Quantum-Safe Security for 5G Networks

Cristian González Maldonado
Master in Computer Science
Advisor: Jeffrey L. Duffany, Ph.D.
Polytechnic University of Puerto Rico
Graduate Project EXPO February 2025

Abstract *— This research investigates post-quantum cryptography's implementation and performance impact in 5G networks using the free5GC platform. Developed a comprehensive framework incorporating CRYSTALS-Kyber algorithms through Docker-containerized network functions and OpenSSL integration. Testing with two virtualized servers (2 vCPU, 4 GB RAM) demonstrated that quantum-resistant security can be achieved without compromising network performance requirements. Results show Kyber variants maintain latency well below 1ms (Kyber512: 0.059702s, Kyber1024: 0.051873s), with manageable bandwidth requirements (Kyber512: 682.99 bytes/packet, Kyber1024: 775.79 bytes/packet). Kyber1024 achieved superior throughput (14,958.19 bytes/second) compared to traditional X25519 (10,496.87 bytes/second. A practical implementation framework through Docker containers with custom Python scripts for performance analysis enables organizations to merge quantum-resistant security with operational network efficiency. This research has developed structures that secure telecommunications frameworks from threats caused by advanced quantum computing techniques.*

Key Terms *— 5G Network Security, CRYSTALS-Kyber, Post-Quantum Cryptography, Quantum-Safe Architecture.*

INTRODUCTION

With 5G technology making its way into the telecommunications marketplace, the continued development of 6G telecommunication networks promises to provide telecommunication at speeds and connectivity that are otherwise unprecedented with novel, diverse applications. These innovations are expected to support high-tech technologies like intelligent automobiles, virtual reality, and a vast scale of IoT nodes [1] [2]. Still, such evolution also implies appropriate security issues, especially with the increasing threat of quantum computing. Employing vast computational ability, quantum computers can become a lethal blow to widely used cryptographic algorithms by solving mathematical problems beyond the reach of traditional computers. These undermine the confidentiality, integrity, and communication availability in contemporary telecommunication systems [3].

5G networks function through a basic three-part framework, which facilitates continuous connectivity and advanced telecom functions, as shown in Figure 1. End-user devices have 5G capabilities and a Universal Subscriber Identity Module (USIM) to engage with the network and form the first User Equipment (UE) component. 5G devices reach the cellular network via the Next Generation Radio Access Network (NG-RAN), its second vital architectural component. The central element of the NG-RAN, which facilitates radio network communication between the user equipment and core network services, is the gNodeB (gNB) base station, which connects to user equipment through the NR-Uu interface and communicates with the core network through the NG interface [4].

Figure 1
5G Network Architecture Components

Within the 5G Core (5GC), vital network functions exist, such as the Access and Mobility Management Function (AMF) and User Plane Function (UPF). Network components function

together to handle user authorization while also delivering session control and network traffic direction. Next-generation applications depend on this architecture because it supports enhanced mobile broadband service, ultra-reliable low-latency communications, and massive machine-type communications [4].

Service-based architecture significantly improves flexibility and scalability over previous network architectures in 5G technology. As illustrated in Figure 2, the architecture consists of three main components: Three key parts include the Service Management and Orchestration layer together with the Radio Access Network (RAN) and the 5G Core [2]. Non-real-time and near-real-time RAN Intelligent Controller components allow the Service Management and Orchestration layer to manage network resources using virtualized applications that orchestrate services through rApps and xApps, respectively.

