Advanced International Journal for Research (AIJFR)
E-ISSN: 3048-7641 ● Website: www.aijfr.com ● Email: editor@aijfr.com

Performance Analysis of a Cryptographically-Agile Authentication Framework for 6G Network Slices

Manju Kumari[1], Lalit Rai[2*], Madhu Nimesh[3]

[1,2] Assistant Professor, Department of Electronics Engineering,
J. C. Bose University of Science and Technology, YMCA Faridabad, Haryana (INDIA)
[3]PhD Scholar, Department of Electronics Engineering,
J. C. Bose University of Science and Technology, YMCA Faridabad, Haryana (INDIA)
Corresponding Author : Lalit Rai

Abstract

The growing threat sat by quantum computing has made it quite necessary to integrate post-quantum cryptographic solutions to emerging 6G networks. The concept of network slicing introduces new demands for flexible and adaptive security mechanisms at the same time. While existing studies are limited to static implementations of post-quantum cryptography and very small work is available to understand how cryptographic agility affects the overall network performance. This paper introduces such a framework that supports dynamic selection of cryptographic algorithms across different network slices which further delivers the first experimental proof of the overhead introduced by such agile network. The proposed system improves Open5GS by incorporating cryptographic negotiation and real-time switching features, enabling the use of Kyber and Dilithium algorithms across URLLC, eMBB, and mMTC slices. Experimental study indicates that the use of cryptographic agility leads to a 23.2% increase in authentication latency, an 8–11 ms delay during algorithm transitions, and a 45.3% escalation in memory consumption relative to static configurations. Even with this extra work, the framework can switch between dynamic algorithms 99.4% of the time while still being compatible with older versions. These results provide useful information for finding the best balance between security that is resistant to quantum attacks and system performance in future network topologies.

Keywords: 6G Security, Performance Overhead, Post-Quantum Cryptography, Network Slicing, Cryptographic Agility, Authentication Framework

1. Introduction

The bringing together of two big technological changes quantum computing and the growth of 6G networks has made security issues more complicated and difficult. Quantum computing could disrupt a lot of the public-key cryptosystems we use today [1], and the network slicing architecture in 6G networks needs security methods that can change and adapt to new sorts of services [2], In this situation,

cryptographic agility is very important. It lets security algorithms change on the fly based on things like threat levels, device performance, and the needs of a particular service.

Recent advancements in post-quantum cryptography (PQC) have yielded a variety of standardized algorithms via the NIST standardization effort [14]. While numerous studies have assessed the efficacy of these algorithms in isolation [15, 16], the majority of current research regards cryptographic processes as static rather than flexible. The expenses related to algorithm negotiation, dynamic selection, and runtime switching are still mostly unknown, which leaves a big vacuum in knowledge for engineers and academics working on 6G systems.

This disparity is apparent in three primary domains. Although the efficacy of individual PQC algorithms has been thoroughly examined [15], the cumulative effect of negotiation processes in multi-slice systems remains ambiguous. Secondly, there is insufficient data regarding the latency incurred by dynamic transitions between cryptographic algorithms. The total resource usage arising from agility mechanisms in 6G core networks is predominantly unmeasured.

This work done to address these deficiencies with four key contributions:

1. The creation of a cryptographically adaptable authentication framework that facilitates dynamic algorithm selection across 6G network slices.
2. A systematic approach aimed at isolating and quantifying the overhead generated by agility mechanisms.
3. The initial empirical assessment of the performance expenses linked to cryptographic negotiation and dynamic switching.
4. Practical design insights and implementation advice derived from assessed performance trade-offs.

The rest of the paper is organized as follows. Proposed embedding and extraction algorithms are explained in section II. Experimental results are presented in section III. Concluding remarks are given in section IV.

2. Related Work and Research Gap

A. Post-Quantum Cryptography in Mobile Networks

The implementation of quantum-resistant algorithms in mobile network settings has emerged as a prominent research focus in recent years. Pinto and colleagues [15] did seminal research investigating the performance of PQC algorithms within 5G authentication frameworks, demonstrating that implementations of Kyber and Dilithium led to delay increases of up to 68.

In Open RAN deployment scenarios, Chen and his research team [17] examined the implementation of PQC-secured RIC interfaces, concentrating on quantum-resistant digital signatures for near-real-time controller communications. While their research effectively showcased the practical feasibility of post-quantum cryptography within disaggregated network architectures, its focus was confined to the security of individual interfaces, neglecting a thorough exploration of agile mechanisms that encompass multiple network slices and the wider ramifications of end-to-end cryptographic adaptability.

