Quantum-Ready Mobile Communications: Cryptographic Agility for Mobile Networks in the Quantum Era

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

Abstract

Cryptographic agility is becoming increasingly essential in mobile networks due to the rapid evolution of network architectures, the growing complexity of security threats, and the anticipated arrival of quantum computing. As mobile networks transition from 5G to 6G, ensuring the adaptability of cryptographic systems to emerging standards and threats is paramount. This paper introduces a novel Cryptographic Management Function (CMF), a centralized software-defined cryptography framework designed to achieve seamless cryptographic agility in mobile networks. The CMF is introduced to enable dynamic, seamless updates to cryptographic algorithms and protocols without disrupting ongoing operations, making it ideal for environments with varying device capabilities and evolving security requirements. It operates by decoupling cryptographic functions from the other network components, centralizing the enforcement of cryptographic policies, and supporting hybrid cryptographic schemes, including Post-Quantum Cryptography (PQC).

This is a preprint of the publication which has been presented at the 26th IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM).

Index Terms

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

I. Introduction

The rapid evolution of mobile networks, driven by the deployment of 5G and ongoing 6G research, has fundamentally transformed the telecommunications landscape. These networks now serve as critical infrastructure for various applications, ranging from autonomous vehicles and smart cities to the Internet of Things (IoT) and Industry 4.0 [1], [2]. As a result, the volume and sensitivity of data being transmitted across mobile networks have grown exponentially, demanding more robust and adaptive security mechanisms. Cryptography serves as the backbone of security in mobile networks, providing essential services such as confidentiality, integrity, and authentication. However, while these cryptographic mechanisms have been effective in protecting data, the dynamic and diverse nature of 5G networks together with the emergence of new threats presents unique challenges.

One of the most pressing challenges is the impending threat posed by quantum computing. Quantum computers, once fully realized, will have the computational power to break many of the cryptographic algorithms that underpin modern network security, such as Rivest-Shamir-Adleman (RSA) and Elliptic Curve Cryptography (ECC). This vulnerability could lead to the collapse of secure communication frameworks in a matter of seconds. As quantum computing draws closer to becoming a reality, the transition to Post-Quantum Cryptographic (PQC) algorithms, designed to resist quantum attacks, has become an urgent necessity [3]. Yet, the migration to quantum-safe alternatives goes beyond simply adopting new algorithms. It raises broader questions about cryptographic agility: How flexible are current systems when it comes to updating cryptographic algorithms, standards, and policies? The history of cryptographic vulnerabilities, such as those found in deprecated standards like RC4, MD5, and DES, highlights the challenges in migrating away from outdated algorithms [4]. The need for a framework that can not only handle the introduction of PQC but also adapt to ongoing cryptographic changes is essential for future-proofing mobile networks.

Cryptographic agility addresses this challenge by enabling systems to switch seamlessly between different cryptographic algorithms and protocols in response to changing security requirements or emerging threats. In the context of mobile networks, cryptographic agility is particularly crucial given the wide variety of devices; from powerful smartphones to low-power IoT sensors; with differing computational capabilities, battery life, and network connectivity. A promising approach to achieving cryptographic agility is Software-Defined Cryptography (SDC), which builds on Software-Defined Networking (SDN) principles to decouple cryptographic functions from hardware [5]. This decoupling enables centralized control and dynamic configuration of cryptographic parameters, allowing for rapid deployment and updates to cryptographic algorithms

across the network. In this context, we propose the introduction of a novel network function, the Cryptographic Management Function (CMF), which will serve as the central authority for managing cryptographic operations in mobile networks. The CMF will provide a comprehensive framework for managing cryptographic operations, including key generation, distribution, and revocation; dynamic algorithm selection; and centralized policy enforcement. By integrating the CMF into the 5G/6G network architecture, operators can achieve true cryptographic agility, ensuring that the network remains secure and resilient against both current and future threats. Furthermore, the CMF can enable hybrid cryptographic schemes, allowing the simultaneous use of classical and post-quantum algorithms, thus facilitating a smooth transition to PQC without compromising the security of existing communications.

