KiviPQC™-KEM

ML-KEM Key Encapsulation IP Core

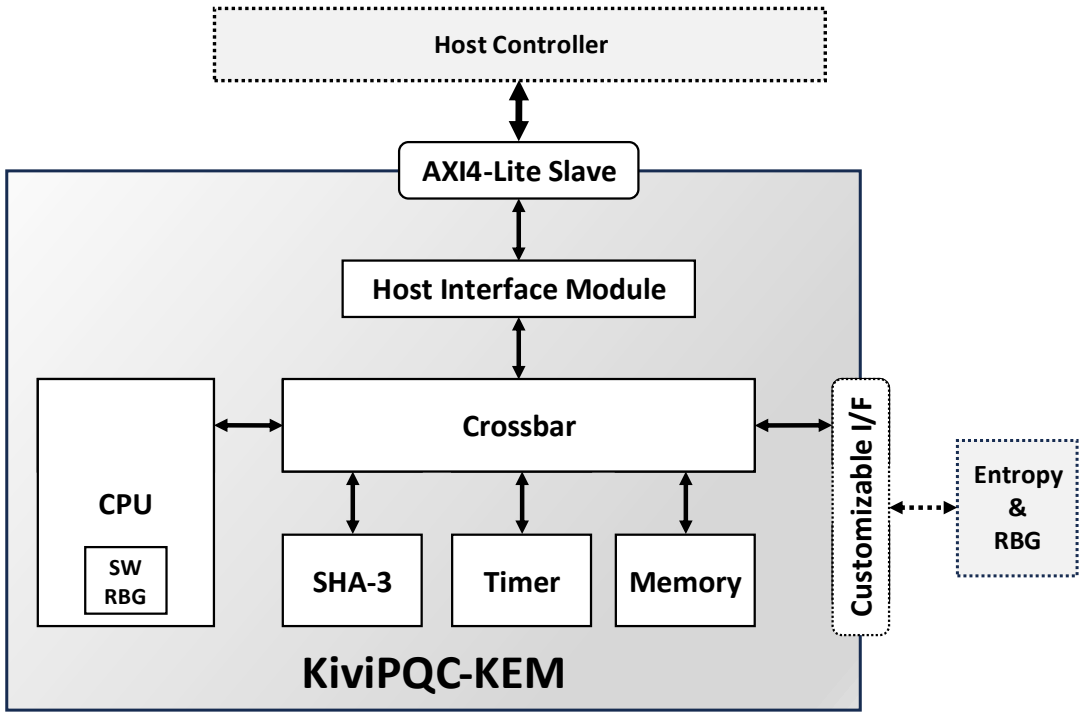
altera™ An Intel Company

The KiviPQC™-KEM IP core is a hardware accelerator for post-quantum cryptographic operations. It implements the Module Lattice-based Key Encapsulation Mechanism (ML-KEM), standardized by NIST in FIPS 203. This mechanism realizes the appropriate procedures for securely exchanging a shared secret key between two parties that communicate over a public channel using a defined set of rules and parameters. The KiviPQC™-KEM IP core supports key generation, encapsulation, and decapsulation procedures, making it suitable for both (client/server) sides of key exchange.

The solution supports all three parameter sets for ML-KEM, i.e. ML-KEM-512, ML-KEM-768, and ML-KEM-1024. It is based on a RISC-V-like SoC topology and includes a 32-bit RISC-V based processor. The resulting shared key is of 32 bytes. Beyond that, the main components of the core are a SHA-3 cryptographic hash accelerator, a hardware timer module, and a crossbar interconnect module for internal data routing. The communication with the host is accomplished by a Host Interface Module handling specific control and data flow, connected with an AMBA® AXI4-Lite slave port. Finally, the core is currently offered with a software implementation of a Random Byte Generator (RBG). Moreover, it is able to be integrated with an external (third-party) entropy source and RBG, via a fully customized interface, depending on the entropy/RBG selection.

The KiviPQC™-KEM IP core provides hardware acceleration for computationally intensive operations while maintaining a small footprint and can be integrated into any system-on-chip (SoC) for ASIC or FPGA implementation. Beyond that, it combines a minimal attack surface with modest resource requirements for future-proof and quantum-safe systems.