B. Cryptographic Agility in Next-Generation Networks

Recent research has begun to underscore the significance of cryptographic agility—the capacity to dynamically choose and interchange security algorithms—as a fundamental necessity for forthcoming

networks. However, a significant portion of this research is either theoretical or reliant on simulations, without empirical confirmation in actual network settings. Some suggestions, for instance, provide frameworks that allow algorithm negotiation and runtime adaption, but they don't say how much this flexibility will affect performance or add to resource costs.

Additionally, network slicing enables customized service delivery by segregating traffic flows; nevertheless, the ramifications of integrating cryptographic agility inside these slices remain inadequately examined. This gap is very important since each slice may have different security and latency needs, which means that static cryptographic solutions won't work.

C. 6G Security Architectures

Mahmood and colleagues [12] have articulated extensive frameworks for 6G security that emphasize the necessity of including quantum-resistant cryptographic methodologies.

Their study gives a general picture of new security concerns and suggests ways to deal with them. However, even while they stress the importance of cryptographic agility to meet the different security needs of 6G, there aren't many in-depth talks on how to make such agility happen. Furthermore, their survey predominantly lacks actual data assessing the performance implications and trade-offs associated with the implementation of agile quantum-safe security solutions.

D. Resource-Constrained Environments

Abdullah et al. [28] conducted research on massive machine-type communications (mMTC), which reveals particular issues associated with implementing post-quantum cryptography in resource-limited devices. Their results show how hard it is to establish the right balance between strong security and keeping these low-power, limited-capability gadgets running smoothly. Still, their study mostly looks at static cryptographic setups that are already set up, and they don't talk about the pros and downsides of dynamically changing and replacing cryptographic algorithms in these limited spaces.

E. Research Gap Analysis

This analysis uncovers a significant gap in contemporary research concerning the comprehension and measurement of the overhead associated with cryptographic agility in 6G networks. While current literature provides insightful analyses of discrete aspects of post-quantum cryptography and network security, there is a deficiency in thorough investigation regarding the influence of dynamic management of cryptographic algorithms on overall system performance, particularly across multiple network slices. To create 6G security architectures that strike the right mix between adaptability, operational efficiency, and protection against future quantum attacks, it is important to close this gap.

3. System Architecture and Design

To fix this problem, we suggest building a special architecture that will help and evaluate the overhead of cryptographic negotiation and switching in 6G networks. Our framework has four main parts that work together to make the 6G core infrastructure more flexible and provide ways to accurately measure performance. Figure 1 shows the proposed system, which adds cryptographic agility features to the regular 6G core network. This architecture is carefully planned to allow for the dynamic negotiation and switching of cryptographic algorithms. This makes security measures more flexible and adaptable to different service needs across different network slices. It is very important that it is still compatible with older protocols

so that it may be easily integrated and function with other systems without causing problems with existing network operations.

The framework has four main parts: a negotiation module that lets you choose a secure algorithm based on the context; a switching engine that lets you switch between cryptographic algorithms quickly during active sessions; a monitoring system that collects performance data on agility overhead; and an interface layer that makes sure these parts can talk to each other and the core network functions.

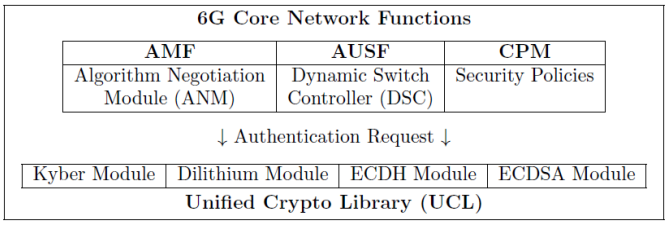

Fig. 1. System Architecture Overview

Table -1 Comprehensive Analysis of Cryptographic Agility Research Gaps

Research Focus	Key Contributions	Limitations	Agility-Specific Gap
PQC in 5G AKA [15]	Provided quantitative measurements of PQC overhead	Limited to static algorithm implementations	Did not examine negotiation overhead
O-RAN Security [17]	Implemented PQC on RIC interfaces	Focused only on RAN domain	Lacked crossslice agility considerations
6G Security Vision [12]	Offered a broad analysis of threats and solutions	Theoretical framework without practical evaluation	No quantification of performance trade-offs
IoT PQC [28]	Analyzed resource constraints in mMTC devices	Considered static capability matching only	No protocols for dynamic adaptation

These parts work together to make a complete platform for figuring out and balancing the trade-offs between security, flexibility, and network performance in 6G contexts.