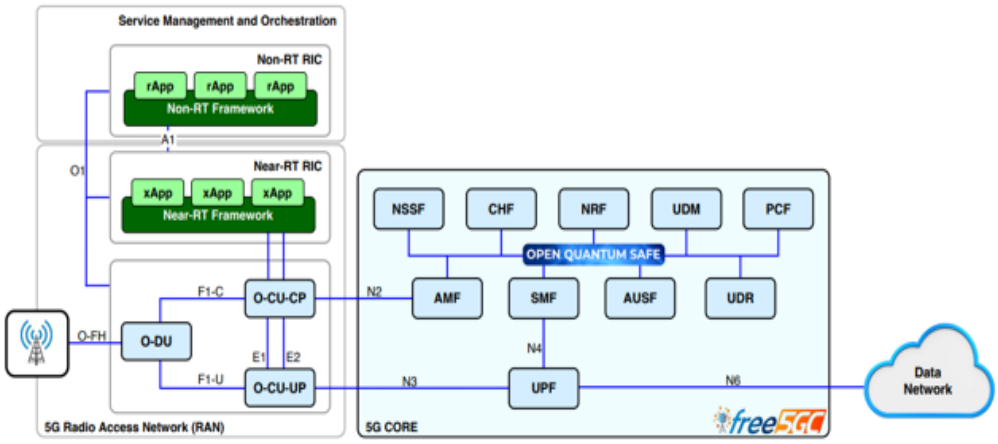

Figure 2
Detailed 5G Network Architecture with Quantum-Safe Security Integration

The Radio Access Network comprises several key elements: the Open Distributed Unit (O-DU), Open Centralized Unit – Control Plane (O-CU-CP), and Open Centralized Unit – User Plane (O-CU-UP). The network components exchange information through standardized interfaces controlling user connections and radio resource management. Using disaggregation enables systems to use resources more productively while improving network performance metrics.

Within the 5G Core Network service-based architecture, multiple Network Functions communicate using standardized interfaces. Access and Mobility Management Function, together with Session Management Function (SMF) and User Plane Function, comprise key network components together with additional specialized functions, including Network Slice Selection Function (NSSF), Policy Control Function (PCF), and Unified Data Management (UDM). Under the Open Quantum Safe framework, these functions offer essential security control to maintain protected communications between network units [2]. Because of its modular design, network operators can establish quantum-safe security protocols across various network functions.

Different interfaces establish secure connectivity between these network components to handle control plane interactions and user plane transmissions. An architectural framework enables enhanced mobile broadband services as well as ultra-reliable low-latency communication (URLLC) and massive machine type-communications (mMTC) essential for next-generation application uses [5].

The most important one is the "store now and decrypt later" threat, implying that attackers collect encrypted data today with a plan to decrypt it when quantum computers gain enough capabilities [1]. This emphasizes the urgent need for quantum-resistant security measures in telecommunications

infrastructure. Due to the global race for secure networks, research into Post-Quantum Cryptography (PQC) is being explored, offering cryptographic algorithms designed to resist classical and quantum attacks.

To counteract these threats, recent advancements in PQC, especially the NIST-endorsed CRYSTAL-Kyber and Crystal-Dilithium algorithms, seem a suitable solution [6]. These algorithms are founded on complex mathematical constructs known as lattice-based cryptography that remain safe from future quantum computing capabilities. Unlike traditional algorithms, however, traditional algorithms utilize asymmetric cryptography and are therefore vulnerable to attacks by quantum computers. PQC gives telecommunication networks a pathway to futureproof networks by ensuring robust encryption. However, realizing these algorithms in real-world 5G/6G systems has a set of challenges, such as high computation complexity, extended key sizes, and the necessity of ultra-reliable low-latency communication, which is a critical requirement for applications such as autonomous vehicles and smart healthcare [7].

Furthermore, integrating quantum-resistant cryptosystems into existing telecommunication infrastructures is also possible, provided the challenges can be addressed sufficiently. This development must be scalable to different deployment densities, from lightly populated rural areas to heavily clustered urban scenarios, and be maintainable, which means connectivity to legacy systems and, most importantly, with constrained processing power and energy resources found in IoT devices [8]. The research investigates different cryptographic approaches between traditional algorithms and PQC to better implement quantum-safe structures.

This research, however, is significant beyond immediate security concerns. It, therefore, lays the foundation for methodologies necessary to integrate PQC into 5G and 6G networks ahead of the quantum computing era. In addition, it provides a foundation for the design of inherently quantum-safe 6G infrastructures, including dealing with technical, global standardization, and interoperability issues. This research will contribute to making the secure, resilient, scalable communication systems of the future.

