quantropi
Bring it on.

QiSpace™

QiSpace™ for Embedded Application Security

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.

Implementing Strong Application Level Security

QiSpace™ offers a software development kit for major embedded platforms that provides product managers and developers with a complete suite of cryptographic functions to protect data, devices and systems, now and forever.

Example Platforms Include:

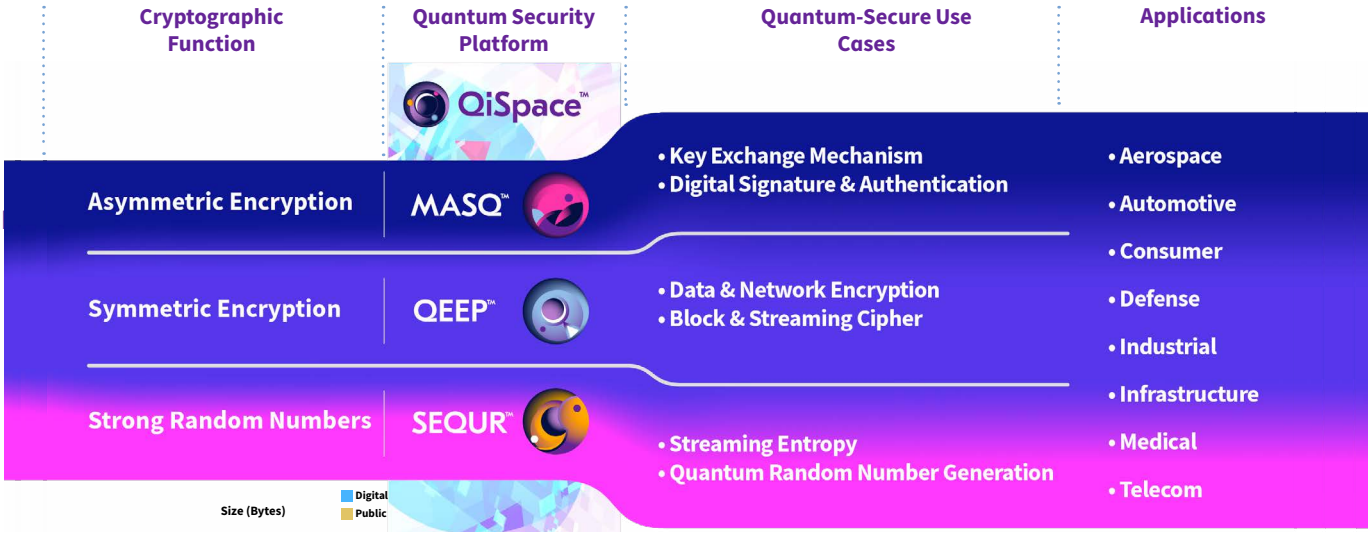
Microchip (SAM V71) | **ST Micro (STM32 H7 & F4)** | **Renesas (RA6M5)**

When you begin your quantum security transition today by using QiSpace™ Quantum Entropy Services to provide quantum entropy (true random numbers) to your device endpoints, you will immediately achieve the full security potential of your current cryptographic functions. Then seamlessly integrate quantum-secure signing capabilities, critical data elements verification capabilities, and application level data encryption capabilities, optimized for high performance in resource constrained environments.

V03/2023.05.17

quantropi
Bring it on.

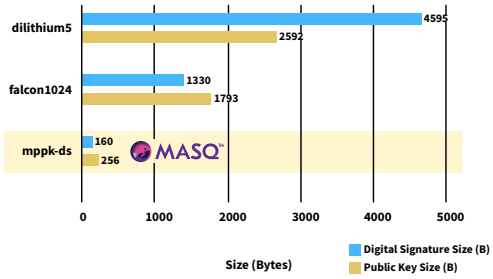
Quantropi's QiSpace™ Quantum Security Platform



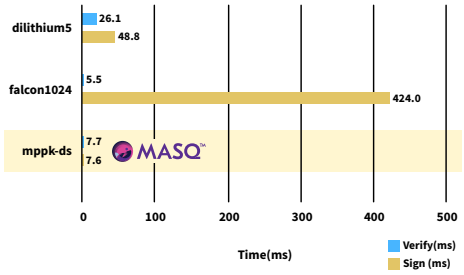
Real-World Performance Highlights

DS – Sign Verify Stats

Public Key & Digital Signature Size

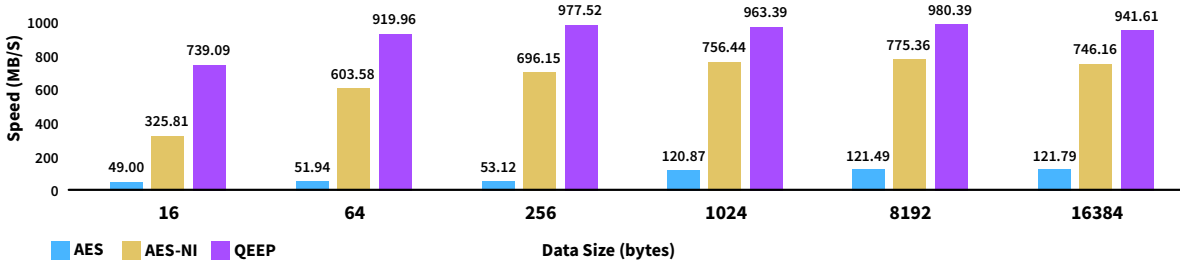


Sign & Verify Time



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

AES – Stats vs. QEEP



Speed Evaluation for Intel® Pentium Silver J5005 CPU@1.5GHZ OS: Linux v18.10

quantropi
Bring it on.

Real-World Performance Highlights

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 10KB

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

Demonstration Overview

MASQ™

- **Test #1: Asymmetric Key Exchange Mechanism**
  - Demonstrate generation of (10) unique Post-quantum Public-Private Key pairs that would be used to share a session key between a device and an external party (ex. cloud or host service, other device, etc.) as part of initiation of typical secure communications session (ex. TLS).
  - Test each Key Pair by encrypting and decrypting a session key. Report test Pass / Fail.
- **Test #2: Digital Signature**
  - Demonstrate generation of (10) unique Post-quantum Digital Signatures that would be used to authenticate identity with external party (ex. cloud or host service, other device, etc.) as part of initiation of typical secure communications session (ex. TLS). Also used for data and code signing.
  - Test each Digital Signature by signing and verifying a test string. Report test Pass / Fail.

QEEP™

- **Test #3: Symmetric Encryption**
  - Demonstrate generation of a NIST Level V Security "Quantum Permutation Pad" that would be used to symmetrically encrypt and decrypt messages based on 256-bit cryptographic key.
  - Test Symmetric Encryption by encrypting and decrypting (10) unique test strings. Report test Pass / Fail.

SEQUR™

- **Test #4: NGen - Quantum Random Number Generation**
  - Demonstrate generation of (10) 256-bit random numbers suitable for use as strong cryptographic keys. Report Numbers.
- **Test #5: QEaaS – Quantum Entropy as a Service (local)**
  - Demonstrate ability to receive quantum-encrypted block of entropy and decrypt locally. In local / offline demo mode, test decryption of pre-shared encrypted file. Report test Pass / Fail.

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