NEWS

KiviCore and CAST Release Post-Quantum Cryptographic Key Encapsulation IP Core

Offers future-proof security to ensure the integrity and confidentiality of communication networks against quantum computer-based attacks

Dresden, Germany and Woodcliff Lake, New Jersey — March 19, 2025 — Cryptographic solutions expert KiviCore and semiconductor intellectual property provider CAST today announced the release of a new post-quantum cryptographic IP core, the KiviPQC™-KEM ML-KEM Key Encapsulation IP Core. It enables the quantum-safe exchange of a shared secret key between two parties communicating over a public channel through a hardware implementation of the NIST-FIPS 203 standard Module-Lattice Key Encapsulation Mechanism (ML-KEM).

As quantum computers move closer to reality, traditional cryptographic systems are facing significant new security risks. With this new core the companies are tackling this challenge head-on, enabling system architects to design future-proof systems that are protected against the cryptography-breaking threat of quantum computers.

About the KiviPQC-KEM IP Core

The KiviPQC-KEM ML-KEM Key Encapsulation IP Core is a standalone hardware acceleration engine that efficiently executes the ML-KEM secret key generation, encapsulation, and decapsulation procedures defined by NIST in FIPS 203. It supports all three ML-KEM parameter sets — ML-KEM-512, ML-KEM-768, and ML-KEM-1024 — and generates a 32-byte shared key.

The self-contained, highly secure core presents a minimal attack surface, with built-in protections against timing-based side channel attacks. It includes a RISC-V processor for efficiently handling the computationally intensive key encapsulation operations without relying on a system's CPU. A simple standard AMBA® AXI4 control interface eases system-on-chip integration.

— more —

The core is remarkably resource-efficient, requiring a modest silicon footprint in ASICs or FPGAs. (See representative performance and hardware implementation results in the product brief.) It is suitable for a wide range of applications, including ensuring public-key infrastructure and cloud security, protecting safety-critical infrastructures and networks, and cryptographic support for IoT device communication.

“KiviPQC-KEM represents a crucial step toward preparing systems for the quantum era. By focusing on resource-efficiency and value, we are enabling companies to adopt post-quantum security solutions without compromise. This first product in the KiviPQC family underscores our commitment to securing the future of communication systems.” said Frank Deicke, CEO at KiviCore.

“Many CAST customers are already looking ahead to the post-quantum computing world and count on us to help them cope with PQC challenges by expanding our point and system security IP line,” said George Athanasiou, security product manager at CAST. “The experts at KiviCore are doing significant work and we are excited to start bringing their very competitive PQC solutions to the wide global market.”

The KiviPQC-KEM ML-KEM Key Encapsulation IP Core is available now in RTL for ASICs and FPGAs or as optimized netlists for FPGAs. Licensing is available with flexible options for single or multi-project licenses and evaluation. To learn more, visit the product page, then contact CAST Sales to discuss the flexible licensing options or arrange an evaluation.

About KiviCore:

KiviCore GmbH is an IP core and solution provider specializing in the development and integration of cutting-edge hardware and software co-designs. The company delivers secure, efficient, and high-performance solutions based on classical and post-quantum cryptographic algorithms that seamlessly integrate into FPGA and ASIC-based systems. Learn more by visiting www.kivicore.com.

About CAST

Computer Aided Software Technologies, Inc. (CAST) is a silicon IP provider founded in 1993. The company's ASIC and FPGA IP product line includes microcontrollers and processors; compression engines for data, images, and video; interfaces for automotive, aerospace, and other applications; various common peripheral devices; and comprehensive SoC security modules. Learn more by visiting www.cast-inc.com.

# # #

Media Contact: Artemis Couroupaki, a.couroupaki@cast-inc.com