BERTEN
Secure Communications

MLDS-B235 IP Core

ML-DSA Crypto Core

Post-Quantum Cryptography (PQC)

Lattice-based Digital Signature
Register-based Configuration
Optimised Performance

Features

- Post-Quantum Digital Signature
- FIPS 204, FIPS 140-3 Compliant
- Hedged Variant Support
- SCA Countermeasures
- Optimised Arithmetic Unit
- Portable to any FPGA or ASIC
- AMBA AXI Interfaces

Applications

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

The **MLDS-B235** IP Core implements the NIST Module-Lattice-Based Digital Signature Standard (ML-DSA) in FPGA, SoC, and ASIC technologies.

Derived from the CRYSTALS-Dilithium scheme, ML-DSA is believed to be secure against large-scale quantum computers to generate and verify digital signatures.

The IP core is compliant with FIPS 204 and supports the three security levels of the NIST standard (ML-DSA-44, ML-DSA-65, ML-DSA-87).

Portable to any AMD (Xilinx), Intel (Altera), or Microchip (Microsemi) device, the IP Core is also compliant with FIPS 140-3 and provides the highest performance in a minimum area.

MLDS-B235 includes AMBA AXI interfaces and a user-programmable register map to select the ML-DSA operation and parameter set. ANSI C drivers are provided for a fast integration into the target platform.

www.bertendsp.com sales@bertendsp.com +34 942 18 10 11

Digital Signature Operations

MLDS-B235 implements the set of algorithms for digital signature according to FIPS 204 Module-Lattice-Based Standard.

This Post-Quantum Cryptography (PQC) IP core includes a sequencer that manages the Polynomial Arithmetic Unit and a high-performance SHAKE Extendable-Output Function (XOF).

Key Generation, Signing, and Verification algorithms are configured through the integrated register map. ML-DSA-44, ML-DSA-65, and ML-DSA-87 parameter sets are available to balance security and performance.

Operation	Estimated Performance, op/s @300MHz		
	ML-DSA-44 🛡🛡	ML-DSA-65 🛡🛡🛡	ML-DSA-87 🛡🛡🛡🛡🛡
Key Generation	16,300	10,250	7,150
Signing [Average]	1,650	1,000	850
Verification	11,200	7,600	5,200

🛡 *Security Level according to FIPS 204 Appendix A.*

Attack Resistance

In addition to the inherent robustness of ML-DSA against Side-Channel Attacks (SCA), the IP core includes specific countermeasures to resist timing and Simple Power Analysis (SPA) attacks.

To improve message data confidentiality, a random seed may be provided to implement the Hedged variant of the signing algorithm.

Automatic and on-demand zeroization of internal memories and registers are also available.

Resources

Resource utilisation for different devices is provided in the table below. Metrics for other FPGA or SoC are available as required.

	Device Family	LUT	Register
AMD / Xilinx	Spartan-7, Artix-7, Kintex-7, Virtex-7	10.3K	8.2K
	Kintex/Virtex Ultrascale	10.2K	8.2K
	Artix/Kintex/Virtex Ultrascale+	10.1K	8.1K
	Versal ACAP	9.5K	8.1K
Intel / Altera	MAX 10, Cyclone 10 [LP]	18.5K	8.1K
	Cyclone V	11.4K	8.1K
	Arria 10	11.4K	8.2K
	Stratix V	11.4K	8.2K

Interfaces

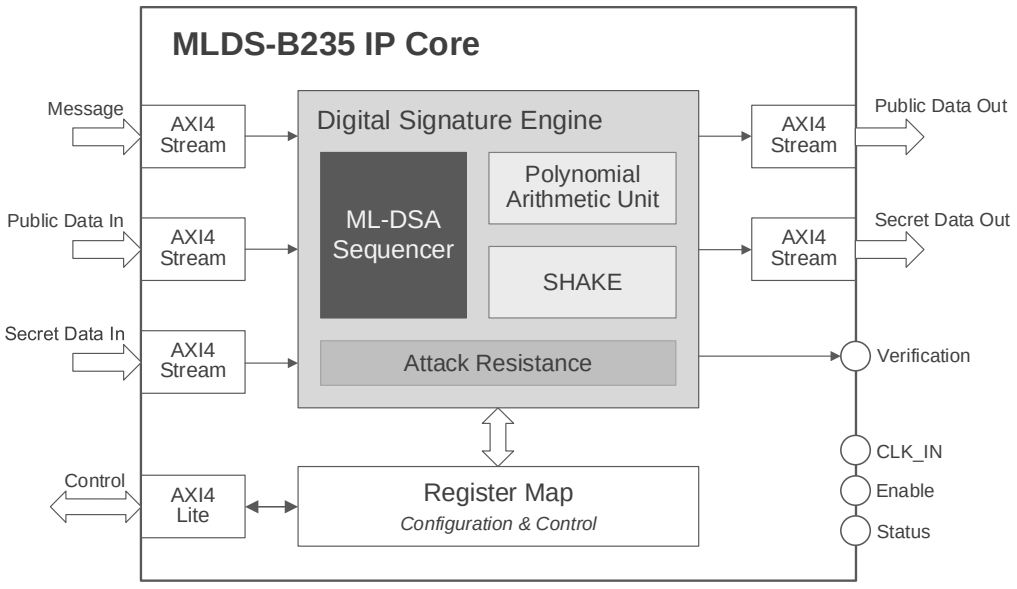
The IP Core implements five AXI4-Stream interfaces for high-speed data transfer. One AXI4-Lite provides access to the register map to select the ML-DSA operation and parameter set. Status and Verification ports are available for events and signature validity notifications.

Licensing

The IP Core is provided as encrypted netlist for one device family, under a perpetual Site Licence. It includes 12 months of maintenance and integration support into the target platform.

Deliverables

- Targeted, timing closed Netlist
- Design Constraints
- Simulation Model
- User Manual
- ANSI C drivers



www.bertendsp.com sales@bertendsp.com +34 942 18 10 11