quantropi®

RA Ecosystem Partner Solution

Quantropi Quantum TLS (TLS-Q)

Solution Summary

Quantropi's® Quantum TLS (TLS-Q) is a quantum-secure addition to the RTOS TLS stack while maintaining reliability, flexibility, and performance. This is the ideal solution to deal with the prospect of breaking classical cryptography by advancements in AI and Quantum Computing. All IoT applications running common real-time operating systems (RTOS) can be configured to use TLS-Q and gain immediate quantum security that works with existing networks. TLS-Q in QiSpace for IoT series supports common real-time operating systems including Eclipse ThreadX, FreeRTOS, and Zephyr and is available for the Renesas RA family of MCUs.

Features/Benefits

- Quantum-secure data and communications between cloud and IoT devices
- MASQ™ featuring crypto-agile suite of PQC algorithms providing authentication and key exchange with smaller signature sizes and better performance
- QEEP™ featuring quantum-secure symmetric encryption with a small dynamic code footprint
- SEQUR™ featuring quantum random numbers generated and delivered quantum-securely for the strongest keys

Diagrams/Graphics
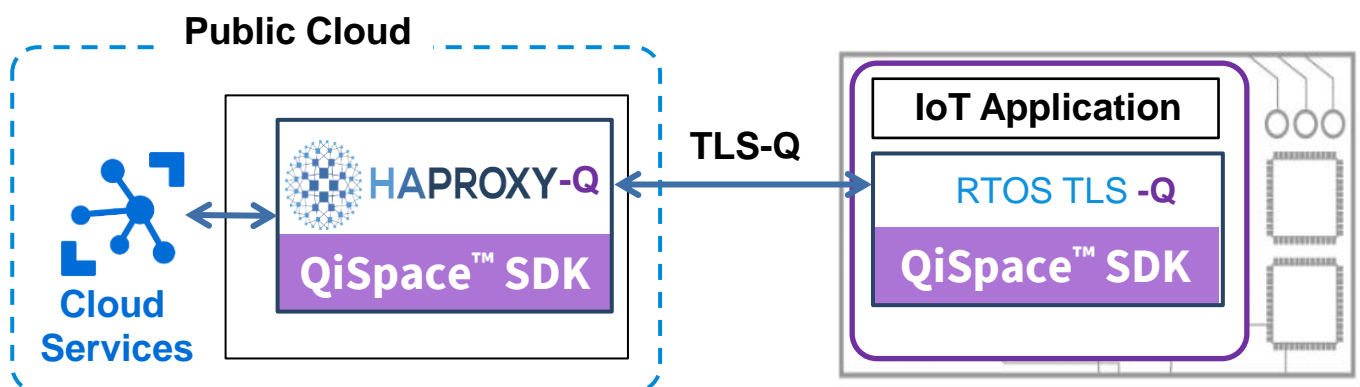
Target Markets and Applications

- Aerospace
- Automotive
- Industrial IoT
- Infrastructure
- Medical
- Telecom

www.quantropi.com/solutions/tls-q

2024.04

QiSpace™ for IoT

The Y2Q Threat

Advancements in Quantum Computing are accelerating, making its prospect of breaking classical cryptography more real with every passing day. At the same time, today's digital societies and economies rely on IoT and connected devices. With over 11 million 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. Quantropi's QiSpace for IoT family of solutions is an extension of the core QiSpace Platform with specific IoT optimized solutions for Application Security, Quantum TLS (TLS-Q), and uLoadXLQ Secure Boot & Installer.

QiSpace™ Platform

QiSpace is the only platform that provides a full suite of quantum-secure cryptographic capabilities and quantum entropy services.

MASQ™ offers crypto-agile algorithms for key exchange and digital signature with support for NIST PQC, hybrid, and Quantropi's novel algorithms.

QEEP™ symmetric encryption with support for both Quantropi's Quantum Permutation Pad and AES-QEEP, a FIPS-compliant double-wrapping for defense in depth.

SEQUR™ quantum entropy services offers quantum random number generation and distribution for quantum enhanced cryptographic keys.

Protect data, networks, connected devices, and communications from today's threats and tomorrow's quantum computing attacks.

Quantropi's QiSpace™ Quantum Security Platform

Cryptographic Function	Quantum Security Platform	Quantum-Secure Use Cases	Applications
	QiSpace™		
Asymmetric Encryption	MASQ™	• Key Exchange Mechanism • Digital Signature & Authentication	• Aerospace • Automotive • Consumer
Symmetric Encryption	QEEP™	• Data & Network Encryption • Block & Streaming Cipher	• Defense • Industrial • Infrastructure
Strong Random Numbers	SEQUR™	• Streaming Entropy • Quantum Random Number Generation	• Medical • Telecom

[Contact | Quantropi](#)