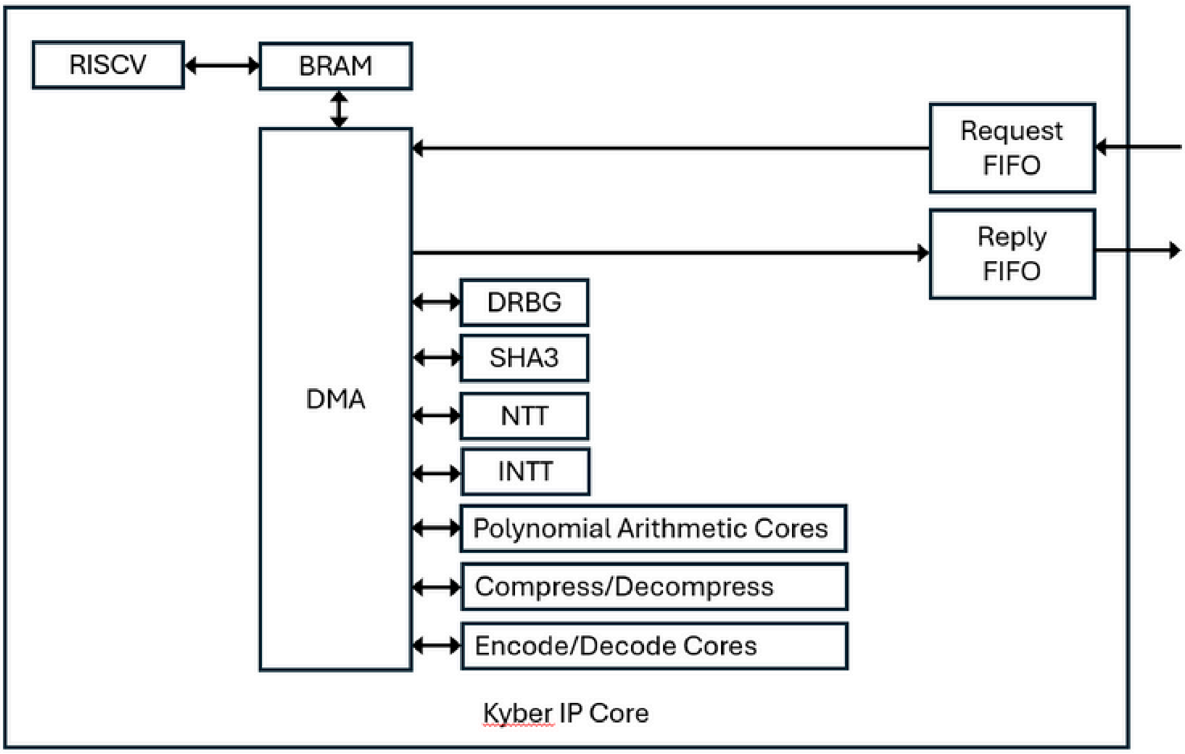
Kyber IP Core
Datasheet

January 2025

OVERVIEW

Kyber IP is a core designed for Kyber post-quantum Key Encapsulation Mechanism (KEM). It currently supports the Encapsulation and Decapsulation functions, with key generation functionality planned for future implementation. This IP is fully compliant with the Kyber specification submitted during Round 3 of the NIST Post-Quantum Cryptography Standardization process. Additionally, Kyber IP will be enhanced in the future to achieve compliance with ML-KEM (FIPS-203).



DELIVERABLES

- Encrypted Netlist
- Synthesis Scripts
- Comprehensive Documentation

FEATURES LIST

Kyber IP Core:

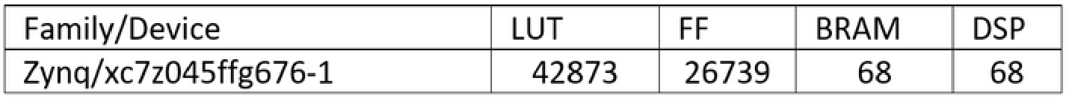
- supports encapsulation and decapsulation operations.
- supports all modes K=2,3,4.
- is compliant with Kyber specification round 3.
- has fully stallable input and output interfaces.
- Key generation feature is going to be implemented in the near future.

Technology Partner

Kyber IP Core

FPGA SYNTHESIS RESULTS

The FPGA resources requirements depend on the configuration.



Family/Device	LUT	FF	BRAM	DSP
Zynq/xc7z045ffg676-1	42873	26739	68	68

LICENSING

A one-time license fee is paid with the initial IP purchase.

- Single project license
- Multi project license

MAINTENANCE & SUPPORT

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

ORDERING

- Purchase order shall include the product number EIP-18009.

Technology Partner

procenne DIGITAL SECURITY