The remainder of this paper is structured as follows: Section II offers an overview of related research. Section III delves into the migration to PQC, covering standardized algorithms and the process involved in transitioning to PQC. Section IV examines PQC migration specifically within the context of mobile communications, providing an overview of the current cryptographic landscape in 5G and proposing a roadmap for transitioning to quantum-safe algorithms in 6G. Section V focuses on cryptographic agility, introducing the proposed Cryptographic Management Function, and elaborating on its architecture, functionality, and potential benefits, while also suggesting avenues for future research. Finally, Section VI concludes the paper by summarizing the key contributions and insights.

II. Related Work

Cryptographic agility has emerged as a critical requirement for 5G networks due to evolving security threats and the anticipated impact of quantum computing. Existing research highlights the need for seamless transitions between cryptographic algorithms, but current solutions fall short in providing practical frameworks. For example, Ecarot et al. discuss the challenges of cryptographic agility in 5G network slices, particularly in multi-vendor environments, but focus on individual network components without offering a comprehensive framework for seamless transitions across the network [6].

Wiesmaier et al. emphasize the importance of PQC migration but acknowledge the fragmented nature of global efforts. Their literature survey provides valuable insights, yet it does not tackle the specific issues related to cryptographic agility in mobile networks [7]. Similarly, Ott and Peikert address the broader challenge of PQC migration, stressing the importance of cryptographic agility for industry-wide adoption. However, their work highlights the complexity of migrating existing systems without delving into the specific architectural requirements for 5G/6G environments [8].

Cho et al. propose SDC as a means to centralize cryptographic governance and enable automated enforcement of cryptographic policies. While their approach is promising, it targets enterprise IT infrastructures [9]. Lastly, Döring et al. introduce a hybrid PQC and QKD architecture for securing 5G networks, but their reliance on quantum key distribution adds complexity and lacks the adaptability required for widespread 5G/6G deployment [10].

Despite significant advancements, gaps remain in developing a flexible cryptographic management system tailored for mobile networks. This paper proposes the CMF, an architectural approach designed to achieve cryptographic agility by dynamically managing transitions between cryptographic algorithms.

III. Post-Quantum Cryptography

Quantum computing substantially threatens traditional public-key cryptographic systems, which have relied on the computational difficulty of factoring large numbers and solving discrete logarithm problems. Shor's algorithm disrupts this security by factoring large numbers and solving discrete logarithms in polynomial time, effectively breaking widely-used systems like RSA and ECC. Similarly, Grover's algorithm reduces the complexity of brute-force attacks on symmetric key cryptography and hash functions by a square root factor. For example, Grover's algorithm reduces the security level of AES-128 from 128 bits to 64 bits and weakens the resistance of hash functions like SHA-256, making them comparable to a 128-bit hash in quantum scenarios. While the impact of Grover's algorithm can be mitigated for symmetric cryptography and hash functions by increasing key and output sizes, asymmetric systems such as RSA and ECC require entirely new, quantum-resistant algorithm replacement to maintain security.

One of the most pressing concerns in the cryptographic community is the "harvest now, decrypt later" attack, where attackers intercept and store encrypted data today with the expectation that quantum computers will eventually break current encryption algorithms. This poses a significant threat to sensitive, long-lived data, such as financial records, medical information, and governmental documents, which must remain secure for decades. Waiting for quantum computers to fully materialize before acting is a dangerous approach. Organizations must proactively begin migrating to PQC to ensure long-term protection against future quantum-based attacks. PQC algorithms are designed to resist both classical and quantum attacks. The National Institute of Standards and Technology (NIST) has taken the lead in global efforts and standardized PQC algorithms; and organizations are urged to begin planning for this migration now, as the process of fully transitioning cryptographic systems to PQC is both complex and time-consuming.

