

Post-Quantum Cryptography Integration to O-RAN

Abdullah Aydeger[†], Engin Zeydan^{*} and Josep Mangués^{*}

[†] Dept. of Electrical Engineering and Computer Science, Florida Institute of Technology, Melbourne, FL, USA

^{*}Centre Tecnològic de Telecomunicacions de Catalunya (CTTC), Barcelona, Spain, 08860.

Email: aaydeger@fit.edu, {engin.zeydan,josep.mangués}@cttc.cat

Abstract—With its disaggregated and open interfaces, the Open Radio Access Network (O-RAN) architecture promises flexibility, innovation, and cost-effectiveness for future wireless networks. However, the increased reliance on software and open interfaces also introduces new security challenges. As the threat of quantum computing looms, the traditional cryptographic algorithms used in O-RAN will become vulnerable to potential attacks. This paper proposes the integration of Post-Quantum Cryptography (PQC) into O-RAN to enhance its security against post-quantum adversaries. We discuss the specific vulnerabilities of current O-RAN security mechanisms to quantum attacks and identify key areas where PQC can be applied, such as key exchange, authentication, and data protection. We present a framework for evaluating the suitability of different PQC algorithms for O-RAN and outline potential challenges and implementation considerations. By proactively integrating PQC into O-RAN, we aim to ensure the long-term security and resilience of this emerging network architecture in the era of quantum computing.

Index Terms—post-quantum cryptography, open radio networks, integration.

I. INTRODUCTION

The Open Radio Access Network (O-RAN) architecture is poised to revolutionize wireless communications by providing flexibility, multi-vendor solutions, and software-defined networks [1]. Operators can independently choose the best solutions for different aspects of the RAN, avoiding vendor lock-in and accelerating innovation. O-RAN's open ecosystem encourages competition between providers, leading to lower equipment costs and capital expenditure (CapEx) for operators. It is a software-defined approach that enables more efficient resource utilization and easier network scaling, reducing the need for expensive hardware upgrades. The O-RAN is thus changing the RAN landscape by creating a more open, flexible, intelligent, and cost-effective approach to building and operating wireless networks. By fostering innovation, competition, and collaboration, O-RAN aims to drive the next generation of wireless communication technologies and services.

From the perspective of security, O-RAN offers both opportunities and challenges. Several studies have addressed various aspects of O-RAN security, including threat modeling, vulnerability analysis, and the development of mitigation strategies [2]–[4]. The current O-RAN security mechanisms are based on classic cryptography in interfaces such as O1 (NETCONF via Transport Layer Security (TLS)), O2 (TLS

and X.509 certificates), A1 (TLS and X.509 certificates), and E2 (TLS and X.509 certificates) for management, control and data exchange between different components. In addition, the open fronthaul interface uses IPsec (IP Security) and MACsec (MAC Security) protocols to secure communication between the O-DU and O-RU. However, these mechanisms are not resistant to attacks from future quantum computers as the emergence of quantum computing threatens the traditional cryptographic algorithms, such as RSA and ECC, that also underpin the security of O-RAN. The integration of Post-Quantum Cryptography (PQC) becomes crucial to protect O-RAN from future quantum attacks. A comprehensive analysis of PQC algorithm families has recently been presented [5] and demonstrated for 5G Core networks in [6]. This paper proposes a framework for integrating PQC into O-RAN, focusing on vulnerable areas such as key exchange, authentication, and data protection within the various interfaces. This paper aims to address these vulnerabilities by exploring the application of PQC algorithms, such as lattice-based cryptography and code-based cryptography, in each of these interfaces. It also discusses the challenges associated with implementing PQC in resource-constrained O-RAN components and proposes feasible solutions. By proactively integrating PQC into O-RAN, we aim to build a quantum-resilient infrastructure that ensures the long-term security and resilience of future wireless networks.

II. MIGRATION FROM CLASSICAL ENCRYPTION TO PQC

Table I provides different techniques between the current classical encryption methods used in O-RAN interfaces and our proposed PQC counterparts. For the O1, O2, A1, and Open Fronthaul interfaces, which currently use TLS for secure communication, the table suggests migrating to PQ-TLS (Post-Quantum TLS) [7]. There are a number of alternatives that could be integrated into PQ-TLS. These include ML-KEM (formerly Kyber [8]) for keys establishment that replace conventional methods such as Diffie-Hellman, and ML-DSA (formerly Dilithium) for digital signatures that may replace RSA and ECDSA in TLS certificates. In addition, ML-SLH (formerly SPHINCS+) offers another digital signature option, and FALCON, which was also selected for standardization, provides an alternative to ML-DSA for scenarios requiring shorter signatures. While the specific implementation details are still under development, it is clear that future O-RAN versions will need to integrate these PQC algorithms to pave the way for quantum-resistant secure communication.

