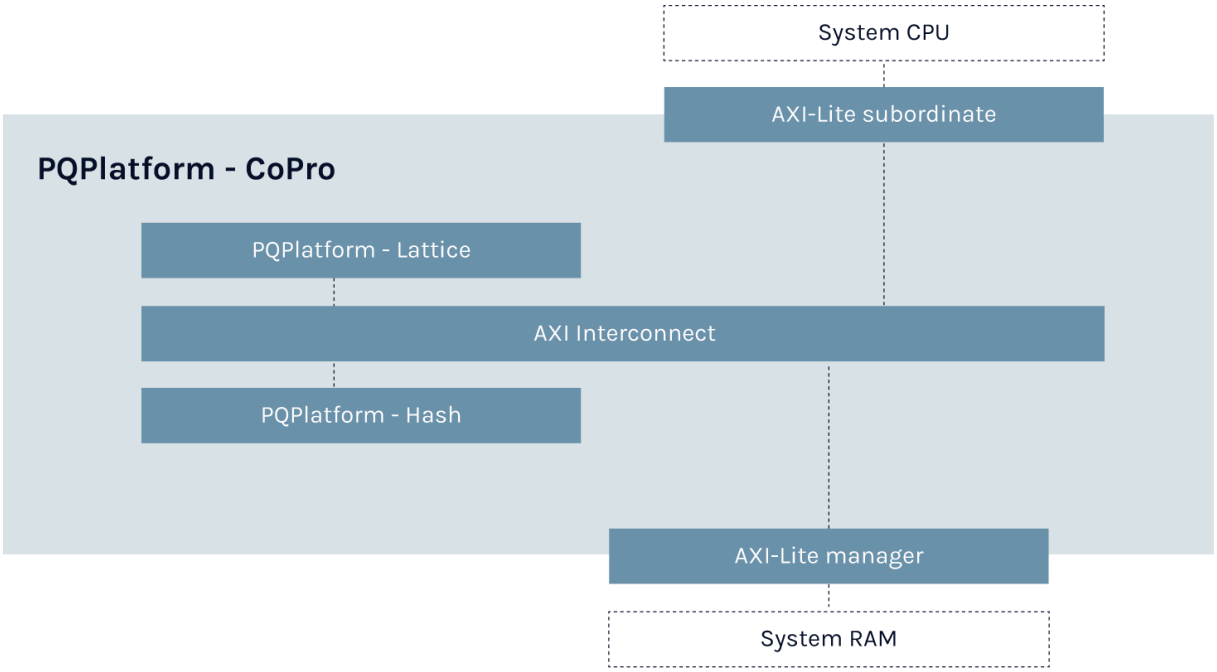
Product Brief

R24.3.1 Jul 12, 2024

PQPlatform-CoPro

State-of-the-art post-quantum cryptography processor

Combining PQShield's lattice-based and hash-based cryptography engines, PQPlatform - CoPro is designed for optimal performance with minimal integration effort, and with crypto-agility in mind. With optional side-channel countermeasures, and support for ML-KEM, ML-DSA, LMS and XMSS, PQPlatform-CoPro offers a high level of performance and compatability, leveraging an existing CPU and deploying PQShield's firmware to provide a complete solution.



Key Features and Parameters: PQPlatform-CoPro

- PQC coprocessor with hardware Keccak accelerator
- NIST SP 800-56A Compliant
- NIST FIPS-202 Compliant
- NIST FIPS 186-4 and 186-5 Compliant
- ANSSI X9.142-2020
- Supports:
    - NIST FIPS-203 ML-KEM 512/768/1024
    - NIST FIPS-204 ML-DSA 44/65/87
    - NIST FIPS-202 SHA3-224/256/384/512
    - NIST FIPS-202 SHAKE 128/256
    - NIST SP 800-56A
    - ECDH and ECDSA
    - Elliptic Curve P-384
    - Optional non-invasive side-channel (power, EM) attack countermeasures for PQC algorithms

- Memory: requires up to 96Kb working memory
- 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
ML-KEM, ML-DSA	~125KGte
ML-KEM, ML-DSA, ECC, DSA	~150Kgte

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

PQPlatform-Lattice

The PQShield lattice-based engine 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.

This component, known as PQPlatform-Lattice, is also available as a separate implementation for situations where an existing Keccak accelerator is present.

PQPlatform-Hash

PQPlatform-Hash is PQShield's dedicated Keccak accelerator. It's designed to handle symmetric primitives SHA-3 and SHAKE, and requires PQShield-supplied firmware to run on the host CPU.

Interfaces

PQPlatform-CoPro has two main interfaces:

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

PQShield Hardware IP

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

Hardware IP		Description
PQP-HW-COP	**PQPlatform-CoPro**	**Adds PQC to your subsystem. Requires integration with host CPU running PQShield firmware.**
PQP-HW-HBS	PQPlatform-Hash	Keccak hardware accelerator.
PQP-HW-LAT	PQPlatform-Lattice	Lattice-based mathematical hardware accelerator.
PQP-HW-SUB	PQPlatform-SubSys	Self-contained cryptographic subsystem performing PQC and classical cryptography.
PQF-HW-LAT	PQPerform-Lattice	High-speed, high-throughput, lattice PQC cryptographic subsystem