A. NIST Standardization Process

NIST is leading efforts to develop and standardize quantum-resistant cryptographic algorithms. It initiated a PQC Standardization process in 2016, inviting submissions of candidate algorithms that could resist quantum attacks. The process has been a rigorous multi-round evaluation, focusing on key-encapsulation

mechanisms (KEMs) and digital signature schemes. In August 2024, NIST released the final versions of its first three standardized algorithms:

- FIPS 203: a Module-Lattice-Based Key-Encapsulation Mechanism (ML-KEM) standard based on the CRYSTALS-Kyber algorithm.
- FIPS 204: a Module-Lattice-Based Digital Signature Algorithm (ML-DSA) standard that leverages the CRYSTALS-Dilithium algorithm.
- FIPS 205: a Stateless Hash-Based Digital Signature Algorithm (SLH-DSA) standard that provides an alternative digital signature scheme based on Sphincs+.

The PQC standardization process continues, and NIST is evaluating additional KEM candidates such as BIKE, Classic McEliece, and HQC. 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 in October 2024, 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.

IV. Quantum Migration in Mobile Networks

The widespread adoption of cryptographic mechanisms in mobile networks, particularly in 5G and emerging 6G architectures, creates a broad attack surface susceptible to quantum threats. A cryptographic-relevant quantum computer (CRQC) would fundamentally undermine the confidentiality, integrity, authentication, and non-repudiation mechanisms underpinning mobile network security.

A. Cryptographic Inventory

This section emphasizes the importance of conducting a comprehensive cryptographic inventory in 5G systems, detailing the critical cryptographic operations, the Network Functions (NFs) they rely on, and their interactions within the broader security architecture. Such an inventory is a crucial prerequisite for effectively planning and implementing PQC migration.

1) Authentication: Authentication is fundamental to 5G security, ensuring that only legitimate users access network services. The primary protocols include 5G Authentication and Key Agreement (5G AKA), which uses pre-shared SIM keys for mutual authentication; EAP-AKA, a flexible SIM-based variant; and EAP-TLS, a certificate-based protocol suited for IoT devices where SIM-based methods may not be practical.

These protocols involve three primary actors in mobile networks. The User Equipment (UE) that initiates the authentication process. The Home Network (HN) manages the long-term keys and subscriber information and the Serving Network (SN) handles the connection between the UE and the network, establishing secure communication links.

Cryptographic algorithms involved in this process include TUAK (based on the Keccak hash function) and MILENAGE (using the AES block cipher), which generate session keys for subsequent encrypted communication. Subscriber privacy is also safeguarded using the Subscription Concealed Identifier (SUCI), an encrypted version of the user's Subscription Permanent Identifier (SUPI) achieved via Elliptic Curve Integrated Encryption Scheme (ECIES). ECIES is vulnerable to quantum attacks and will have to be replaced by a quantum-safe scheme like ML-KEM. Quantum attacks do not yet break TUAK and MILENAGE [11].

Interaction between Network Functions:

- The Access and Mobility Management Function (AMF) communicates with the Authentication Server Function (AUSF) to authenticate the UE and establish security contexts.
- The Unified Data Management (UDM) stores and manages the cryptographic keys necessary for authentication and provides secure access to subscriber data.

2) NAS and AS Encryption: Once authentication is complete, encryption mechanisms protect the communication channels between the UE, the network's core, and the base station (gNB). Two types of signaling require cryptographic protection:

- Non-Access Stratum Encryption: Protects signaling messages between the UE and the AMF, using symmetric encryption algorithms such as AES, SNOW, and ZUC.
- Access Stratum Encryption: Ensures that data exchanged between the UE and the gNB remains confidential, relying on similar encryption mechanisms.

Current encryption methods achieve a 128-bit security level, but quantum threats demand stronger cryptographic protections. To future-proof 5G/6G encryption against quantum attacks, algorithms like 256-bit security AES, SNOW 5G and ZUC 256 should be considered to address weaknesses in existing systems.

3) Core Network Security: The 5G core network relies heavily on cryptographic operations to secure communications between NFs and to control access to network services. OAuth 2.0 is the framework used for access control, ensuring that only authorized entities can interact with NFs.

- JSON Web Tokens (JWTs) protected by JSON Web Signature (JWS) are employed to authenticate and authorize secure communication between VNFs.
- The Network Repository Function (NRF) serves as the authorization server, managing JWTs and ensuring that network services communicate securely via TLS.