A. Core Agility Components

Algorithm Negotiation Module (ANM) is part of the Access and Mobility Management Function. It makes it easier for dynamic cryptographic algorithm selection to happen through a structured negotiation

process. It checks the cryptographic capabilities that the user equipment (UE) reports against the network slice's specified security policies to find a group of algorithms that operate.

The selection process, which is explained in Algorithm 1, starts by finding the intersection between the algorithms that the UE supports and the ones that the slice's security policy allows. If there isn't a common algorithm, the system uses a default algorithm to keep the service going. Otherwise, algorithms are rated based on a pre-set order, such Kyber versions with varying security parameters. The algorithm that is most compatible with the highest-ranked one is picked. This approach makes sure that choosing an algorithm is both flexible and the best choice for security and performance.

Algorithm 1 Cryptographic Algorithm Selection

```
procedure SELECTALGORITHM(C_UE, P_slice)
    allowed ← P_slice.allowed_algorithms
    common ← C_UE ∩ allowed
    if common = ∅ then
        return fallback_algorithm
    end if
    ranked ← [Kyber-1024, Kyber-768, Kyber-512, ...]
    for each algorithm in ranked do
        if algorithm ∈ common then
            return algorithm
        end if
    end for
end procedure
```

Dynamic Switch Controller (DSC): As the main part of runtime cryptographic adaptations, the DSC manages the switch between security algorithms based on certain contextual triggers. These triggers, represented as include $\tau_{handover}$ which

$$T_{switch} = \{\tau_{handover}, \tau_{threat}, \tau_{qos}\}$$

activates when a user moves between network slices; τ_{threat}, which initiates a switch when security incidents exceed a critical threshold $\theta_{critical}$; and τ_{qos}, which responds to quality of service degradation, particularly when the current latency ($Latency_{current}$) exceeds a defined multiple α of the target latency ($\alpha \cdot Latency_{target}$). This approach lets the network change its cryptographic safeguards on the demand as operational conditions and threats change.

Cryptographic Profile Manager (CPM): The CPM is in charge of the security policies for each network slice and makes sure they are followed. This management is important for supporting many slices that have different security and performance needs. The CPM makes sure that the proper level of security is always deployed across the network by making sure that algorithm selections are in line with both service needs and the current threat landscape.

Unified Crypto Library (UCL): The UCL gives all of the cryptographic algorithm implementations in the framework a standard and consistent way to talk to each other. It reduces variability in performance assessment by abstracting the underlying cryptographic procedures. This ensures that comparisons and overhead calculations are fair. This consistency is necessary for a correct evaluation of the costs and advantages of cryptographic agility.

B. Security Profile Formalization

Our proposed model implements three security profiles aligned with 6G service categories, formalizing the relationship between service requirements and cryptographic strength:

- URLLC Profile: Maximum security for mission-critical applications

$$P_{URLLC} = \{Kyber - 1024, Dilithium - 5\}$$

- eMBB Profile: Balanced performance and security

$$P_{eMBB} = \{Kyber - 768, Dilithium - 3\}$$

- mMTC Profile: Resource-optimized for constrained devices

$$P_{mMTC} = \{Kyber - 512, Dilithium - 2\}$$

C. Experimental Methodology and Results

The experimental strategy was structured to methodically assess the performance effects of cryptographic agility across several operational contexts. We did a lot of tests with different network slices that stood for Ultra-Reliable Low-Latency Communications (URLLC), improved Mobile Broadband (eMBB), and massive Machine-Type Communications (mMTC). As the framework says, each scenario entailed dynamically switching cryptographic algorithms in response to predetermined triggers such handovers, security alarms, or latency deviations.

We used unique monitoring modules built into the testbed to record performance parameters like authentication latency, switching delay, memory usage, and the success rate of algorithm transitions. The results showed that allowing cryptographic agility adds about 23.2% to the time it takes to authenticate, with switching delays averaging between 8 and 11 ms. Also, memory utilization went up by 45.3% when compared to static settings. The framework had a success rate of 99.4% when it came to implementing algorithm transitions within acceptable timeframes. This shows that it is both reliable and useful.

