ML-KEM-X Post-Quantum Cryptography Core

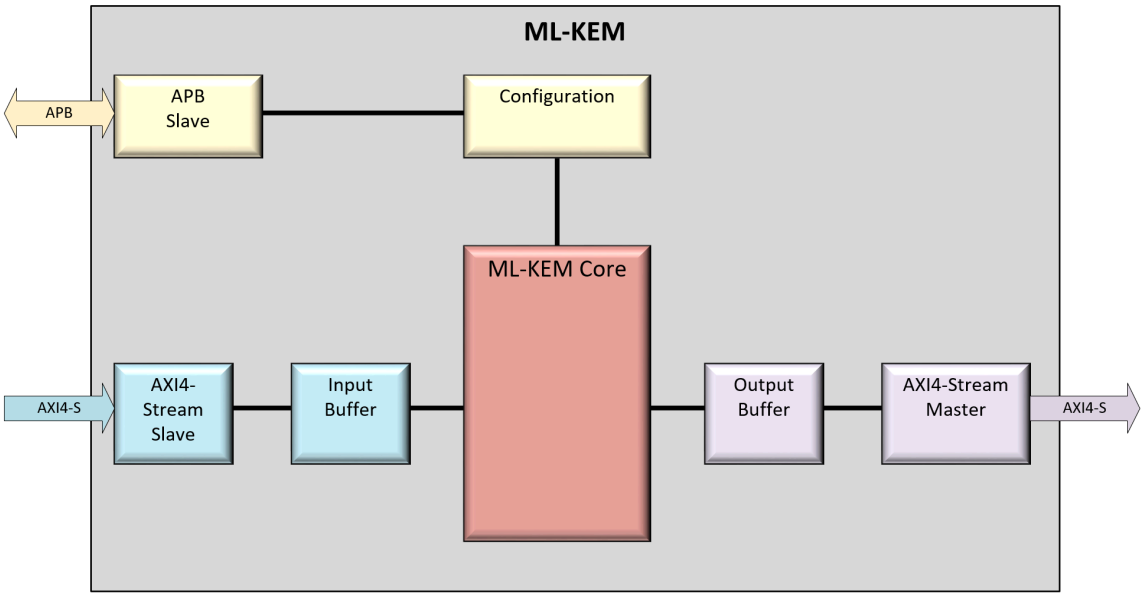
Scalable, Parameterized, ACVP-Validated Key Encapsulation IP for FIPS 203 Compliance

Overview

The **VIC-ML-KEM-X** is a highly efficient, production-ready hardware IP core implementing the ML-KEM Post-Quantum Cryptography (PQC) standard, fully compliant with the definitive NIST FIPS 203 specification.

Featuring a flexible, compile-time parameterized architecture, the core can be configured to support a single dedicated security strength or a dual-mode configuration with dynamic, software-driven runtime selection. The core accelerates the entire post-quantum public-key cryptographic loop—including Key Generation, Encapsulation, and Decapsulation—shielding communications against future quantum-tier threats while optimizing resource allocation for constraint-driven System-on-Chip (SoC) architectures.

Block Diagram



Key Features & Benefits

Feature	Benefit
Definitive FIPS 203 Compliance	Implements the finalized NIST ML-KEM standard, eliminating regulatory risk and ensuring long-term cryptographic interoperability.
Scalable Architecture Profiles	Configurable via pre-synthesis parameters to instantiate dedicated standalone hardware (512-only or 768-only) or a dynamic dual-mode configuration.
100% ACVP Validated	Proven architectures; successfully passes 100% of the official NIST ACVP internal projection vector suites across all execution paths (KeyGen, Encap, Decap) for both 512 and 768 profiles.
Ultra-Lean Footprint	Fits inside a compact 12.45k LUT envelope in the baseline configuration, leaving ample programmable logic available for application-layer circuits.
Aggressive Timing Closure	Achieves a **6.25 ns** core clock period target, allowing seamless integration into high-frequency embedded clock domains.
Native Montgomery Domain Processing	Keeps polynomial coefficients within the Montgomery domain throughout back-to-back lattice arithmetic operations (NTT/INTT), eliminating redundant reduction cycles and maximizing pipeline efficiency.
Minimal DSP Utilization	Consumes only 6 DSP blocks, meticulously optimized to preserve scarce math tiles on budget-sensitive target FPGAs.
Side-Channel Analysis (SCA) Defense	Features advanced, localized temporal jitter mitigation within the underlying Keccak (SHA3/SHAKE) processing engines to counter non-invasive physical attacks.
Full Subsystem Monolithic Core	Combines KeyGen, Encap, and Decap into a single tightly coupled state machine, minimizing integration complexity and processor interaction.
Standardized SoC Interfaces	Packaged with industry-standard control and data interfaces to optimize bus mapping, processor offloading, and standard DMA controller pairing.

