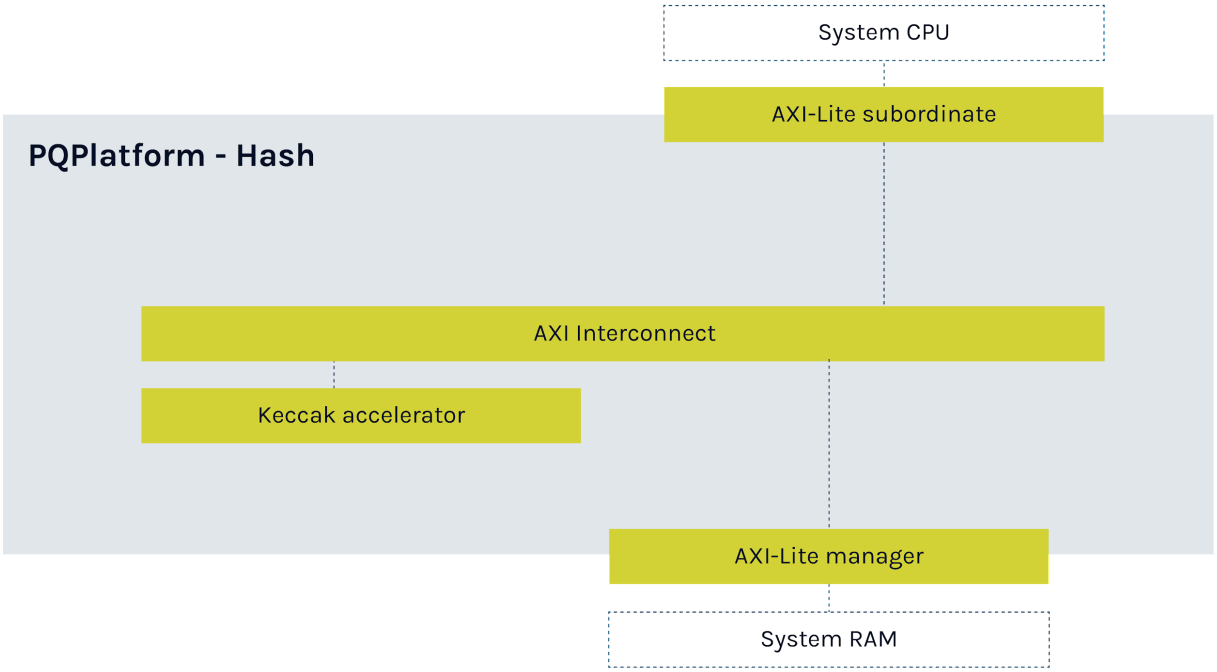
Document version	v2.0	Release R24.1	5 Feb 2024

PQPlatform-Hash

Post-Quantum Hardware Accelerator (PQP-HW-HBS)

PQPlatform-Hash (PQP-HW-HBS) is a power side-channel-secure Keccak hardware accelerator for the SHA-3 and SHAKE algorithms. It includes the PQShield-supplied firmware required to run the accelerator from a host CPU.



Key Features: PQPlatform-Hash

- Power side-channel secure (SCA) Keccak engine
- AXI4-Lite (64-bit 1x subordinate)
- Algorithms:
  - Keccak
  - Hardware support for SHA-3/SHAKE 128/256
- NIST FIPS 140-3 level 4 ready
- 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

IP Overview

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

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