Cross-network communication (e.g., between different Public Land Mobile Networks or PLMNs) is protected by Security Edge Protection Proxies (SEPP), which handle both mutual authentication and message integrity protection over the N32 interface.

4) Transport Network Security: In 5G, the security of the transport network – which facilitates communication between the Radio Access Network (RAN) and the core – is paramount. Security Gateways (SecGWs) are used to provide secure communication channels via IPSec tunnels, ensuring the confidentiality and integrity of data exchanged between base stations and core network functions.

- IKE and TLS protocols are used to establish secure channels.
- Public Key Infrastructure (PKI) is employed to authenticate base stations and SecGWs, using digital certificates to verify the identity of these network elements.

IKE and TLS are particularly vulnerable to "harvest now, decrypt later" attacks To address this, the Internet Engineering Task Force (IETF) is developing hybrid schemes for protocols such as TLS, IKEv2, and X.509, combining classical cryptography with post-quantum algorithms. Quantum security challenges extend beyond traditional network traffic, impacting Machine-to-Machine (M2M) and IoT communications.

B. Quantum Threats to Mobile Network Security

Quantum threats introduce sophisticated attack vectors that exploit the computational superiority of CRQCs. Malicious actors, ranging from nation-states to advanced cybercriminal organizations, could target mobile networks to decrypt communications, impersonate network components, or disrupt service delivery. The consequences of these vulnerabilities are severe. Subscriber privacy would be eradicated as attackers gain access to user identities, sensitive communications, and stored data. Authentication mechanisms could be compromised, facilitating unauthorized impersonation of users and devices, while network integrity would deteriorate under quantum-enabled manipulation of signaling protocols, configurations, and operational data. The loss of non-repudiation mechanisms would allow adversaries to forge or revoke critical actions, such as financial transactions, call records, and emergency communications, eroding trust in the reliability of mobile systems. Adding to these risks is the looming threat of "store-now-decrypt-later" which endangers not only real-time communications but also long-term sensitive data, exposing subscriber information and business-critical records to future compromise.

C. Proposed PQC Migration Strategy for 6G Networks

6G technology is set to revolutionize industries by delivering ultra-high-speed, low-latency, and extensive connectivity that enables real-time, personalized experiences, particularly benefiting sectors like healthcare, public safety, and entertainment. However, the anticipated transition to quantum-safe cryptographic solutions poses a substantial challenge, as integrating PQC into 6G networks demands a strategic approach. PQC migration can be achieved through the following steps: preparation, planning, and execution. The preparation phase focuses on evaluating PQC algorithms to ensure compatibility with 6G's performance demands, such as high-speed, resource-constrained environments. It also involves identifying diverse 6G use cases and security requirements within different network domains, including network access and Service-Based Architecture. In essence, this phase should determine where PQC will be essential and identify appropriate algorithms to meet the required security and performance levels. Planning establishes a roadmap for migration. PQC solutions are mapped to the specific use cases and security needs of the 6G ecosystem. It also involves deploying PQC in controlled, test environments that replicate real-world 6G conditions. These environments should allow for a detailed evaluation of PQC algorithms based on key metrics like latency, throughput, and energy consumption. Excecution focuses on the practical rollout of PQC solutions, prioritizing critical infrastructure components (e.g., Public Key Infrastructure), and implementing modular designs that allow for easy updates as new algorithms emerge. Flexible deployment methods; such as hybrid or gradual migration; are essential to maintain security while minimizing disruptions.

Embedding crypto-agility in this process ensures that 6G networks remain resilient and adaptable, dynamically responding to evolving cryptographic threats and leveraging advancements in quantum-safe solutions. Introducing a cryptographic management function within mobile networks from the start of the quantum migration process can significantly enhance crypto-agility.