PROBLEM STATEMENT

Quantum computing advances create new security risks that threaten the 5G infrastructure and any new 6G systems that will emerge. 5G security depends on public key cryptography like RSA and ECC, which face serious vulnerabilities. The operation of Shor's algorithm represents a direct danger to current security methodologies in communication networks. It can attack the entire security framework, down to key exchange, authentication schemes, and digital signatures in 5G networks.

Implementing PQC solutions poses significant performance challenges that must be handled well. While these algorithms tend to require larger key sizes and more computational resources than traditional cryptographic methods, these become critical limits on resource-constrained devices that contain the network ecosystem [3]. Furthermore, security requirements are still severe when considering IoT devices with limited processing power and energy resources.

URLLC is a critical consideration of 5G/6G networks, with such requirements asking for end-to-end delays of less than 1 ms [8]. However, introducing quantum-resistant security measures comes with associated computational overhead that may pose a risk to latency requirements and result in a complex tradeoff between security and performance. The complexity of the task grows because of the need to maintain consistent performance across multiple network conditions and usage scenarios.

Another important issue with implementing a resistant security scheme is scalability. PQC algorithms have substantially larger key sizes and more computational overheads, preventing large-scale 5G/6G deployments, especially in dense urban environments where millions of devices may be

connected simultaneously. The scalability problem is not just a technical question but limits practical network management and resource allocation.

PROJECT GOAL

This research project aims to create and validate a practical framework to realize quantum-resistant cryptographic protocols within 5G network architectures while ensuring requisite performance requirements. The framework aims to solve the imminent quantum computing threat to current cryptographic systems while guaranteeing the unaltered promise of functionalities such as ultra-low latency, high bandwidth, and massive connectivity as 5G technology.

RESEARCH QUESTIONS

In this research, the 5G network is explored with quantum-resistant security measures implemented to overcome complex challenges with the structure framework:

- Given the existence of post-quantum cryptography protocols (e.g., CRYSTALS-Kyber), how can these protocols be offered to the 5G network architecture in a way that ensures the satisfaction of the most important 5G performance metrics, subject to different network conditions and usage scenarios?
- How can we further optimize quantum-resistant protocols to be secure on devices ranging from resource-constrained IoT sensors to high-capacity edge computing nodes in dense 5G network environments?
- Which testing and validation frameworks shall be necessary for robustness, reliability, and performance of quantum-resistant security measures in operational 5G networks?
- How can we incorporate quantum-resistant protocol into 5G security architectures already deployed in a backward compatible, interoperable, and least intrusive manner possible when deploying it?

RELEVANCE AND SIGNIFICANCE

This research is important beyond immediate security concerns because it forms a critical pivot point in enabling telecommunications infrastructure preparedness in the post-quantum era. As our quantum computing capabilities speedily, the threat to our current cryptographic systems becomes an imminent reality. This paper fills the gap between the theory of quantum-resistant algorithms and implementation at the time of operation in real 5G networks to cope with a key security issue for the telecommunications industry.

Future Implications

This research is important to the evolution of 6G networks, in which quantum-resistant security will become a necessary baseline. This work helps lay the groundwork for designing inherently quantum-safe desired next network generations by establishing methodologies for integrating and validating quantum-resistant protocols in existing 5G networks. The resulting validation frameworks and performance optimization strategies developed here will be critical for defining the security architecture for 6G and beyond.

Furthermore, this research is of value to cybersecurity at large by showing how to fulfill security requirements while respecting performance in complex network settings. Based on the work results, contribute methodologies with applications beyond telecommunications that could provide insights into other critical infrastructure systems, like healthcare, energy, and finance, where performance and security are equally important.

METHODOLOGY

The methodology for integrating Post-Quantum Cryptography algorithms into a 5G network relies on a complete integration framework on the free5GC open-source core platform. For a scalable and secure free5GC testing environment, the implementation uses Docker containerization to deploy free5GC. Configuration files were modified for each node to make encrypted communication possible across the

network. Figure 3 shows various Virtualized Network Functions (VNFs) created and initialized in a modular, containerized environment. It allows PQC algorithms to be easily incorporated into the testing infrastructure while maintaining the security of the testing infrastructure and making the approach easier to scale in a containerized fashion.

