

CAST and Achronix Expand Partnership to Deliver Secure FPGA Solutions

Woodcliff Lake, New Jersey — March 1, 2022 — Semiconductor intellectual property provider CAST and fabless semiconductor firm Achronix Semiconductor Corporation have worked together to integrate CAST's encryption technology into the Achronix Speedster7t FPGA devices.

The partnership expands on the [concurrent use](#) of data compression IP from CAST that enables the high-speed FPGA performance Achronix delivers. The security capability built into select Achronix Speedster7t FPGAs employs a version of CAST's [Authenticated](#)

[Encrypt/Decrypt Engine IP Core](#) (AES-GCM) with a high-performance architecture. This enables 128-bit data encryption without impacting Speedster7t FPGAs' high throughput and low latency.

"After evaluation of several security IP solutions, we selected CAST because of their small footprint and high performance," said Steve Mensor, vice president of marketing at Achronix. "It has enabled us to expand our addressable markets for designs that require high-performance, in-line encryption capabilities. The AES IP core meets our challenging security and performance requirements while the CAST team continues to prove themselves with high-quality products and excellent IP support services."

About the AES Encryption Feature

Part of CAST's broad [Encryption Primitives](#) family, the AES-GCM IP core implements 128-bit Rijndael encoding and decoding using the Galois Counter authenticate-and-encrypt block cipher mode.



The core is certified by the US National Institute of Standards and Technology (NIST) as complying with NIST's Federal Information Processing Standard (FIPS) Publication 197 and successive Special Publications. Versions of the core are available optimized for small silicon area, high performance, or exceptional throughput.

The AES IP core powers a cryptographic engine within select Achronix Speedster7t FPGAs family members. Speedster7t FPGAs, with industry-leading features such as a 20Tbps 2D NoC, 4Tbps of GDDR6 memory, PCIe Gen 5 and 400GbE, are high-bandwidth, low latency devices suitable for a wide variety of applications. The AES encryption and decryption capabilities support the increasing concern for security and growing requirements for end-to-end encryption in many systems, with performance and throughput that complement the Speedster7t FPGA capabilities.

About Achronix

Achronix Semiconductor Corporation is a fabless semiconductor corporation based in Santa Clara, California, offering high-end FPGA-based data acceleration solutions, designed to address high-performance, compute-intensive and real-time processing applications. Achronix is the only supplier to have both high-performance, high-density standalone FPGAs and licensed eFPGA IP solutions. Achronix [Speedster®7t FPGA](#) and [Speedcore™ eFPGA](#) IP offerings are further enhanced by ready-to-use [VectorPath® accelerator cards](#) targeting AI, machine learning, networking, and data center applications. All Achronix products are fully supported by the [Achronix Tool Suite](#), which enables customers to quickly develop their own custom applications.

About CAST

Computer Aided Software Technologies, Inc. (CAST) is a global firm providing reusable silicon IP since 1997. In addition to the AES and other encryption cores, CAST's ASIC and FPGA IP product line includes RISC-V and other microcontrollers and processors; data, video, and image compression engines; interfaces for automotive, aerospace, and other applications; various common peripheral devices; and comprehensive SoC security modules. Learn more by visiting www.cast-inc.com.

Achronix, Speedster is a registered trademark of Achronix Semiconductor Corporation.

CAST is a trademark of CAST, Inc.

Other trademarks are the property of their respective owners.

###

Media Contact:

Artemis Couroupaki, a.couroupaki@cast-inc.com