KiviPQC-DSA

KiviCore

IP Core Product Brief 20251029

Post-Quantum Digital Signature IP Core

The KiviPQC-DSA is an IP core implementing the ML-DSA (Module-Lattice-based Digital Signature Algorithm) a post-quantum cryptographic standard defined by NIST FIPS 204. Designed to withstand both classical and quantum computer attacks, ML-DSA ensures the authenticity and integrity of signed data.

Supporting all ML-DSA parameter sets, the KiviPQC-DSA enables to:

- Generate private/public key pair to create signatures and verify signed data
- Generate digital signatures to verify data integrity and detect any unauthorized modifications of signed data
- Ensure authenticity by proving that a digital signature was created by the stated signer (non-repudiation)

The IP core offers dedicated hardware acceleration for the most computationally intensive operations, achieving high throughput and low latency while maintaining a compact logic footprint. It delivers complete protection against time-based side-channel attacks (SCA). Engineered as a self-contained hardware/software co-design, the core integrates all ML-DSA functions and comes ready for seamless deployment. It includes AMBA® hardware interface for straightforward system integration and a generic software API for flexible control from the host processor.

It is available as an option for digital signature verification only. This is ideal for devices that only need to verify signed data, such as those used for secure boot, secure update, data and message authentication, access control and licensing, verification of signed control commands, signed configuration or policy updates.

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

Applications

- Software and firmware validation
- Data and message authentication
- Access control & licensing
- Digital content and media
- Configuration or policy validation
- Control command validation
- Critical infrastructures

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

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

Benefits

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

Key Features

- NIST FIPS 204 compliant
- 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
- Self-contained engine with a minimal attack surface
- Hardware offloading and acceleration for ML-DSA 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

FPGA Implementation Results

	KiviPQC-DSA-Tiny		KiviPQC-DSA-Fast	
Altera	**ALM**	**fmax (MHz)**	**ALM**	**fmax (MHz)**
Stratix 10	3059	154.7	10537	139.2
Agilex 7	2881	215.6	11295	213.3
Arria 10	2652	192.8	10437	192.3
Cyclone 10 GX	2639	192.0	10440	185.9
Efinix	**XLR**	**fmax (MHz)**	**XLR**	**fmax (MHz)**
Titanium	6291	148.6	16694	143.7
AMD (Xilinx)	**LUTs**	**fmax (MHz)**	**LUTs**	**fmax (MHz)**
Spartan 7	3725	84.0	12174	75.4
Kintex 7	3755	128.6	12184	127.1
Zync US+ MPSoC	3666	195.4	12165	194.0
Versal AI Cores Series	5456	187.1	14595	208.3
Microchip	**LUT4**	**fmax (MHz)**	**LUT4**	**fmax (MHz)**
PolarFire SoC	5999	65.0	19202	65.3
PolarFire	5999	65.0	19202	65.3
Igloo2	5958	50.2	18449	49.1
RTG4	7590	43.7	20166	41.5
SmartFusion 2	5958	50.2	18449	49.1

Want to learn more? Visit the product web page.

KiviPQC-DSA