

May 2026

OVERVIEW

PQC Co-Proc IP core is a co-processor that supports NIST's selected Post-Quantum Cryptography (PQC) standards, ML-KEM (Kyber), ML-DSA (Dilithium), SLH-DSA (SPHINCS+), and FN-DSA (Falcon). This IP is fully compliant with the NIST's published standards, and offers countermeasures against Side-Channel Analysis attacks.

FEATURES LIST

- i. Supported Algorithms (algorithm set is customizable):
 - **ML-KEM**
 - FIPS-203 compliant
 - Key Generation, Encapsulation, Decapsulation
 - All security levels: ML-KEM-512, ML-KEM-768, ML-KEM-1024
 - **ML-DSA**
 - FIPS-204 compliant
 - Key Generation, Signature Generation, Signature Verification
 - All security levels: ML-DSA-44, ML-DSA-65, ML-DSA-87
 - **SLH-DSA**
 - FIPS-205 compliant
 - Key Generation, Signature Generation, Signature Verification
 - All security levels: SLH-DSA-SHAKE-128s/f, SLH-DSA-SHAKE-192s/f, SLH-DSA-SHAKE-256s/f
 - **FN-DSA**
 - Falcon Round 3 Submission compliant. Will be updated with FIPS-206 upon its publication
 - Signature Verification
 - All security levels: Falcon-512, Falcon-1024
- ii. Optional Side-Channel Analysis and Fault Injection attacks countermeasures (e.g., masking)
- iii. AXI4 interface for system integration available upon request
- iv. Crypto-agility: Modifications to existing implementations (e.g., new countermeasures) and new algorithms can be implemented by re-programming the RISC-V core's firmware

Technology Partner



PQC Co-Proc IP Core

DELIVERABLES

- Encrypted Netlist
- Synthesis Scripts
- Firmware (binary)
- Comprehensive Documentation

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

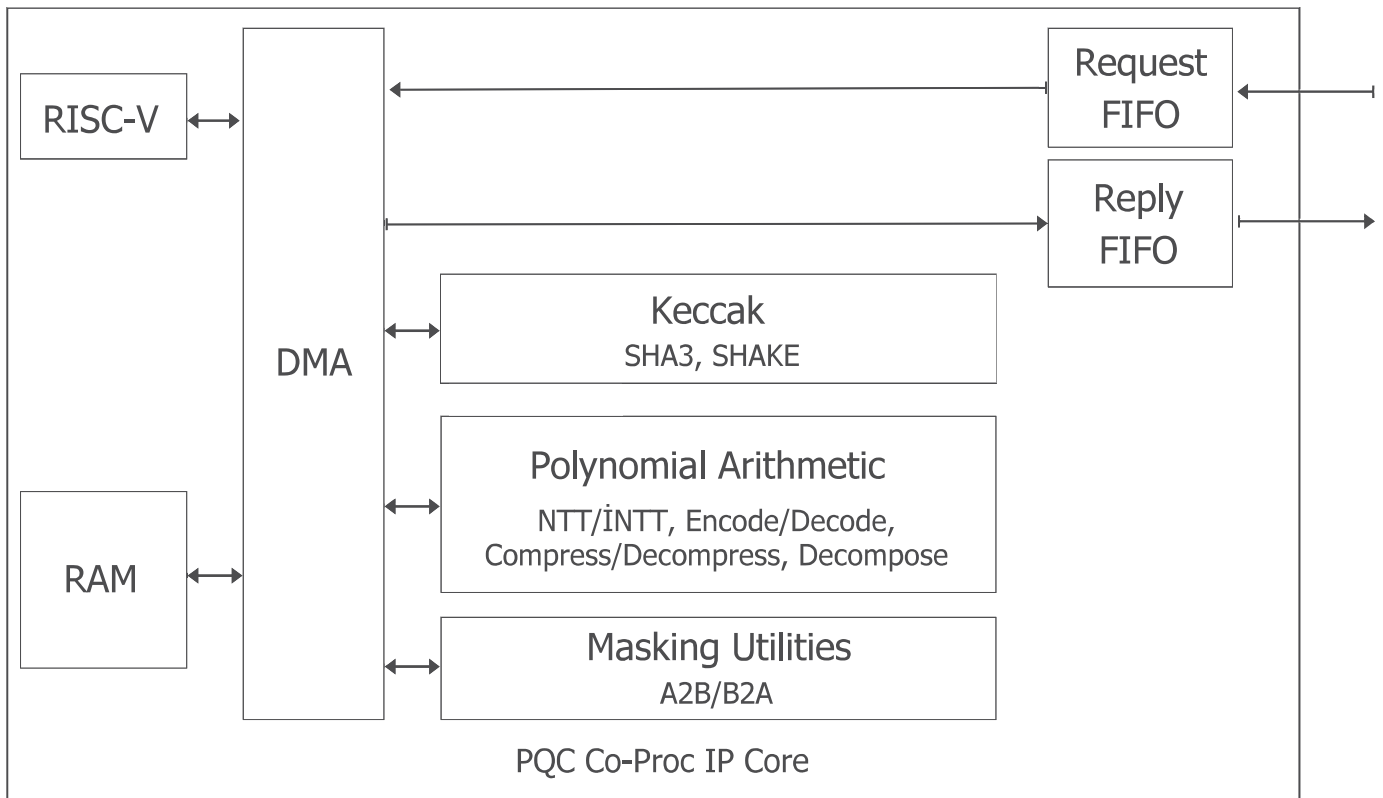
ORDERING

Purchase order shall include the product number EIP-30010002.

FPGA SYNTHESIS RESULT

Family/Device	SCA+FI Countermeasures	LUT	FF	BRAM	DSP
Zynq/xc7z020clg400-1	No	15672	8126	81.5	9
	Yes	30074	21460	81.5	15

BLOCK DIAGRAM



Technology Partner

enCRYPTON
LABS