quantropi

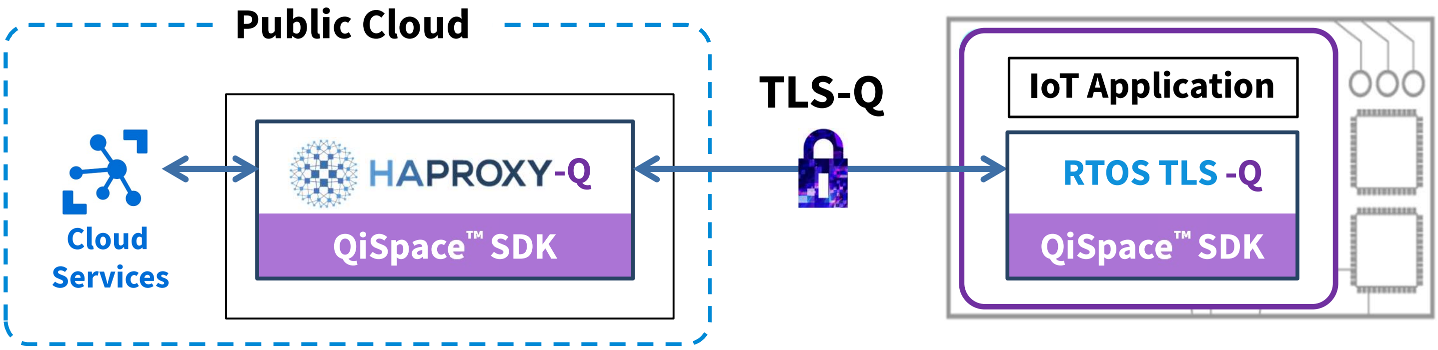
Quantum TLS (TLS-Q) Security for IoT to Cloud

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 to cloud.

Quantropi TLS-Q

Available on major MCU chipsets, 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 Quantropi's TLS-Q provides an immediate quantum security protection upgrade that works with existing network infrastructures.



Secure IoT Data and Communications with TLS-Q

Any IoT application running on a supported RTOS can be configured to use TLS-Q which includes:

- MASQ™ crypto-agile algorithms for key exchange and digital signature with support for NIST PQC, hybrid, and Quantropi's novel algorithms
- QEEP™ quantum-based symmetric encryption and an AES-QEEP FIPS-compliant "double-wrap" for defense in depth
- SEQUR™ quantum entropy services for quantum key generation or quantum-enhanced pseudorandom keys

To provide a quantum-secure endpoint in the cloud, HAProxy-Q is a QiSpace™ powered implementation of HAProxy built on TLS-Q. Running as a virtual machine, HAProxy-Q seamlessly bridges the quantum-secure communications between IoT devices and public cloud services.

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:

ST life.augmented Authorized Partner

- 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!