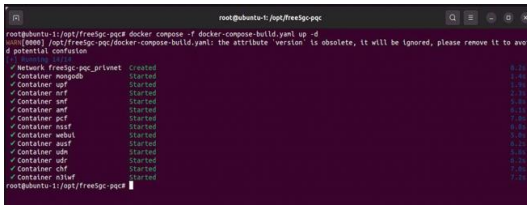

Figure 3
Docker Compose Virtualized Network Functions

The second step was configuring OpenSSL to accept quantum-resistant algorithms by adding the Open Quantum Safe (OQS) module. The OQS module enabled post-quantum key exchange algorithms within the OpenSSL library. Figure 4 shows how the configuration file illustrates the activation process of OQS and implementing advanced cryptography mechanisms. All nodes were configured to accept self-signed certificates. However, in a production environment, a CA-signed certificate would be necessary. Then, such certificates are generated and deployed throughout all 5G core network nodes, underpinning secure communications.

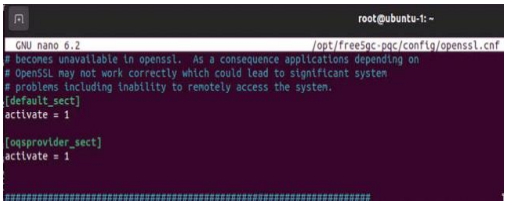

Figure 4
Open Quantum Safe on OpenSSL Configuration File

Then, the gNodeB and the core network simulator UERANSIM created a haven for the gNB and User Equipment. Stream Control Transmission Protocol (SCTP) was configured so the gNB could communicate with the free5GC core. In Figure 5, the connection between the radio access network and the core network is established despite the successful establishment, including the NG setup process, for secure communication.

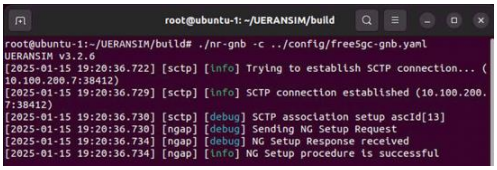

Figure 5
gNB Connection with AMF free5GC Server

When the gNB setup process was completed, UERANSUM was also used to simulate the UE registration and network connection. As illustrated in Figure 6, the UE went through several states while successfully registering and connecting. Accordingly, it demonstrates the robustness of PQC-enhanced Transport Layer Security (TLS) in addressing user authentication and communication.

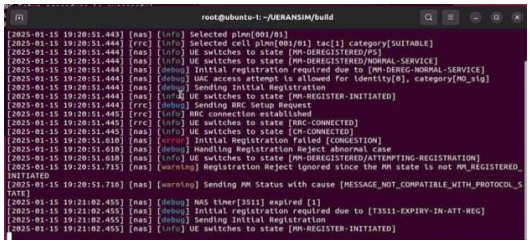

Figure 6
UE Connection with AMF free5GC Server

A lattice-base cryptographic algorithm recommended by NIST, CRYSTAL-Kyber, was specifically configured with OpenSSL and further boosted between the Kyber521 and Kyber1024 levels of security the user offers, as seen in Figure 7. The OpenSSL configuration provides flexibility in selecting different OQS cryptographic algorithms and dynamically switching between them. There is also flexibility in selecting between underlying cryptographic algorithms. These configurations are resilient to attacks using quantum cryptography while achieving optimum performance.

Figure 7
Kyber-1024 Cryptography Configuration

Then, a custom Python script was created with a pyshark library for in-depth packet analysis to evaluate the implementation performance. The script was designed to measure four key metrics: The evaluation metrics are average latency between consecutive packets in the TLS handshake process, bandwidth usage represented by the rate of data being transmitted in bytes per second, and packet loss during transfer. Our testing methodology captures and analyzes network traffic for 50 UE connections at a seven-second activation between connections to obtain a statistically accurate measurement.

