CS5265/75

AES Simplex Encryption/Decryption Cores

AMPHION™
Virtual Components for the Converging World

The CS5265 and CS5275 Simplex AES encryption/decryption[1] cores are designed to achieve data privacy in digital broadband, wireless, and multimedia systems. These high performance application specific cores support the AES (Rijndael) algorithm as described in the NIST Federal Information Processing Standard. They offer an efficient means of providing both AES encryption and decryption in one core in order to rapidly construct complete security solutions. The CS5265 / CS5275 cores are available in both ASIC and programmable logic versions that have been hand crafted by Amphion to deliver high performance while minimizing power consumption and silicon area.

The Amphion CS5265 Compact Simplex AES Core is designed to offer an efficient yet high performance means of both AES encryption and decryption. The Amphion CS5275 Fast Simplex AES Core offers an increased data throughput in comparison to the CS5265 Compact Simplex AES Core, while still achieving a highly efficient hardware implementation of AES.

The Amphion CS5200 series of AES cores offer a complete solution to modern data encryption needs, offering a simple interface, no internal memory usage, no external keyspace processing, and a highly efficient design offering superior performance.

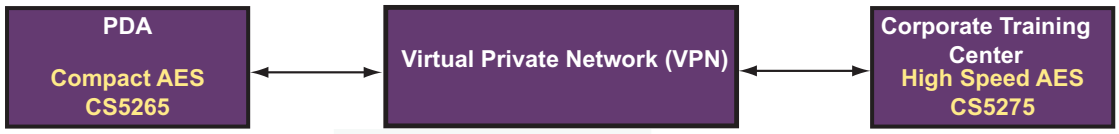

Figure 1: Example of a Secure Distance Corporate Training Scheme Using AES

1. Patent Pending

FEATURES

- **Fully compliant with AES NIST FIPS**
- **Encryption and Decryption on the same core**
- **128-bit data block**
- **128-bit key**
- **32-bit I/O**
- **Electronic Codebook mode (ECB)**
- **Output Feedback mode (OFB)**
- **Cipher Block Chaining mode (CBC)**
- **Cipher Feedback mode (CFB)**
- **Counter mode (CTR)**

APPLICATIONS

- **Electronic financial transactions**
  - eCommerce
  - Banking
  - Securities exchange
  - Point-of-Sale
- **Secure corporate communications**
  - Storage Area Networks (SAN)
  - Virtual private networks (VPN)
  - Video conferencing
  - Voice services
- **Personal mobile communications**
  - Video phones
  - PDA
  - Point-to-Point Wireless
  - Wearable computers
- **Secure environments**
  - Satellite communications
  - Surveillance systems
  - Network appliances

CS5265/75 SYMBOL AND PIN DESCRIPTION

Table 1 gives the descriptions of the input and output ports (shown graphically in Figure 2) of the CS5265/75 AES simplex encrytion/decryption cores. Unless otherwise stated, all signals are active high and bit(0) is the least significant bit.

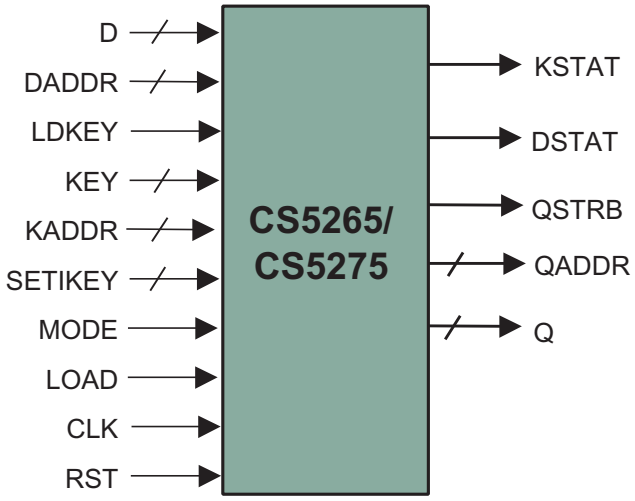

Figure 2: CS5265/75 Symbol

Table 1: CS5265/75 AES Simplex Encryption/Decryption Interface Signal Definitions

