

May 2026

OVERVIEW

PQC HW/SW IP Suite is composed of three dedicated HW IP cores (PolyCore, KeccakCore, MaskCore) and the software stack leveraging these IP cores to implement PQC algorithms. It is designed to support 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. PQC hardware IP core set is customizable, and the standard offering includes three cores targeting PQC algorithms:
 - KeccakCore, PolyCore, MaskCore
- ii. 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
- iii. Optional Side-Channel Analysis and Fault Injection attacks countermeasures (e.g., masking)
- iv. AXI4 interface for system integration and drivers available upon request
- v. Crypto-agility: Modifications to existing implementations (e.g., new countermeasures) and new algorithms can be implemented by updating the software layer

Technology Partner



PQC HW/SW 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

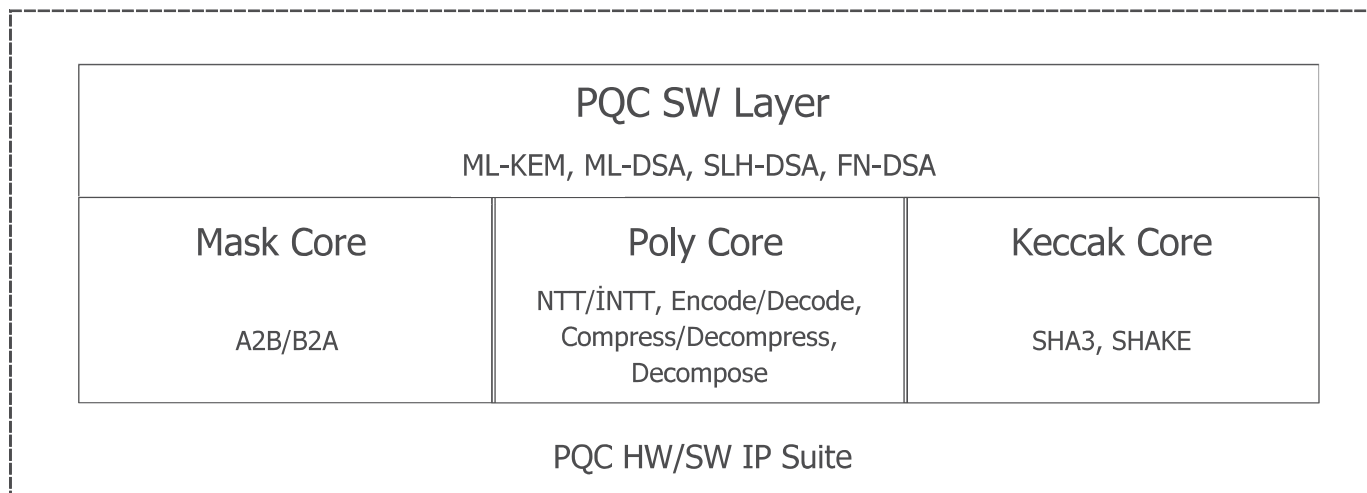
ORDERING

Purchase order shall include the product number EIP-30010003.

FPGA SYNTHESIS RESULT

Family/Device	IP Core	SCA+FI Countermeasures	LUT	FF	DSP	BRAM
Zynq/xc7z020clg400-1	Keccak Core	No	4792	3455	0	0
		Yes	9777	7626	0	0
	Poly Core	No	5064	1934	9	1.5
		Yes	5064	1934	15	1.5
	Mask Core	Yes	9409	9163	0	0

BLOCK DIAGRAM



Technology Partner

