Document version	v1.0	Release R24.2	26 Mar 2024

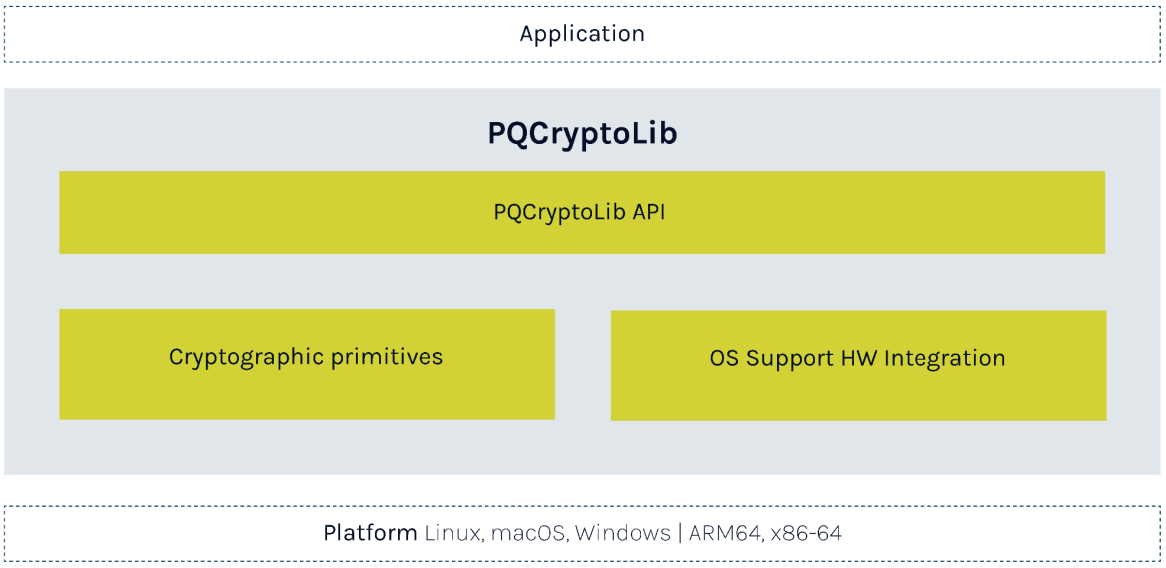
PQCryptoLib

Post-Quantum Software Library (PQS-SW-CLB)

PQCryptoLib (PQS-SW-CLB) is a generic software library with a C/C++ interface of FIPS 140-3-ready, post-quantum (PQC) and classical cryptographic algorithms. It can be used to design your own SDK, or be implemented as part of PQShield's software development kit, PQSDK.

PQCryptoLib is designed to provide post-quantum security using multiple algorithms, including those supported by NIST. The goal of PQCryptoLib is to help organizations transition to quantum-resistant cryptographic schemes, by providing support for classical and post-quantum key derivation, as well as providing an implementation of hybrid-key derivation within the TLS key schedule.

Key Features: PQCryptoLib



A complete set of documentation and examples are provided with PQCryptoLib.

Note: Implementations of cryptographic primitives within PQCryptoLib (with the exception of Falcon's signing operation) are resistant to time-based side-channel attacks.

PQC Algorithms

Cryptographic Service	Algorithm	Supported Standards	Supported in FIPS build
PQ asymmetric signing	ML-DSA 2/3/5	FIPS-204-ipd	NO
PQ asymmetric signing	Falcon 512/1024	NIST R3	NO
PQ key agreement	ML-KEM 512/768/1024	FIPS-203-ipd	YES
PQ Key agreement	FrodoKEM 640/976/1344	NIST R3	NO
PQ asymmetric signing (hash-based)	LMS/HSS (all parameters)	SP800-208	NO

Classical cryptography

The following algorithms are CAVP tested for FIPS, certification of which can be seen in the NIST Cryptographic Algorithm Validation Program, certificate A3011.

Cryptographic Service	**Algorithm**	**Supported Standards**	**Supported in FIPS build**
Asymmetric Signing	ECDSA	FIPS 186-4	YES
Deterministic Random Bit Generation	DRBG (Hash)	SP800-90A	YES
Deterministic Random Bit Generation	DRBG (HMAC)	SP800-90A	NO
Hash	SHA-2	FIPS 180-4	YES
Hash	SHA-3/SHAKE	FIPS 202	YES

Hybrid/composite cryptography

In FIPS mode, PQCryptoLib supports hybrid key derivation using:

- ECDH/p256 + ML-KEM (512/768/1024)

In non-FIPS mode, PQCryptolib also supports:

- ECDH/p256 + FrodoKEM (640/976/1344)

PQCryptoLib provides a high-level API for the TLS 1.3 KDF.