The packet analysis process was automated using a Python script in which each cryptographic implementation (X25519, Kyber512, and Kyber1024) was introduced into packet captures for analysis. The script extracted packet timestamps for latency calculation, packet sizes to analyze for bandwidth, total data transfer rate calculation for throughput, and packet sequence analysis for loss detection. This automated approach resulted in consistent and accurate measurement of performance metrics for all implementations. matplotlib was used to visualize the results using comparative bar charts of each metric so that performance differences between the cryptographic implementations could be easily visualized. This comprehensive evaluation approach could characterize the security enhancement and the associated performance implications of integrating PQC in our 5G test network environment and provide quantifiable metrics for contrasting several cryptography solutions in a trusted network environment.

RESULTS

In the experiment evaluation, the performance impact of applying selected cryptographic methods in a 5G Core Network implemented with free5GC is measured and focused on comparing three key implementations: X25519 using the traditional ECC combined with two variants of the post-quantum Kyber algorithms, Kyber512 and Kyber1024. To experiment, two virtual servers were created, Ubuntu 22.04 LTS running with 2vCPU, 4 GB RAM, and 50 GB storage. For the free5GC core network components, a single server was created to run, and another server was created to run UERANSIM to simulate gNodeB and UE connectivity. Each test scenario consisted of 50 UE connections with a seven-second cadence between connections to ensure the above-mentioned statistical relevance of the results and provide enough time to capture and measure each TLS handshake.

A packet analysis of these implementations was done using a custom Python script implemented with pyshark to identify all performance metrics across the three implementations. As described in Figure 8, different algorithms use different bandwidth usage. X25519 has 693.71 bytes per packet, Kyber512 uses slightly fewer, 682.99 bytes per packet, and Kyber1024 uses more bandwidth, with 775.59 bytes per packet. With Kyber1024, this bandwidth usage increased due to its larger key size, while the difference is not as significant as one would expect initially in a virtualized environment.

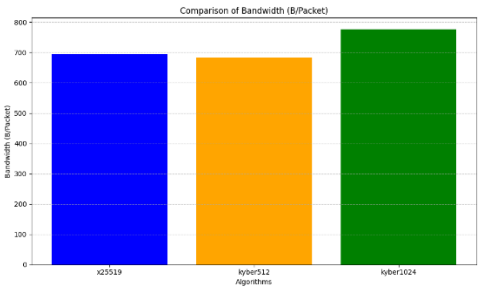

Figure 8
Average Bandwidth Comparison of Cryptographic Algorithms

Figure 9 compares the implementations' latency. X25519's latency is 0.066.96 seconds, followed by Kyber512's latency at 0.059702 seconds and Kyber1024's latency at 0.051873 seconds. All three algorithms maintain average latencies within the 1ms required for a 5G network. Adopting post-quantum cryptography does not impact the 5G network latency requirements, even in a virtualized environment, as demonstrated across all implementations.

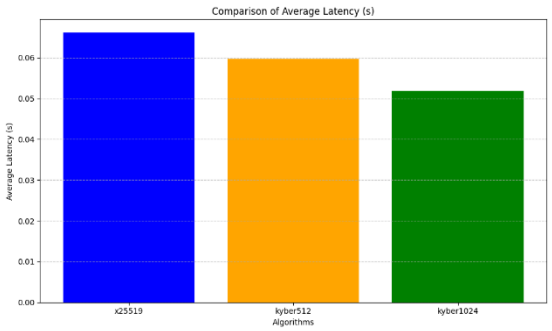

Figure 9
Average Latency Comparison of Cryptographic Algorithms

In Figure 10, the throughput analysis demonstrates an ongoing improvement in the implementation. A throughput of bytes X25519 is achieved, 10,496.87 bytes per second. We determined that Kyber1024 led the performance rankings in our virtualized setup since it reached 14,958.19 bytes per second throughput, confirming that servers handle big key sizes efficiently. Throughout this evaluation phase, all three cryptographic methods operated with high stability and without any packet losses.

