NEWS

CAST

CAST to Enter the Post-Quantum Cryptography Era with New KiviPQC-KEM IP Core

New core combines KiviCore research and development expertise with CAST quality and usability standards for a better PQC IP experience

Woodcliff Lake, New Jersey — January 16, 2025—CAST, a leading semiconductor intellectual property (IP) core provider, is excited to announce the upcoming release of its new *KiviPQC™-KEM IP* core and invites early adopters to engage in product evaluations. This new IP core implements the Module-Lattice Key Encapsulation Mechanism (ML-KEM) as specified in the NIST FIPS 203 standard, and is CAST's first product leveraging the power of the NIST-standardized post-quantum cryptography (PQC) algorithms to secure future SoC designs.

Overview of the *KiviPQC-KEM IP Core*

Designed by cryptographic solutions expert KiviCore, the new core efficiently handles secret key generation, encapsulation, and decapsulation using any of the ML-KEM variants provisioned by the NIST standard. The core's key features are:

- **Secure-by-Design**: Operates as a self-contained engine, with minimal attack surface and optional protection against time-based side-channel attacks (SCA);
- **Configurable Performance**: The hardware accelerated operation can be tuned to meet the performance, latency, and silicon resources needs of different applications; and
- **Easy-to-integrate**: Employs industry-standard AMBA® hardware interfaces and provides a comprehensive software API.

The core conforms to CAST's stringent design and verification standards, is supported by CAST's 24/7 support infrastructure with access to the core's

— more —

developers, and is available with CAST's flexible licensing schemes. It thus delivers PQC cryptography with CAST's promise for a Better IP Experience.

Potential applications of the KiviPQC-KEM IP core include data communication connections with the MACSec and CANSec cores also offered by CAST, as well as IPSec, Transport Layer Security (TLS), and many other protocols.

Ready for Early Adopters

"We have managed to implement the secure key management functions needed for the post-quantum computing era in a high-quality IP core with a focus on resource efficiency, simplicity, and seamless integration," said Frank Deicke, KiviCore co-founder. "One of the earliest — and we believe the most reliable yet flexible — such IP cores available, this first in our KiviPQC series will dramatically simplify cryptographic system development in many fields."

The KiviPQC-KEM IP is expected to meet product-level verification and quality assurance goals and be ready for customer release within the first quarter of 2025. Meanwhile, early adopters are invited to contact CAST (info@cast-inc.com) to evaluate the KiviPQC-KEM core using a readily available FPGA-based reference design.

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.

# # #

CAST is a trademark of Computer Aided Software Technologies Inc. KiviPQC is a trademark of KiviCore GmbH. Other trademarks are the property of their respective owners.

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