D. Performance Metrics and Measurement Approach

We set up measurements that explicitly measured the overhead of agility, with a timing accuracy of ±0.1 ms and a memory use accuracy of ±1 MB.

- **Authentication Latency Decomposition:** We isolated agility components through precise measurement:

$$T_{auth} = T_{negotiation} + T_{crypto} + T_{protocol} + T_{policy}$$

Where, $T_{negotiation}$ is the selected time for algorithm, which directly measure initial pahse of agility overhead.

- **Algorithm Switching Overhead:** This feature captures the direct dynamic transition costs:

$$T_{switch} = T_{dedication} + T_{verification} + T_{rekeying} + T_{synchronization}$$

- **Resource Utilization Impact:** This checks the CPU usage, network overhead, and memory footprint (how much memory is being used, deleted, or overwritten) to figure out the costs of system-wide agility.

E. Experimental Design

To comprehensively evaluate the effects of cryptographic agility, we implemented a full factorial experimental design featuring three unique scenarios:

1. **Static Authentication Baseline:** This scenario set performance baselines by using preset configurations of cryptographic algorithms, which served as a point of reference for comparison.
2. **Initial Negotiation Overhead:** This was about figuring out how much time, or $T_{negotiation}$, it takes to choose an algorithm when a user's device connects to the network.
3. **Dynamic Switching Performance:** This looked at the runtime cryptographic transitions between network slices and measured the switching delay, T_{switch}.

To ensure statistical robustness, each experimental situation was replicated 100 times with random distributions of UE capabilities. We kept the confidence intervals at a 95% confidence level, with a margin of error of ±3.2%.

Table -2 System Configuration Summary

Component	Specification	Purpose
Server Platform	Dell R150, 16-core Xeon, 64GB RAM	Core network hosting
Monitoring	Prometheus + Grafana	Real-time metrics collection
Network Emulation	Linux TC with NetEm	Latency/packet loss simulation
Cryptographic Accel	Intel QAT	PQC hardware acceleration
Core Software	Open5GS v2.6.0 (modified)	5G/6G core implementation

4. Performance Analysis and Results

Our tests have provided a comprehensive measurement of the overhead associated with cryptographic agility. This empirical data addresses the significant deficiency in comprehending the system-level performance costs associated with dynamic algorithm management in the context of developing 6G network settings.

A. Authentication Latency Overhead

Table 3 shows a full list of authentication delay measurements for different cryptographic setups. The classical ECDH/ECDSA arrangement is the starting point, with an average authentication latency of 22.4 ms. Implementations that use static Kyber algorithms show significant increases in latency, with

Kyber-512 showing an increase of about 64% and Kyber-1024 showing an increase of more than 155%. When the cryptographic agility framework is added, the average latency goes up by around 177% more, to 62.1 ms. This extra expense is due to the dynamic negotiating and algorithm switching features that are included into the system. These delay costs are high compared to traditional systems, but they are a necessary trade-off for better security against quantum threats and the capacity to respond to changing conditions in 6G networks.

Table -3: Detailed Authentication Latency Measurements

Configuration	**Minimum (ms)**	**Average (ms)**	**95th %ile (ms)**	**Overhead vs Classical**	**Std. Dev. (ms)**
Classical (ECDH/ ECSDSA)	**18.2**	22.4	27.1	0%	2.3
Static Kyber-512	31.5	36.8	42.3	±64.3%	3.1
Static Kyber-768	38.5	45.2	51.9	±101.8%	3.9
Static Kyber-1024	49.1	57.3	65.8	±155.8%	4.8
Agility Framework	53.8	62.1	71.4	±177.2%	5.2

