quantropi®
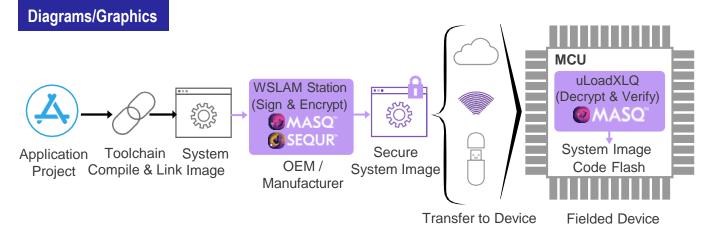
RA Ecosystem Partner Solution

Quantropi uLoadXLQ

Solution Summary

Quantropi's® uLoadXLQ, QiSpace for IoT Secure Boot & Installer, delivers quantum-secure bootloader and software update solutions for embedded platforms. uLoadXLQ integrates Quantropi's lightweight post-quantum digital signature algorithm featuring short signatures and fast verification and is uniquely engineered for performance in embedded systems with limited compute and memory resources. uLoadXLQ is available for the Renesas RA family of MCUs.

Features/Benefits

- Advanced post-quantum IoT secure root of trust, firmware authentication, integrity and safety, and software lifecycle update
- MASQ™
    - Crypto-agile suite of PQC algorithms providing authentication and key exchange with smaller signature sizes and better performance
- SEQUR™
    - Quantum random number generated and delivered quantum-securely for the strongest keys
- uLoadXLQ decrypts and verifies the image and application signatures, executes system integrity checks, and automatically performs configurable fallback and recovery steps at power-up or reset

Diagrams/Graphics

Target Markets and Applications

- Aerospace
- Automotive
- Industrial IoT
- Infrastructure
- Medical
- Telecom

www.quantropi.com/solutions/uloadxlq

2024.04

quantropi®

QiSpace™ for IoT

The Y2Q Threat

Advancements in Quantum Computing are accelerating, making its prospect of breaking classical cryptography more real with every passing day. At the same time, today's digital societies and economies rely on IoT and connected devices. With over 11 million new IoT devices coming online daily, and their functions becoming more mission critical, it is important to ensure their data and communications are quantum-secure. Quantropi's QiSpace for IoT family of solutions is an extension of the core QiSpace Platform with specific IoT optimized solutions for Application Security, Quantum TLS (TLS-Q), and uLoadXLQ Secure Boot & Installer.

QiSpace™ Platform

QiSpace is the only platform that provides a full suite of quantum-secure cryptographic capabilities and quantum entropy services.

> MASQ™ offers crypto-agile algorithms for key exchange and digital signature with support for NIST PQC, hybrid, and Quantropi's novel algorithms.

> QEEP™ symmetric encryption with support for both Quantropi's Quantum Permutation Pad and AES-QEEP, a FIPS-compliant double-wrapping for defence in depth.

> SEQUR™ quantum entropy services offers quantum random number generation and distribution for quantum enhanced cryptographic keys.

Protect data, networks, connected devices, and communications from today's threats and tomorrow's quantum computing attacks.

Quantropi's QiSpace™ Quantum Security Platform

[Contact | Quantropi](#)