CELTIC-NEXT
Eureka Cluster

CYBER QUANTA

11 SEPTEMBER 2025 PROPOSERS' BROKERAGE DAY

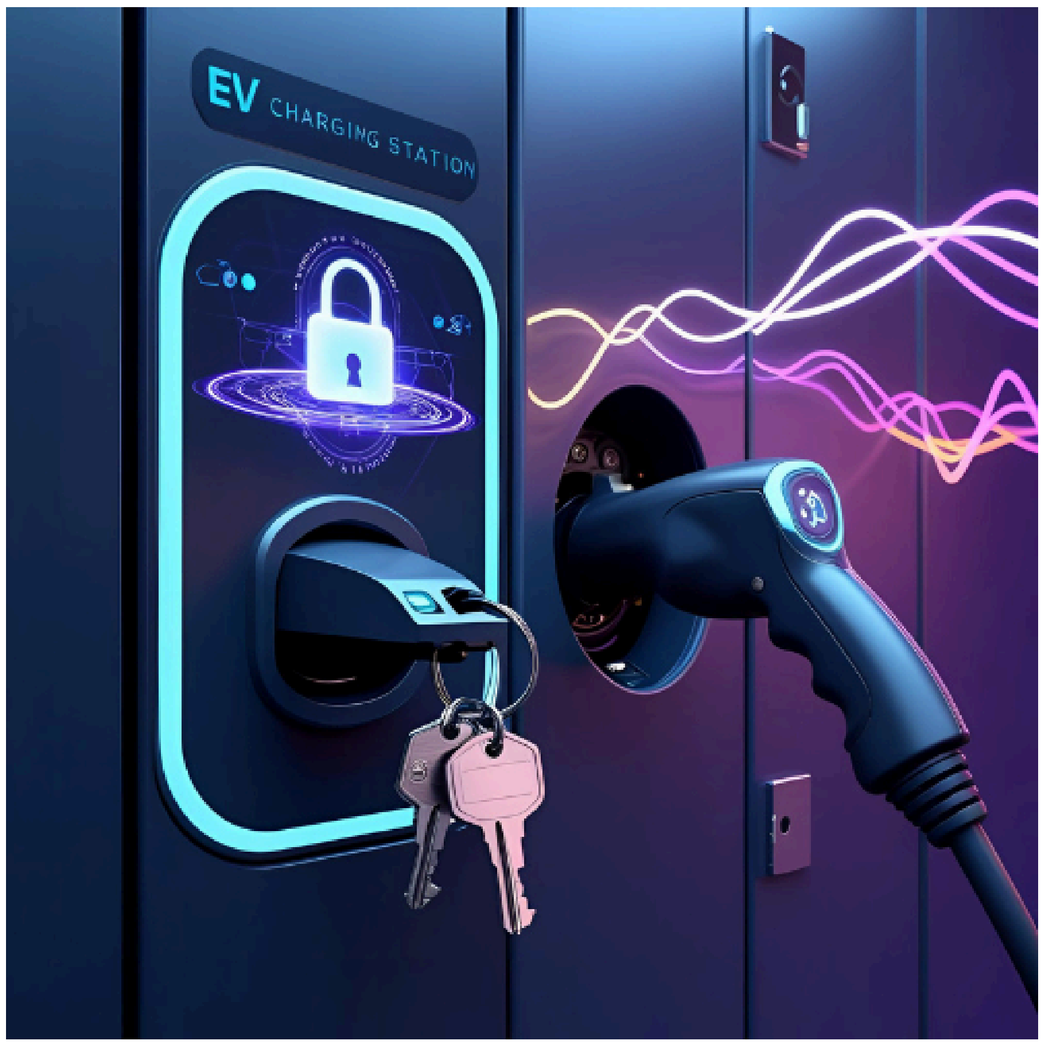
SPARC

SPARC

Secure Post-quantum Architecture for Resilient Charging

Future-proof EV charging infrastructure against quantum threats.

This proposal aims to develop a **post-quantum secure EV charging infrastructure**, integrating PQC algorithms (ML-KEM, HAWK, ML-DSA) into ISO 15118 and OCPP protocols, combined with hardware-based security (Secure Boot, TrustZone, HSM/TPM, encrypted flash). The approach also ensures **CRA/NIS2/GDPR compliance** and **Eichrecht-compliant measurement integrity**, providing a scalable and future-proof path to secure Europe's smart grid and e-mobility ecosystem.



Main Benefit:

A practical Post-Quantum Cryptography (PQC) upgrade path for EV charging stations — securing the smart grid against quantum threats.

Added Value:

- Real-world performance benchmarks for next-gen quantum-safe encryption.
- Future-proof EV charging protocols with embedded PQC.
- Trusted key protection using secure hardware (HSM/TEE).

Why Join:

Help shape Europe's PQC-ready EV infrastructure — standards-based, future-proof, and open-source-driven.

Consortium Members

- Cyber Quanta (Türkiye): System integration, PQC migration, secure key management
- University of Tartu (Estonia): PQC algorithm evaluation, cryptographic benchmarking

Looking For Partners With Expertise In:

- Electric vehicle charging systems, OCPP/mobility platforms, and secure protocol stack development
- Embedded system design teams capable of secure boot, filesystem encryption, and integration of hardware-based secure elements on Linux platforms
- Companies with experience in secure IoT device manufacturing and field deployment of cryptographic hardware

Contact

Dr. Faruk SARI, Cyber Quanta
faruk.sari@cyber-quanta.com
+90 216 212 55 40
www.cyber-quanta.com

photo of the presenter