CAST adds Ascon Lightweight Encryption Engine to Security IP Cores Line

The new core is one of the smallest and fastest Ascon hardware cryptographic engines available for ASICs and FPGAs

Woodcliff Lake, New Jersey — **September 11, 2023** — Semiconductor intellectual property provider CAST today announced the availability of an ASIC and FPGA IP core that implements the Ascon lightweight encryption standard recently adopted by the National Institute of Standards and Technology (NIST).

The new **ASCON-F** Ascon Authenticated Encryption & Hashing Engine core provides a competitively small and fast hardware engine for the lightweight security functions detailed in the Ascon v1.2 specification. Its lean standard version supports Ascon-128 and -128a, the primary AEAD (authenticated encryption with associated data) cryptographic functions. It also supports Ascon-Hash and -Hasha, the algorithm's primary hash functions. Support for Ascon-80pq, Ascon-Xof, and Ascon-Xofa is also available when designers require these. The company will extend the core for additional Ascon algorithms when they are added to the standard.

The core's lightweight security functions use minimal resources while adequately protecting miniature and short-lived devices. Applications include embedded medical devices, intelligent lightbulbs, and RFID tags; these need some security but don't need protection from quantum computing or other severe attacks.

"With security consciousness growing worldwide, our encryption core customers have been asking for a way to build protection into edge devices and other products where the hardware resources for AES or SHA just aren't available," said Newton Abdalla, security product manager for CAST. "Ascon gives them the ideal security/hardware trade-off, plus this new core offers some of the best Ascon performance per silicon area available today."

Engineered by long-time partner Ocean Logic, the new ASCON-F core requires approximately 11,000 ASIC gates and can run at more than 2 GHz in modern ASIC technologies. Its throughput is remarkably high, processing for example Ascon-128a

— more —

at 16 bits/cycle. Also available for FPGAs, it typically uses just 1,200 LUTs or ALMs and runs at 500 MHz on mid-range devices from popular FPGA providers.

The new ASCON-F IP core is available now. It joins the security primitives CAST has already shipped to hundreds of customers, including multiple NIST-certified AES encryption and decryption cores, SHA hashing engines, and more. Visit the website or contact CAST Sales (info@cast-inc.com) for more information.

About CAST

Computer Aided Software Technologies, Inc. (CAST) is a silicon IP provider founded in 1993 and celebrating its 30th anniversary this year. CAST'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. All conform to CAST's strict quality standards for design, verification, and productization. Together with CAST's responsive technical support, this ensures that designers using IP from CAST enjoy *A Better IP Experience*. Learn more by visiting www.cast-inc.com.

# # #

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