continued collaboration and timely action will be key to maintaining secure global communications as we transition into a quantum-driven era.

Acknowledgment

This work has been supported by the Federal Ministry of Education and Research of the Federal Republic of Germany (Förderkennzeichen Open6GHub 16KISK003K). The authors alone are responsible for the content of the paper.

References

[1] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM Journal on Computing*, vol. 26, no. 5, pp. 1484–1509, 1997.

[2] L. K. Grover, "Afast quantum mechanical algorithm for database search," in *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing*, 1996, pp. 212–219.

[3] Q. Li and Z. Niu, "5G Network Capacity: Key Elements and Technologies," *IEEE Vehicular Technology Magazine*, vol. 13, no. 2, pp. 71–78, 2018.

[4] J. Partala, "Post-quantum Cryptography in 6G," in *Post-Quantum Cryptography in 6G*, Springer International Publishing, 2021, pp. 431–448.

[5] M. Kumar, "Post-quantum cryptography algorithm's standardization and performance analysis," *Array*, vol. 15, p. 100 242, 2022.

[6] P. W. Shor, "Algorithms for quantum computation: discrete logarithms and factoring," in *35th Annual Symposium on Foundations of Computer Science (Santa Fe, NM, 1994)*, IEEE Comput. Soc. Press, Los Alamitos, CA, 1994, pp. 124–134. DOI: 10.1109/SFCS.1994.365700. [Online]. Available: https://doi.org/10.1109/SFCS.1994.365700.

[7] R. Campbell, W. Diffie, and C. Robinson, "Advancements in Quantum Computing and AI May Impact PQC Migration Timelines," *Preprints*, Feb. 2024, Posted: 22 February 2024, doi:10.20944/preprints202402.1299.v1.

[8] D. Bulger, W. P. Baritompa, and G. R. Wood, "Implementing pure adaptive search with Grover's quantum algorithm," *Journal of optimization theory and applications*, vol. 116, pp. 517–529, 2003.

[9] A. W. Harrow, A. Hassidim, and S. Lloyd, "Quantum Algorithm for Linear Systems of Equations," *Physical Review Letters*, vol. 103, no. 15, p. 150 502, Oct. 2009. DOI: 10.1103/PhysRevLett.103.150502.

[10] G. Alagic, D. Apon, D. Cooper, Q. Dang, T. Dang, J. Kelsey, J. Lichtinger, C. Miller, D. Moody, R. Peralta, *et al.*, "Status report on the third round of the NIST post-quantum cryptography standardization process," *US Department of Commerce, NIST*, 2022.

[11] National Institute of Standards and Technology, *Announcing Approval of Three Federal Information Processing Standards (FIPS) for Post-Quantum Cryptography*, Accessed: 2024-08-13, 2024. [Online]. Available: https : / / csrc . nist . gov / News / 2024 / postquantum - cryptography-fips-approved.

[12] Y. Chen, *Quantum Algorithms for Lattice Problems*, Cryptology ePrint Archive, Paper 2024/555, 2024. [Online]. Available: https://eprint.iacr.org/2024/555.

[13] S. P. Sanon, I. Alzalam, and H. D. Schotten, "Quantum and Post-Quantum Security in Future Networks," in *2023 IEEE Future Networks World Forum (FNWF)*, 2023, pp. 1–6. DOI: 10 . 1109 / FNWF58287 . 2023 . 10520624.

[14] National Institute of Standards and Technology (NIST), *PQC Digital Signature Project: Round 1 Additional Signatures*, https : / / csrc . nist . gov / projects / pqc - dig - sig/round-1-additional-signatures, Accessed: 2024-08-19, 2019.

[15] GSMA, *Post Quantum Cryptography – Guidelines for Telecom Use Cases*, Accessed: 2024-08-13, 2024. [Online]. Available: https://www.gsma.com/newsroom/wp-content/uploads//PQ.03-Post-Quantum-Cryptography-Guidelines-for-Telecom-Use-v1.0.pdf.

[16] ETSI, *CYBER; Migration Strategies and Recommendations to Quantum Safe Schemes*, Accessed: 2024-08-13, 2024. [Online]. Available: https://www.etsi.org/deliver/etsi_tr/103600_103699/103619/01.01.01_60/tr_103619v010101p.pdf.

[17] BSI, *Quantum-Safe Cryptography – Fundamentals, Current Developments and Recommendations*, Accessed: 2024-08-13, 2024. [Online]. Available: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Brochure/quantum-safe-cryptography.pdf?__blob=publicationFile&v=6.

[18] International Telecommunication Union, "Security guidelines for applying quantum-safe algorithms in 5G systems," International Telecommunication Union, Recommendation ITU-T X.1811, 2021.