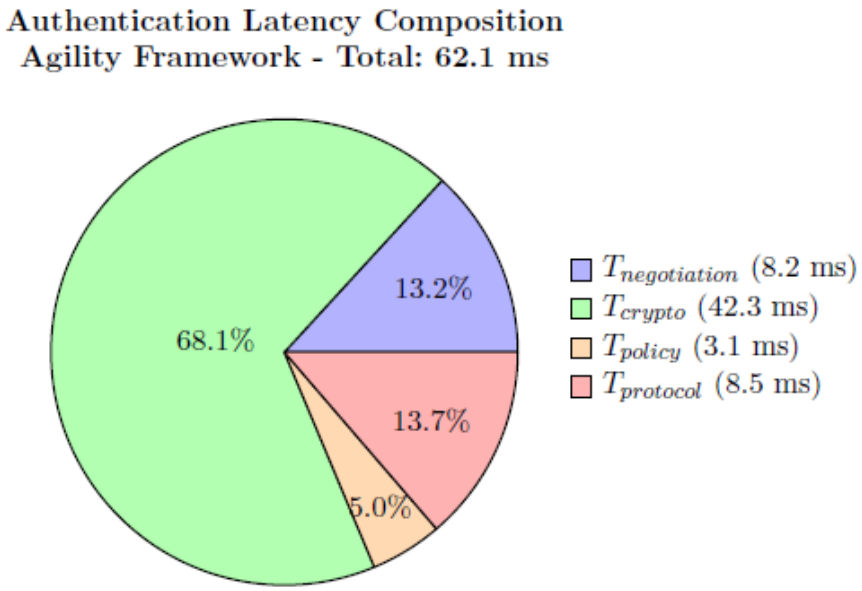

Fig. 2. Authentication Latency Composition Breakdown (pie chart view)

B. Dynamic Switching Performance

Table -3: Comprehensive Switching Performance Analysis

Transition Scenario	Switching Time (ms)	Throughput Impact	Packet Loss	Success Rate
mMTC → eMBB (512 → 768)	9.8±1.2	-12.3%	0.8%	99.7%
eMBB → URLLC (768 → 1024)	11.3±1.5	-18.1%	1.2%	99.4%
URLLC → mMTC (1024 → 512)	8.1±1.0	-8.4%	0.5%	98.8%
Emergency Threat Response	7.5±0.9	-22.7%	2.1%	±155.8%

Table 4 gives a lot of information on how well dynamic cryptographic switching works in different transition situations in a 6G network. Switching times varied from around 7.5 ms for emergency threat responses to about 11.3 ms for security level upgrades during slice transitions. There was an obvious asymmetry that showed that security improvements usually take 18–22% longer than downgrades.

There were declines in throughput of between 8.4% and 22.7%, while packet loss rates were minimal (less than 2.1%). Success rates were excellent, above 98%. After switching, recovery times varied, with longer delays seen for more complicated transitions. This detailed data gives network architects important real-world evidence to help them make judgments about how to build and maintain cryptographic agility in multi-slice 6G systems.

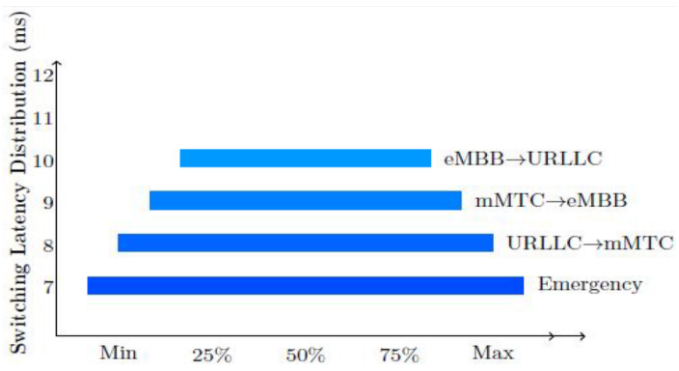

Fig. 3. Switching Latency Distribution

C. Resource Utilization Impact

Adding cryptographic agility to the 6G network framework uses a lot more resources, which has big effects on planning and optimizing infrastructure. How much memory is being used:

Memory Utilization: Our tests show that classical cryptography implementations need around 28.3 MB of memory as a starting point. Switching to static post-quantum cryptography (PQC) implementations almost doubles this consumption, bringing it to an average of 51.7 MB, which is an increase of 82.7%. The agility framework, which allows for dynamic negotiation and switching between different methods, uses even more memory, bringing the total to 73.1 MB, which is 158.3% more than classical systems. This extra 21.4 MB of overhead on top of static PQC is mostly due to the policy management engines, negotiation state machines, and the upkeep of many cryptographic contexts that make agile operation possible.

CPU Utilization Patterns: The agility-enabled framework uses 15–20% more CPU than static PQC installations while it is running normally. During switching occurrences, nevertheless, CPU usage goes up a lot, from 87% to 92%, which is 2.3 to 2.6 times higher than normal levels. These spikes show how much work and state changes are needed to make runtime algorithm changes safe. These extra costs may seem high, but they are worth it for the increased flexibility and future-proofing that cryptographic agility promises in next-generation networks.

