

QSCAN demonstration in the Portuguese quantum communications infrastructure (PTQCI)



On 26 November 2025, QSCAN's secure computation service was showcased during the final demonstration of the Portuguese Quantum Communications Infrastructure (PQCI) project. Fully integrated into the operational network, the service demonstrated the end-to-end feasibility of quantum-generating, distributing, and consuming oblivious keys to enable relevant secure computation services.

A pair of continuous-variable quantum key distribution (CV-QKD) devices developed by Instituto de Telecomunicações were deployed to generate quantum oblivious keys. These keys were distributed through the network's key management layer, orchestrated by an software-defined network (SDN) layer, and consumed by QSCAN's service to secure the execution of oblivious transfer (OT) - a fundamental cryptographic primitive underpinning the OT-based multiparty computation protocols.

The deployed service enabled the secure computation of in-orbit collision probabilities between space objects tracked by two distinct network nodes, without either party disclosing private information about the state of their respective objects.

This deployment and respective demonstration was a crucial opportunity to validate some of the work carried out to date by QSCAN's consortium within a real-world infrastructure. It encompassed the full stack of the solution: from the physical implementation of the QKD devices to generate oblivious keys, solutions for integrating oblivious keys in the current QKD network standardization landscape, and the practical realization of a quantum-safe multiparty computation service leveraging QKD within an operational infrastructure.