CS5250-80

High Performance AES Decryption Cores

AMPHION™
Virtual Components for the Converging World

The CS5250-80 series of decryption cores[1] are designed to achieve data privacy and authenticity in digital broadband, wireless, and multimedia systems. These high performance application specific silicon cores support the AES (Rijndael) algorithm as described in the NIST Federal Information Processing Standard. They can be used in conjunction with the CS5210-40 series of Amphion AES encryption cores to rapidly construct complete security solutions. The CS5200 family of 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.

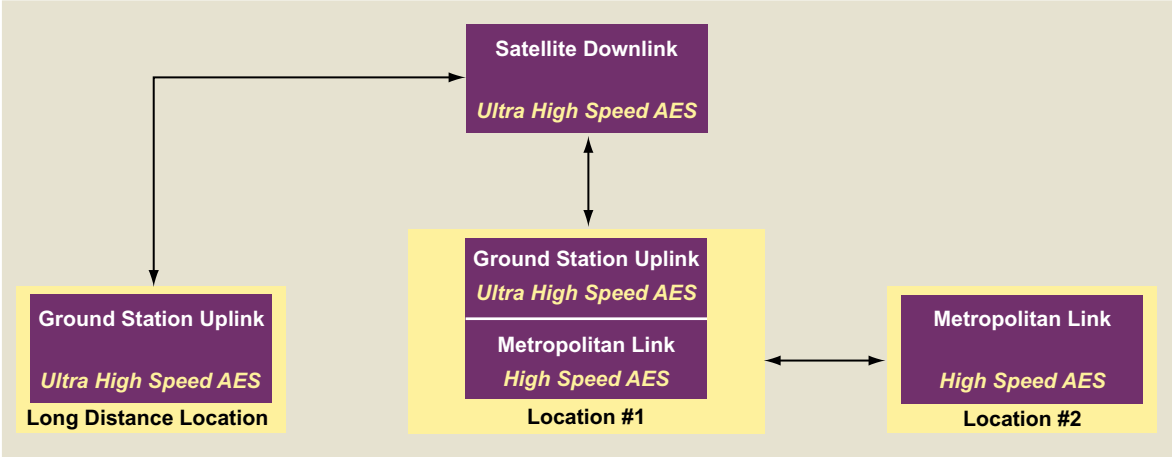

Figure 1: Example of a Satellite and Point-to-Point Secure Communication Scheme Using AES

1. Patent pending

DECRYPTION CORE FEATURES

Table 1: CS5250-80 Features at a Glance

	CS5250 Standard	CS5260 Compact	CS5270 High Speed	CS5280 Ultra High Speed
Fully compliant with AES NIST FIPS	•	•	•	•
128-bit data block	•	•	•	•
128-, 192-, 256-bit keys on-line selectable	•			
128-bit keys only		•	•	•
32-bit I/O	•	•	•	
128-bit I/O				•
Electronic Codebook mode (ECB)	•	•	•	•
Output Feedback mode (OFB)	•	•	•	•
Cipher Block Chaining mode (CBC)	•	•	•	
Cipher Feedback mode (CFB)	•	•	•	

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

CS5250-80 SYMBOL AND PIN DESCRIPTION

Table 2 gives the descriptions of the input and output ports (shown graphically in Figure 2) of the CS5250-80 series of AES decryption cores. Unless otherwise stated, all signals are active high and bit(0) is the least significant bit.

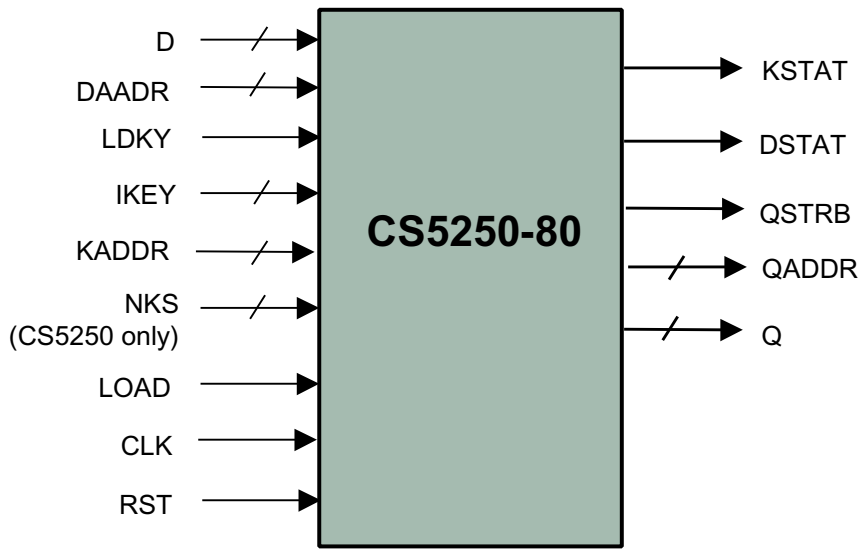

Figure 2: CS5250-80 Symbol

Table 2: CS5250-80 Standard Rijndael Decryption Interface Signal Definitions

Signal	I/O	Width (Bits)	Description
D	I	32 (128)	Cipher text data (128-bit width for CS5280)
DADDR	I	2	Cipher text data address, 0: the lowest 32-bit word
LDKEY	I	1	Load inverse cipher key
IKEY	I	32 (128)	Inverse cipher key (128-bit width for CS5280)
KADDR	I	3[a]	Inverse cipher key address, 0: the lowest 32-bit word
NKS	I	2	Inverse cipher key size select (CS5250 only) When 00: Selects a 128-bit Key When 01: Selects a 192-bit Key When 1X: Selects a 256-bit Key
LOAD	I	1	Load ciphertext enable
CLK	I	1	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 decryption 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 word Q is valid
QADDR	O	2	Plaintext data address, 0: the lowest 32-bit word
Q	O	32 (128)	Plaintext data (128-bit width for CS5280)

a. 3 bits wide for the standard; 2 bits wide for compact/high speed cores; not applicable for ultra high speed core

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 decryption 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

All four versions of the Amphion AES decryption cores follow the block diagram shown in Figure 3.