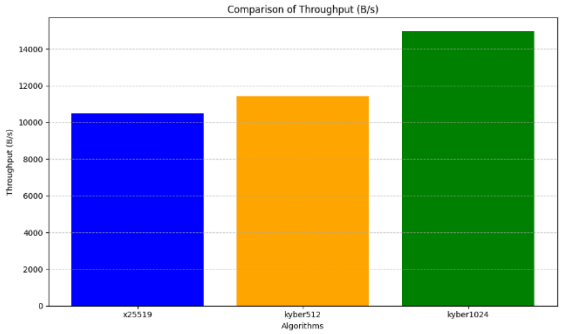

Figure 10
Average Throughput Comparison of Cryptographic Algorithms

The performance metrics in these details imply that post-quantum cryptography implementations, specifically Kyber variants, can meet its performance requirement for 5G networks today. Despite the higher bandwidth per packet required by Kyber1024, its capacity to maintain latency to acceptable limits and deliver reasonable throughput suggests that the algorithms fit the available system resources in our virtualized testing environment well.

These results indicate that Kyber variants may present viable quantum-safe security implementation options for deployments with specifications similar to our test environment. The research also showed that with marginally more significant bandwidth requirements, Kyber512 offers a balance. However, Kyber1024 proves that its improved security features can be implemented with performance comparable to the required network parameters. The results of our work are most relevant for organizations that have to plan for quantum-safe security in the presence of virtualized infrastructure constraints.

DISCUSSION

The implementation of post-quantum cryptography in 5G test networks and analysis investigate the research questions and objectives in depth. Integrating quantum-resistant protocols into existing 5G architectures is feasible while preserving all critical performance requirements.

For the first research question about implementing CRYSTAL-Kyber protocols to 5G networks network architecture, the results demonstrate that the Kyber variant can be integrated successfully without sacrificing key performance results. Latency measurements for both Kyber512 (0.059702 seconds) and Kyber1024 (0.051873 seconds) were well below the 1ms required for 5G networks and, thus, show that post-quantum security can be achieved without sacrificing latency requirements. Compared with traditional X25519, the analysis observes that the Kyber1024 bandwidth is higher per packet; however, the additional bandwidth can easily be accommodated in the network.

Implementing these protocols in the virtualized system with limited resources (2 vCPU, 4 GB RAM) demonstrated that these protocols can still be operated successfully with modest hardware requirements. However, of special interest is the throughput analysis, in which Kyber1024 reports 14,958.19 bytes per second, surpassing X25519 and even Kyber512. This shows that the implementation efficiently utilizes system resources, making the

solution flexible, and can be deployed to various scenarios, including resource-constrained IoT devices and high-capacity edge computing nodes.

The research found the testing and validation framework (implemented through a custom Python script for packet analysis) helpful in measuring and validating the performance of quantum-resistant security measures. Comprehensive data regarding latency, bandwidth, and throughput of 50 UE connections served in seven second intervals was collected through automated analysis. Most notably, no packet loss was observed in all the implemented scenarios, which indicates excellent reliability, which is critical in real-world 5G networks.

Regarding backward compatibility and interoperability, our implementation backward on the free5GC platform showed that PQC can be retrofitted into a standard 5G architecture without breaking core functionality. We also successfully configured OpenSSL with the OQS module and CTYSTAL-Kyber to demonstrate that quantum-resistant security can be achieved in a way that is backward and compatible with existing protocols and standards.

The results have broad implications for future 5G/6G security. Kyber variants, especially Kyber1024, have been successfully implemented, implying that networks can be quantum-resistant with negligibly poor performance penalties. For this, protecting against "store now, decrypt later" attacks is crucial: Future quantum computers could compromise the data currently gathered.

The research could, however, point out where more attention is needed. Kyber1024's increased bandwidth requirements have become more significant in our test environment and could be more so in massive deployment scenarios. This reveals that network planning and resource allocation strategies may have to be reexamined when considering the large-scale implementation of quantum-resistant security.

In addition, the performance difference between Kyber512 and Kyber1024 poses an interesting security performance tradeoff. Kyber1024 has stronger security guarantees but can be bandwidth-demanding in high-density deployment. This is a question of which variants an organization will adopt depending on its security requirements and network capabilities.

The research illustrates the need for a comprehensive testing framework to quantify security when testing quantum-resistant implementation. Our results may aid future implementations and evaluations of post-quantum cryptography in operational networks through packet analysis, performance monitoring, and testing automation.

