quantropi

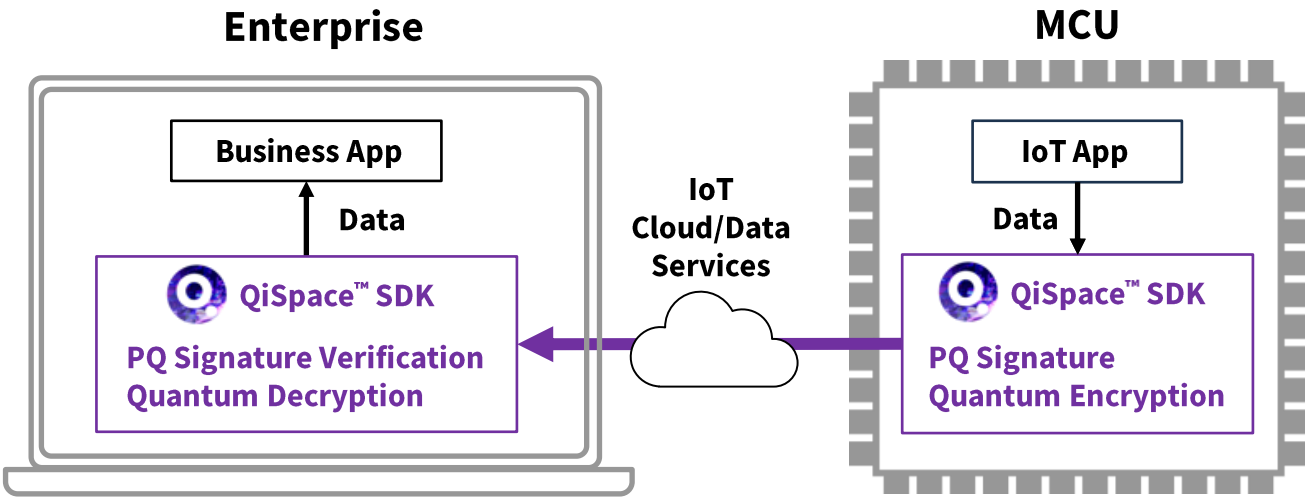
QiSpace™ for IoT Application Security

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 embedded applications and data are quantum-secure.

Implement Strong Application Level Security

The QiSpace™ SDK provides a complete set of cryptographic capabilities to harden security for applications running on major embedded platforms. It includes post-quantum asymmetric and symmetric cryptographic functions and quantum random numbers in a modular package delivering maximum flexibility for adding quantum security to any application.



- ✓ Add quantum random numbers to achieve the full security potential of your current cryptographic functions.
- ✓ Integrate quantum-secure signing and verification and data encryption capabilities optimized for high performance in resource constrained environments.

QiSpace™ SDK Components

MASQ™

- Crypto-agile asymmetric encryption with support for NIST PQC finalists
- Available Quantropi novel PQC with significantly smaller signature sizes and better performance compared to current PQC finalists

QEEP™

- Quantum-secure symmetric encryption on any IP network or device
- Up to 18x faster than software AES-256
- Dynamic code footprint as small as 2.4KB

SEQUR™

- NGen – Efficient and high-performance local pseudo-quantum random number generation
- QEaaS – Quantum-secure entropy distribution over the Internet leveraging high-performance FIPS-certified QRNGs

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:

- 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 chipsets available based on customer specific requirements.

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

Try QiSpace™ For Free!