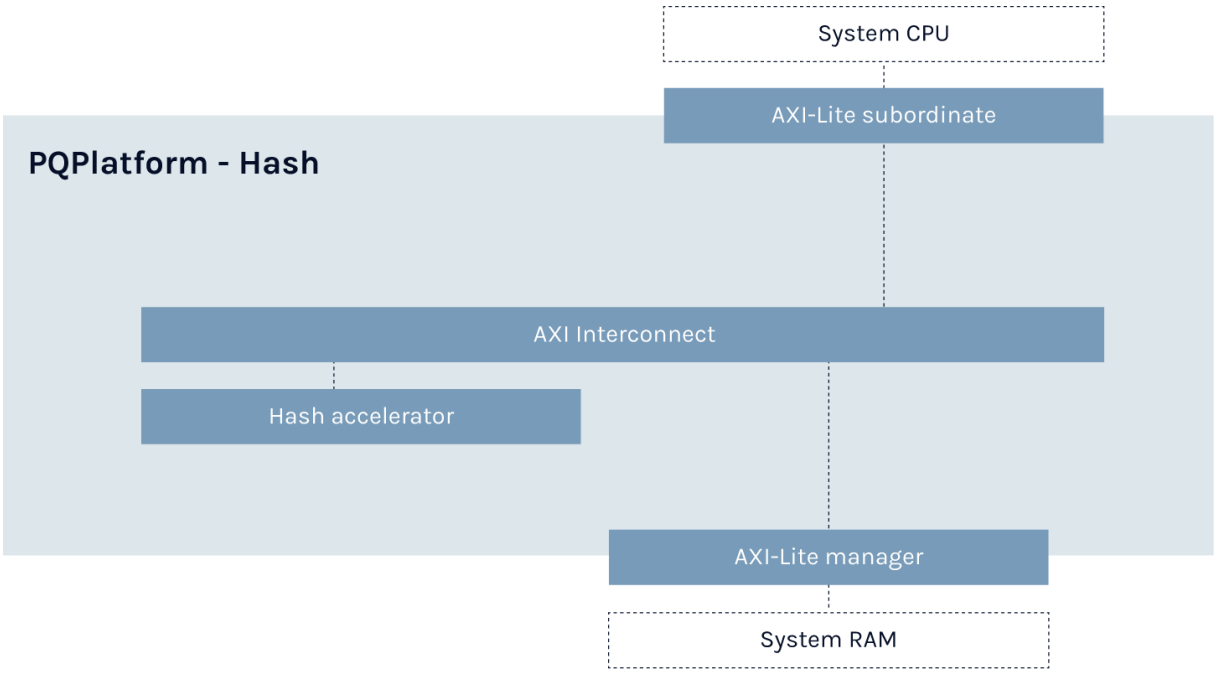
Product Brief R24.3.1 Jul 12, 2024

PQPlatform-Hash

Post-Quantum Hardware Accelerator

PQPlatform-Hash is a side-channel-secure hardware accelerator supporting a wide range of Hash-Based Signature Schemes (HBSS). Deploying LMS and XMSS, quantum-safe algorithms that can be deployed in a non-hybrid configuration, it's optimized for resource constrained devices, maximizing high performance and high security. PQPlatform-Hash includes PQShield's world-class firmware which runs the accelerator from a host CPU.



Key Features: PQPlatform-Hash

- Power side-channel secure (SCA) Keccak engine
- AXI4-Lite (64-bit 1x subordinate)
- Algorithms:
  - LMS, XMSS
  - SHA2/SHA-3/SHAKE 128/256
- NIST FIPS 140-3 level 4 ready
- NIST FIPS 180-4 compliant
- NIST SP800-208 compliant
- NIST FIPS 202 compliant

Size and Performance

Config Information	IP Area	IP Performance
Base Config (standard implementation)	38KGte	24 cycle Keccak permutation computation
Hardware SCA Protected	145KGte	24 cycle Keccak permutation computation

Keccak accelerator

The central Keccak accelerator implements the Keccak permutation in hardware. In addition, the SHA-3 and SHAKE algorithms are implemented using PQShield-supplied firmware.

Bus Interface

PQPlatform-Hash uses an AXI4-Lite bus, enabling simultaneous read and write access to the state.

SCA hardware countermeasures

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

PQShield Hardware IP

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

Hardware IP		Description
PQP-HW-HBS	**PQPlatform-Hash**	**Hash-based post-quantum hardware accelerator**
PQP-HW-LAT	PQPlatform-Lattice	Lattice-based post-quantum Processing Engine
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