V. Cryptographic Agility in Mobile Networks

Cryptographic agility has increasingly gained attention with the advancements in PQC, yet the concept has existed for over two decades. It encompasses a multifaceted approach to handling cryptographic components within systems, making it challenging to summarize in a single, universally accepted definition. Originally focused on enabling flexible algorithm replacements in cryptography, the term has expanded to include agility in protocols, applications, and IT infrastructures as well [12].

A. Cryptographic Agility

Crypto-agility spans a broad range of cryptographic elements, including algorithms, protocols, applications, cloud services, and distributed infrastructures. It plays a critical role in mitigating risks and adapting to emerging threats, such as implementation flaws, side-channel attacks, and evolving legal or compliance standards. Its relevance extends from IoT systems, where devices must be capable of adopting cryptographic updates seamlessly, to cloud services, which must maintain interoperability across diverse international regulatory frameworks [8]. Key properties of crypto-agility include effectiveness, enforceability, security, and backward compatibility, enabling systems to adapt to changing cryptographic requirements without impacting performance. Characteristics like scalability, interoperability, and real-time capability are

fundamental for systems operating in diverse environments, ensuring that cryptographic measures remain effective as systems evolve [13]. Crypto-agility manifests in various forms: algorithmic agility, which allows the replacement of algorithms as needed; implementation agility, facilitating the agile integration of cryptography into both software and hardware; composability agility, supporting the secure combination of multiple cryptographic keys or schemes; and security strength agility, enabling dynamic adjustments to security levels in response to new threats. It also includes platform agility, ensuring compatibility across different hardware and software platforms; context agility, which adapts cryptographic configurations based on system attributes; migration agility, allowing smooth transitions between cryptographic methods; and retirement agility, which enables the secure phase-out of outdated algorithms [14].

B. Proposed Cryptographic Management Function (CMF)

The introduction of the CMF in mobile networks is motivated by the increasing complexity of cryptographic management. As mobile networks evolve, their infrastructures become more complex, encompassing not only the core network but also edge computing, cloud environments, and hybrid architectures. These intricate infrastructures pose unique challenges for cryptographic operations and the seamless transition to PQC. The CMF is introduced as a pivotal addition to mobile networks to centralize and abstract cryptographic operations, ensuring efficiency, flexibility, and security. It provides a framework to manage cryptographic primitives, tools, modules, and providers in a structured and unified manner. This function addresses the challenges of cryptographic agility, offering a holistic solution for managing cryptographic processes across various network components. This work provides an overview of the CMF, while detailed specifications of its interfaces, integration within mobile networks, and implementation will be addressed in future research.

1) Components of CMF: The CMF is divided into two core components using the SDC framework in [5]: the Cryptographic Policy Decision Point (C-PDP) and the Cryptographic Policy Enforcement Point (C-PEP). Each serves distinct roles to maintain a seamless cryptographic environment within mobile networks:

- Cryptographic Policy Decision Point: The C-PDP handles the governance aspect of cryptographic processes. This component is responsible for managing cryptographic policies, decisions, and control mechanisms. It evaluates security requirements, monitors algorithm efficacy, and determines when cryptographic transitions should occur, such as when a vulnerability in an algorithm is identified or when a transition to PQC is necessary. The C-PDP interacts with other NFs to ensure that cryptographic policies remain consistent and are enforced network-wide, preventing mismatches or lapses in security.
- Cryptographic Policy Enforcement Point: The C-PEP is the operational side of the CMF, providing the cryptographic primitives, tools, modules, and cryptographic providers. It serves as the interface for executing the cryptographic tasks dictated by the C-PDP. The C-PEP ensures that cryptographic operations such as encryption, decryption, key management, and hashing are performed according to the policies set by the C-PDP. It abstracts the complexities of cryptographic tools, allowing other NFs to seamlessly integrate cryptographic functions without needing to manage the underlying cryptographic infrastructure themselves.

2) Proposed interaction with other network components in 5G: The CMF is designed to interface with other mobile network components through a well-defined interface, Ncmf, providing cryptographic services in a centralized manner.