This work was partially funded by “ERDF A way of making Europe” and MCIN/AEI/ 10.13039/501100011033 project Grant PID2021-126431OB-I00, Generalitat de Catalunya grant 2021 SGR 00770 and Spanish MINECO - Program UNICO I+D (grants TSI-063000-2021-54 and -55)

TABLE I: O-RAN Interface Migration from Classical Encryption to PQC in O-RAN Domain

O-RAN Interface	Classical Encryption	Post Quantum Encryption
O1 Interface	TLS	PQ-TLS (e.g., Kyber)
O2 Interface	TLS	PQ-TLS (e.g., Kyber)
A1 Interface	TLS	PQ-TLS (e.g., Kyber)
E2 Interface	IPSec	PQ-IPSec (e.g., NTRU)
Open Fronthaul Interface	TLS	PQ-TLS (e.g., Kyber)
Open Midhaul Interface	IPSec	PQ-IPSec (e.g., NewHope)
Authentication	OAuth	PQ-DSA (e.g., Crystals-DILITHIUM)
Random Number Generation	PRNG	QRNG (Quantum Random Number Generator)

TABLE II: Comparison of PQC Alternatives for O-RAN

Alternative	Advantages	Disadvantages
Hybrid Approach	<ul style="list-style-type: none"> Ensures backward compatibility with existing systems. Allows gradual transition to fully quantum-resistant solutions. Provides immediate protection against some quantum attacks. 	<ul style="list-style-type: none"> Not completely quantum-safe. Increased complexity due to the need to support both classical and PQC algorithms.
Kyber (KEM)	<ul style="list-style-type: none"> Strong security against known quantum attacks. Relatively efficient compared to some other PQC algorithms. Actively being standardized by NIST. 	<ul style="list-style-type: none"> Key sizes can be larger than classical algorithms. Requires careful implementation to mitigate side-channel attacks in mobile and low-power devices.
NTRU (KEM)	<ul style="list-style-type: none"> Well-studied and relatively mature PQC algorithm. Offers good performance and security. 	<ul style="list-style-type: none"> Not selected for NIST standardization (but still considered secure).
Dilithium (Signature)	<ul style="list-style-type: none"> Strong security against known quantum attacks. Actively being standardized by NIST. 	<ul style="list-style-type: none"> Signature sizes can be larger than classical algorithms. Verification can be resource-intensive, potentially increasing latency for some mobile network applications.
Falcon (Signature)	<ul style="list-style-type: none"> Shorter signatures compared to Dilithium. Actively being standardized by NIST. 	<ul style="list-style-type: none"> May be less efficient than Dilithium for verification.

The E2 and Open Midhaul interfaces, which are currently based on IPSec, can also use various options. The first option being considered is Kyber, the primary PQC algorithm, for key establishment in IPSec. It was selected as a finalist in the NIST PQC standardization process and offers strong security and good performance. SIKE is another finalist in the NIST PQC competition. It is based on a different mathematical problem than Kyber and offers an alternative for those concerned about relying on a single algorithm. Classic McEliece is a code-based PQC algorithm that has been around for decades and is considered very secure. However, it has larger key sizes and may not be as efficient as some of the newer algorithms. This ensures increased security for these critical communication links. In addition, the authentication processes traditionally secured by OAuth should also be migrated to PQ-DSA, with Crystals-DILITHIUM [9] serving as a potential candidate for secure digital signatures in a post-quantum world. Finally, the table addresses the need for improved random number generation and proposes a move from classical Pseudo Random Number Generators (PRNG) to Quantum Random Number Generators (QRNG) that utilize quantum mechanics to ensure true randomness and security. This comprehensive migration plan emphasizes the importance of adopting PQC to secure O-RAN networks against impending quantum computing. The detailed comparison of the PQC alternatives for O-RAN interfaces are provided in Table II.

III. CONCLUSIONS

In this paper, we investigated the potential use of PQC algorithms in the context of O-RAN. The migration of the O-

RAN interfaces from classic encryption to PQC is discussed in detail, and a recommended algorithm for each of the interfaces is provided. In future work, we plan to compare different potential PQC techniques for each of the given O-RAN interfaces and display their scalability and applicability within the O-RAN ecosystem.

REFERENCES

- [1] A. Garcia-Saavedra and X. Costa-Perez, "O-ran: Disrupting the virtualized ran ecosystem," *IEEE Communications Standards Magazine*, vol. 5, no. 4, pp. 96–103, 2021.
- [2] A. S. Abdalla and V. Marojevic, "End-to-end o-ran security architecture, threat surface, coverage, and the case of the open fronthaul," *IEEE Communications Standards Magazine*, vol. 8, no. 1, pp. 36–43, 2024.
- [3] E. Zeydan *et al.*, "Integrating quantum-secured blockchain identity management in open ran for 6g networks," in *2024 IEEE 49th Conference on Local Computer Networks (LCN)*. IEEE, 2024, pp. 1–7.
- [4] D. Mimran, R. Bitton, Y. Kfir, E. Klevansky, O. Brodt, H. Lehmann, Y. Elovici, and A. Shabtai, "Security of open radio access networks," *Computers & Security*, vol. 122, p. 102890, 2022.
- [5] S. Hoque, A. Aydeger, and E. Zeydan, "Exploring post quantum cryptography with quantum key distribution for sustainable mobile network architecture design," in *Proceedings of the 4th Workshop on Performance and Energy Efficiency in Concurrent and Distributed Systems*, 2024, pp. 9–16.
- [6] —, "Post-quantum secure ue-to-ue communications," in *2024 15th International Conference on Network of the Future (NoF)*. IEEE, 2024, pp. 28–30.
- [7] A. Aydeger, E. Zeydan, A. K. Yadav, K. T. Hemachandra, and M. Liyanage, "Towards a quantum-resilient future: Strategies for transitioning to post-quantum cryptography," in *2024 15th International Conference on Network of the Future (NoF)*. IEEE, 2024, pp. 195–203.
- [8] J. Bos *et al.*, "Crystals-kyber: a cca-secure module-lattice-based kem," in *2018 IEEE European Symposium on Security and Privacy (EuroS&P)*. IEEE, 2018, pp. 353–367.
- [9] L. Ducas *et al.*, "Crystals-dilithium: Digital signatures from module lattices," 2018.