These findings will point to several future research directions ahead., including:

- Deployment of PQC for specific use cases, such as IoT deployments.
- An adaptive security framework can balance security levels with network conditions.
- A study of a hybrid approach to combining classical and post-quantum cryptography to achieve optimum security and performance.
- Discuss scaling strategies to meet dense urban deployment with high device counts.

Finally, the research shows that post-quantum cryptography can be implemented in 5G networks with satisfactory performance requirements. The results offer a practical framework to help organizations maintain their efficient and reliable communication infrastructure and get armed with as much network security as possible against the inevitable threats of quantum attacks.

CONCLUSION

the research has shown that implementing post-quantum cryptography in 5G networks using the free5GC platform is feasible and practical. The analysis has demonstrated that quantum-resistant security measures can be integrated into the existing 5G architectures via comprehensive testing and analysis while meeting key performance requirements. In particular, our implementation of CRYSTAL-Kyber, specializing in Kyber512 and Kyber 1024, demonstrates that these postquantum

allocations of newer variants can be protected without trading faster performance.

Results from testing our environment, comprised of two virtual servers with mode specifications, reveal that post-quantum cryptography can work well with limited resources. Latency measurements are also well below the 1ms timeline required for 5G networks for all implementations, and the bandwidth requirements are manageable. In addition, the throughput analysis of Kyber1024 indicated that it could perform better with 14,958.19 bytes per second. This also shows that this protocol is an efficient resource since it provides extra security features.

Through this implementation framework, organizations can evaluate the deployment of quantum resistance security measures in 5G networks using Docker containers and custom Python scripts for performance analysis. This method systematically reviews and adopts post-quantum cryptographic systems, maintaining network performance and reliability.

This study proves that quantum-safe security can be integrated alongside established network protocols when OQS becomes part of OpenSSL alongside CRYSTAL working with Kyber. Organizations focusing on strengthening their security against quantum attacks can rely on this discovery even without significant infrastructure investments.

This research provides a solid basis for the sustained evolution of telecommunication security. Such methodologies and implementations, which demonstrate the ability to work using the capabilities of experimental quantum computers, show a practical way of protecting critical communication infrastructure as quantum computing becomes more capable. Future studies must focus on using case-specific implementation optimization and investigate adaptive security frameworks and scaling techniques for dense urban infrastructure deployment.

This study contributes substantially to research by developing a workable framework that establishes quantum-resistant security capabilities for 5G networks. Results indicate that post-quantum cryptography can seamlessly incorporate into canonical network architectures without harming performance requirements to secure telecommunications infrastructure against current and future quantum threats.

REFERENCE

[1] Ericsson. "Decoding quantum-safe encryption: Key to ensuring confidentiality in networks." Ericsson White Paper, 2024.

[2] Vomvas, M.; Ludant, N.; Noubir, G. "Establishing Trust in the Beyond-5G Core Network using Trusted Execution Environments." arXiv preprint arXiv:2405.12177, 2024.

[3] Scalise, P.; Garcia, R.; Boeding, M.; Hempel, M.; Sharif, H. "An Applied Analysis of Securing 5G/6G Core Networks with Post-Quantum Key Encapsulation Methods." Electronics, 2024, 13, 4258. Available: https://doi.org/10.3390/electronics13214258.

[4] 3GPP.. “5G system overview.” 2022. Available: https://www.3gpp.org/technologies/5g-system-overview

[5] 3GPP. "Service requirements for the 5G system." 3GPP TS 22.261 v16.14.0, 2021.

[6] Scalise, P.; Boeding, M.; Hempel, M.; Sharif, H.; Delloiacovo, J.; Reed, J. "A Systematic Survey on 5G and 6G Security Considerations, Challenges, Trends, and Research Areas." Future Internet, 2024, 16, 67. Available: https://doi.org/10.3390/fi16030067.

[7] Damir, M. T.; Meskanen, T.; Ramezanian, S.; Niemi, V. "A Beyond-5G Authentication and Key Agreement Protocol." arXiv preprint arXiv:2207.06144, 2022.

[8] Alagic, G., et al. "Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process." NISTIR 8309, 2020.