

May 2026

OVERVIEW

The Poly IP core supports the polynomial arithmetic required by lattice-based cryptography algorithms, including NIST's selected Post-Quantum Cryptography (PQC) standards: ML-KEM (Kyber), ML-DSA (Dilithium), and FN-DSA (Falcon).

FEATURES LIST

- i. Efficient polynomial arithmetic
- ii. Supported Algorithms:
 - **ML-KEM, ML-DSA**
 - FIPS-203 and FIPS-204 compliant
 - **FN-DSA** (verification only, FFT not supported)
- iii. Supported (Coefficient) vectors of size 256 and 32-bit
 - Can be customized upon request
- iv. Dual mode: doubled throughput for half-word (16-bit) processing required by ML-KEM and FN-DSA
- v. Run-time configurable parameter sets
- vi. Supported operation codes:
 - Forward/backward NTT
 - Element-wise multiplication/addition/subtraction/multiply-accumulate
 - Including ML-KEM's special multiplication
 - Encoding/decoding (used in ML-KEM, ML-DSA, FN-DSA)
 - ML-KEM supporting functions:
 - Compress, decompress
 - ML-DSA supporting functions:
 - Decompose, make hint, use hint, check infinity norm
 - FN-DSA supporting functions:
 - Check L1 norm, decompress
 - Pseudo-random sampling:
 - CBD sampling (ML-KEM)
 - Rejection sampling (ML-KEM, ML-DSA, FN-DSA)
- vii. Optimized global memory access
- viii. AXI4 interface for system integration and drivers available upon request

Technology Partner



Poly IP Core

DELIVERABLES

- Encrypted Netlist
- Synthesis Scripts
- Comprehensive Documentation
- Drivers upon request

MAINTENANCE & SUPPORT

- M&S fee of 15% is mandatory for the first year.
- Telephone and email support is included under M&S agreement.
- IP Core updates are included in M&S.

LICENSING

Following licensing models are available:

- Encrypted Netlist
- Encrypted RTL

ORDERING

Purchase order shall include the product number EIP-30010000.

FPGA SYNTHESIS RESULT

Family/Device	LUT	FF	DSP	BRAM
Zynq/xc7z020clg400-1	5064	1934	9 / 15 *	1.5

Technology Partner

