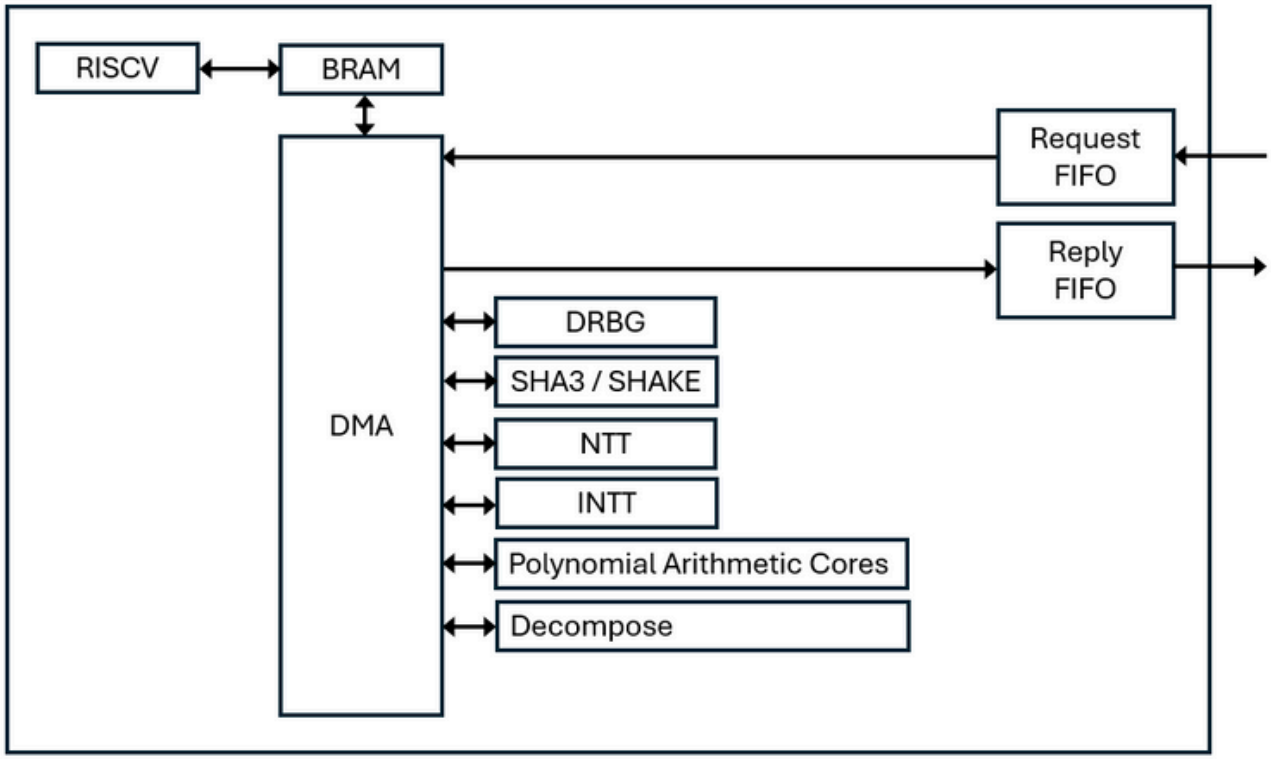
Dilithium IP Core
Datasheet

March 2025

OVERVIEW

Dilithium IP Core is a post-quantum digital signature algorithm (DSA). It currently supports Sign and Verify functions, with key generation functionality planned for future implementation. This IP is compliant with Dilithium specification submitted on round 3 of NIST Post-Quantum Cryptography Standardization process. Additionally, Dilithium IP will be enhanced in the future to achieve compliance with ML-DSA (FIPS-204).



DELIVERABLES

- Encrypted Netlist
- Synthesis Scripts
- Comprehensive Documentation

FEATURES LIST

Dilithium IP Core:

- Supports sign and verify operations.
- Supports all three Dilithium modes.
- Has fully stallable input and output interfaces.
- Key generation feature is going to be implemented in the near future.

Technology Partner

Dilithium IP Core

FPGA SYNTHESIS RESULTS

The FPGA resources requirements depend on the configuration.

Family/Device	LUT	FF	BRAM	DSP
Zynq/xc7z045ffg676-1	53364	37552	68	86

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-19009.

Technology Partner