The CMF would supply the AMF and AUSF with the necessary primitives for key derivation, authentication vectors, and encryption tools, handling algorithms like TUAK and MILENAGE. By abstracting these cryptographic operations, the CMF enables them to initiate authentication without handling the cryptographic intricacies directly. Similarly, the SMF and UPF would rely on the CMF for data encryption and integrity protection. As these functions manage user data and session setup, the C-PDP enforces policies regarding data encryption and integrity protocols. For instance, it determines the use of AES-256 to resist quantum attacks, as well as other compliance-focused requirements for data protection. The C-PEP supports these policies by supplying the necessary encryption and integrity primitives for NAS and AS signaling. The SMF and UPF can maintain high data protection standards while relying on the CMF's flexibility to update algorithms and key lengths as required by evolving security policies.

The NRF would use the CMF to secure service discovery and registration, benefiting from the C-PDP's policies on secure token management and the C-PEP's tools for token encryption and signing, which enhance authentication across network services. Inter-PLMN communication would rely on the CMF to maintain secure exchanges between PLMNs via the SEPP, where the C-PDP enforces cryptographic policies and the C-PEP provides encryption and signing tools.

In the transport network, SecGWs would depend on the CMF for establishing IPSec tunnels and securing RAN-core network communications. The C-PDP dictates the protocols and encryption standards necessary for IPSec tunnels, requiring PKI policies and, when appropriate, transitioning to quantum-resistant alternatives for TLS protocol. The C-PEP offers encryption tools for IPSec, as well as digital certificate management and secure key exchange protocols. The UDM function would depend on the CMF for secure handling of sensitive subscriber information, adhering to stringent encryption policies set by the C-PDP. With encryption tools provided by the C-PEP, the UDM/SIDF ensures secure storage and retrieval, particularly for data masked with SUCI. Lastly, the Application Function (AF) would interact with the CMF for secure data exchanges

and application-level security. Policies governed by the C-PDP ensure compliance with encryption and authentication standards, while the C-PEP provides encryption and signing tools to secure AF communications with external networks.

3) Key Advantages: The centralized structure of the CMF brings several key advantages to mobile networks. First, it ensures consistency and compliance by enforcing unified cryptographic policies across all network components, reducing the risk of inconsistencies and ensuring adherence to security standards and regulations. The CMF also enhances cryptographic agility, allowing seamless transitions between cryptographic algorithms, such as the shift to PQC or the adoption of innovative cryptographic technologies like Fully Homomorphic Encryption [15], [16], without requiring system-wide reconfigurations. Additionally, it supports scalability and flexibility, accommodating the expansion of 5G into diverse use cases like IoT and massive machine-type communication, while maintaining a cohesive cryptographic policy framework. By centralizing the decision-making and enforcement of cryptographic operations, the CMF strengthens the network's overall security posture, reducing the attack surface and ensuring continuous monitoring and optimization of cryptographic processes. The introduction of the CMF marks a significant advancement in the cryptographic architecture of mobile networks and ensures that they remain resilient and scalable in the face of evolving cryptographic challenges. It has the potential for achieving self-configured cryptography, highly compatible with the self-organized network vision in future networks.

4) Challenges and Security consideration: While the CMF centralizes cryptographic operations and enhances agility in mobile networks, it also introduces vulnerabilities that must be addressed to ensure security. A key risk is the complexity of cryptographic agility, which can open new attack vectors like downgrade attacks, where adversaries manipulate protocol negotiations to force weaker cryptographic configurations. Additionally, offering less secure or untested cryptographic suites for backward compatibility may increase the attack surface. The CMF's interfaces, which allow for interaction between various NFs, must be carefully designed to prevent misconfigurations or outdated settings. Balancing flexibility and security is essential, particularly as the CMF transitions to PQC, ensuring that agility mechanisms do not inadvertently introduce new weaknesses.

C. Areas for Further Exploration

As mobile networks grow more complex, the CMF offers a promising solution for managing cryptographic operations, but several key areas need further exploration to unlock its full potential. Integrating machine learning into the CMF could enhance cryptographic agility, allowing it to adapt proactively to network conditions and emerging threats. Context-aware cryptographic agility, where the CMF adjusts cryptographic configurations based on data type, location, or regulatory requirements, presents another valuable direction for research. Additionally, refining user interfaces for cryptographic management is crucial to prevent misconfigurations and streamline secure operations. Addressing these areas will help ensure the CMF's effectiveness in securing 5G networks and beyond.

