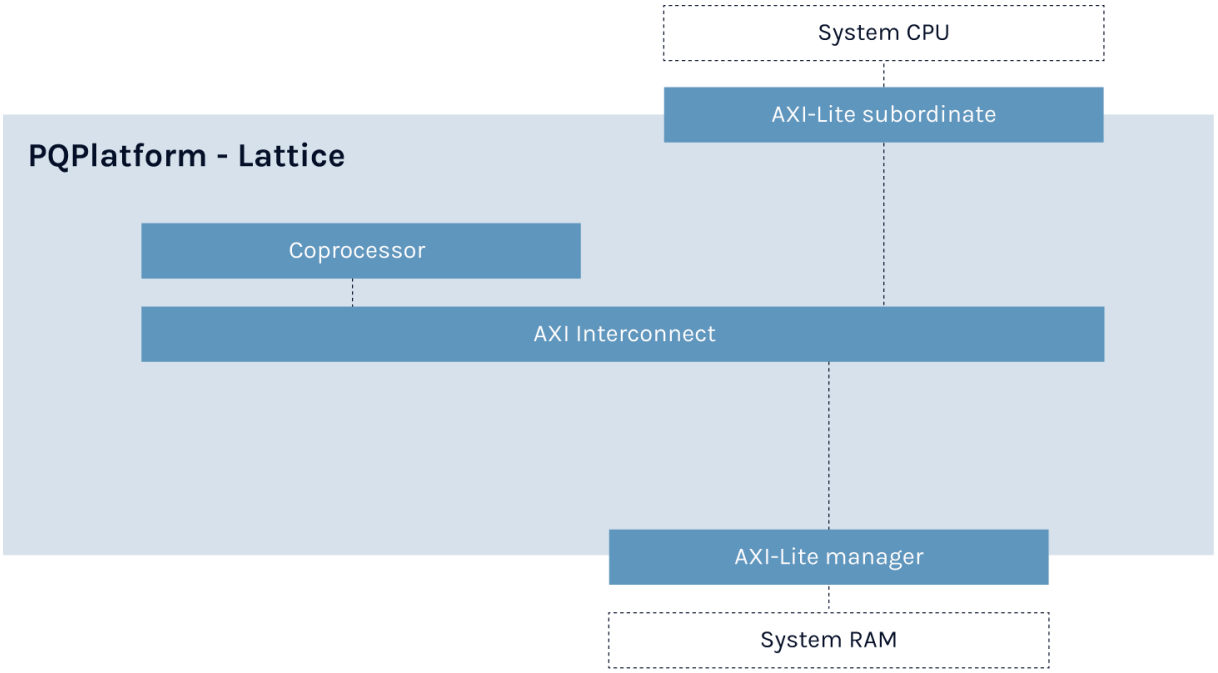
Product Brief R24.3.1 Jul 12, 2024

PQPlatform-Lattice

Post-Quantum Cryptography Processing Engine

PQPlatform-Lattice adds support for lattice-based cryptographic operations for key generation and signature verification, ML-KEM and ML-DSA. Powered by PQShield's firmware, it can be deployed inside an existing security subsystem, and is designed for maximum compatibility, offering low area alongside world-class side-channel-analysis technology, ideal for the protection of hardware keys against harvest-now-decypt later attacks.



Key Features and Parameters: PQPlatform-Lattice

- PQC (post-quantum cryptography) engine
- NIST SP 800-56A complaint
- NIST FIPS 186-4 and 186-5 compliant
- ANSSI X9.142-2020 compliant
- Supports:
    - NIST FIPS-204 ML-DSA 44/65/87
    - NIST FIPS-203 ML-KEM 512/768/1024
    - NIST FIPS 140-3 level 4 ready
    - Optional non-invasive side-channel (power, EM) attack countermeasures for PQC algorithms.

- Hardware support for:
    - Elliptic Curve P-384
    - ECDH, DSA, and ECDSA

- Interfaces:
    - 64-bit AXI4-Lite manager interface for connection with working memory
    - 64-bit AXI4-Lite subordinate interface for controlling the coprocessor via the host CPU.

Size Requirements

Config Information	IP Area
Typical configuration (GF12LP)	75KGte

Performance Expectations

Algorithm	Security Level	Max Performance (cycles)
ML-KEM Key generation	ML-KEM-512	500K
ML-KEM Encapsulation	ML-KEM 512	700K
ML-KEM Decapsulation	ML-KEM 512	1M
ML-DSA Key generation	ML-DSA 44	1.2M
ML-DSA Signing	ML-DSA 44	5.25M
ML-DSA Verification	ML-DSA 44	270K

Coprocessor

The lattice-based coprocessor is used to perform post-quantum operations. Optional SCA countermeasures, implemented in firmware, can provide protection against non-invasive power and EM side-channel attacks.

Interfaces

PQPlatform-Lattice has two main interfaces:

- A 64-bit AXI4-Lite subordinate, through which the system CPU (and PQShield-supplied firmware) controls PQCoPro
- A 64-bit AXI4-Lite manager, through which PQPlatform-Lattice accesses the working memory while running.

SCA countermeasures

SCA countermeasures are defences that prevent non-invasive detection of cryptographic secrets by either timing or power side channels (side-channel attack).

SCA countermeasures are optional, depending on whether you need to optimize your system for high security or high performance.

PQShield Hardware IP

The following table shows how PQPlatform-Lattice compares to PQShield's security suite.

Hardware IP		Description
PQP-HW-LAT	**PQPlatform-Lattice**	**Lattice-based post-quantum Processing Engine**
PQP-HW-HBS	PQPlatform-Hash	Hash-based post-quantum hardware accelerator
PQP-HW-COP	PQPlatform-CoPro	Post-Quantum Cryptography Processor, combining Lattice and Hash
PQP-HW-SUB	PQPlatform-SubSys	Self-contained cryptographic subsystem designed for PQC + classical, minimal integration effort, with SCA protection
PQF-HW-LAT	PQPerform-Lattice	High capacity post-quantum cryptography, designed for high throughput and high speed