QGram: a Hybrid PQC and QKD Architecture for Quantum-Safe Messaging

Ugo Chirico[1] **Salvatore Cuomo**[2]

1. Quantum2pi S.r.l., Napoli, Italy, 2. Università di Napoli Federico II

Abstract: We present QGram, a messaging platform combining NIST-standardized post-quantum cryptography (ML-KEM, ML-DSA) with Quantum Key Distribution in a layered hybrid architecture, providing quantum-safe end-to-end communications resilient to both current and future cryptanalytic threats.

The growing threat posed by quantum computing to classical public-key cryptography demands immediate action from the security community. Large-scale quantum computers running Shor's algorithm will be able to break RSA and elliptic-curve cryptosystems, compromising the confidentiality and authenticity of digital communications. The "Harvest Now, Decrypt Later" (HNDL) paradigm, where adversaries intercept and store encrypted data today for future decryption, makes this threat already relevant for information requiring long-term protection [1].

In this work, we present the architecture and design principles of QGram, a secure messaging platform developed by Quantum2pi that integrates post-quantum cryptography (PQC) and Quantum Key Distribution (QKD) into a unified, layered security framework. QGram addresses both the encryption and authentication dimensions of quantum-safe communications through two complementary defence layers.

At the cryptographic layer, QGram employs two NIST-standardized post-quantum algorithms implemented through purpose-built libraries. *KyberLib* implements the ML-KEM key encapsulation mechanism (FIPS 203), providing quantum-resistant key exchange based on the Module Learning With Errors problem [2]. *DilithiumLib* implements the ML-DSA digital signature scheme (FIPS 204), ensuring message authentication and integrity through lattice-based signatures [3]. Both libraries support multiple parameter sets (ML-KEM-512/768/1024 and ML-DSA-44/65/87) and are designed for integration into standard communication protocols.

At the communication layer, QGram adopts a hybrid key exchange model. The PQC-based key encapsulation is complemented by a QKD channel, where cryptographic keys are distributed using the quantum properties of single photons. Since QKD security relies on fundamental physical principles — the no-cloning theorem and the Heisenberg uncertainty principle — rather than computational assumptions, it provides information-theoretic security for key distribution [4]. This layered approach ensures that the system remains secure even if one layer is compromised, following a defence-in-depth strategy.

The hybrid architecture offers several advantages. While PQC provides scalable, software-based protection deployable on classical hardware, its security rests on the assumed hardness of mathematical problems. QKD provides unconditional security but requires dedicated hardware and is constrained by optical distance. By combining both, QGram achieves a crypto-agile design: the PQC layer ensures broad deployability; the QKD layer adds unconditional security where the quantum infrastructure is available [5].

QGram is currently developed within the FintechFactor program of the Italian Ministry of Economy and Finance, targeting secure financial communications. Future work includes performance benchmarking of the hybrid key exchange, integration with the Italian QKD backbone network, and extension to healthcare and public administration use cases, contributing to Italy's quantum-safe transition roadmap.

References

[1] NIST, "Transition to Post-Quantum Cryptography Standards," NIST IR 8547 (2024).
[2] NIST, "Module-Lattice-Based Key-Encapsulation Mechanism Standard," FIPS 203 (2024).
[3] NIST, "Module-Lattice-Based Digital Signature Standard," FIPS 204 (2024).
[4] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," *Theor. Comput. Sci.* **560**, 7–11 (2014).
[5] ETSI, "Quantum Key Distribution (QKD); Protocol and data format of REST-based key delivery API," ETSI GS QKD 014 V1.1.1 (2019).