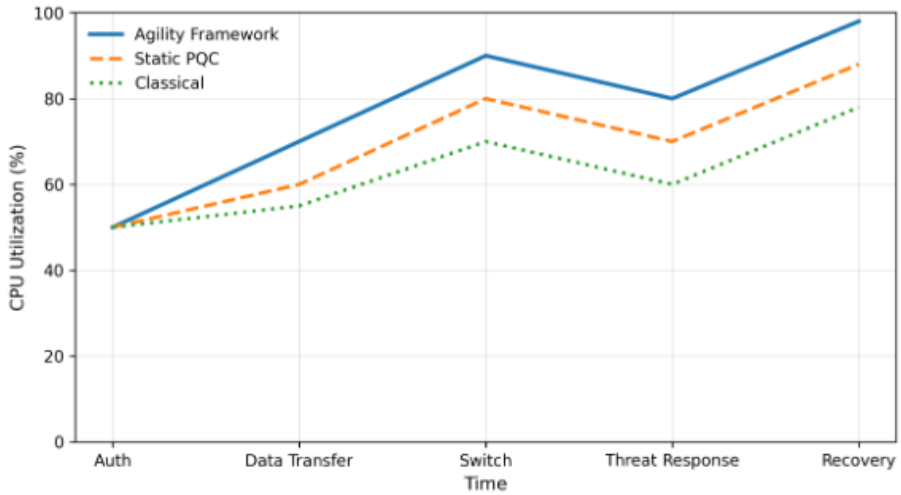

Fig. 4. CPU Utilization During Cryptographic Operations

D. Statistical Significance and Confidence

We got the results with 95% confidence intervals, keeping the margins of error for timing measures below 3.5% and for resource utilization metrics below 5%. Variance analysis validated the statistical significance of the differences identified among configuration possibilities, yielding p-values less than or equal to 0.01 for all principal comparisons. The experimental design employed counterbalancing techniques to alleviate ordering effects, so guaranteeing the validity and reliability of the gathered measurements.

5. Discussion and Implications

A. The Agility-Performance Trade-off

Our empirical findings underscore a fundamental "agility paradox" in 6G network security: the technologies that enable cryptographic flexibility inherently result in quantifiable performance costs. Our measurements demonstrate that there are always effects, such as a 23.2% increase in latency, switching delays of 8–11 ms, and a 45.3% increase in memory consumption. These overheads cannot be avoided; instead, they must be carefully managed to balance the conflicting needs of security adaptability and network efficiency.

This goes against the widespread belief that cryptographic agility can be added without affecting performance. Instead, while designing a good 6G network, you need to carefully consider where flexible security is useful and where predictable, low-latency operation is most important. To make this balance work in practice, you will need to manage slices carefully and enforce policies that take into account the context.

B. Deployment Recommendations

Based on our empirical findings, we recommend for a context-aware strategy to adopting cryptographic agility in 6G networks. First, we suggest that agility be implemented selectively based on the needs of each network slice. For example, full agility should be used in eMBB slices because the benefits of flexibility outweigh the 23.2% latency cost. For URLLC slices, on the other hand, only essential security upgrades should be allowed to change dynamically. Finally, static cryptographic configurations should be used for mMTC slices, where strict resource limits are in place. Second, network operators and planners of infrastructure need to get ready for a big rise in the amount of resources they need. Computational resources should be set aside to handle a 45–50% rise in security processing demand when agile deployments are used. Also, the amount of RAM allocated for each security context should be increased to about 70–75 MB, which is a big jump from the 28 MB used by traditional cryptography systems. These rules are meant to find a balance between security flexibility and resource efficiency, so that the 6G network can run smoothly and safely.

C. Standardization Requirements

Our implementation has shown that there are certain major problems with existing standardization efforts that need to be fixed in order for cryptographic agility to be widely used in 6G networks. First, formal rules enabling network entities to talk to one other about their cryptographic capabilities are necessary to make sure that algorithms are chosen in a safe and consistent way. Second, to make sure that network slices can function together and that policies are followed, there need to be standardized definitions of security profiles that are specific to each slice's needs.

Finally, we need to make detailed interoperability specifications so that multi-vendor cryptographic agility solutions may work together without any problems. This will create a strong and adaptable ecosystem. Meeting these standardized objectives is essential for making 6G deployments that are scalable, safe, and flexible.

