VIC-ML-DSA-X Post-Quantum Digital Signature Core

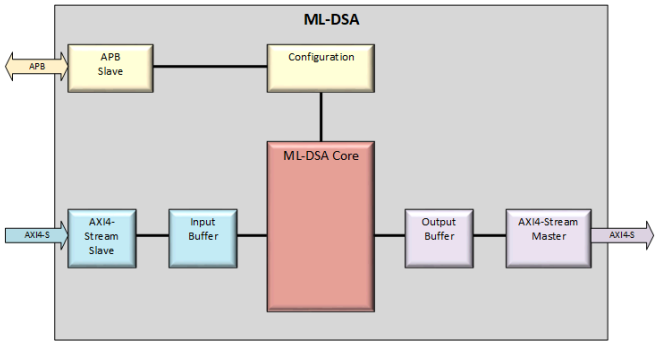
Ultra-Lean, ACVP-Verified, SCA-Protected IP Core for FIPS 204 Compliance

Overview

VIC-ML-DSA-X is a monolithic hardware IP core implementing the NIST FIPS 204 Module-Lattice-Based Digital Signature Algorithm (ML-DSA) standard for **ML-DSA-44** and **ML-DSA-65**. Built as a self-contained hardware state machine without a soft processor or external firmware dependency, it performs key generation, signing and verification in hardware.

Designed for security-sensitive IoT, automotive, industrial and space systems, the core suits signature use cases such as secure boot, firmware and bitstream signing, and update authentication.

Block Diagram



Key Features & Benefits

- **Full FIPS 204 Parameter Set Support:** Supports ML-DSA-44 and ML-DSA-65 parameter sets. A single configurable RTL core supports both parameter sets through a Verilog parameter, with the selected configuration defined at synthesis time.
- **ACVP Simulation Verified:** Successfully passes all NIST Automated Cryptographic Validation Program (ACVP) test vectors for ML-DSA Key Generation, Signature Generation, and Signature Verification in RTL simulation. *(Simulation-verified; external CAVP lab validation is separate. No CAVP certificate.)*.
- **Pure Monolithic RTL:** Self-contained hardware state machine with zero embedded CPU or firmware dependencies.
- **Standard Interfaces:** APB control interface and AXI4-Stream data interface. Verified in synchronous and asynchronous AXI modes.
- **Compact Footprint & High Clock:** Synthesizes compactly on 7-Series FPGA fabric at **8 ns (125 MHz)**.
- **Algorithmic SCA Protection:** Timing-hiding mitigation with always-on Keccak random stall injection and pre-synthesis optional constant-iteration signing flow.
- **Clean IP Provenance:** Developed in-house by Vicip with zero third-party IP dependencies.

Side-Channel Protection & Timing Hiding Architecture

1. **Keccak Time Desynchronization:** Pseudo-random cycle stall injection inside the SHAKE/Keccak sponge datapath to disrupt power and electromagnetic trace alignment across signing executions.
2. **Optional Constant-Iteration Signing Flow:** Synthesis-time option completing full signing iterations on invalid z or h checks before the next $\varkappa$ attempt to limit early-exit timing leakage.

Performance & Utilization Summary

Target: AMD/Xilinx Artix-7 200T, 125 MHz (8 ns clock period). All cycle counts include always-on Keccak random stall injection (with non-zero seed enforcement). The secret key state remains internal between KeyGen and Signature without external serialization.

Vicip Ltd.

Email: info@vic-ip.com
Website: www.vic-ip.com

Latency & Throughput

Operation	ML-DSA-44	ML-DSA-65	Notes
KeyGen (avg, N=500)	19,805 cyc (158.4 µs)	30,730 cyc (245.8 µs)	Includes internal NTT setup of s1, s2
Sign (min)	37,721 cyc (301.8 µs)	54,540 cyc (436.3 µs)	Init + one accepted iteration (min. observed)
Sign (avg, N=500)	109,564 cyc (876.5 µs)	172,779 cyc (1.382 ms)	Measured mean ~4.37/~4.85 iterations (44/65)
Verify	20,918 cyc (167.3 µs)	30,853 cyc (246.8 µs)	Valid signature
KeyGen + Sign (min)	57,526 cyc (460.2 µs)	85,270 cyc (682.2 µs)	Sum of KeyGen (avg) and Sign (min)
KeyGen + Sign (avg, N=500)	129,369 cyc (1.035 ms)	203,509 cyc (1.628 ms)	Sum of the KeyGen and Sign averages

FPGA Resource Utilization

Metric	ML-DSA-44	ML-DSA-65
Slice LUTs	18,728	18,203
LUT as Logic	18,677	18,153
LUT as Memory	51	50
Slice Registers	11,354	11,472
Slices	6,087	5,937
Block RAM Tile	10.5	11.5
DSPs	32	32
F7 / F8 Muxes	464 / 104	412 / 103
BUFGCTRL	1	1

Technical Specifications

- **Control Plane:** AMBA APB slave interface for command control, status, and runtime mode selection.
- **Data Plane:** AXI4-Stream interface for streaming seeds, keys, messages and signatures.
- **Modes:** Pre-synthesis standalone (ML-DSA-44 or ML-DSA-65).

Target Applications & Deliverables

- **Applications:** Post-quantum secure boot, automotive V2X/ECU security, industrial IoT TLS/DTLS gateways, and space/radiation-tolerant communications.
- **Deliverables:** Synthesizable Verilog/SystemVerilog RTL, self-checking ACVP simulation testbenches, and integration documentation.

Contact Vicip for evaluation licensing, ASIC target metrics, or custom parameter configurations.

Disclaimer: ML-DSA is standardized in NIST FIPS 204. This core has not been validated under the NIST CAVP. Reported cycle counts, timing and resource utilization depend on target device, speed grade and synthesis settings.