mercury

PQ Ultra

Defend Against Quantum Computing Threats

Protects ASIC and FPGA applications against quantum computing threats

- Unified hardware accelerator of ML-DSA and ML-KEM post-quantum cryptography algorithms
- No embedded processors required
- Cryptography protection for current and future system threats
- Verified side channel attack resistant countermeasures

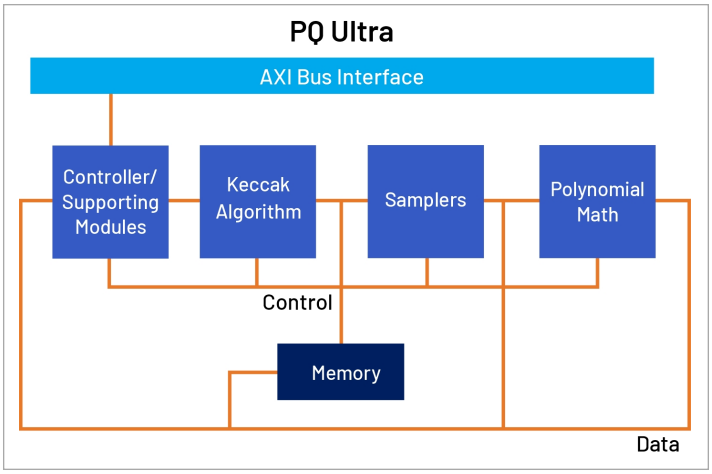
Quantum computing is an evolving threat and may be used to break cryptographic algorithms currently in use, gaining access to vital protected data. In this "harvest now, decrypt later" environment, PQ Ultra is a turnkey solution to secure sensitive information from quantum computing threats. It is an ASIC and FPGA-suitable IP core that provides key encapsulation and digital signature support for CNSA 2.0 applications.

With an AXI memory-mapped interface and software drivers, PQ Ultra gives host applications a simple way to access high-performance hardware implementations of post-quantum algorithms. It supports all parameter sets for both FIPS 203 key encapsulation (ML-KEM) and FIPS 204 digital signatures (ML-DSA).

Configurable for a variety of use cases based on area, performance, and side-channel attack resistance requirements; PQ Ultra can be delivered as an integrated component of Mercury's runtime cryptography engine, SecRun, or as a standalone IP block.

HIGHLIGHTS

- Side-channel attack countermeasures.
- Platform-agnostic support for all major FPGA vendors and ASIC nodes.
- Supports key encapsulation according to FIPS 203 and digital signatures according to FIPS 204.
- Supports all NIST-defined parameter sets.
- Integration with KeyGuard, Mercury's hardware-based key manager.
- Software drivers and examples allow for easy integration.
- Configurable and scalable solution that is easy to integrate.



Hardware Modules Within PQ Ultra

USE CASES

PQ Ultra provides key encapsulation and digital signature capabilities to a host application, enabling a range of use cases including but not limited to:

- data integrity.
- secure boot.
- device authentication.
- verified firmware updates.

PQ Ultra can replace the use of ECC and RSA, or it can be used alongside Mercury's classic public key cryptography core, the EC Ultra, in a hybrid scheme.

KEY FEATURES

Configurable

PQ Ultra can be generated with multiple underlying Number Theoretic Transformations (NTT) data paths and memory configurations. This enables PQ Ultra configurations that leverage the same underlying verification infrastructure and SKC C API while supporting deployment in embedded systems where power and area is critical, as well as high-throughput cloud environments.

Standard Parameter Sets

Supporting all standardized parameter sets, PQ Ultra is suitable for applications at a variety of security and performance levels. These parameter sets include:

- FIPS 203: ML-KEM-512, ML-KEM-768, ML-KEM-1024.
- FIPS 204: ML-DSA-44, ML-DSA-65, ML-DSA-87.

Easy Integration

PQ Ultra is delivered with the SKC C driver library, making it easily accessible by a host application through a set of simple APIs.

Non-Blocking Operation

PQ Ultra's SKC APIs enable non-blocking operation of the core. The application may choose when to poll or use interrupts to effectively offload the execution of post-quantum algorithms and perform other tasks.

Supported Vendors and Technologies

FPGA designs: Microchip, AMD, Intel.
ASICs: Across all node sizes.

Corporate Headquarters
50 Minuteman Road
Andover, MA 01810 USA
+1 978.967.1401 tel
+1 866.627.6951 tel
+1 978.256.3599 fax

International Headquarters
Mercury International
Avenue Eugène-Lance, 38
PO Box 584
CH-1212 Grand-Lancy 1
Geneva, Switzerland
+41 22 884 5100 tel

Learn more
Visit: mrcy.com/
Contact: mrcy.com/contact-us

The Mercury Systems logo is a registered trademark of Mercury Systems, Inc. Other marks used herein may be trademarks or registered trademarks of their respective holders. Mercury products identified in this document conform with the specifications and standards described herein. Conformance to any such standards is based solely on Mercury's internal processes and methods. The information contained in this document is subject to change at any time without notice.

MADE IN USA

© 2026 Mercury Systems, Inc. 1-0-022626-DS-PQ-Ultra-Defend Against-Quantum-Computing-Threats