

Quantum Secure Boot (Add-On)

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

The Quantum Threat to IoT

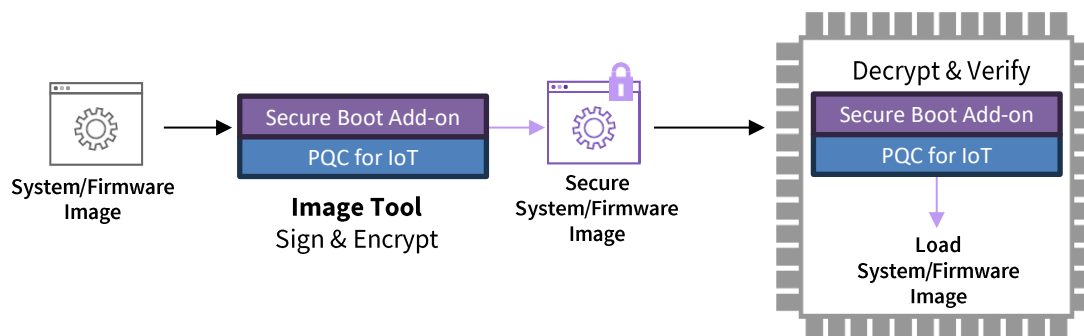
Many critical components of today's digital societies and economies rely on IoT and connected devices; yet the asymmetric encryption algorithms used to verify genuine code and for secure boot & installation, including ECC and RSA, are vulnerable to future quantum computing attacks. With real-world advancements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

QiSpace™ PQC for IoT Secure Boot Add-on

The QiSpace™ PQC for IoT Secure Boot Add-on combines NIST PQC and Quantropi Novel algorithms with the proven reliability of MCUboot to deliver a quantum-secure bootloader that validates system images and firmware updates while preventing unauthorized software from running. It is uniquely engineered for high-performance in embedded systems with limited compute and memory resources and provides the crypto-agility to easily switch cryptographic algorithms based on the specific use case requirements and limitations.

Features

- Easy upgrade path for MCUboot implementations
- Crypto-agility for easy algorithm switching
- Fast, low-footprint post-quantum cryptographic digital signature algorithms
- Available strong cryptographic keys derived from quantum random numbers
- Image file encryption, integrity and authentication, code sign and verify — image cannot be accessed or modified if lost or intercepted



Availability and OS Support

The QiSpace™ PQC for IoT Secure Boot Add-on is available for Baseline and Premium SDK packages.

The Baseline Add-on includes:

- NIST PQC standards
- Classic/PQC hybrids

The Premium Add-on additionally includes:

- Quantropi novel PQC
- Quantropi novel PQC hybrids
- Strong cryptographic keys from quantum random numbers

OS Support includes:

Zephyr, FreeRTOS

QiSpace™ for IoT Solution Family Pricing

QiSpace™ PQC for IoT	Baseline			Premium		
	Dev	Standard	Enterprise	Dev	Standard	Enterprise
Subscription	\$7.5K / year	\$10K / year	\$30K / year	\$7.5K / year	\$20K / year	\$40K / year
Secure Boot Add-on	\$7.5K / year	\$10K / year	\$10K / year	\$7.5K / year	\$15K / year	\$15K / year
Secure Network Add-on	\$7.5K / year	\$10K / year	\$10K / year	\$7.5K / year	\$15K / year	\$15K / year
NIST FIPS 203 / 204	●	●	●	●	●	●
Novel GHPPK / HPPK	○	○	○	●	●	●
Source Code Included	○	○	○	●	●	●
# Support Incidents included	5	10	Unlimited	5	25	Unlimited
Standard Email Support	●	●	●	●	●	●
Live Call Support	○	○	●	○	●	●
24/7/365 Support	○	○	●	○	○	●

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



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



- 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



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

Support for additional MCU manufacturers and chipsets available. Contact sales for details.

Contact Us:

sales@quantropi.com
www.quantropi.com

Try QiSpace™
PQC for IoT

