Post-Quantum-Cryptography Key Encapsulation Mechanism (PQC-KEM)

The KiviPQC-KEM is an IP core for ML-KEM key encapsulation that supports key generation, encapsulation and decapsulation for all ML-KEM variants standardized by NIST in FIPS 203. ML-KEM belongs to the Key Encapsulation Mechanism (KEM) algorithm and is designed to be robust against a quantum computer attack. It can be used by two parties to establish a shared secret key over a public channel. The IP core provides hardware acceleration for compute-intensive operations while maintaining a small footprint. In addition, it is a self-contained and encapsulated IP core that can be integrated into any System on Chip (SoC) for ASIC or FPGA implementation.

- Highly cost-efficient: Solution that ensures excellent performance with low purchasing costs
- Security by design: A self-contained engine with a minimal attack surface
- Resource-Efficient: Designed to have minimal logic utilization

Key Features

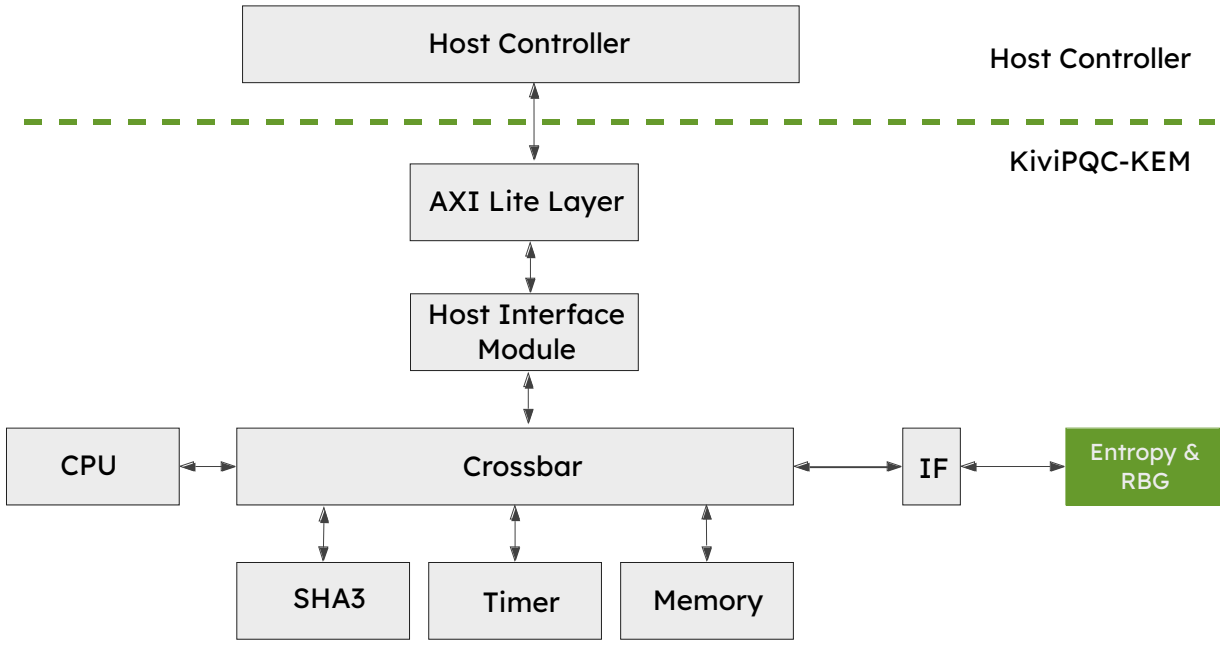
- FIPS 203 compliant
- Supports ML-KEM 512/768/1024 sets
- Self-contained engine with a minimal attack surface
- Hardware offloading and acceleration for core ML-KEM operations
- Protection against timing-based side channel attacks
- AMBA® AXI4-Interface
- For any FPGA and ASIC

Deliverables

- System Verilog RTL Source Code
- Testbenches
- Integration examples
- Software example source code
- Documentation

Licensing & Services

- One-time license fee
- Single or multi project license
- Evaluation/Prototype license
- Technical Support by email
- Maintenance & updates of IP cores



Block Diagram

Device	Logic (LUTs)	Registers (FF)	fmax (MHz)
AMD Zync Ultrascale MPSoC	8189	9296	175.3
AMD Kintex-7	8158	9296	119.3
AMD Spartan 7	8158	9296	75.8
Efinix Titanium Ti120	8461	9110	135.2
Intel (Altera) Agilex 7	14796	11406	230.8
Intel (Altera) Arria 10	7839	9710	115.8
Intel (Altera) Cyclone 10 GX	7977	9706	154.1
Intel (Altera) Stratix 10	14065	10423	143.1
Lattice Avant E	8130	9627	98.7

Resource Utilization

Need more detailed technical information?

Get documentation