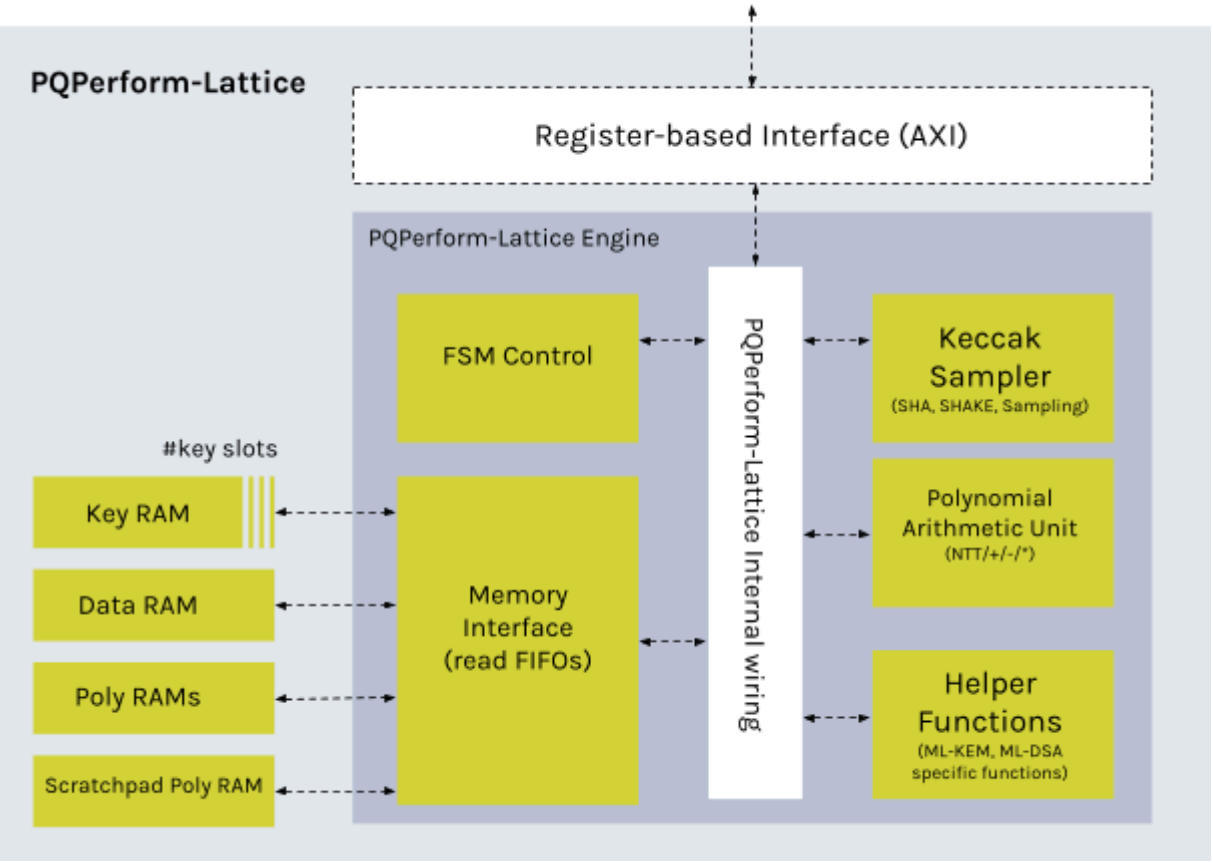
Document version	v2.0	Release R24.1	5 Feb 2024

PQPerform-Lattice

High Capacity Post-Quantum Cryptography Processor (PQF-HW-LAT)

PQPerform-Lattice (PQF-HW-LAT) is an autonomous, hardware-based product that is designed for high throughput and high speed. PQF-HW-LAT adds post-quantum defences for applications that handle a large number of transactions, such as high-capacity network hardware applications, or HSMs (hardware security modules) requiring fast performance.



Key Features and Parameters: PQPerform-Lattice

- ML-KEM (Kyber) Specific Functions (FIPS-203)
  - ML-KEM 512/768/1024
  - Key generation
  - Key import/export
  - Encapsulation
  - Decapsulation
- ML-DSA (Dilithium) Specific Functions (FIPS-204)
  - ML-DSA 44/65/87
  - Key generation
  - Key import/export
  - Signing and verification

Size Requirements

Config Information	IP Area
Typical configuration (GF12LP)	~320Kgte

Performance Expectations

Algorithm	Security Level	Max Performance (cycles)
ML-KEM Key generation	ML-KEM-512	2300
ML-KEM Encapsulation	ML-KEM 512	3200
ML-KEM Decapsulation	ML-KEM 512	4700
ML-DSA Key generation	ML-DSA 44	10400
ML-DSA Signing	ML-DSA 44	11250
ML-DSA Verification	ML-DSA 44	6800

IP Overview

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

Keccak Sampler

- Combines hashing and sampling capabilities, supporting SHA-3 and SHAKE algorithms

Polynomial Arithmetic Unit (PAU)

A number of the post-quantum algorithms rely on the efficiency of polynomial multiplication. PQPerform-Lattice uses the PAU to perform this level of efficient multiplication at speed.

Firmware

PQPerform-Lattice is designed to use a Linux Kernel Driver to deliver PQShield firmware.

PQShield Hardware IP

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

Hardware IP	Description
PQPerform-Lattice / PQF-HW-LAT	**High-speed, high-throughput, autonomous lattice PQC cryptographic subsystem**
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.
PQPerform-SubSys / PQP-HW-SUB	Autonomous cryptographic subsystem performing PQC and classical cryptography.