Product Brief

PQ MicroLib Core

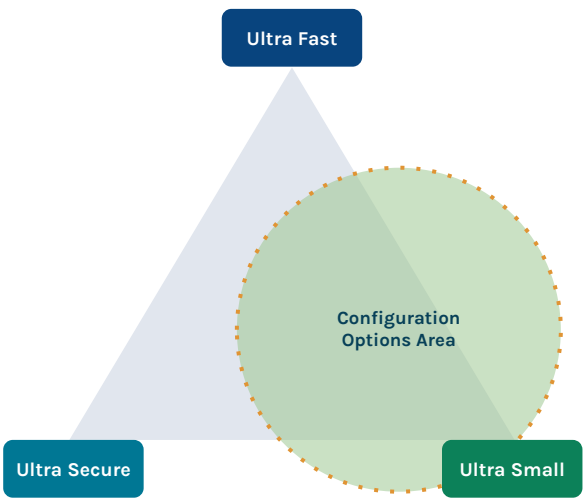
Bare-metal post-quantum security with minimal RAM footprint and optional DPA protection

Overview

PQMicroLib-Core is PQShield's ultra-small PQC library engineered for bare metal, with support for real-time operating systems. It is CAVP-ready tailored for highly constrained embedded devices. The library offers selectable implementations enabling control of RAM consumption, code size, and performance while keeping full portability across toolchains and architectures.

An optional PSA Crypto API interface on top of PQMicroLib-Core provides standards-based integration with ecosystems and SDKs, while the core library itself remains lightweight and free of mandatory abstraction layers. Optional side-channel-resistant variants provide countermeasures against physical attacks such as Differential Power Analysis (DPA) where required, and all configurations follow constant-time design principles to mitigate timing side-channel risks.

Design Space



Key Benefits

- Ultra-small, optimized RAM footprint (< 5 KB profiles available)
- Bare-metal and RTOS ready – no OS dependency, minimal runtime requirements
- Selectable size/performance/assurance configurations
- Optional side-channel-resistant variants (DPA) – software countermeasures for higher-assurance devices
- Constant-time cryptographic implementations to mitigate timing side-channel leakage
- Optional PSA Crypto API interface to enable MbedTLS and chip-vendor SDK integration
- Hardware-acceleration ready – extension APIs to leverage existing crypto accelerators when present
- Extensive functional and security validation – fuzzing, side-channel, and regression testing
- CAVP-Ready architecture
- CNSA 2.0 and NIST PQC algorithm support
- Portable across architectures – ARM, RISC-V, x86, and standard C toolchains
- Integration support and documentation

Common Use Cases

- Secure boot and flrmware/OS verification
- Secure firmware updates (OTA)
- Device authentication and identity
- Remote Attestation
- Embedded TLS and secure comms
- Post-quantum key establishment (M2M/device-to-cloud)
- Data at rest encryption, integrity and authenticity
- Secure device provisioning and key injection
- Secure product configuration and lifecycle management
- Post-quantum migration for existing embedded devices (brownfield upgrade)

Contact our experts

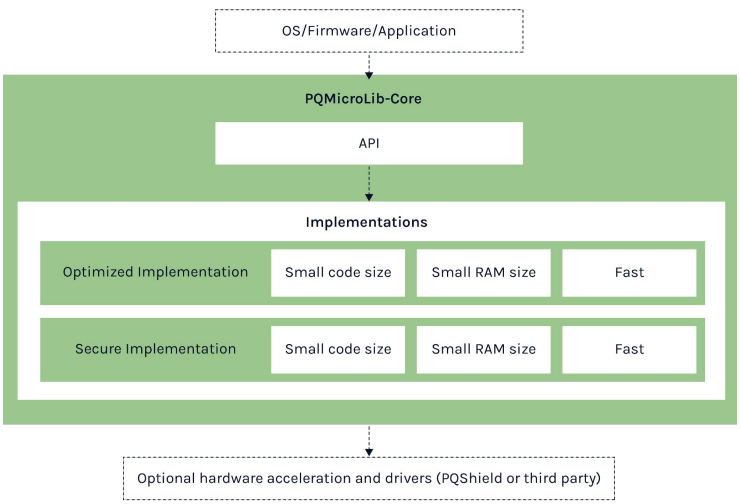
Product Brief

PQ MicroLib Core

Technical Specification

PQMicroLib-Core provides software implementations of post-quantum cryptographic algorithms. Designed for portability across constrained embedded targets, the library supports multiple bare-metal environments and architectures such as ARM32, ARM64, RISC-V, x86, and x86-64. It operates without an OS and with minimal runtime requirements, making it well suited for early boot stages, microcontrollers, and IoT devices with strict memory, CPU, and power constraints.

The library exposes a clean and minimal C API tailored for embedded development, with optional extensions including a PSA Crypto API interface and optional hardware-acceleration hooks. Config-based builds enable tight control over RAM footprint and code size while maintaining portability across toolchains. PQMicroLib-Core integrates into existing firmware and build environments, helping streamline development and support certification and compliance preparation for quantum-secure embedded products.



PQSHIELD

PQShield is a global leader in Post-Quantum Cryptography, with a team of around 90 experts across 11 countries who co-authored the first NIST PQC standards and continue to be major contributors to the industry at large. As a leading authority on real-world PQC implementation who has filed more than 40 patents, PQShield provides high-quality software and hardware IP to the global secure products supply chain.

Main Features

Cryptographic Algorithms

- ML-DSA (NIST FIPS 204)
- ML-KEM (NIST FIPS 203)
- SLH-DSA (NIST FIPS 205)
- XMSS and LMS
- SHA-2 / SHA-3 hash functions
- DRBG

APIs

- Simple C API – minimal footprint integration
- Streaming API – large message and low-RAM processing
- Side-Channel-Aware API (optional) – enables DPA-resistant variants
- PSA Crypto API Interface (optional) – standards-based integration with MbedTLS and chip-vendor SDKs
- Hardware Acceleration Extension API (optional) – hooks for SHA-2 / SHA-3 and existing crypto accelerators

Deliverables

- User manual and integration guide
- API reference
- Sample Code and Reference Projects
- Delivery Packages
- Pre-built binaries
- Source code (when applicable)
- Performance Benchmarks
- Functional Test Reports
- Includes CAVP execution logs
- Security Evaluation Reports
- Constant-time analysis
- Fuzzing analysis and SCA evaluation

See also

- PQCryptoLib-Core pure software PQC solution
- PQCryptoLib-SDK OpenSSL provider
- PQPlatform CoPro Flexible PQC HW IP for existing subsystems
- Discover the UltraPQ-Suite in full
- Visit PQShield's website
- Listen to our Podcast

Contact our experts