CAST NEWS

AES Encryption IP Cores from CAST Receive NIST Certification

Commercially proven AES encryption and decryption engines now certified to meet standard for function and interoperability

Woodcliff Lake, NJ — October 24, 2019 — Semiconductor intellectual property (IP) provider CAST, Inc. today announced that its IP cores for AES encryption have received certification from the US National Institute of Standards and Technology (NIST) as being in compliance with NIST's Federal Information Processing Standard (FIPS) Publication 197 and successive Special Publications.

Since 2001 when NIST first adopted it, AES, the Advanced Encryption Standard, has been the de facto standard for strong data protection. The FIPS conformance of CAST's cores was tested by an independent laboratory, and the results reviewed and approved by NIST, which granted the AES certification.

"Our encryption cores are already proven in shipping products by several dozen customers, but this NIST certification provides an additional guarantee of reliability and interoperability make these AES cores even more competitive with the best available crypto engines," said CAST CEO Nikos Zervas.

About the Certification

The AES cores are sourced from partner Ocean Logic (www.ocean-logic.com). They have been certified for the six main AES confidentiality encryption modes—Electronic Code Book (ECB), Cipher Block Chaining (CBC), Output Feedback (OFB), Cipher Feedback (CFB), Counter (CTR), and XTS-AES—and the primary AES combination modes—Counter with CBC-MAC (CCM) and Galois/Counter (GCM)—plus the Liskov-Rivest-Wagner (LRW) mode.

The AES cores were certified for all three possible encryption key sizes—128-bit, 192-bit, and 256-bit—except for the XTS-AES, which only supports 128- and 256-bit keys.

The 256-bit SHA cryptoprocessor (SHA-256) offered by CAST and sourced from Ocean Logic also successfully underwent NIST certification.

Review these NIST certification details at CAST's Cryptographic Algorithm Validation Program entry.

— *more* —

About the IP Cores

CAST offers several fixed and programmable AES IP cores that produce hardware encryption and decryption engines with a range of features, performance, and silicon characteristics to suit a variety of applications. These and the SHA 256-bit Cryptoprocessor Core are part of the company's Security IP family, which also includes other encryption primitives and the GEON Security Platform, a solution for complete system-on-chip (SoC) protection.

The Security cores are in turn part of CAST's broader IP portfolio, including 32- and 8-bit processors; hardware compression/decompression engines for data, images, and video; and numerous interfaces and peripherals. Learn more about CAST's complete line of IP by visiting www.cast-inc.com, emailing info@cast-inc.com, or calling +1 202.891.8300.

CAST, Inc., 50 Tice Blvd, Suite 340, Woodcliff Lake, NJ 07677 USA • phone: +1 201.391.8300

# # #

Media Contact: Paul Lindemann, Montage Marketing, paul@montmark.com, +1 603.490.4985