

PQC1

Post-Quantum Cryptography Accelerator IP Core

Datasheet

Date: 5/20/2025

***IP CORES, INC. CONFIDENTIAL:** This document and the information contained in it are confidential, and cannot be copied or disclosed in whole or in part without the expressed written consent of IP Cores, Inc.*

Revision History

Date	Revision	Description
5/20/2025	1.1	Initial release

General Description

The PQC1 core implements ML-KEM (FIPS-203) and ML-DSA (FIPS-204) post-quantum cryptography digital signature standards. The system interface is microprocessor slave bus (APB, AHB, AXI options are available).

The design is fully synchronous and requires only minimal CPU intervention due to internal microprogramming sequencer. The sequencer also provides flexibility for the case of a change in standards. The core uses dedicated RAM for data and microprogram storage. The size of the RAM can be traded off against the performance and complexity of firmware. The minimum size is about 3.5 KB, the recommended configuration is 10.5 KB. With this memory size, the CPU operation is limited to programming the parameters and microprograms into the internal RAM and executing few microprograms for an MLDSA/MLKEM primitive.

PQC1 core is supplied as a Verilog source code thus allowing customers to carry out an internal code review to ensure its security. The core is compact (about 110K gates).

Base Core Features

Accelerates the post-quantum cryptography operations. Intended for support of ML-KEM (FIPS-203, Kyber) and ML-DSA algorithms (FIPS-204, Dilithium), with the built-in NTT and SHAKE128/SHAKE256/SHA-3 engines accessible externally.

Supports all ML-DSA algorithms defined in FIPS-204 (from Category 2 ML-DSA-44, Category 3 ML-DSA-65, Category 5 ML-DSA-87) and all FIPS-203 ML-KEM algorithms (ML-KEM-512, ML-KEM-768, and ML-KEM-1024).

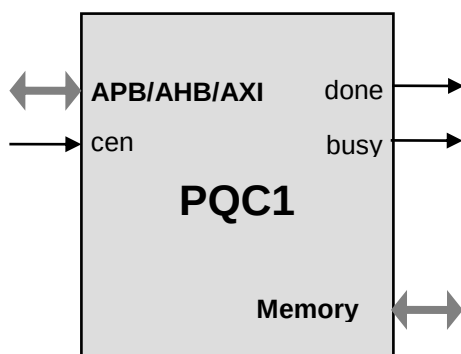
Deliverables include Verilog test bench and test vectors

Self-contained, except for the single-port external RAM banks.

An SDK is provided for software development with support for ML-DSA (key generation, signing, and signature verification) and ML-KEM (key generation, key encapsulation, and key decapsulation).

High clock rate. Timing closure at 1 GHz clock is easy, higher frequencies are possible.

Symbol



Functional Description

The core contains three accelerators:

- The number theoretic transform NTT accelerator also capable of other vector polynomial operations.
- The FIPS-202 accelerator supporting SHA-3, SHAKE128 and SHAKE256 algorithms
- The packing/unpacking accelerator that handles the key and signature formats defined by FIPS-203 and FIPS-204

True random number generator (needed for key generation or randomization of signing) is not included. The true random generator IP core TRNG1 can be used for that purpose.

Export Permits

US Bureau of Industry and Security has assigned the export control classification number 5E002 to the core. See the IP Cores, Inc. licensing basics page, <http://ipcores.com/exportinformation.htm>, for links to US government sites and more details.

Deliverables

HDL Source Licenses

- Synthesizable Verilog RTL source code
- Testbench (self-checking)
- Test vectors
- Expected results
- Software Development Kit (SDK)
- User Documentation

Performance

The numbers in the table do not include the I/O (bus) overhead.

Operation	Category	Performance, ops/sec
ML-DSA signature generation ¹	2	15,000
	3	10,000
	5	7,000
ML-DSA key generation	2	30,000
	3	20,000
	5	12,000
ML-DSA signature verification	2	33,000
	3	21,000
	5	13,000
ML-KEM key generation	1	95,000
	3	55,000
	5	35,000
ML-KEM encryption	1	65,000
	3	40,000
	5	28,000
ML-KEM decryption	1	230,000
	3	180,000
	5	145,000

Contact Information

IP Cores, Inc.

3731 Middlefield Rd.

Palo Alto, CA 94303, USA

Phone: +1 (650) 815-7996

E-mail: info@ipcores.com

www.ipcores.com

¹ Assumes an immediate success with the ML-DSA signature generation