QiSpace™ for Embedded Application Security

QiSpace™ for 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 embedded applications and data are quantum-secure. Quantropi's QiSpace™ 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.

When you begin your quantum security transition today by using QiSpace™ Quantum Entropy

QiSpace™ SDK Components

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
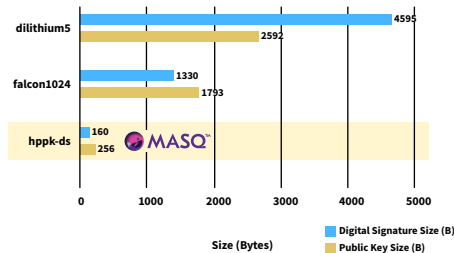- Dynamic code footprint as small as 2.4KB

SEQUR™
- NGen – Efficient and high-performance local pseudo-quantum random number generation
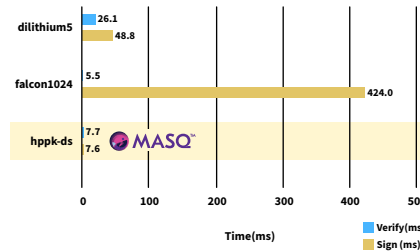- QEaaS – Quantum-secure entropy distribution over the Internet leveraging high-performance FIPS-certified QRNGs

Real-World Performance Highlights

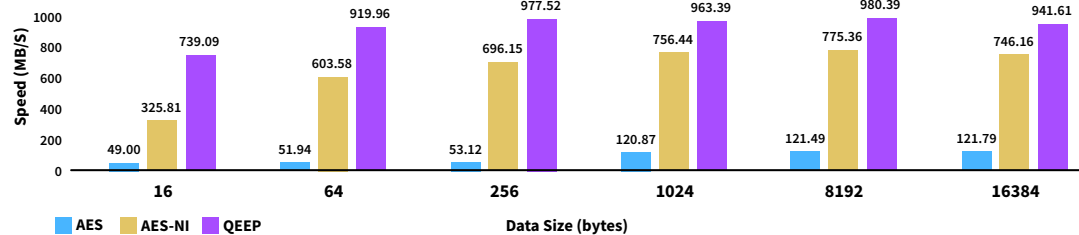## DS – Sign Verify Stats

Public Key & Digital Signature Size

dilithium5	4595	
	2592	
falcon1024	1330	
	1793	
hppk-ds	160 MASQ™	
	256	

0 1000 2000 3000 4000 5000

Size (Bytes)

■ Digital Signature Size (B)
■ Public Key Size (B)

Sign & Verify Time

dilithium5	26.1	
	48.8	
falcon1024	5.5	
	424.0	
hppk-ds	7.7 MASQ™	
	7.6	

0 100 200 300 400 500

Time(ms)

■ Verify(ms)
■ Sign (ms)

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

AES – Stats vs. QEEP

Data Size (bytes)	AES	AES-NI	QEEP
16	49.00	325.81	739.09
64	51.94	603.58	919.96
256	53.12	696.15	977.52
1024	120.87	756.44	963.39
8192	121.49	775.36	980.39
16384	121.79	746.16	941.61

Speed (MB/S)

■ AES ■ AES-NI ■ QEEP

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

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.