Entropy

- On Intel platforms, PQCryptoLib uses the RDSEED instruction.
- On Linux platforms the getrandom syscall is used as an additional entropy source.
- Random number generation is thread-safe, with one DRBG context per thread.

Performance Expectations

Example config: Intel(R) Xeon(R) Platinum 8276 CPU @ 2.2GHz

Signing

Algorithm	Key gen (cycles)	Signing (cycles)	Verify (cycles)
Falcon 512	2,381,580	1,189,250	198,934
Falcon 1024	71,566,800	2,359,550	374,823
ML-DSA-44	244,982	1,299,090	281,908
ML-DSA-65	439,422	2,098,570	445,524
ML-DSA-87	614,006	2,448,970	657,273
LMS (SHA2, M=32, H5, W2)	22,773	436,955	343,509
LMS (SHA2, M=32, H5, W8)	326,506,000	5,024,940	4,959,460
LMS (SHA2, M=24, H5, W2)	16,765,300	336,929	256,245
LMS (SHAKE, M=32, H5, W2)	27,817,100	542,959	394,838
ECDSA - p256	824,471	1,045,140	1,050,990

KEM

Algorithm	Key gen (cycles)	Encaps (cycles)	Decaps (cycles)
ML-KEM-512	77,584	64,120	63,519

ML-KEM-768	117,358	89,586	88,499
ML-KEM-1024	167,601	125,034	124,384
Frodo640	5,018,010	5,462,310	5,354,520
Frodo976	10,901,400	11,902,500	11,727,800
Frodo1344	19,264,000	21,075,000	20,927,600
ML-KEM-512	77,584	64,120	63,519
ML-KEM-768	117,358	89,586	88,499
ML-KEM-1024	167,601	125,034	124,384
Frodo640	5,018,010	5,462,310	5,354,520
Frodo976	10,901,400	11,902,500	11,727,800
Frodo1344	19,264,000	21,075,000	20,927,600

DH Key Exchange

Algorithm	Key gen (cycles)	Exchange (cycles)
ECDH-p256	824,804	375,800

Hash

Algorithm	64 B (cycles)	8198 B (cycles)	1 MB (cycles)
SHA2-224	2,290	132,161	16,749,800
SHA2-256	2,291	132,147	16,748,800
SHA2-384	1,425	78,277	9,837,120
SHA2-512	1,442	78,305	9,835,810
SHA3-224	1,597	79,973	10,192,800
SHA3-256	1,602	85,508	10,779,500
SHA3-384	1,588	110,113	14,028,200
SHA3-512	1,595	158,213	20,182,600

SHAKE-128	1,617	69,000	8,762,450
SHAKE-256	1,608	85,483	10,775,700

DRBG

Hash	32 B (cycles)	64 B (cycles)	128 B (cycles)
Hash-256	4,112	5,285	7,582
HMAC-256	14,461	19,278	28,808

FIPS 140-3 validation

PQCryptoLib is currently undergoing FIPS 140-3 level 1 certification as part of NIST's Cryptographic Module Validation Program (CMVP).

The goal of FIPS validation for PQCryptoLib is to provide support for hybrid key derivation that can be used in TLS v.1.3 key exchange.

The hybrid key derivation process follows NIST Special Publication 800-56Cr2, and is a FIPS-approved technique of deriving symmetric keys from two separate shared secrets, where at least one was generated during the execution of a FIPS-approved key-establishment scheme.

The FIPS build of PQCryptoLib provides all necessary classical and post-quantum primitives that can be used to perform hybrid key derivation, using ECDH (NIST P-256) and ML-KEM (FIPS-203).

PQCryptoLib can be provided in both FIPS and non-FIPS modes. Both variants are built from the same source code, though some algorithms are only supported in non-FIPS mode.

Platform support

Supported Operating Systems

- Linux
- Windows (7+)
- MacOS
- Bare metal (no OS)

Supported CPU architectures

- x86_64 (including hardware acceleration through AVX2 and BMI)
- ARM64

PQShield Software IP

The following table shows how PQCryptoLib compares to PQShield's software IP.

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