BERTEN
Secure Communications

MLKE-B135 IP Core

ML-KEM Crypto Core

Post-Quantum Cryptography (PQC)

Lattice-based Key Encapsulation
Register-based Configuration
Optimised Performance

Features

- Post-Quantum Key Establishment
- FIPS 203, FIPS 140-3 Compliant
- SCA Countermeasures
- Optimised Arithmetic Unit
- Input Key Checking
- Portable to any FPGA or ASIC
- AMBA AXI Interfaces

Applications

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

The **MLKE-B135** IP Core implements the NIST Module-Lattice-Based Key Encapsulation Mechanism (ML-KEM) in FPGA, SoC, and ASIC technologies.

Derived from the CRYSTALS-Kyber scheme, ML-KEM is a key exchange algorithm believed to be secure against large-scale quantum computers.

The IP core is compliant with FIPS 203 and supports the three security levels of the NIST standard (ML-KEM-512, ML-KEM-768, ML-KEM-1024).

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.

MLKE-B135 includes AMBA AXI interfaces and a user-programmable register map to select the ML-KEM 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

Key Exchange Operations

MLKE-B135 implements the set of algorithms for key encapsulation according to FIPS 203 Module-Lattice-Based Standard.

This Post-Quantum Cryptography (PQC) IP core includes a sequencer that manages the Polynomial Arithmetic Unit and high-performance SHA3 and SHAKE functions.

Key Generation, Encapsulation, and Decapsulation algorithms are configured through the integrated register map. ML-KEM-512, ML-KEM-768, and ML-KEM-1024 parameter sets are available to balance security and performance.

	Average Performance, op/s @300MHz		
Operation	ML-KEM-512 🛡	ML-KEM-768 🛡🛡🛡	ML-KEM-1024 🛡🛡🛡🛡🛡
Key Generation	87,050	53,500	36,500
Encapsulation	70,500	45,750	32,200
Decapsulation	52,300	35,200	25,600

🛡 *Security Level according to FIPS 203.*

Attack Resistance

In addition to the inherent robustness of ML-KEM against Side-Channel Attacks (SCA), the IP core has been designed to resist timing and Simple Power Analysis (SPA) attacks.

To prevent the use of invalid keys in encapsulation and decapsulation operations, MLKE-B135 implements input checking according to FIPS 203.

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	9.0K	7.4K
	Kintex/Virtex Ultrascale	8.9K	7.4K
	Artix/Kintex/Virtex Ultrascale+	8.9K	7.4K
	Versal ACAP	8.6K	7.4K
Intel / Altera	MAX 10, Cyclone 10 ^{LP}	17.4K^{LE}	7.8K
	Cyclone V	7.5K^{ALM}	7.8K
	Arria 10	7.4K^{ALM}	8.0K
	Stratix V	7.5K^{ALM}	8.0K
	Agilex 5	7.4K^{ALM}	7.9K

Interfaces

The IP Core implements four AXI4-Stream interfaces for high-speed data transfer. One AXI4-Lite provides access to the register map to select the ML-KEM operation and parameter set. A Status port is available for event notification.

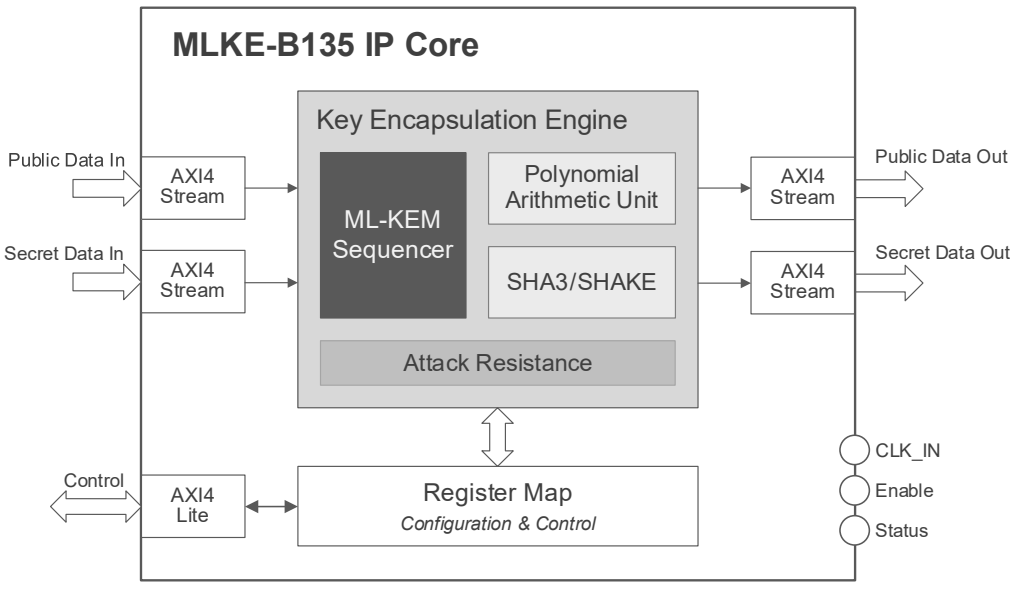
Licensing

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.

Export Classification: 5D002.c.1 / 5A002.a.1.

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