Signal	I/O	Width (Bits)	Description
D	I	2	Plaintext/Ciphertext data
DADDR	I	32	Plaintext/Ciphertext data address, 0: the lowest 32-bit word
LDKEY	I	1	Load encryption key
KEY	I	32	Encryption key data
KADDR	I	3	Encryption key address, 0: the lowest 32-bit word
SETIKEY	I	2	Set inverse (decryption) key. By asserting SETIKEY when the highest encryption key word is loaded (KADDR = 11), for one or more, but less than 10 cycles, the inverse key will be derived from the encryption key which is loaded in the normal manner. If the encrypt and decrypt keys are loaded and remain unchanged, the operating mode can be changed block by block with no dead cycles. If the keys are different, the decryption key should be loaded first and SETIKEY should be *Asserted*. The encryption key can then be loaded while the core is preparing the decryption round keys.
MODE	I	1	Encryption/Decryption mode select - 0: Encryption, 1: Decryption
LOAD	I	1	Load Plaintext / Ciphertext enable
CLK	I	1	Synchronous system clock, rising edge active
RST	I	1	Asynchronous reset
KSTAT	O	1	Key port status. When *Asserted*, loading of cipher keys is not allowed
DSTAT	O	1	Input port status The next cycle after text D[3] (the highest word of 128-bit clock) is loaded, DSTAT will be *De-asserted* to indicate encryption is in progress. It will be *Asserted* when the core is ready for loading the highest word of the next 128-bit text. The lower three words can be loaded at anytime in the period when DSTAT is LOW depending on the key-size selection.
QSTRB	O	1	Output strobe indicating the Plaintext/Ciphertext word Q is valid
QADDR	O	2	Plaintext / Ciphertext data address, 0: the lowest 32-bit word
Q	O	32	Plaintext / Ciphertext data

FUNCTIONAL DESCRIPTION

The Rijndael algorithm is an iterated block cipher that encrypts and decrypts data in 128-bit data blocks using a 128-bit, 192-bit, or 256-bit key. The algorithm consists of:

- An initial data/key addition
- Nine, eleven or thirteen rounds when the length is 128-bits, 192-bits, or 256-bits respectively
- A final round which is a variation of the typical round

Figure 3 represents a block diagram of the Rijndael encryption algorithm. A Rijndael round transforms the data using permutations, non-linear substitutions, additions and Galois field multiplications. The Rijndael key schedule consists of two parts:

1. Key Expansion - expands the cipher key into a linear array of 4-byte words
2. Round Key Selection - selection of the required number of Round Keys from the expanded key array

Both versions of the Amphion AES simplex encryption/decryption cores follow the block diagram shown in Figure 3.

The CS5200 AES encryption cores are excellent complements to other Amphion cores. For instance, they can be combined with the CS3500 series of Turbo Coders to rapidly construct a secure transmission channel, and they can be combined with the CS4191 ADPCM codec to achieve secure, high speed, high channel-count speech processing in Voice-over-Packet (VoP) systems.

The Amphion encryption/decryption cores are also an excellent choice for VPN security ICs incorporated into broadband switches, routers, firewalls and remote access concentrators. Likewise, the cores are an ideal fit for the Secure Socket Layer (SSL) channel ICs used in Web servers, WAP gateways and other access applications requiring a high number of parallel SSL channels to carry out eCommerce.

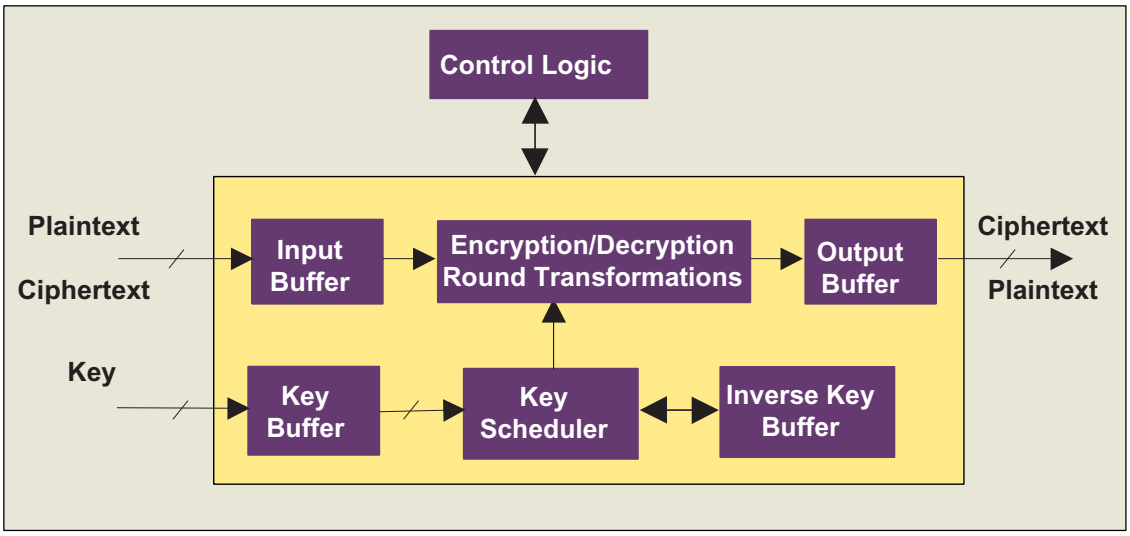

Figure 3: Block Diagram of CS5265 - CS5275 AES Simplex Encryption/Decryption Cores

