



**QiSpace™**

**RENESAS**

# TrUE Quantum Cryptography. Ultra-High Performance.

With the advent of quantum computers and Y2Q fast approaching, it's critical to act immediately. Protect your embedded systems against immediate and long term threats by transitioning today to a permanent post-quantum security posture.

QiSpace™ SDK is a software toolkit for the Renesas RA6 Series from the RA Family of Arm® Cortex®-M based MCUs that provides product managers and embedded developers with a complete suite of cryptographic functions to protect data, devices and systems, now and forever.

## Quantropi's QiSpace™ Quantum Security Platform

Cryptographic Function	Quantum Security Platform	Quantum-Secure Use Cases	Applications
Asymmetric Encryption	<b>MASQ™</b> 	<ul style="list-style-type: none"> <li>• Key Exchange Mechanism</li> <li>• Digital Signature &amp; Authentication</li> </ul>	<ul style="list-style-type: none"> <li>• Aerospace</li> <li>• Automotive</li> <li>• Consumer</li> <li>• Defense</li> <li>• Industrial</li> <li>• Infrastructure</li> <li>• Medical</li> <li>• Telecom</li> </ul>
Symmetric Encryption	<b>QEEP™</b> 	<ul style="list-style-type: none"> <li>• Data &amp; Network Encryption</li> <li>• Block &amp; Streaming Cipher</li> </ul>	
Strong Random Numbers	<b>SEQR™</b> 	<ul style="list-style-type: none"> <li>• Streaming Entropy</li> <li>• Quantum Random Number Generation</li> </ul>	

## QiSpace™ Product Families



Asymmetric Encryption used for Key Exchange, Digital Signature and Zero Knowledge Proof.



Symmetric Encryption based on quantum permutation pads that achieves Shannon perfect secrecy.



Quantum Entropy Services for the generation and quantum-secure distribution of random numbers and keys.

[www.quantropi.com](http://www.quantropi.com)



## Real-World Performance Highlights



- 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



- 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



- **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

### Platform Support

- Renesas RA6M5

## Demonstration Overview



- **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



- **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



- **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

Learn More



[www.quantropi.com](http://www.quantropi.com)

