Crypto Quantique

Quantum-Secure Cryptography for Resource-Constrained IoT Devices (QS_IoT)

The Challenge - Connected Devices Security

The rapid adoption of Internet of Things (IoT) devices brings significant benefits but also critical cybersecurity risks, as demonstrated by the devastating Mirai botnet attack. With 27 billion IoT devices expected by 2029 and the emergence of quantum computing threatening current cryptography, a robust, quantum-safe security solution is crucial. Crypto Quantique's consortium aims to address this challenge by combining quantum-driven hardware security with post-quantum cryptographic algorithms, creating an end-to-end IoT security platform that can protect the billions of resource-constrained devices across homes, businesses, and vital infrastructure, safeguarding sensitive data from chip to cloud.

The Solution - QS_IoT

Crypto Quantique, in collaboration with their partners CryptoEng and Liverpool John Moores University, proposes to develop a comprehensive, quantum-safe security solution for the Internet of Things (IoT). The project will advance Crypto Quantique's patented quantum-driven hardware IP, QDID, to operate efficiently at 28nm semiconductor nodes and below, targeting a 10x improvement in latency, a 33% reduction in silicon area, and a 50% reduction in raw Bit Error Rate (BER) compared to previous generations.
CryptoEng will focus on implementing optimised and formally verified post-quantum cryptographic algorithms, specifically one variant each of ML-KEM for encryption and ML-DSA for digital signatures, with key generation times under 10ms and 80ms respectively. The project aims to create a full-stack solution, with an FPGA reference design showcasing successful integration.

The Funding

With support from Neon's expert team, Crypto Quantique successfully secured the £871k grant funding needed to accelerate the final steps to market.

The Impact

By capturing a 0.7% share of the deep submicron IoT device market - around 82 million secured devices - the partners aim to generate €84 million in revenue by 2029 and support the creation of 60 high-value jobs. The collaboration will also strengthen the UK-Germany technology ecosystem, fostering knowledge exchange and innovation in the critical fields of IoT security and post-quantum cryptography.

CRYPTO QUANTIQUE

UKRI Innovate UK

24 months

£871,000 Grant

Crypto Quantique (UK)
Liverpool John Moores University (UK)
CryptoEng (D)

neon innovation