AVAILABILITY AND IMPLEMENTATION INFORMATION

Hardware accelerated AES technology is governed internationally by export regulations. The Amphion AES cores listed in this datasheet have been officially reviewed and classified by the UK Department of Trade and Industry and US Bureau of Export Administration. These cores are licensed for immediate export to the following countries:

Austria	Denmark	Hungary	New Zealand	Spain
Australia	Finland	Ireland	The Netherlands	Sweden
Belgium	France	Italy	Norway	Switzerland
Canada	Germany	Japan	Poland	United Kingdom
Czech Republic	Greece	Luxembourg	Portugal	United States

For delivery to other destinations, please contact Amphion. Approval is subject to applicable export regulations. Licensees of the Amphion AES cores are responsible for complying with applicable requirements for the re-export of electronics containing AES technology.

ASIC CORES

For applications that require the high performance, low cost and high integration of an ASIC, Amphion delivers application specific silicon cores that are pre-optimized to a targeted ASIC technology by Amphion experts.

Consult your local Amphion representative for product specific performance information, current availability of individual products, and lead times on ASIC core porting.

Table 2: CS5265 / CS5275 ASIC Cores Using TSMC 180 nm Process and Standard Cell Libraries

PRODUCT ID	LOGIC GATES	CYCLES PER OPERATION	TIMING CONSTRAINT (MHz)	DATA RATE (MBITS/SEC)
CS5265TK	25K	44	200	581[a]
CS5275TK	49.3K	11	200	2327

a. Data rate refers to maximum throughput of plaintext/ciphertext in ECB mode

PROGRAMMABLE LOGIC CORES

For ASIC prototyping or for projects requiring the fast time-to-market of a programmable logic solution, Amphion delivers programmable logic core solutions that offer the silicon-aware performance tuning found in all Amphion products, combined with the rapid design times offered by today's leading programmable logic solutions.

Table 3: CS5265 / CS5275 Programmable Logic Cores using Altera APEX20KE-1

PRODUCT ID	LOGIC USED (LE)	MEMORY USED (ESB)	CYCLES PER OPERATION	CLOCK SPEED (MHz)	DATA RATE (MBITS/Sec)
CS5265AA	1666	12	44	71	206
CS5275AA	2297	36	11	43	500

Table 4: CS5265 / CS5275 Programmable Logic Cores using Xilinx Virtex-2

PRODUCT ID	SLICES	MEMORY USED (BRAM)	CYCLES PER OPERATION	CLOCK SPEED (MHz)	DATA RATE (MBITS/Sec)
CS5265X2	799	6	44	100	290
CS5275X2	1256	18	11	80	930

