NEWS

CAST Partners with KiviCore for Post-Quantum Cryptography

Upcoming IP cores for hardware crypto engines will help developers defend systems against attacks from future quantum computers.

Woodcliff Lake, New Jersey — **October 15, 2024**—Semiconductor intellectual property provider CAST and classical and post-quantum cryptographic solutions developer KiviCore today announced they are partnering to deliver IP cores for post-quantum cryptographic hardware engines.

The emerging post-quantum cryptography (PQC) field focuses on secure data solutions able to withstand attacks from the large-scale quantum computers now on the horizon. While traditional cryptographic methods essentially rely on the difficulty of solving mathematical problems—which won't be difficult at all for quantum computers—PQC researchers are instead developing new cryptographic algorithms believed to be resistant to quantum computer attacks.

KiviCore was founded in 2023 by R&D engineers and managers from Fraunhofer IPMS. The company already offers IP cores for SHA-3 crypto and Keccak hash hardware engines and expects to begin delivering PQC cores later this year. KiviCore has selected CAST to lead marketing and sales efforts and handle front-line support for the upcoming PQC IP cores.

KiviCore
Secure Solutions

"Having worked with the CAST team for years in a past life, we are fully confident that they are the best partners to help KiviCore bring the benefits of post-quantum cryptography to system developers in many industries," said Frank Deicke, KiviCore

— more —

co-founder. “Our research is breaking new ground with PQC, and CAST is among the best at providing practical, reliable IP cores for exciting new technologies like this.”

“Many savvy CAST customers are already looking ahead to their next projects, and this partnership with KiViCore gives us a solid pathway for helping those customers secure their systems in the challenging post-quantum days ahead,” said Nikos Zervas, chief operating officer for CAST.

Potential PQC customers should contact CAST (info@cast-inc.com) to discuss their anticipated requirements and get updates on expected late 2024 first PQC IP core delivery dates.

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.

About KiviCore

KiviCore 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.

###

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