KiviPQC-Box

KiviCore

IP Core Product Brief 20251028

Post-Quantum Key Encapsulation and Digital Signature IP Core

The KiviPQC-Box is an IP core that combines the algorithms ML-DSA and ML-KEM into one single package. ML-DSA and ML-KEM are standardized by NIST as post-quantum algorithms defined in FIPS 204 and FIPS 203 and provide cyber secure protection against the threat of quantum computers. ML-KEM enables two parties to securely establish a shared secret key over an untrusted public channel and ML-DSA ensures the authenticity and integrity of signed data far into the future. It delivers complete protection against time-based side-channel attacks (SCA).

With both algorithms implemented, KiviPQC-Box enables to:

- Generate digital signatures to verify data integrity and detect unauthorized modifications of signed data
- Ensure authenticity by proving that a digital signature was created by the stated signer (non-repudiation).
- Securely establish a shared secret key over an untrusted public channel

The KiviPQC-Box is a self-contained, standalone module that integrates effortlessly into any SoC design. It includes a standard AMBA® AXI4-Lite interface for easy hardware integration and provides platform-independent C code, HAL, and API drivers to simplify software integration with the host processor.

Variants	Description
KiviPQC-Box-Tiny	Optimized for minimal logic resource usage. Ideal when FPGA resources or power budgets are tight.
KiviPQC-Box-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

Key Features

- NIST FIPS 203 and FIPS 204 compliant
- Supports ML-KEM 512/768/1024 parameter sets
- Supports ML-DSA 44/65/87 parameter sets
- Supports ML-DSA.KeyGen, ML-DSA.Sign, ML-DSA.Verify functions
- Supports pre-hash ML-DSA functions HashML-DSA.Sign and HashML-DSA.Verify
- Supports hedged and deterministic signing
- Supports context string
- Supports ML-KEM.KeyGen, ML-KEM.Encaps, ML-KEM.Decaps functions
- Hardware offloading and acceleration for ML-KEM and ML-DSA operations
- Protection against timing-based side channel attacks

Benefits

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

Easy integration

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

Licensing & Services

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

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-Box-Tiny		KiviPQC-Box-Fast	
Altera	**ALM**	**fmax (MHz)**	**ALM**	**fmax (MHz)**
Stratix 10	3190	148.2	11149	155.5
Agilex 7	3050	212.2	11036	212.6
Arria 10	2746	207.0	10357	207.2
Cyclone 10 GX	2753	184.8	10339	179.5
Efinix	**XLR**	**fmax (MHz)**	**XLR**	**fmax (MHz)**
Titanium	6476	137.2	17090	146.3
AMD (Xilinx)	**LUTs**	**fmax (MHz)**	**LUTs**	**fmax (MHz)**
Spartan 7	3912	76.5	12387	78.3
Kintex 7	3946	128.5	12365	128.2
Zync US+ MPSoC	3874	205.2	12341	198.3
Versal AI Cores Series	5912	202.6	14999	206.1
Microchip	**LUT4**	**fmax (MHz)**	**LUT4**	**fmax (MHz)**
PolarFire SoC	6301	67.0	19470	64.5
PolarFire	6301	67.0	19470	64.5
Igloo2	6242	50.9	18729	49.8
RTG4	7915	42.3	20521	43.5
SmartFusion 2	6242	50.9	18729	49.8

Want to learn more? Visit the product web page.

KiviPQC-Box