Accelerate SHA-3 Cryptographic Hash Processing with New Hardware IP Core

WOODCLIFF LAKE, NEW JERSEY — October 5, 2016 — A new intellectual property core supports the latest standard for protecting the integrity of electronic transmissions, Secure Hash Algorithm-3 (SHA-3), in a flexible, high-throughput, area-efficient hardware accelerator.

Developed by Beyond Semiconductor and available from CAST, Inc., the new IP core is compliant with the latest cryptographic standard from the National Institute of Standards and Technology (NIST)—FIPS 202—and the SHA-3 functions in FIPS 180-4.

One of the few IP cores supporting these standards, it offers competitively high throughput—up to 48 Mbits/MHz—and low silicon area—as small as 28K gates.

“Our hardware implementation of the SHA-3 algorithm gives developers a state-of-the-art cryptographic primitive with which they can harness the advantages of hardware-based security to protect their devices against current and future threats,” said Matjaž Breskvar, chief executive officer of Beyond Semiconductor. “While simply implementing cryptographic primitives is not enough to ensure device security, our efficient hardware implementation of the Keccak sponge function family presents a solid foundation for any secure, future-proof design.”

Designers can configure the new SHA-3 Secure Hash Function Core to provide an optimum solution for a variety of application challenges. The hash accelerator can implement any one of the fixed-length or Extendable Output (XOF) hashing functions that are provisioned by the standards: SHA3-224, SHA3-256, SHA3-384, SHA3-512, SHAKE-128, and SHAKE-256. Users can also trade off performance and silicon area in two ways: by opting for a sophisticated input buffering scheme that allows receiving the next input message while the previous message is being processed, and by altering the number of hashing rounds per clock.

“Developers wishing to build the most secure, future-looking security into their devices and systems will want to consider using SHA-3,” said Nikos Zervas, chief executive officer for CAST. “This new core makes it easy to integrate SHA-3 hashing into a variety of products with aggressive performance and low-power requirements, and adds a new choice to our encryption cores family that helps developers boost security without requiring extensive cryptography knowledge.”

— more —

Availability and Licensing

The new SHA-3 core is available now in synthesizable RTL for ASICs or optimized netlists for FPGAs. Visit the CAST website (www.cast-inc.com) to learn more, then contact CAST to arrange an evaluation or discuss licensing (info@cast-inc.com, +1 201.391.8300).

To learn more about Beyond Semiconductor, visit www.beyondsemi.com, call +1 650.488.7413, or email info@beyondsemi.com.

About Secure Hash Algorithm-3

While the SHA-2 standard continues to be secure and is safe to use, NIST believes that SHA-3 provides a greater degree of future proofing against attacks. NIST began the search for a new hashing function algorithmically dissimilar to SHA-2 with the launch of an international competition in 2005. Of the 64 submissions, the winning algorithm, Kacaak, became the basis for the FIPS 202 SHA-3 standard. The new standard was approved on August 5, 2015.

Like other hash functions, fixed-length SHA-3 functions convert a digital message into a brief, fixed-length “message digest” that can act as a digital signature. Any change in the original message results in an easy-to-detect change in the digest, offering a degree of protection against purposeful or accidental modifications of the message. Hashing thus provides security for message authentication, and a check for data integrity in many electronic communication applications. The extendable-length XOF SHA-3 hashing functions allow developers to use these SHAKE algorithms as encryption ciphers, or as part of key derivation functions.

Because SHA-3 by design runs much more efficiently in hardware than other hashing functions, this new standard is considered an excellent choice for Internet of Things and other devices needing inexpensive, low-power circuitry but a high degree of security.

CAST, Inc., 50 Tice Blvd, Suite 340, Woodcliff Lake, NJ 07677 USA • phone: +1 201.391.8300
Beyond Semiconductor, Brnčičeva ulica 41G, SI-1231 Ljubljana-Črnuče, Slovenia • phone: +386 5 90 90 100

# # #

Media Contacts:
Nikos Zervas, CAST, Inc. +1 201.894.5511, n.zervas@cast-inc.com,
Paul Lindemann, Montage Marketing, +1 603.490.4985, paul@montmark.com
Katarina Nahtigal, Beyond Semiconductor, +386 5 90 90 110, katarina.nahtigal@beyondsemi.com