CAST Deciphers Security System Design Challenges with New AES Encryption IP

Woodcliff Lake, NJ, December 3, 2008 — Silicon Intellectual Property (IP) provider CAST, Inc. today announced a new family of AES IP cores that make it easier for designers to include fast hardware encryption in security-sensitive electronic systems.

AES — the Advanced Encryption Standard — is the cryptographic algorithm mandated by US government agencies and used extensively to protect data around the world. The new CAST IP covers a range of AES requirements by offering a programmable, multi-purpose encrypt/decrypt core and a leaner pre-configured core with versions optimized for specific applications.

The CAST AES cores are available now, for either ASICs (HDL source code) or FPGAs (netlists). An introductory discount of 20% is available through the end of the year (December 31, 2008).

"With five years experience working with AES IPs and helping eighty-some customers use encryption cores successfully, we've never seen AES products as efficient, flexible, and easy to integrate as this latest generation," said Hal Barbour, president of CAST, Inc., "The special 20% discount makes these cores a real bargain for design teams that can order by December 31."

About AES Encryption

The Advanced Encryption Standard (AES) is an implementation of the Rijndael block cipher encryption algorithm. In 2001 the US National Institute of Standards and Technology (NIST) approved it as Federal Information Processing Standard Publication 197 (FIPS 197).

The algorithm accepts a block of input data, processes it using a supplied encryption key, and outputs a block of encrypted data. (Decryption works in the reverse, using the same key.) Longer key lengths make the encryption more secure, and various cipher modes can modify the operation of the basic algorithm. AES can be executed in software, but hardware-based AES is generally required for real-time data encryption or decryption.

Learn more about AES including an explanation of its cipher modes and hardware design issues in a white paper at www.cast-inc.com/encryption.

– more –

CAST's New AES IP Cores

The new AES core family was developed by long-time CAST partner Alma Technologies S.A., in Greece. Two basic products cover a broad range of user requirements for silicon area, transmission bit rate, power consumption, and degree of encryption protection:

- The AES-P programmable core offers multi-use flexibility in a single module, with built-in support for all five common block cipher modes (ECB, CBC, CFB, OFB, and CTR) and real-time switching among them as needed.

- The AES-C codec core offers a leaner implementation, requiring half the chip area with better performance but supporting just one block cipher mode (selected prior to synthesis).

An efficient design allows each core to handle both encryption and decryption as needed, simplifying system integration. Each can also be real-time switched to use 128-, 192-, or 256-bit long encryption keys, trading off quicker processing with greater protection.

Two architectural options are available for each core: one uses a 32-bit data path so it requires less chip area and needs 44 clock cycles for AES processing (with a 128-bit key); the other uses a 128-bit data path so it is a little larger but only needs 11 clock cycles.

CAST believes the cores yield implementation results and data transmission rates (throughput) as good or better than competing products. Multiple ASIC and FPGA implementation statistics are readily available on the CAST website; representative ASIC and FPGA results follow.

Core	Technology	Data Path Architecture	Approx. Area	Frequency	Throughput
AES-P	ASIC TSMC 90-nm	128-bit	12K Gates	500 MHz	5.82 Gbps
	Altera Stratix-III	128-bit	2,133 ALUTs, 22 M9K	186 MHz	2.16 Gbps
	XIlinx Virtex-4	128-bit	1,280 Slices, 10 BRAM	192 MHz	2.23 Gbps
AES-C	ASIC TSMC 90-nm	32-bit	5K Gates	500 MHz	1.45 Gbps
	Altera Stratix-III	32-bit	630 Slices, 6 M4k	208 MHz	693 Mbps
	XIlinx Virtex-4	32-bit	415 Slices, 3 BRAM	188 MHz	545 Mbps
Configuration Notes: 128-bit key; Key Expander not included; SRAM and ROM memories not included; synthesis optimized for speed. Throughput is for ECB mode.					

An optional Key Expander module automatically generates and stores internal key values in real time as needed by each core, good when the encryption key changes often. The cores can alternatively work with keys generated in system software; this saves silicon resources but takes more processing time, and is suited to applications with infrequent encryption key changes.

– more –

An uncommon yet versatile feature is a set of fully-stallable input and output interfaces. This means the user's system software can readily pause input processing (e.g., to match a slow input transmission rate) or output processing (e.g., to allow a slower application to catch up with the decrypted data) to maintain AES processing.

Thorough verification of encryption IP is extremely important. The new CAST cores have been rigorously verified against the AES FIPS 197 standard using the Known Answer Tests (KAT) of the NIST AES Algorithm Validation Suite (AESAVS), plus the block cipher modes tests of NIST document SP800-38A, plus additional random test vectors to further exercise the cores. Standard deliverables for the core include all these tests, and (uniquely) a bit-accurate model (BAM) with which users can generate test vectors to facilitate further testing and evaluation.

Strong encryption technology like these new AES IP cores is governed internationally by strict export regulations. Immediate export of the cores to many countries is already approved, and CAST's encryption sales associates can answer questions and give advice concerning others. See the CAST website for more information, or call +1 (201) 391-8300.

About CAST, Inc. and Alma Technologies S.A.

CAST provides over 100 popular and standards-based IP cores for ASICs and FPGAs. Privately owned and operating since 1993, CAST has established a reputation for high-quality IP products, simple licensing, and responsive technical support. The company is headquartered near New York City, partners with IP developers around the world, and works with select sales consultants and distributors throughout Europe and Asia. Learn more at www.cast-inc.com.

CAST has been closely partnered with Alma Technologies since 2001. Alma's engineers are experts at the most complex data processing applications, providing CAST's image and video compression cores as well as most of its encryption IP product line. Learn more at their website: www.alma-tech.com.

<div align="center"># # #</div>

Contacts:
Hal Barbour, CAST, Inc., +1 (201) 391-8300 ext. 111, h.barbour@cast-inc.com
Paul Lindemann, Montage Marketing, +1 (603) 434-3534, paul@montmark.com

CAST, Inc. 50 Tice Blvd., Suite 340, Woodcliff Lake, NJ 07677 Tel: 201/391-8300 Fax: 201/391-8694 www.cast-inc.com

CAST is a trademark of CAST, Inc. All other trademarks are the property of their respective owners.