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

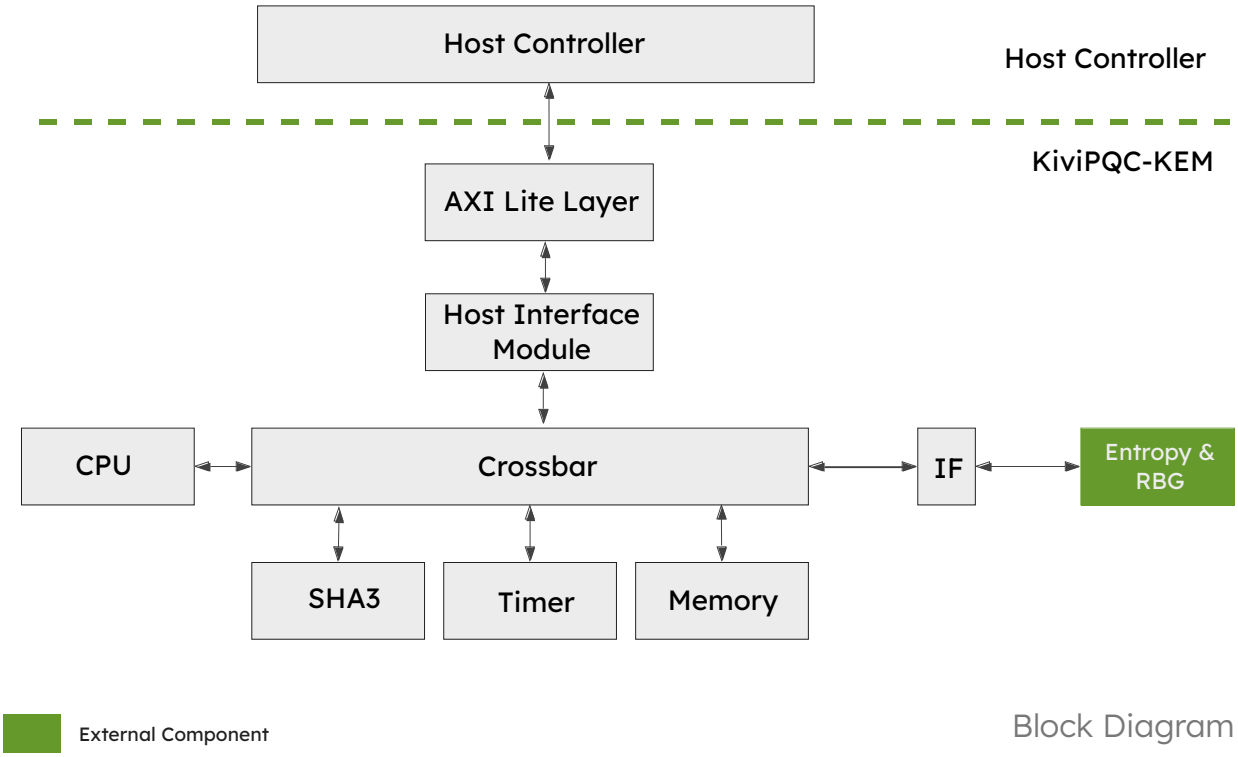
- FIPS 203 compliant
- Supports ML-KEM 512/768/1024 sets
- Self-contained engine with a minimal attack surface
- Hardware offloading and acceleration for core ML-KEM operations
- Protection against timing-based side channel attacks
- AMBA® AXI4-Interface
- For any FPGA and ASIC

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)
Efinix Titanium Ti375	8461	9110	135.2

Resource Utilization

Need more detailed technical information?

Get documentation

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

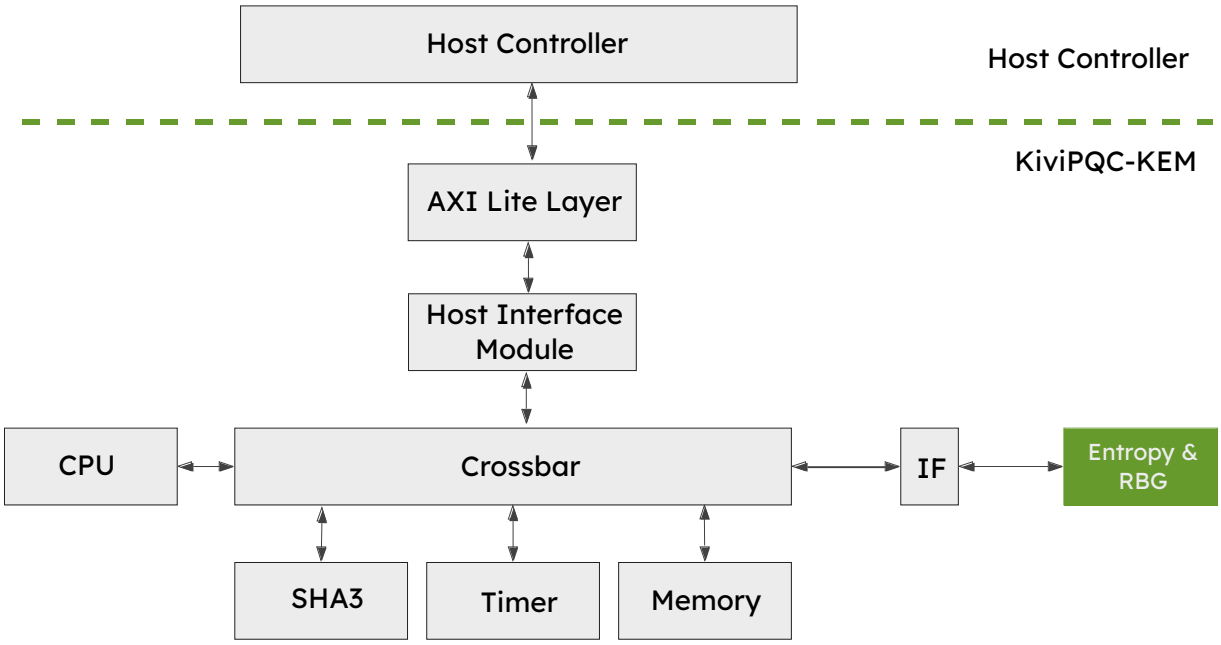
- FIPS 203 compliant
- Supports ML-KEM 512/768/1024 sets
- Self-contained engine with a minimal attack surface
- Hardware offloading and acceleration for core ML-KEM operations
- Protection against timing-based side channel attacks
- AMBA® AXI4-Interface
- For any FPGA and ASIC

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

Parameter Set	Technology	Frequency (MHz)	NAND2 Gate Counts
ML-KEM 512	TSMC 7 nm	700	124 k
	TSMC 16 nm	600	114 k
	TSMC 28 nm	100	101 k
	TSMC 40 nm	500	111 k
ML-KEM 768	TSMC 7 nm	100	132 k
	TSMC 16 nm	600	146 k
	TSMC 40 nm	100	156 k
ML-KEM 1024	TSMC 7 nm	100	165 k
	TSMC 16 nm	600	181 k
	TSMC 40 nm	100	194 k

Resource Utilization

Need more detailed technical information?

Get documentation