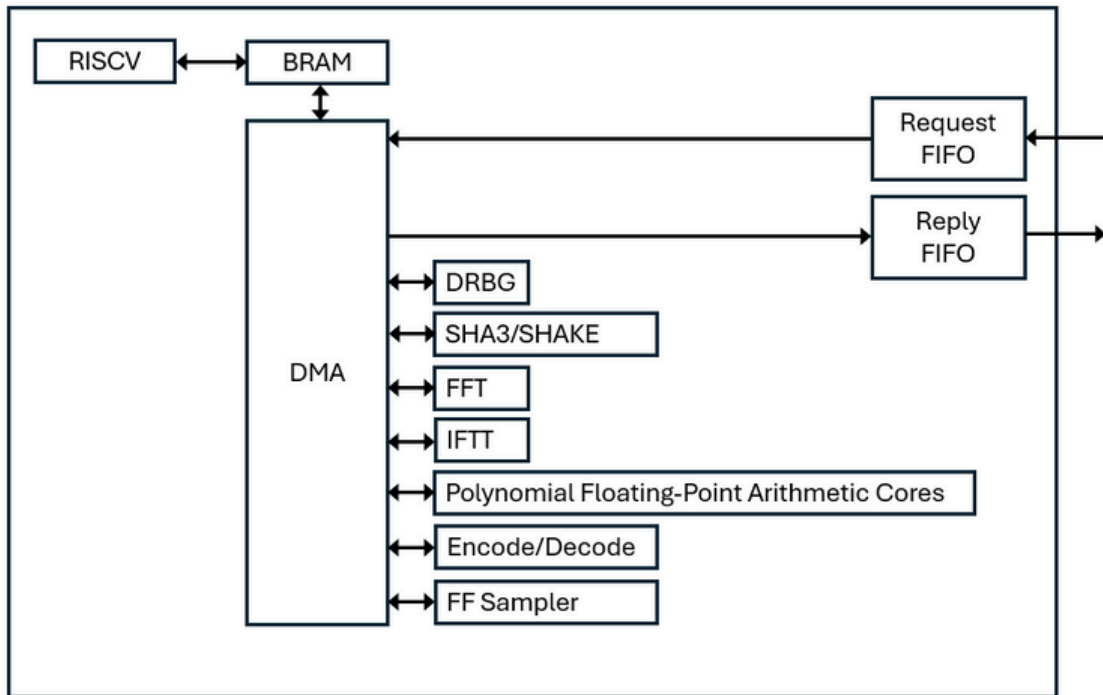March 2025

OVERVIEW

Falcon IP Core is a post-quantum digital signature algorithm (DSA). It is currently under development. It is going to be compliant with Falcon specification submitted on round 3 of NIST Post-Quantum Cryptography Standardization process. Additionally, Falcon IP Core will be enhanced to achieve compliance with NIST Falcon Standart when it is released.

DELIVERABLES

- Encrypted Netlist
- Synthesis Scripts
- Comprehensive Documentation

LICENSING

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

ORDERING

- Purchase order shall include the product number EIP-20009.

FEATURES LIST

Falcon IP Core:
- is going to support sign and verify operations
- is going to support all two Falcon modes
- has fully stallable input and output interfaces

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.

Technology Partner