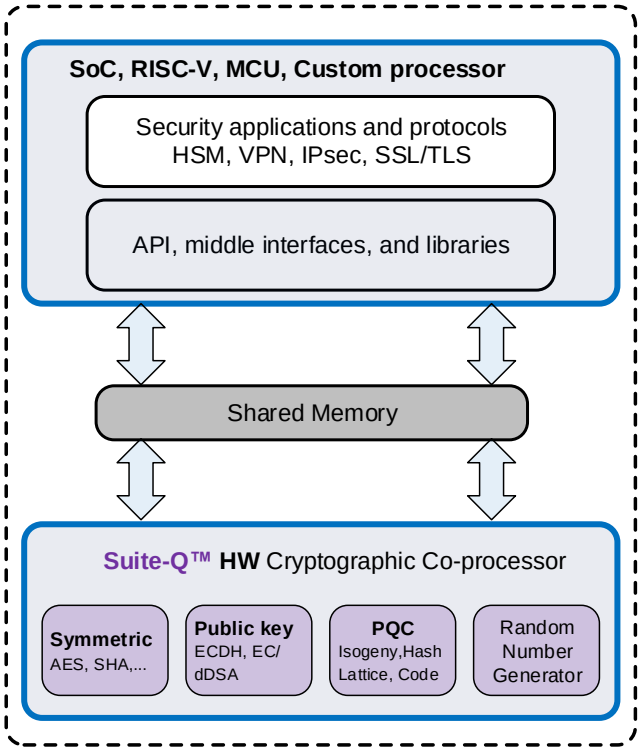
Overview:

PQSecure™ Technologies, LLC is a leading provider of quantum-safe cryptographic solutions including symmetric and asymmetric algorithms for embedded devices. PQSecure's hardware and software IP solutions offer various levels of recommended security, size, and performance configurability in numerous markets and applications.

PQSecure's pre- and post-quantum public key crypto-processors enable designers to offload all asymmetric cryptographic operations to hardware and provide support for efficient execution of Elliptic curve cryptography, lattice-based cryptography, code-based cryptography, and isogeny-based cryptography. Our solutions support various performance and security levels recommended by standardization organizations.



Products:

Suite-Q™ HW is a complete system-on-chip (SoC) design features all standardized cryptography needed for secure protocols in a small and efficient package. The SoC design of **Suite-Q™** targets two specific product lines: **high-end servers** and **low-end embedded systems**. The same hardware accelerators is used on both products. However, the main differences between the two products will be the choice of soft processor core, connectivity solutions, and operating clock frequency.

Suite-Q™ HW offloads the following symmetric and asymmetric cryptographic operations and makes the executions more efficient.

- **True Random Number Generator**: NIST 800-90-compliant TRNG
- **Classical Public key cryptography**: ECDSA (NIST FIPS 186-4), Ed25519 (NIST 800-186), Curve25519 (NIST 800-186), Curve448 (NIST 800-186), Ed448 (NIST 800-186), and ECDH (NIST sp800-56).
- **Post-Quantum Public Key Exchange**: Isogeny-based Cryptography, Lattice-based Cryptography, and Code-based cryptography. (Awaiting NIST standardization)
- **Post-Quantum Digital Signatures**: Lattice-based cryptography, hash-based signatures, stateful hash-based signature (XMSS and LMS NIST FIPS 186)
- **Secure Hashing Algorithm (SHA)**: SHA-2 (FIPS 180-4) SHA-3 (FIPS 202), HMAC (FIPS 198-1)
- **Advanced Encryption Standard (AES)**: AES-128, AES-256, CCM, GCM, CMAC, CTR, CBC, ECB, XTS.

Features:

- Ease of integration into various SoC and FPGA architectures and development flow
- Offering several performance grades versus silicon footprint trade-offs
- Complete CPU offload of computationally intensive cryptographic operations

- Optional DPA countermeasures with protections validated with standardized techniques
- Availability of testbench, known answer test vectors (KATs) for verification, integration data, and simulation and synthesis scripts.
- Substantial power reductions in comparison to software implementations

Suite-Q™ SW is a cryptographic software library that can configure to optimize code size, stack usage, and performance. **Suite-Q™ SW** is available in portable C code as well as high-speed hand-optimized assembly on various 8-, 16-, 32-, and 64-bit embedded processor and MCUs. We want to make sure that we give our customers plenty of space for their own applications as well as making sure that our program fits on memory-limited devices.

Features:

- Fully portable and dedicated libraries for various development environments
- Simple plug-in modules and support for hardware offload
- Available in various configurations for speed vs. memory size options to meet custom specs
- Support for general-purpose and embedded CPUs
- Availability of validations tests and performance measurements

Support:

PQSecure team has wide experience in aspects of secure protocol design, research and development, cryptographic engineering, training, as well as post-quantum cryptography. Our expertise and skill set will help customers to meet and exceed their goals a timely and cost-effective manner. The cryptographic engineering and security is a cutting edge area and gets updates as technology progresses. Our highly qualified team with extensive mathematics and engineering background with cross affiliations with academia are highly up-to-date to address the customers' to date needs.

Contact Information:
PQSecure Technologies, LLC.
903 NW 35th St
Boca Raton, FL 33431 USA
Phone: (201) 844-5743