Quantum-Safe Security for 5G Network

Author: Cristian González Maldonado
Advisor: Jeffrey L. Duffany, Ph.D.
Electrical & Computer Engineering and Computer Science Department

Abstract

The research explores post-quantum cryptography deployment within 5G networks through free5GC platform implementation while examining its operational capabilities. The research developed an extensive framework that combined CRYSTAL-Kyber algorithms with Docker-containerized network functions and OpenSSL integration. During testing, two virtualized servers were used to prove that implementing quantum-resistant security goals does not affect network performance metrics. Kyber variants exhibit post-quantum cryptographic performance by maintaining latency under 1 ms while working within traditional X25519 bandwidth usage parameters. The framework utilizes Docker containers and custom Python scripts to create a practical deployment solution that integrates quantum-resistant security technologies with regular network operational characteristics to empower organizational implementations. The research findings established protective frameworks to defend telecommunications infrastructure from vulnerabilities created by advanced quantum algorithms.

Introduction

Communication networks advancing from 5G standards to 6G infrastructure will establish unmatched speed and connectivity capabilities for smart vehicles and IoT nodes with virtual reality technology [1] [2]. Quantum computing creates significant security vulnerabilities that can break present cryptographic algorithms and compromise telecommunication network confidentiality and data integrity [3].

Figure 1 demonstrates a service-based architecture that contains the foundation layers of underlying 5G network systems. The 5G network employs quantum-proof security features with CRYSTALS-Kyber from the Open Quantum Safe platform to prevent all cyber-attacks yet preserve network performance levels [3].

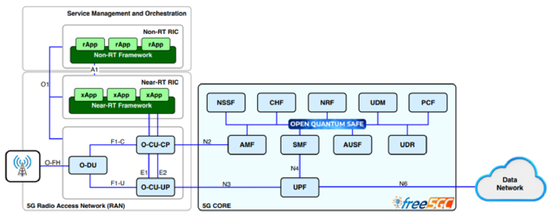

Figure 1
Detailed 5G Network Architecture with Quantum-Safe Security Integration

Background

The service-based architecture of the 5G Core Network brings together the Access and Mobility Management Function (AMF), Session Management Function (SMF), and User Plane Function (UPF) to provide end-users with enhanced mobile broadband and ultra-low-latency communication capabilities [4]. These functions support network protection through essential security control mechanisms of the Open Quantum Safe framework [2].

The most concerning security threat originates from attackers who store encrypted data today and plan to decrypt it when quantum computers reach sufficient power [1]. CRYSTAL-Kyber algorithms deliver quantum-resistant security via lattice-based cryptography to solve the primary security challenge as supported by NIST [4]. Unlike traditional encryption methods within the threat range of quantum computers, these new cryptographic advancements ensure future telecommunication networks remain secure.

Problem

The emergence of quantum computing introduces additional security threats to 5G networks because RSA and ECC public key cryptography, which are essential for 5G security. This show major weakness when utilized in conjunction with Shor's algorithm's quantum capabilities. This research explore the following questions:

- How can post-quantum cryptography protocols be integrated into 5G architecture while maintaining critical performance metrics?
- How can quantum-resistant protocols be optimized for devices ranging from IoT sensors to edge computing nodes?
- What testing framework are needed to validate security measures in operational 5G networks?
- How can quantum-resistant protocols be incorporated into existing 5G architectures with minimal disruption?

Methodology

To implement Post-Quantum Cryptography algorithms within a 5G network, an universal integration framework must be deployed through the free5GC open-source core platform. The implementation deploys free5GC for scalable and secure testing through Docker containerization methods. Each node received configuration changes that enabled encryption across the network.

Post-quantum key exchange functionality was enabled in OpenSSL by integrating and configuring the Open Quantum Safe (OQS) module for quantum-resistant algorithm support. NIST-approved CRYSTAL-Kyber, implemented within OpenSSL, displays security between Kyber512 and Kyber1024. The configurations maintain resistance to quantum cryptographic attacks and provide maximum performance efficiency. Several different cryptographic algorithms remain available.

The setup of core network simulator UERANSIM served to simulate gNodeB (gNB) communication with User Equipment (UE). Stream Control Transmission Protocol implemented secure communication between gNB and free5GC core to establish backbone connectivity that links core and radio access components. We completed the gNB setup with UERANSIM to simulate UE registration and network connection, which proved PQC-enhanced Transport Layer Security (TLS) maintains robust user authentication and communication.

Then, a custom Python script using pyshark library was created for in-depth packet analysis, measuring four key metrics:

- Average latency between consecutive packets in the TLS handshake process.
- Bandwidth usage represented by the rate of data being transmitted in bytes per second.
- Total data transfer rate calculation for throughput.
- Packet loss during transfer.