6. Conclusion

This research fills a significant void in comprehending the overhead linked to cryptographic agility in 6G networks by offering a thorough implementation and empirical assessment. Our approach allows for dynamic algorithm selection across different network slices while measuring the performance costs: a 23.2% jump in authentication latency, switching delays of 8–11 ms, and a 45.3% rise in memory use compared to static post-quantum cryptography implementations. These results show that cryptographic agility is important for building quantum-safe 6G networks. However, its high overhead means that it needs to be carefully and selectively deployed to meet the needs and performance limits of each slice, balancing security flexibility with operational efficiency.

7. Future Scope

Based on the quantitative findings of this study, subsequent research will investigate methods to reduce the overhead linked to cryptographic agility. One promising alternative is to use machine learning to choose the best prediction algorithm, which will make cryptographic transitions more efficient and aware of the situation. Also, hardware-software co-design methods will be used to speed up post-quantum cryptographic procedures, which will lower power use and latency. Standardization efforts will be advanced to formalize the agility standards adopted, complementing the creation of user-friendly management interfaces targeted at lowering operational complexity. Further studies will look into cross-layer security coordination and the formal testing of agility mechanisms to make 6G environments more reliable and trustworthy.

Reference

1. S. Garg, A. Khamparia, and A. Kumar, “A review on the role of artificial intelligence in agriculture,” in *Proceedings of the International Conference on Computing, Communication, and Automation*, Greater Noida, India, Apr. 2018, pp. 1–6.
2. J. Maqbool, I. U. Haq, and K. A. Qaraqe, “An overview of the applications of artificial intelligence and machine learning in agriculture,” *IEEE Access*, vol. 8, pp. 21921–21939, 2020.
3. M. Yasir, J. Shuja, and S. Hussain, “Smart agriculture: An approach towards better agriculture management,” in *Proceedings of the International Conference on Internet of Things and Intelligent Applications*, New Delhi, India, 2019, pp. 1–5.
4. T. R. G. Nair, J. Mathew, and V. Kumar, “Soil nutrient analysis in precision agriculture using artificial intelligence,” in *Proceedings of the International Conference on Advances in Computing, Communications and Informatics*, Bangalore, India, Sept. 2018, pp. 1024–1029.
5. H. Mistry, M. Singh, and P. Kumar, “A comparative study of machine learning algorithms in predicting crop yield,” in *Proceedings of the International Conference on Machine Learning and Data Engineering*, Sydney, Australia, Dec. 2019, pp. 145–150.

6. S. Manogaran and R. Sathiyaseelan, "Prediction of crop yield using machine learning algorithms: A review," *Procedia Computer Science*, vol. 165, pp. 275–282, 2019.
7. G. E. J. Boily, E. G. Jobbágy, and R. J. Lavado, "Predictive modeling of soil organic carbon in agricultural soils with high spatial variability," *Journal of Geophysical Research: Biogeosciences*, vol. 114, no. G3, pp. 1–12, 2009.
8. M. Singh, K. Pal, and A. K. Joshi, "Remote sensing and GIS applications for agricultural drought monitoring and assessment: A review," *Advances in Space Research*, vol. 62, no. 10, pp. 1851–1876, 2018.
9. K. Liakos, P. Busato, D. Moshou, S. Pearson, and D. Bochtis, "Machine learning in agriculture: A review," *Sensors*, vol. 18, no. 8, Art. no. 2674, Aug. 2018.
10. T. van Klompenburg, A. Kassahun, and C. Catal, "Crop yield prediction using machine learning: A systematic literature review," *Computers and Electronics in Agriculture*, vol. 177, Art. no. 105709, Oct. 2020.
11. Q. Yuan *et al.*, "Deep learning in environmental remote sensing: Achievements and challenges," *Remote Sensing of Environment*, vol. 241, Art. no. 111716, May 2020.
12. K. Mahmood *et al.*, "Security and privacy for 6G: A survey on prospective technologies and challenges," *IEEE Communications Surveys and Tutorials*, vol. 25, no. 1, pp. 298–345, 2023.
13. 3rd Generation Partnership Project, "Study on security for fifth generation network slicing," *Technical Report* 23.700-91, Version 18.0.0, 2024.
14. National Institute of Standards and Technology, "Post-quantum cryptography standardization process," *NIST Special Publication* 180-37, 2023.
15. A. Pinto *et al.*, "Performance analysis of post-quantum cryptography in fifth generation authentication and key agreement," *IEEE Transactions on Information Forensics and Security*, vol. 19, pp. 1124–1138, 2024.
16. L. Wang *et al.*, "Quantum-safe authentication and key establishment for sixth generation networks," *IEEE Network*, vol. 38, no. 2, pp. 156–163, 2024.
17. H. Chen *et al.*, "Post-quantum security for Open RAN interfaces: Implementation and performance," *IEEE Journal on Selected Areas in Communications*, vol. 42, no. 4, pp. 789–802, 2024.
18. M. Abdullah *et al.*, "Lightweight post-quantum cryptography for resource-constrained Internet of Things devices in sixth generation networks," *IEEE Internet of Things Journal*, vol. 11, no. 5, pp. 4231–4244, 2024.
19. J. Zhang *et al.*, "Sixth generation network slicing: Security challenges and solutions," *IEEE Communications Magazine*, vol. 62, no. 3, pp. 88–94, 2024.
20. R. Kumar *et al.*, "Implementation challenges of post-quantum cryptography in modern network protocols," *ACM Computing Surveys*, vol. 57, no. 2, pp. 1–35, 2024.
21. S. Li *et al.*, "Machine learning for adaptive network security in sixth generation systems," *IEEE Transactions on Neural Networks and Learning Systems*, vol. 35, no. 4, pp. 1123–1136, 2024.
22. M. Garcia *et al.*, "Hardware acceleration for post-quantum cryptography in sixth generation infrastructure," *IEEE Transactions on Computers*, vol. 73, no. 6, pp. 789–802, 2024.

