quantropi

uLoadXLQ Quantum Secure Boot & Installer

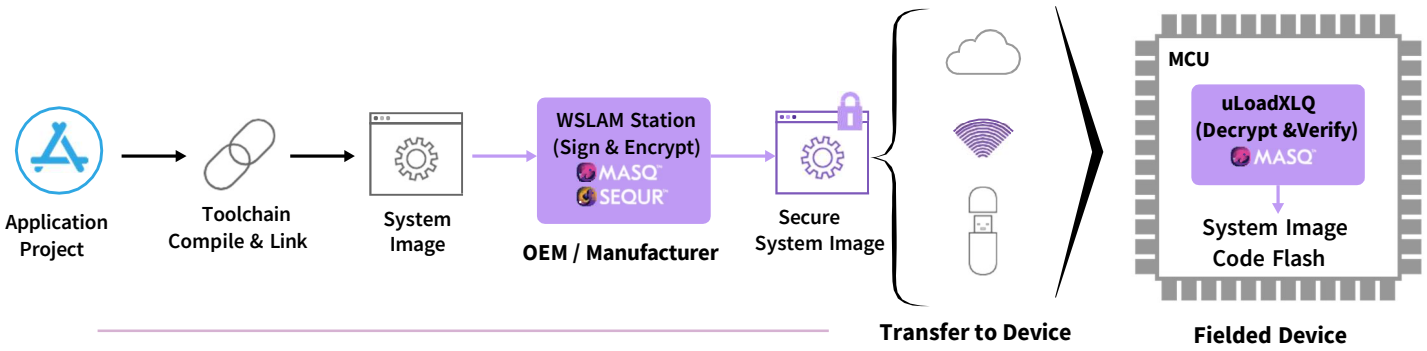
Advanced post quantum solution for IoT secure root of trust, firmware authentication, integrity and safety, and software lifecycle update

The Quantum 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

quantropi

QiSpace™ for IoT Solution Family

Application Security

The QiSpace™ SDK includes a complete set of post-quantum asymmetric and symmetric cryptographic functions and strong random numbers to harden application security. Using the SDK, a developer can quantum securely sign and verify data records and add quantum protection to data transmission and storage.

Quantum TLS (TLS-Q)

TLS-Q is an enhanced version the TLS networking protocol compatible with popular RTOSs that provides Post-quantum security to network communications for embedded devices. TLS-Q includes the complete suite of required quantum secure cryptographic enhancements including asymmetric encryption, symmetric encryption, and quantum random number generation.

Secure Boot & Installer

uLoadXLQ provides quantum-secure boot and installation for embedded platforms by integrating MASQ light-weight post-quantum digital signature algorithm with short signatures and fast verification.

Performance Advantage for Novel Algorithms

- ✓ Quantropi's novel key exchange (HPPK-KEM) is specifically optimized for IoT solutions with an efficient 208-byte ciphertext size and ~8K of memory utilization at NIST L5.
- ✓ Quantropi's novel digital signature (GHPPK-DS) is specifically optimized for IoT solutions with an efficient 272-byte signature size and less than 11K of memory utilization at NIST L5.

Support for leading MCU Platforms

QiSpace™ for IoT supports chipsets from leading vendors ranging from high-performance down to ultra-low-power MCUs. Current supported chipsets are listed below:

Authorized Partner
life.augmented

- STM32 Cortex M Series MCU
- STM32 Cortex M Series MPU
- Legacy Arm Processors
- SPC5 32-bit Automotive
- Stellar 32-bit Automotive

RENESAS RA READY

- RA Cortex M Series MCU
- RL Low Power Series
- RX 32-bit
- RZ 32/64-bit Multicore MPUs
- RH850 Automotive Series MCUs
- RISC-V Processors

MICROCHIP

- PIC32 Cortex M Series MCU
- SAM Cortex M Series MCU
- Legacy Arm Processors
- RISC-V Processors
- AVR32

Support for additional chipsets available based on customer specific requirements.

Contact Us:
sales@quantropi.com
www.quantropi.com

Try QiSpace™ For Free!