VI. Conclusion and Outlook

In this paper, the Cryptographic Management Function was presented as a novel approach to achieving cryptographic agility in mobile networks. A centralized framework is provided by the CMF for managing cryptographic operations, allowing seamless transitions between algorithms and protocols as security requirements evolve. By decoupling cryptographic functions from other network components, rapid updates are facilitated, which is crucial for Post-Quantum Cryptography. Policy enforcement is centralized to minimize human error. Hybrid cryptographic schemes are supported, ensuring a smooth transition to quantum-safe solutions while maintaining compatibility with current systems. As networks progress toward 6G and quantum computing, the CMF is positioned as a scalable and flexible solution to future-proof mobile communications.

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] W. Jiang, B. Han, M. A. Habibi, and H. D. Schotten, "The road towards 6G: A comprehensive survey," *IEEE Open Journal of the Communications Society*, vol. 2, pp. 334–366, 2021.

[2] W. Saad, M. Bennis, and M. Chen, "Avision of 6G wireless systems: Applications, trends, technologies, and open research problems," *IEEE network*, vol. 34, no. 3, pp. 134–142, 2019.

[3] D. J. Bernstein and T. Lange, "Post-quantum cryptography," *Nature*, vol. 549, no. 7671, pp. 188–194, 2017.

[4] L. Hornquist Astrand and T. Yu, *RFC 6649: Deprecate DES, RC4-HMAC-EXP, and Other Weak Cryptographic Algorithms in Kerberos*, 2012.

[5] J. Cho, C. Lee, E. Kim, J. Lee, and B. Cho, *Software-Defined Cryptography: A Design Feature of Cryptographic Agility*, Cryptology ePrint Archive, Paper 2024/518, 2024.

[6] T. Ecarot, P.-M. Tardif, and T. Raynaud, "Cryptographic Agility Evaluation for 5G Slices: Challenges and Solutions," *IEEE Communications Magazine*, 2021.

[7] A. Wiesmaier, N. Alnahawi, and T. Grasmeyer, "On PQC Migration and Crypto-Agility," *International Journal of Information Security*, 2019.

[8] D. Ott and C. Peikert, "Identifying Research Challenges in Post Quantum Cryptography Migration and Cryptographic Agility," in *Computing Community Consortium Workshop*, 2019.

[9] J. Cho, C. Lee, E. Kim, B. Cho, and J. Lee, "Software-Defined Cryptography: A Design Feature of Cryptographic Agility," *IEEE Transactions on Information Forensics and Security*, 2020.

[10] R. Döring, M. Geitz, and R.-P. Braun, "Post-Quantum Cryptography Key Exchange to Extend a High-Security QKD Platform into the Mobile 5G/6G Networks," *IEEE Quantum Communications Journal*, 2021.

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

[12] N. Alnahawi, N. Schmitt, A. Wiesmaier, A. Heinemann, and T. Grasmeyer, "On the state of crypto-agility," *Cryptology ePrint Archive*, 2023.

[13] H. A. Mehrez and O. El Omri, "The crypto-agility properties," in *The 12th International Conference on Society, Cybernetics and Informatics*, 2018, pp. 99–103.

[14] T. Macaulay and R. Henderson, “Cryptographic agility in practice: emerging use-cases,” *Infosec Global*, 2019.
[15] S. P. Sanon, C. Lipps, and H. D. Schotten, “Fully Homomorphic Encryption: Precision Loss in Wireless Mobile Communication,” *2023 European Conference on Networks and Communications (EuCNC) & 6G Summit.*,
[16] S. P. Sanon, I. Ademi, M. Zentara, and H. D. Schotten, “Applicability of Fully Homomorphic Encryption in Mobile Communication,” in *2024 3rd International Conference on 6G Networking (6GNet)*, 2024, pp. 234–240.