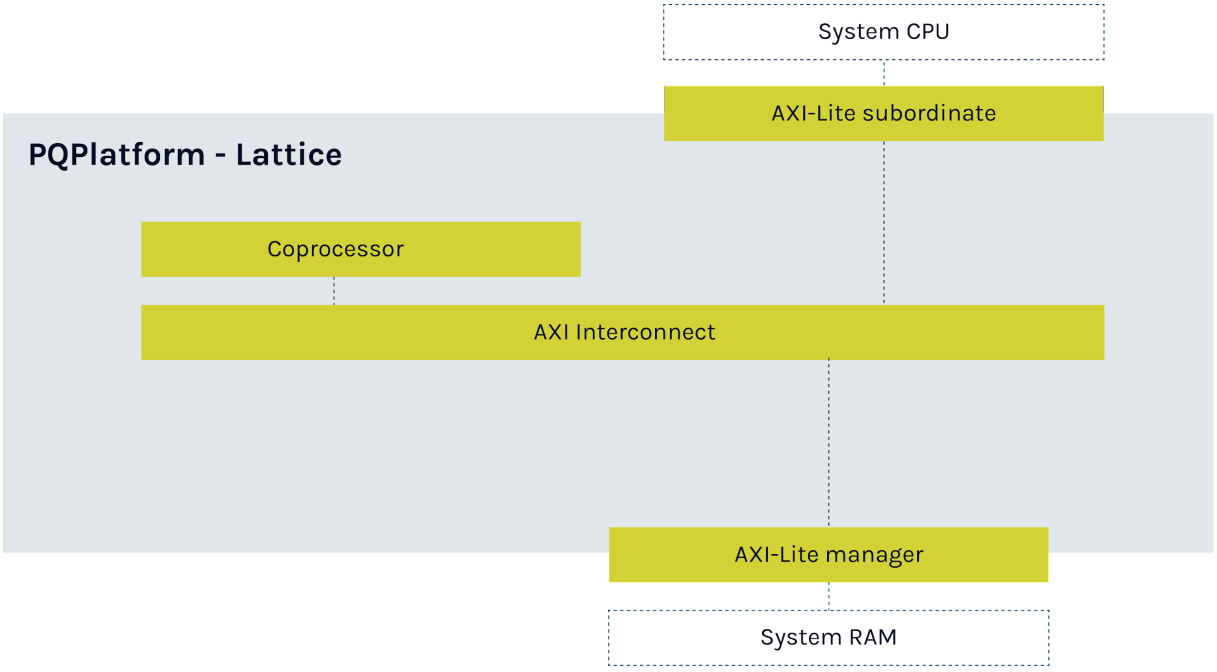
Document version	v1.0	Release R24.2	26 Mar 2024

PQPlatform-Lattice

Post-Quantum Cryptography Processing Engine (PQP-HW-LAT)

PQPlatform-Lattice (PQP-HW-LAT) is a lattice engine that implements the ML-KEM and ML-DSA post-quantum algorithms. It is powered by PQShield-supplied firmware, which implements cryptographic operations.

PQP-HW-LAT can be deployed inside an existing security sub-system, with optional firmware-backed side-channel analysis resistance (SCA). It is designed to fit a sub-system that already contains a compatible Keccak accelerator.



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

IP Overview

This section gives an overview of the interfaces and integration requirements for PQPlatform-Lattice.

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
PQPlatform-Lattice /PQP-HW-LAT	**Lattice-based mathematical hardware accelerator.**
PQPlatform-Hash / PQP-HW-HBS	Keccak hardware accelerator.
PQPlatform-CoPro / PQP-HW-COP	PQ processor that adds post-quantum cryptography to your sub-system. PQP-Platform-CoPro includes a Keccak accelerator.
PQPlatform-SubSys / PQP-HW-SUB	Adds PQC to your subsystem. Requires integration with host CPU running PQShield firmware.
PQPerform-Lattice / PQF-HW-LAT	Autonomous cryptographic subsystem performing PQC and classical cryptography.