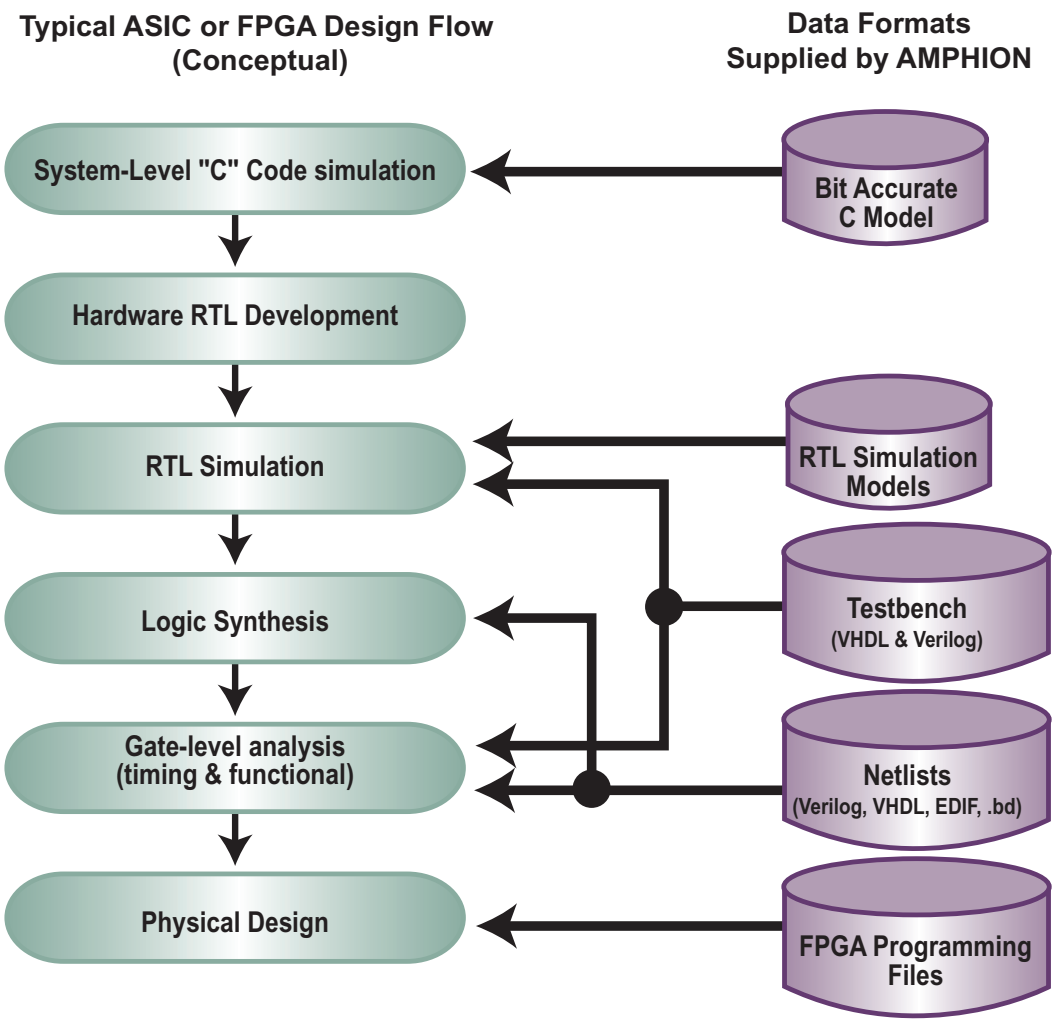

Figure 4: Design Data Formats Supplied by Amphion

ABOUT AMPHION

Amphion (formerly Integrated Silicon Systems) is the leading supplier of speech coding, video/image processing and channel coding application specific silicon cores for system-on-a-chip (SoC) solutions in the broadband, wireless, and mulitmedia markets

Web: www.amphion.com

Email: info@amphion.com

CORPORATE HEADQUARTERS

Amphion Semiconductor Ltd
50 Malone Road
Belfast BT9 5BS
Northern Ireland, UK

Tel: +44.28.9050.4000
Fax: +44.28.9050.4001

WORLDWIDE SALES & MARKETING

Amphion Semiconductor, Inc
2001 Gateway Place, Suite 130W
San Jose, CA 95110

Tel: (408) 441 1248
Fax: (408) 441 1239

EUROPEAN SALES

Amphion Semiconductor Ltd
CBXII, West Wing
382-390 Midsummer Boulevard
Central Milton Keynes
MK9 2RG England, UK

Tel: +44 1908 847109
Fax: +44 1908 847580

CANADA & EAST COAST US SALES

Amphion Semiconductor, Inc
Montreal
Quebec
Canada

Tel: (450) 455 5544
Fax: (450) 455 5543

SALES AGENTS

Voyageur Technical Sales Inc
1 Rue Holiday
Tour Est, Suite 501
Point Claire, Quebec
Canada H9R 5N3

Tel: (905) 672 0361
Fax: (905) 677 4986

Phoenix Technologies Ltd
3 Gavish Street
Kfar-Saba, 44424
Israel

Tel: +972 9 7644 800
Fax: +972 9 7644 801

SPINNAKER SYSTEMS INC
Hatchobori SF Bldg. 5F 3-12-8
Hatchobori, Chuo-ku
Tokyo 104-0033 Japan

Tel: +81 3 3551 2275
Fax: +81 3 3351 2614

JASONTECH, INC
Hansang Building, Suite 300
Bangyidong 181-3, Songpaku
Seoul Korea 138-050

Tel: +82 2 420 6700
Fax: +82 2 420 8600

SPS-DA PTE LTD
21 Science Park Rd
#03-19 The Aquarius
Singapore Science P ark II
Singapore 117628

Tel: +65 774 9070
Fax: +65 774 9071