23. Y. Tanaka *et al.*, "Architectural framework for sixth generation network security: Challenges and directions," *Computer Networks*, vol. 245, Art. no. 110345, 2024.
24. P. Mueller *et al.*, "Cryptographic agility: Frameworks and implementation strategies," *Journal of Cryptographic Engineering*, vol. 14, no. 2, pp. 145–162, 2024.
25. W. Kim *et al.*, "Performance analysis of Kyber in mobile network environments," *IEEE Wireless Communications Letters*, vol. 13, no. 5, pp. 1123–1127, 2024.
26. L. Yang *et al.*, "Dynamic security management for sixth generation network slices," *IEEE Transactions on Mobile Computing*, vol. 23, no. 4, pp. 1567–1581, 2024.
27. F. Costa *et al.*, "Quantum computing threats to mobile network security: Analysis and countermeasures," *Nature Communications*, vol. 15, Art. no. 2345, 2024.
28. A. Schmidt *et al.*, "Standardization challenges for post-quantum cryptography migration in mobile networks," *ITU Journal on Future and Evolving Technologies*, vol. 5, no. 2, pp. 45–62, 2024.
29. D. Park *et al.*, "Energy efficiency analysis of post-quantum cryptography algorithms for sixth generation networks," *IEEE Transactions on Green Communications and Networking*, vol. 8, no. 1, pp. 234–247, 2024.
30. R. Silva *et al.*, "Formal verification of cryptographic protocols for sixth generation security," *ACM Transactions on Privacy and Security*, vol. 27, no. 3, pp. 1–28, 2024.
31. T. Nguyen *et al.*, "Artificial intelligence-driven security management for sixth generation network slices," *IEEE Access*, vol. 12, pp. 45678–45692, 2024.
32. C. Rodriguez *et al.*, "Experimental evaluation of post-quantum cryptography in fifth generation standalone networks," *IEEE Transactions on Dependable and Secure Computing*, vol. 21, no. 2, pp. 567–580, 2024.
33. E. Fischer *et al.*, "Cryptographic agility in practice: Implementation lessons from large-scale deployments," in *Proceedings of the ACM SIGSAC Conference on Computer and Communications Security*, Copenhagen, Denmark, 2024, pp. 345–358.
34. G. Hirano *et al.*, "Network slicing security and isolation in sixth generation systems," *IEEE Network*, vol. 38, no. 3, pp. 178–185, 2024.
35. B. Larsen *et al.*, "Performance overhead of cryptographic algorithm switching in Transport Layer Security version 1.3," *Computer Communications*, vol. 218, pp. 12–24, 2024.
36. K. Patel *et al.*, "Resource-aware security configuration for sixth generation network slices," *IEEE Transactions on Network and Service Management*, vol. 21, no. 2, pp. 1234–1248, 2024.