

A Research testbed for Multi-Domain QKD and PQC Network Applications and Services

Angela Diaz-Bricio

Blanca Lopez, Javier Perez-Monrabal, Ivan Vidal, Francisco Valera

IMDEA Networks. Avenida Mar Mediterráneo, 22, 28918. Leganés, Madrid. Spain
angela.diaz@imdea.org

This work presents a hybrid testbed for quantum security, integrating quantum and post-quantum cryptographic (PQC) devices using emulated Quantum Key Distribution (QKD) nodes. Deployed in the 5TONIC laboratory (<https://www.5tonic.org/>), the testbed addresses interoperability challenges by enabling cooperation between otherwise incompatible devices. Digital twins are virtual software replicas of physical systems, designed to simulate and predict real-world behaviours. They constitute a risk-free environment for testing scenarios without requiring direct interaction with the physical entities they replicate. In this context, we use Quditto [1], an open-source orchestration tool of QKD networks, to enable real-world experimentation without the constraints of expensive quantum hardware.

The testbed, illustrated in Figure 1, includes commercial QKD systems (Cerberis XGR by IDQ), PQC devices (pQKD by Quantum Blockchains), physical unclonable function (PUF)-based authentication mechanisms, and emulated Quditto nodes. This flexible architecture supports cost-effective testing, dynamic and scalable topology configurations, and seamless network expansion.

The interoperability is ensured by a dedicated key management plane [2], where virtualized Key Management Entities (KMEs) support scalable key exchange and centralized cryptographic services. By leveraging ETSI-standard APIs (ETSI QKD 004 [3] and 014 [4]), clients can request cryptographic keys without direct interaction with quantum hardware, simplifying system updates, enhancing

scalability, and enabling seamless integration of advanced cryptographic features.

The testbed has been validated through multiple experiments [5] and enhances the study of quantum-secured networks by enabling interoperability testing and contributing to the development of future quantum communication infrastructures.

References

- [1] Quditto. Available online at www.quditto.io. 2024
- [2] Blanca Lopez, Ivan Vidal, Francisco Valera, Diego R. Lopez. IEEE Network PP(99):1-1. 2025. An Enhanced Virtualized Control and Key Management Model for QKD Networks
- [3] ETSI. Quantum Key Distribution (QKD); Application Interface. 2020
- [4] ETSI. Quantum Key Distribution (QKD); Protocol and Data Format of REST-Based Key Delivery API. 2019.
- [5] Demonstrative video of the experiments available at https://www.it.uc3m.es/fvalera/despliegue_testbed_madq_en.mp4

Figures

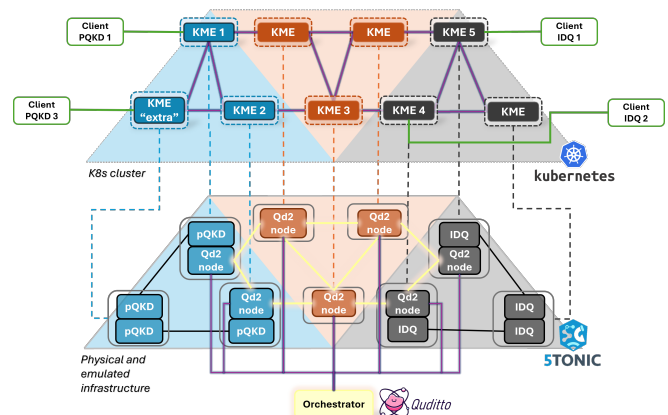


Figure 1: Deployed testbed blueprint

This publication is part of the I+D+I project MADQuantum-CM, financed by the European Union NextGeneration-EU, Madrid Government and by the PRTR. This work has also been partially supported by the EU Horizon Europe project Quantum Security Networks Partnership (QSNP), under grant 101114043.