quantropi
Bring it on.

Authorized Partner

Eclipse ThreadX-Q TrUE Quantum Security for IoT to Cloud

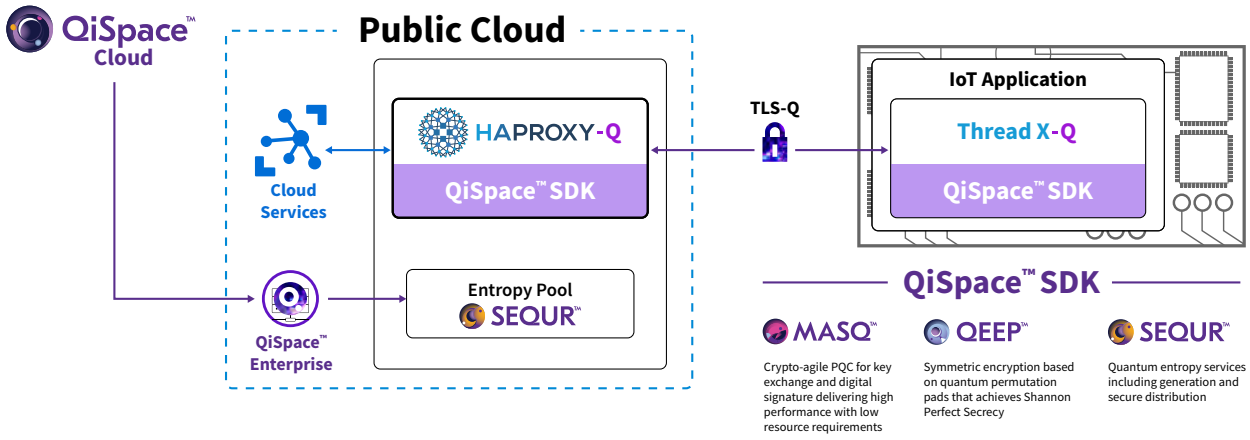
QiSpace™ for X-Cube-Azure and X-Cube-AWS

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 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 between IoT device to cloud. Quantropi's Eclipse ThreadX-Q is a TrUE solution offering Trust, Uncertainty, and Entropy.

Eclipse ThreadX-Q

Available on all major MCU chipsets, ThreadX-Q is Quantropi's quantum-secure extension of the Eclipse ThreadX NetX Duo networking stack. Quantropi's QiSpace™ Platform (MASQ™, QEEP™, and SEQUR™) provides asymmetric cryptography, symmetric cryptography, and quantum entropy while maintaining the reliability, flexibility, and performance of Eclipse ThreadX NetX Duo. Quantropi's ThreadX-Q provides immediate quantum security protection that works with existing network infrastructure.



Secure IoT Data and Communications with ThreadX-Q

Any IoT application running Eclipse ThreadX NetX Duo can be configured to use ThreadX-Q which includes:

- Trust – MASQ™ crypto-agile algorithms for key exchange and digital signature with support for NIST PQC, hybrid, and Quantropi's novel algorithms
- Uncertainty – QEEP™ symmetric encryption with support for both AES, and AES-QEEP FIPS-compliant double-wrapping for defense in depth
- Entropy – SEQUR™ quantum entropy services for quantum random keys or quantum enhanced pseudorandom keys

V01/2023.04.13

quantropi
Bring it on.

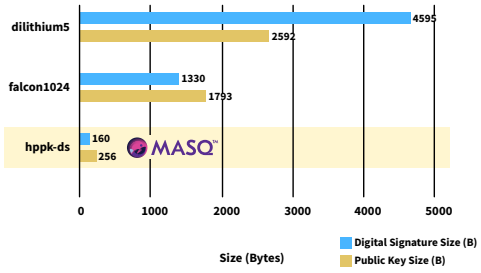
To provide a quantum-secure endpoint in the cloud, HAProxy-Q is a QiSpace™ powered implementation of HAProxy built with our QiSpace™ SDK. Running as a virtual machine HAProxy-Q seamlessly bridges the quantum-secure communications between IoT devices and the Public Cloud IoT services.

Additionally, HAProxy-Q generates strong cryptographic keys using quantum entropy from SEQUR™, which is transparently feeds strong random into the VM entropy pool.

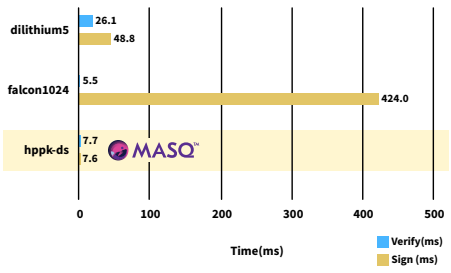
MASQ™

Quantropi novel algorithms (HPPK-KEM & MPPK-DS) for applications with resource constraints and/or stringent performance requirements.

Public Key & Digital Signature Size

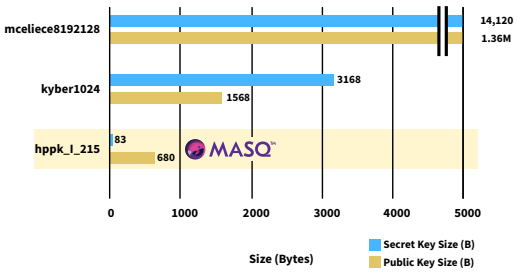


Sign & Verify Time

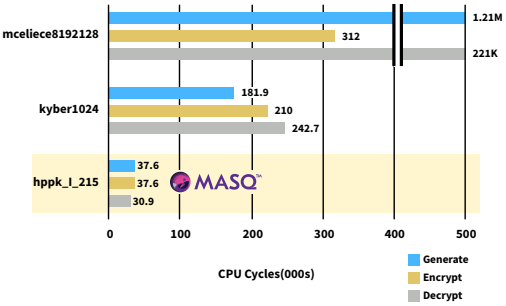


HPPK-DS offers small digital signature sizes of 160B and high performance on both sign and verify operations. Has been submitted to NIST for standardization following the new call for digital signature proposals

Public Key & Secret Key Size Comparison



Generate, Encrypt & Decrypt Comparison



HPPK-KEM offers small public and secret key sizes and fast key generation, encryption, and decryption capabilities

QEEP™

QEEP™ is a Quantropi novel symmetric algorithm which supports symmetric key lengths up to 32,768 bits. It performs up to 18x fast- er than software AES-256 and up to 2x faster than AES-NI (hardware accelerated), and can implemented together with AES in a FIPS- compliant manner for defense in depth. With a code footprint as small as 2.4KB it is engineered to for performance in constrained environments such as IoT.

SEQUR™

SEQUR™ provides quantum entropy services including the generation and distribution of quantum entropy. Source quantum entropy from Quantropi hosted QRNG devices and also supports custom implementations for distribution of customer controlled entropy sources.

SEQUR™ NGen provides QiSpace™ a PRNG that supports up to 100KB of entropy, outclassing existing PRNG options. QiSpace™ entropy passes industry standard statistical tests including: NIST STS, ENT, and DIEHARDER

For Pricing and Availability Contact:

Quantropi Inc.
1545 Carling Ave, Suite 620
Ottawa ON, K1Z 8P9 CANDA
+1 (613) 695-5711
www.quantropi.com

QiSpace™ TLS-Q for IoT