quantropi Bring it on.

Cypherbridge®
Trusted, safe and secure

Authorized Partner

uLoadXLQ

uLoadXLQ Quantum Secure Boot & Installer

Advanced post quantum solution for IoT secure root of trust, firmware authentication, integrity and safety, and software lifecycle update

The Quantum Computing Threat to IoT

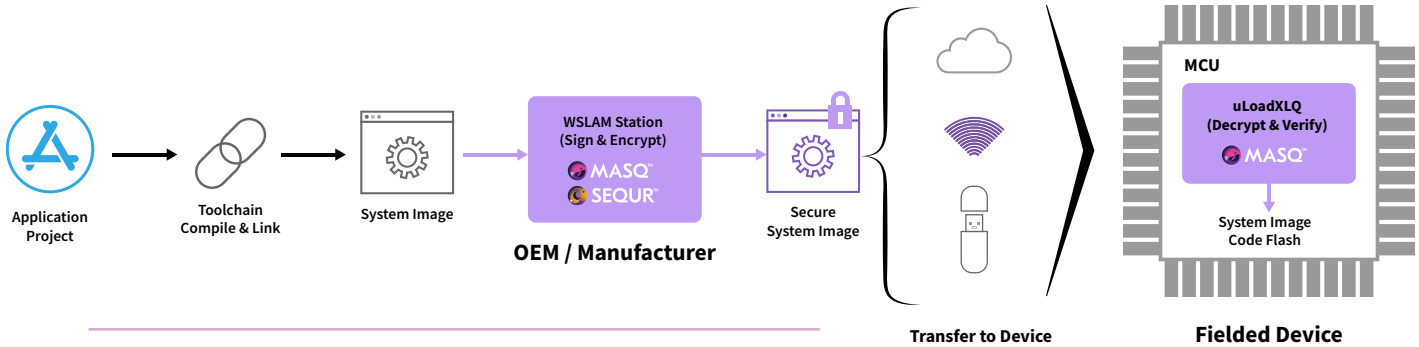
Many critical components of today's digital societies and economies rely on IoT and connected devices; yet the asymmetric encryption algorithms used to verify genuine code and for secure boot & installation, including ECC and RSA, are vulnerable to future quantum computing attacks. With real-world advancements in Quantum Computing accelerating every day, and IoT devices becoming more mission critical, it is important to safeguard them against compromise to ensure secure and reliable operation in a post-quantum world.

Software Lifecycle Solution

Built on the industry proven uLoadXL product suite, uLoadXLQ delivers quantum-secure boot loader and software update solutions for embedded platforms. uLoadXLQ integrates Quantropi's MASQ-DS lightweight post-quantum digital signature algorithm featuring small signatures and fast verification, and SEQUR™ Quantum Entropy Services to generate and distribute quantum random numbers for true random cryptographic keys. uLoadXLQ is uniquely engineered for performance in embedded systems with limited compute and memory resources.

Features

- Fast, low-footprint post-quantum cryptographic digital signature algorithm
- Strong cryptographic keys derived from quantum random numbers
- Robust system integrity, safety and reliability including recovery and failsafe operation
- Secure boot root of trust protects IP and blocks malware
- Multi-image update for system application, graphic menus, FPGA bit files
- Image file encryption, integrity and authentication, code sign and verify — image cannot be hacked if lost or intercepted
- Install OTA, flash drive, serial port
- Windows WSLAM Software Management Station GUI
- Use standard toolchain to compile and link the system application image
- Multiple public key management for key rotation and revocation
- LCD graphic progress messages and progress bar display framework
- NIST 800-193 Firmware Protect, Detect and Recover
- Platform Kits available for off-the-shelf MCU evaluation kits



QiSpace™

Quantropi's hybrid SaaS platform uniquely provides quantum-secure cryptographic functions in resource constrained environments.

MASQ™

PQC digital signature featuring small signature size and fast verification.

SEQUR™

QRNG derived true random numbers for encryption keys.

V11/2023.12.01

quantropi Bring it on.

Cypherbridge®

Trusted, safe and secure

How It Works

The WSLAM Software Management Station manages secure software updates and distribution for routine maintenance and to address identified vulnerabilities. The WSLAM Windows GUI provides image processing, code signing and encryption, and firmware push to target. Secure managed images can be transferred by OTA, by email, removable flash drive, or serial port.

