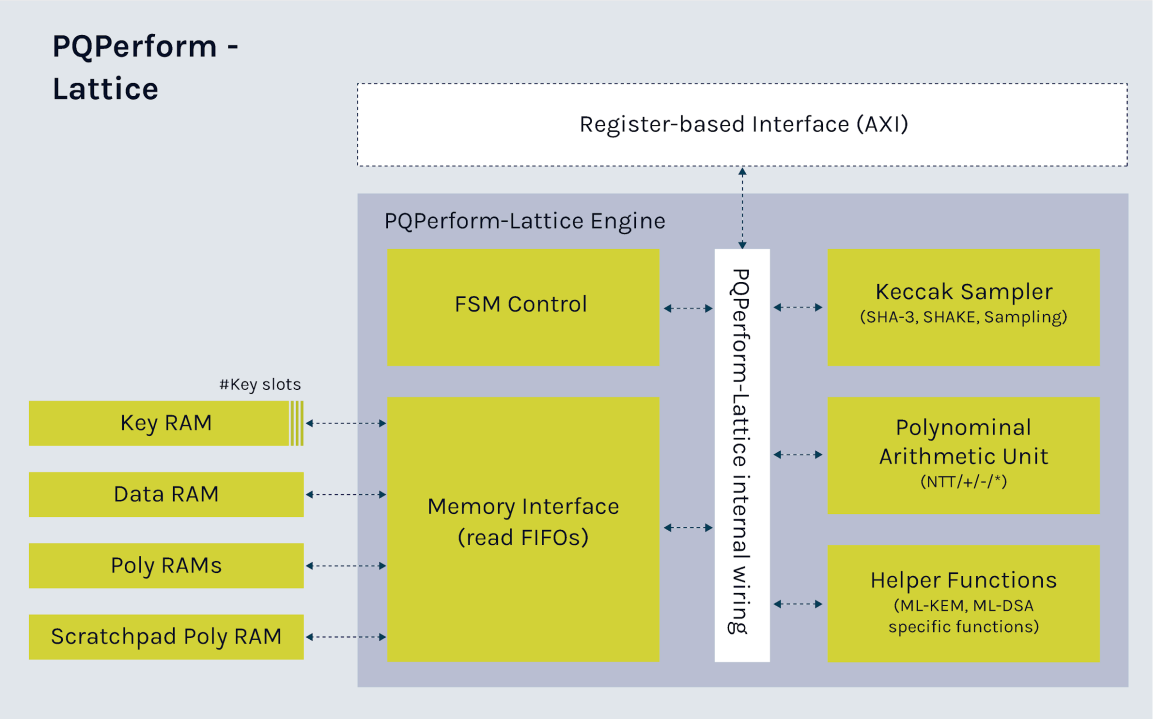
v R24.2.2

Perform-Lattice

13 May 2024

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

PQPerform-Lattice (PQF-HW-LAT) is a powerful hardware-based product that is designed for high throughput and high speed. PQF-HW-LAT adds post-quantum cryptography for securing 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 Specific Functions (FIPS 203)
  - ML-KEM-512/768/1024
  - Keypair generation
  - Key material import
  - Key material export
  - Encapsulation
  - Decapsulation

- ML-DSA Specific Functions (FIPS 204)
  - ML-DSA-44/65/87
  - Keypair generation
  - Key material import
  - Key material export
  - Signing
  - Verification

- Supports CNSA 2.0 quantum-resistant public-key algorithms

- Software ecosystems support.
  - Linux: Kernel driver and user space support libraries
  - Bare metal environments: Hardware Abstraction Layer (on request)

- Scalable architecture. PQPerform-Lattice can be instantiated many times on the same bus for parallelisation.
  - Supported by PQShield Linux software stack.

- Software is optional depending on integration needs. PQPerform-Lattice can be driven entirely by customer-provided hardware IP.

- Customer configurable number of key slots (dependent on memory availability)

Size Requirements

Config Information	IP Area
Typical configuration with ML-KEM and ML-DSA (GF12LP)[1]	~380Kgte (excluding memories)

[1] Either complete algorithm can also be provided.

Performance Expectations

Algorithm	Operation	Security Level	Minimum latency (cycles)
ML-KEM	Keypair generation	ML-KEM-512	2,300
	Encapsulation	ML-KEM-512	3,200
	Decapsulation	ML-KEM-512	4,700
ML-DSA	Keypair generation	ML-DSA-44	10,400
	Signing	ML-DSA-44	11,250
	Verification	ML-DSA-44	6,800

PQShield Hardware IP

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