quantropi
Bring it on.

QiSpace™

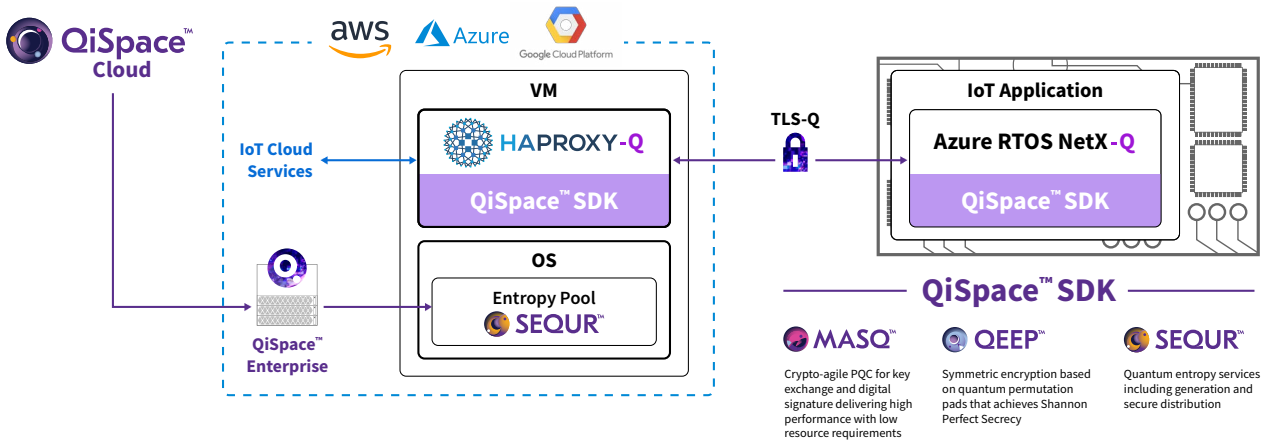
QiSpace™ TLS-Q for IoT

The Quantum Threat to IoT

Advancements in Quantum Computing are accelerating, making the prospect of its 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 ever more mission-critical, it is important to ensure data and communications are quantum-secure between IoT device and cloud. Quantropi's QiSpace™ TLS-Q for IoT provides connected platforms and devices with all three "**TrUE**" cryptographic components – **Tr**ust, **U**ncertainty, and **E**ntropy – required for complete quantum security.

Quantum-Securing TLS

QiSpace™ TLS-Q for IoT is a quantum-secure implementation of a typical networking stack leveraging HAProxy in the Cloud. The QiSpace™ Platform (MASQ™, QEEP™, and SEQUR™) provides asymmetric cryptography, symmetric cryptography, and quantum entropy, while maintaining the reliability, flexibility, and performance of the Cloud. This provides immediate quantum security protection for TLS-Q that works with existing network infrastructures.



Secure IoT Data and Communications with TLS-Q

IoT applications can be configured to use TLS-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

V05/2023.08.10

quantropi
Bring it on.

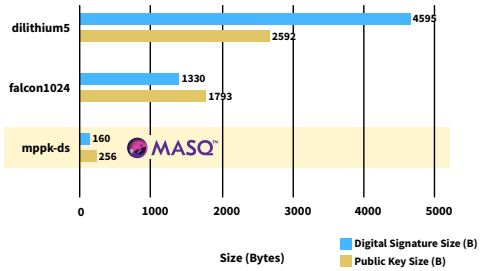
HAProxy-Q is a QiSpace™ powered implementation of HAProxy built on TLS-Q to provide a quantum-secure endpoint in the cloud. Running as a virtual machine, HAProxy-Q seamlessly ensures quantum-secure communications between IoT devices and IoT Cloud Services.

In addition to TLS-Q, HAProxy-Q generates strong cryptographic keys using quantum entropy from SEQUR™ Nject which transparently feeds strong random into the OS entropy pool.

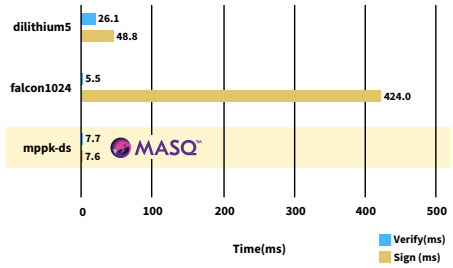
MASQ™

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

Public Key & Digital Signature Size

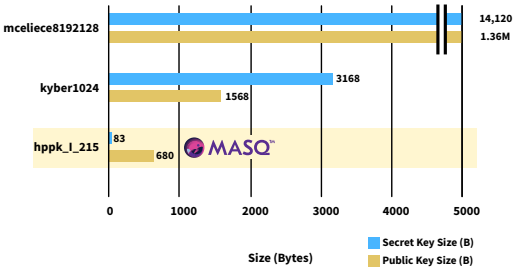


Sign & Verify Time

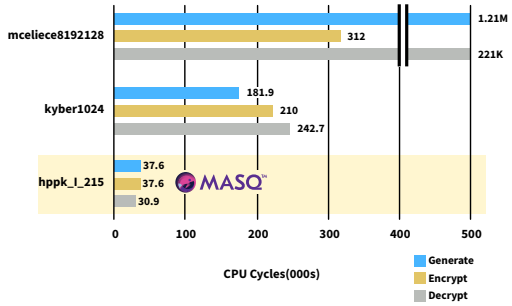


MPPK-DS offers small digital signature sizes of 160B and high performance on both sign and verify operations.

Public Key & Secret Key Size Comparison



Generate, Encrypt & Decrypt Comparison



MPPK-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 100,000 bits. It performs up to 18x faster than software AES-256 and up to 2x faster than AES-NI (hardware accelerated), and can be 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.

- Sources 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 CANADA
+1 (888) 987-5789
+1 (613) 695-5711
www.quantropi.com