On the IoT device, uLoadXLQ decrypts and verifies the image signature before saving it to the target code flash. If the verification fails, the code is blocked from installing and executing. At power-up or reset, uLoadXLQ executes system integrity checks, verifying application signatures, and automatically performing configurable fallback and recovery steps.

Platform Kit

uLoadXL APIs are interfaced to the embedded target via integrated Platform Kit including standalone drivers for internal MCU flash, external QSPI flash, removable media and serial I/O channels.

Multiple Images

The uLoadXL embedded system and APIs can manage multiple images. Workflow can be programmed to install, save and activate A/B image firmware and auxiliary files.

Registry

Loader maintains image registry information including status and authentication signatures. System application is verified before starting execution to detect corrupt image or malware intrusion attempt.

Security Model

uLoadXL implements an advanced key system, selectable cipher suite, code sign and verify and protected embedded key material container, with anti-rollback protection.

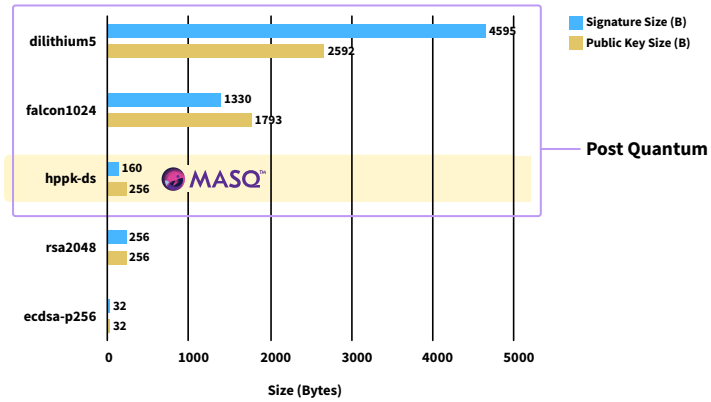
Robust

System integrity, safety and availability features include primary and backup registry copies, power fail recovery, primary and recovery image, and failsafe options.

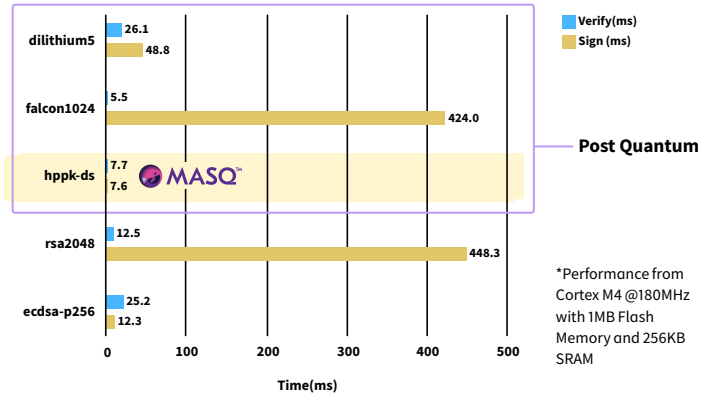
MASQ-DS: Lightweight. Fast. Quantum-Secure.

At NIST Level V, MASQ-DS (hppk-ds) offers the smallest public key and signature sizes of any post-quantum algorithm, and fastest combined sign and verify performance. The unique combination of small size and fast performance make it the optimal choice in IoT and resource constrained settings.

Public Key & Digital Signature Size



Sign & Verify Time



*Performance from Cortex M4 @180MHz with 1MB Flash Memory and 256KB SRAM

SEQUR™: Strong. Limitless. True Random.

Limited entropy is a common problem, especially in IoT systems, which can result in weak cryptographic keys and diminished security. SEQUR™ quantum entropy services provides quantum random numbers on-demand at up to 1Gbps to create the strongest true random cryptographic keys. SEQUR™ random numbers have passed industry standard statistical tests including ENT, DIEHARDER, and NIST SP 800-22.

For Pricing and Availability Contact:

Quantropi Inc.
1545 Carling Ave, Suite 620
Ottawa ON, K1Z 8P9 CANDA
+1 (613) 695-5711
www.quantropi.com

Cypherbridge Systems LLC
7040 Avenida Encinas #104211
Carlsbad CA 92011 USA
+1 (760) 814-1575
www.cypherbridge.com
sales@cypherbridge.com

Quantropi uLoadXLQ Solution

Cypherbridge Systems