The measurement technique recorded network traffic data, using Wireshark, from 50 UE connections over seven-second periods to evaluate X25519, Kyber512, and Kyber1024 performance during the testing process. An experimentation system contained two virtual servers (each with 2vCPU and 4 GB RAM) that operated Ubuntu 22.04 LTS—one handled free5GC core components, and another ran UERANSIM simulation.

Results and Discussion

In the experiment evaluation, the performance impact of applying selected cryptographic methods in a 5G Core Network implemented with free5GC was measured, comparing three implementations: Traditional ECC was employed with X25519 alongside two post-quantum Kyber variants Kyber512 and Kyber1024.

Figure 2 displays different bandwidth figures according to a packet analysis. Packet data analysis indicates that X25519 employs 693.71 bytes per packet, Kyber512 requires 682.99 bytes per packet, and Kyber1024 needs 775.79 bytes per packet. Bandwidth usage from Kyber1024 grew because of its larger key size yet stayed within practical limits for virtualized systems.

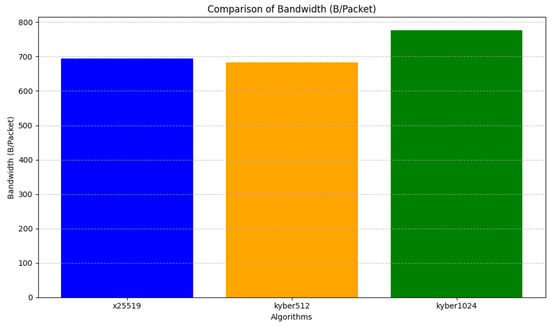

Figure 2
Average Bandwidth Comparison of Cryptographic Algorithms

Figure 3 compares the implementations' latency. Latency benchmarks show that X25519 operates with 0.066.96-second performance while Kyber512 has 0.059702-second operation time and Kyber1024 runs on 0.051873 seconds. Kyber1024 outcompetes X25519 with a throughput of 14,958.19 bytes/second alongside every algorithm achieving under 1ms latency to meet 5G network standards. The results validate Kyber variants as practical security selections that sustain adequate performance equivalent to established algorithms even under quantum attack scenarios. The research demonstrates that Kyber512 achieves a good balance between security performance given slightly larger bandwidth needs, while Kyber1024 increases security functions without causing network performance degradation.

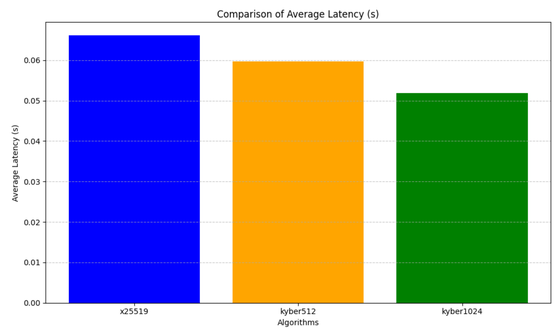

Figure 3
Average Latency Comparison of Cryptographic Algorithms

Conclusions

Free5GC platform makes implementing post-quantum cryptographic techniques in 5G networks a viable and practical solution for researchers. Our study has proven that security frameworks that protect against quantum attacks fit well within current 5G architectural designs yet achieve required performance standards. Our specialized CRYSTAL-Kyber implementation for Kyber512 and Kyber1024 proves that it is possible to adopt post-quantum cryptographic methods without reducing network performance levels.

Post-quantum cryptography demonstrates strong performance on limited resource systems by maintaining network latency below 1ms for 5G applications and optimizing bandwidth use. The throughput performance of Kyber1024 hit 14,958.19 bytes per second which demonstrates that the protocol delivers additional security while remaining efficient. The study delivers an actionable guide helping organizations to assess and implement quantum-resistant security features into 5G setups without sacrificing existing network performance or reliability.

Future Work

Future work in post-quantum cryptography should focus on implementing solutions tailored for specialized applications, particularly Internet of Things (IoT) systems facing resource constraints. Developing an adaptable security framework that dynamically adjusts security parameters based on real-time network conditions is essential. Additionally, exploring hybrid cryptographic methods that integrate conventional techniques with post-quantum technologies could unlock advanced security capabilities and optimize performance. The next generation of research should prioritize scalable quantum-resistant protocol implementations capable of meeting the demands of dense urban environments, where managing large numbers of interconnected devices simultaneously is a critical challenge.

Acknowledgements

I would like to extend my sincerest gratitude to Dr. Jeffrey L. Duffany for his invaluable guidance and unwavering support throughout this research project. His expertise, insightful feedback, and steadfast encouragement have been instrumental in shaping the direction and success of this study. I am deeply appreciative of his mentorship, which has not only enhanced the quality of this research but also inspired me to pursue excellence with dedication and confidence.

References

[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. https://doi.org/10.3390/electronics13214258.
[4] 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. https://doi.org/10.3390/fi16030067.