Block Diagram



FEATURES

NIST FIPS Compliant

- Module Lattice-based Key Encapsulation Mechanism (ML-KEM)
  - NIST FIPS 203
- All three ML-KEM parameter sets
  - 512 / 768 / 1024

Enhanced Security

- Self-contained engine with a minimal attack surface
- Protection against timing-based side channel attacks

Resource-efficient Acceleration

- Hardware offloading and acceleration of time-consuming PQC operations
- Minimal logic utilization

Straightforward SoC Integration

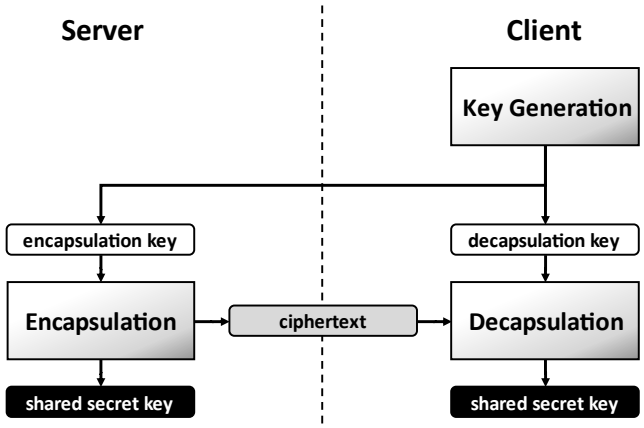
- Lightweight, simple-control AMBA® AXI4 Interface
- Re-usable design, LINT-clean

Deliverables

- RTL source code (System Verilog)
- HAL and drivers for integration
- Complete testbenches
- Simulation and synthesis scripts
- Documentation

Applications

The core realizes a quantum-safe exchange of a shared secret key between two parties (client and server) communicating over a public channel. During the key sharing, the client generates a decapsulation key and an encapsulation key, keeps the first as private and sends the second as public to the server. The server generates a copy of the shared key and an associated ciphertext using the client's encapsulation key and sends it to the client. Finally, the client generates a copy of the same shared key using the ciphertext received from the server and the kept private decapsulation key.



The KiviPQC™-KEM IP core offers quantum-resistant security for a wide range of applications. In public-key infrastructure and cloud security, it ensures long-term confidentiality and integrity for sensitive information. It can play a vital role in safety-critical infrastructure and networks, safeguarding communication and exchange channels from potential threats. In the realm of secure IoT device communication, the core provides strong cryptographic support to protect shared secret keys. Additionally, it is well-suited for hardware security modules (HSMs) and Trusted Platform Modules (TPMs), enhancing secure key management and cryptographic processing. Its capabilities extend to supporting MACsec key agreement (MKA) protocols for secure Ethernet communications, Internet Key Exchange (IKEv2) protocols, strengthening VPN and secure network authentication mechanisms, and edge computing.

Implementation Results

The KiviPQC™-KEM core can be mapped to any Altera® FPGA device (provided sufficient silicon resources are available). The following are sample results, for ML-KEM-512 FIPS-203 parameter, with all core I/Os assumed to be routed on-chip.

Family (Speed Grade)	Logic Resources	Memory Resources	Frequency
Agilex 7 (-2)	14,796 ALMs	72 RAMB18	230 MHz
Arria 10 (-2)	7,839 ALMs	72 RAMB18	115 MHz
Cyclone 10 GX (-5)	7,977 ALMs	72 RAMB18	154 MHz
Stratix 10 (-3)	14,065 ALMs	72 RAMB18	143 MHz

The provided figures do not represent the highest speed or smallest area possible for the core. Please contact CAST to get characterization data for your target configuration and technology.

Related Products

SHA-3 Secure Hash Crypto Engine is also available from CAST as a stand-alone core.

Support

The core as delivered is warranted against defects for ninety days from purchase. Thirty days of phone and email technical support are included, starting with the first interaction. Additional maintenance and support options are available.

Export Permits

This core implements encryption functions and as such it is subject to export control regulations. Export to your country may or may not require a special export license. Please contact CAST to determine what applies in your specific case.

Deliverables

The core is available in RTL (System Verilog) source code, or as a targeted FPGA netlist. Its deliverable package includes the following:

- Self-checking HDL testbench
- Hardware Abstraction Layer (HAL) and driver for the application processor
- Sample simulation & synthesis scripts
- User documentation