Configuration Flexibility

The VIC-ML-KEM-X core features a flexible, pre-synthesis configuration architecture that allows you to optimize the hardware footprint based on your exact application needs. The core can be delivered in three operational modes:

- **Dedicated ML-KEM-512 Mode:** Fully optimized for baseline post-quantum security, delivering the smallest possible silicon and memory footprint.
- **Dedicated ML-KEM-768 Mode:** Hardwired for standalone mid-tier quantum security where baseline support is not required.
- **Dynamic Dual-Mode:** Instantiates a versatile engine supporting **both**

ML-KEM-512 and ML-KEM-768, dynamically switchable at runtime via software configuration registers over the APB control plane.

Performance & Utilization Summary

The following resource utilization and performance metrics represent an optimized implementation targeted for entry-level, low-power FPGA architectures (e.g., AMD/Xilinx 7-Series) configured for the baseline **ML-KEM-512** profile.

Resource Type	Utilized
Slice LUTs	12,452
Slice Registers	8,455
Dedicated DSP Blocks	6
Internal RAM / Block RAM	4.8 kB 4.5 BRAM
Clock Period / Frequency	6,25 ns 160 MHz

Cryptographic Operation	Execution Cycles/Time
Key Generation	10,560 cycles 66 µs
Encapsulation	14,240 cycles 89 µs
Decapsulation	19680 cycles 123 µs

Technical Specifications

Control & Data Plane Interfaces

- **Control Plane (APB Slave):** Industry-standard Advanced Peripheral Bus (APB) interface for command submission, interrupt handling, execution mode selection, and core status monitoring.
- **Data Plane (AXI4-Stream):** Decoupled, high-throughput streaming interface for loading seed parameters, public keys (*ek*), private keys (*dk*), and offloading resulting ciphertexts (*c*).

Typical Use Cases

- **Post-Quantum Secure Boot:** Validating or generating epistemic root key exchanges during low-power processor boot sequence steps.
- **Automotive MCU Security:** Securing critical V2X communications and Electronic Control Unit (ECU) gateways against quantum-era interception.
- **Industrial IoT Gateways:** Compact edge hardware acceleration allowing small, battery-operated units to securely establish TLS/DTLS sessions using post-quantum key exchanges.

- **Space-Grade Protocol Integration:** Fits the ultra-tight logic boundaries of radiation-tolerant FPGAs, enabling low-power CubeSats and deep-space communication payloads to mitigate "Harvest Now, Decrypt Later" vulnerabilities over open RF downlinks.

Why Choose This IP Core?

1. **Production Ruggedness:** Validated down to the single bit against the comprehensive NIST ACVP projection profiles, removing verification overhead from your engineering timeline.
2. **Pure Monolithic Hardware RTL:** Unlike ultra-small alternative cores that require integration with an external microcontroller or a hidden RISC-V processor to function, the VIC-ML-KEM-X is entirely self-contained. It requires no secondary CPU toolchains, firmware management, or complex processor integrations, delivering up to 50x faster execution times via dedicated hardware state machines.
3. **Clean Provenance and Zero Third-Party IP:** Built 100% from the ground up by Vicip. The entire architecture contains no third-party code, open-source wrappers, or black-box components. This guarantees full design transparency for security audits, simplifies export compliance, and allows Vicip to provide unambiguous legal IP indemnification.
   Rigorous Verification: Core functionality and timing boundaries fully verified through comprehensive post-synthesis Gate-Level Simulations (GLS).
4. **SCA Awareness:** By protecting the high-risk symmetric primitives (Keccak/SHAKE) with temporal defenses, the design mitigates early leakage threat profiles.

Getting Started

Vicip delivers the complete, synthesizable RTL source code package (Verilog/SystemVerilog), an automated self-checking simulation verification environment mapping to the official FIPS 203 internal vector sets, gate-level simulation scripts, and comprehensive software/hardware integration guides.

Contact us today to receive evaluation licensing details, specific node synthesis results, or customized configurations to license the VIC-ML-KEM-X IP core.

Disclaimer: *ML-KEM is a NIST-standardized algorithm. This IP core is a hardware implementation of that algorithm. Performance and utilization figures are representative and will vary based on target technology, synthesis tools, and configuration settings.*