v R24.2.2

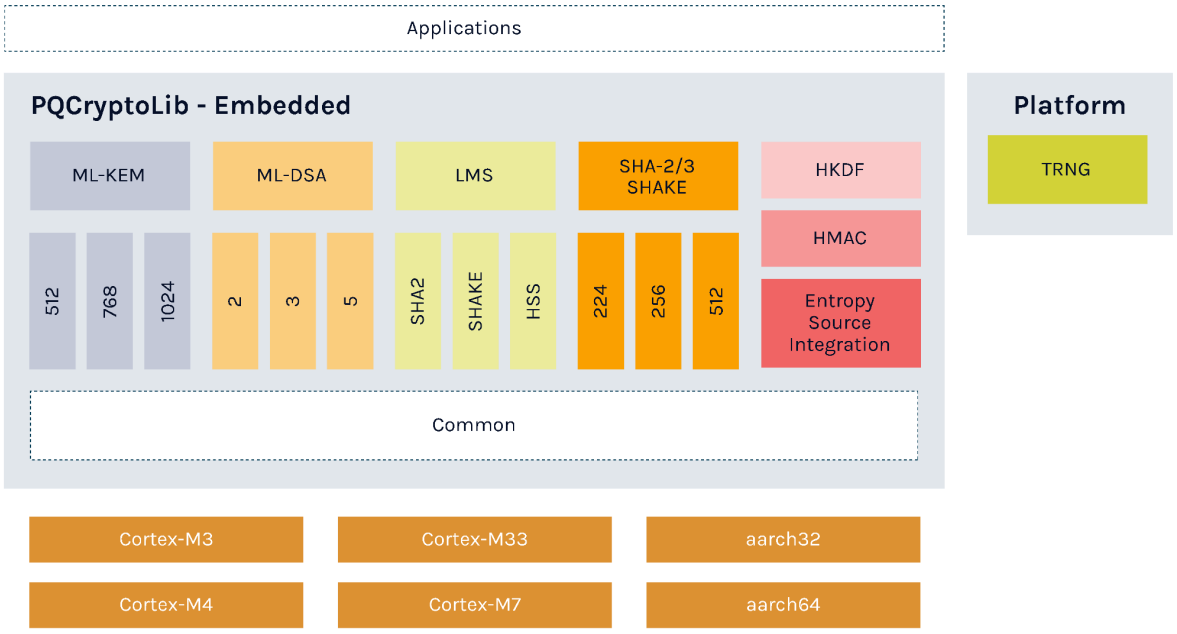
Crypto-Lib Embedded

13 May 2024

Post-quantum cryptography library for memory-constrained platforms (PQS-SW-CLE)

PQCryptoLib-Embedded is a version of PQCryptoLib, PQShield's library of PQC (post-quantum cryptography) algorithms, which is designed for microcontrollers or memory-constrained platforms.

The library is highly configurable at build time, ensuring that it can be deployed with the algorithms required to minimize binary size and memory footprint as much as possible.



Key Features: PQCryptoLib-Embedded

PQCryptoLib-Embedded enables secure quantum-resistance on embedded platforms; for example, resource-constrained microcontrollers, IoT for edge, and communication protocols.

- Optimized memory and binary size (ML-DSA)
- Bare metal implementation
- NIST FIPS 202, 203, 204 compliant
- Resistant to time-based SCA
- C interface

PQC algorithms supported

Cryptographic service	Algorithm	Supported Standards
Post-quantum key establishment	ML-KEM 512/768/1024	FIPS-203
Post-quantum asymmetric signing	ML-DSA 44/65/87	FIPS-204
Post-quantum asymmetric signing	LMS (verification)	RFC8554/SP800-208

Classical algorithms supported

Cryptographic service	Algorithm	Supported Standards
Hash	SHA-2	FIPS 180-4
Hash	SHA-3	FIPS 202
Key derivation	HKDF	RFC 5869 / SP800-56C r2
Keyed hashing	HMAC	RFC 2014 / FIPS 198-1
Variable size digest generation	SHAKE	FIPS 202

Supported CPU architectures

- x86_64
- ARM64
- ARM Cortex-M3/M4

PQShield Software IP

The following table shows how PQCryptoLib-Embedded compares to PQShield's security suite.

Software IP		Description
PQS-SW-CLE	**PQCryptoLib-Embedded**	**Modified cryptography library designed to add PQC capability to microcontrollers, embedded software, or memory-constrained systems.**
PQS-SW-CLB	PQCryptoLib	PQShield's generic software library containing post-quantum and classical algorithms.
PQS-SW-SDK	PQSDK	PQShield's software development kit, with interface to TLS (OpenSSL and MbedTLS).