Quantum Secure Network (Add-on)

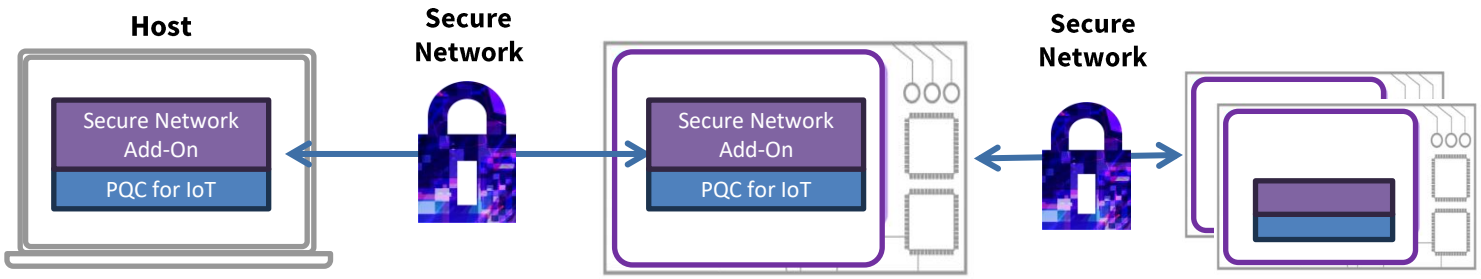
The Quantum Threat to IoT

Advancements in Quantum Computing are accelerating, making its prospect of breaking classical cryptography more real with every passing day. At the same time, many critical components of today's digital societies and economies rely on IoT and connected devices. With millions of 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 between IoT device and cloud.

QiSpace™ PQC for IoT Secure Network Add-on

The QiSpace™ PQC for IoT Secure Network Add-on provides customized Mbed TLS Extensions and OpenSSL Crypto Providers optimized for embedded devices. Featuring both NIST PQC and Quantropi Novel algorithms optimized for high-performance in resource constrained systems, this solution provides both flexibility and crypto-agility for establishing quantum-secure TLS 1.3 network connections from desktops and servers down to the most resource constrained embedded devices. The Quantum Secure Network Add-on includes:

1. OpenSSL Cryptographic Provider module provides the cryptographic functions needed to establish quantum-secure TLS 1.3 network connections. With OpenSSL 3.2 or higher supporting a provider-based architecture, this custom module can be easily used to dynamically add post quantum security to any OpenSLL 3.x server.
2. Mbed TLS Quantum Safe Extension extends the capabilities of Mbed TLS by adding the key exchange and digital signature algorithms needed to establish quantum-secure TLS 1.3 network connections.



Availability and OS Support

The QiSpace™ PQC for IoT Secure Network Add-on is available for both Baseline and Premium 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

OS Support includes:
OpenSSL – Linux, Windows
Mbed TLS – Embedded Linux, Zephyr, FreeRTOS, Azure/Eclipse RTOS

quantropi

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