KiviPQC-KEM

KiviCore

IP Core Product Brief 20251027

Post-Quantum Key Encapsulation IP Core

The KiviPQC-KEM is an IP core implementing the ML-KEM (Module-Lattice-based Key Encapsulation Mechanism) a post quantum cryptographic (PQC) algorithm standard defined by NIST FIPS 203. PQC is engineered to withstand both classical and quantum computer attacks.

Supporting all ML-KEM parameter sets, the KiviPQC-KEM enables:

- Two parties to securely establish a shared secret key over a public channel. This key enables the use of symmetric-key cryptographic algorithms to perform secure communication tasks, such as encryption and authentication.

The IP core provides dedicated hardware acceleration for the most computationally demanding operations, ensuring high throughput and low latency while keeping the logic footprint compact. Designed as a standalone, self-contained module, the KiviPQC-KEM can be integrated seamlessly into any SoC design. It features a standard AMBA® AXI4-Lite interface for hardware integration and platform-independent C code, HAL, and API drivers for simple software integration into the host processor.

Variants	Description
KiviPQC-KEM-Tiny	Optimized for minimal logic resource usage. Ideal when FPGA resources or power budgets are tight.
KiviPQC-KEM-Fast	Optimized for fast processing. For designs that desire higher performance while maintaining efficient resource utilization.

Applications

- Quantum-Resistant Networks
- Public Key Infrastructures
- Network Security: MACsec, IPsec
- Transport Protocols: TLS, SSL
- Secure Communications
- Electronic Transactions

Benefits

- Easy integration
- Highly cost-efficient
- Minimal logic utilization

Key Features

- NIST FIPS 203 compliant
- Supports ML-KEM 512/768/1024 sets
- Supports ML-KEM.KeyGen, ML-KEM.Encaps/Decaps functions
- Self-contained engine with a minimal attack surface
- Hardware offloading and acceleration for core ML-KEM operations
- Protection against timing-based side channel attacks

Licensing & Services

- Product license
  - One-time license fee
  - Single or multi project license
- Free evaluation license
- Technical support by email
- Maintenance & updates

Easy integration

- Platform agnostic for any FPGA
- AMBA® AXI4 lite Interface
- Platform agnostic C source code
- HAL, API and software driver included
- Software examples included
- Software user guide
- Fast support within 8 hours

Deliverables

- Product license
  - System Verilog RTL source code or netlist format
- Free evaluation license
  - Netlist format, time bombed
- Testbenches
- Integration examples
- Software HAL & driver source code
- Software example
- Documentation

FPGA Implementation Results

	KiviPQC-KEM-Tiny		KiviPQC-KEM-Fast	
Altera	**ALM**	**fmax (MHz)**	**ALM**	**fmax (MHz)**
Stratix 10	3120	153.0	11016	153.8
Agilex 7	2920	223.6	11243	216.8
Arria 10	2674	196.7	10489	193.1
Cyclone 10 GX	2682	178.6	10131	170.4
Efinix	**XLR**	**fmax (MHz)**	**XLR**	**fmax (MHz)**
Titanium	6368	147.4	16592	138.5

	KiviPQC-KEM-Tiny		KiviPQC-KEM-Fast	
AMD (Xilinx)	**LUTs**	**fmax (MHz)**	**LUTs**	**fmax (MHz)**
Spartan 7	3714	81.4	12156	78.5
Kintex 7	3728	129.8	12157	130.2
Zync US+ MPSoC	3652	196.7	12154	178.6
Versal AI Cores Series	5730	199.2	14762	205.8
Microchip	**LUT4**	**fmax (MHz)**	**LUT4**	**fmax (MHz)**
PolarFire SoC	6008	63.4	19197	65.3
PolarFire	6008	63.4	19197	65.3
Igloo2	6095	50.0	18295	50.9
RTG4	7602	43.0	20066	42.8
SmartFusion 2	6095	50.0	18925	50.9

Want to learn more? Visit the product web page.

KiviPQC-KEM