The CS5200 AES decryption cores are outstanding matches with other Amphion cores. For instance they can be combined with the CS6650 MPEG2 Decoder to easily provide a secure high definition closed-circuit TV system, and they can be combined with the CS3252 FEC Codec as part of a secure wireless access point.

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.

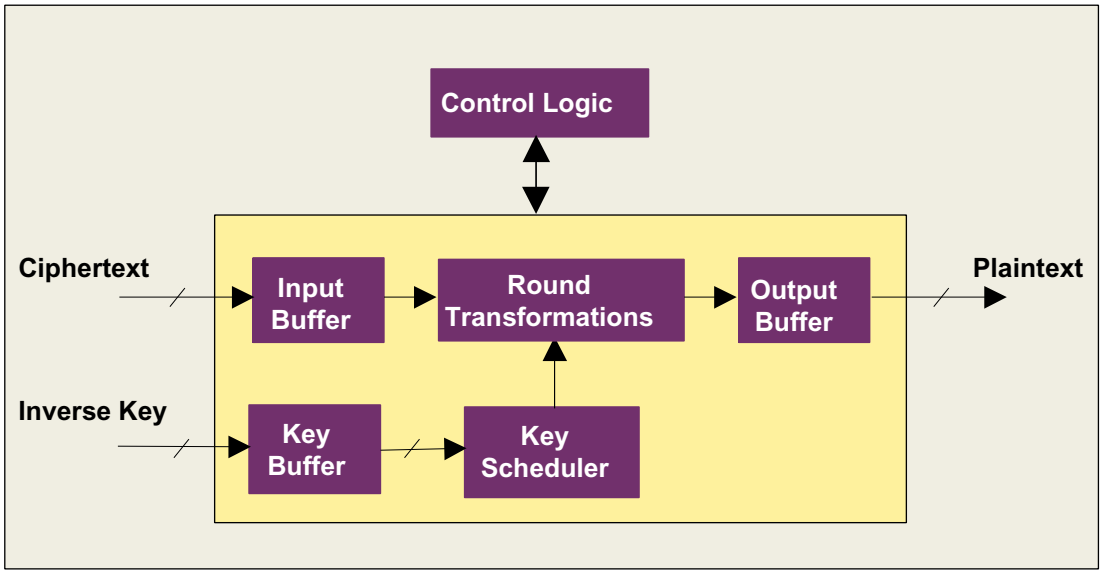

Figure 3: Block Diagram of CS5250-80 Series of Decryption Cores

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	Australia	Belgium	Canada	Czech Republic
Denmark	Finland	France	Germany	Greece
Hungary	Ireland	Italy	Japan	Luxembourg
New Zealand	The Netherlands	Norway	Poland	Portugal
Spain	Sweden	Switzerland	United Kingdom	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 the 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 3: CS5250-80 Family of ASIC Cores using TSMC 180nm Process and Standard Cell Libraries

PRODUCT ID	LOGIC GATES	CYCLES PER OPERATION	TIMING CONSTRAINT (MHz)	DATA RATE (MBITS/Sec)
CS5250TK	19.2K	44[a] 52[b] 60[c]	200	581[a] 492[b] 426[c]
CS5260TK	16.4K	44	200	581
CS5270TK	34K	11	200	2,327
CS5280TK	283K	1	200	25,600

a. Implementation of 128-bit key length
b. Implementation of 192-bit key length
c. Implementation of 256-bit key length

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 4: CS5250-80 Family of 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)
CS5250AA	1560	8	44[a] 52[b] 60[c]	74.1	215[a] 182[b] 158[c]
CS5260AA	1176	11	44	80.4	233
CS5270AA	1481	20	11	62.5	727

Table 5: CS5250-80 Family of Programmable Logic Cores Using Xilinx VirtexE-8

PRODUCT ID	SLICES	MEMORY USED (BRAM)	CYCLES PER OPERATION	CLOCK SPEED (MHZ)	DATA RATE (MBITS/Sec)
CS5250XV	745	4	44[a] 52[b] 60[c]	84.7	246[a] 208[b] 181[c]
CS5260XV	549	4	44	91	264
CS5270XV	778	10	11	77	896
CS5280XV	4626	100	1	68	8704

a. Implementation of 128-bit key length
b. Implementation of 192-bit key length
c. Implementation of 256-bit key length

Table 6: CS5250-80 Family of Programmable Logic Cores Using Xilinx Virtex2-5

PRODUCT ID	SLICES	MEMORY USED (BRAM)	CYCLES PER OPERATION	CLOCK SPEED (MHZ)	DATA RATE (MBITS/Sec)
CS5250XV	746	4	44[a] 52[b] 60[c]	100	290[a] 369[b] 426[c]
CS5260XV	549	4	44	100	290
CS5270XV	778	10	11	91.5	1064
CS5280XV	3998	100	1	73	9344

a. Implementation of 128-bit key length
b. Implementation of 192-bit key length
c. Implementation of 256-bit key length

Table 7: CS5250-80 Family of Programmable Logic Cores using Actel ProASICPlus

PRODUCT ID	DEVICE	CORE CELLS	MEMORY USED (CELLS)	CYCLES PER OPERATION	CLOCK SPEED (MHz)	DATA RATE (MBITS/Sec)
CS5250RQ	APA300	3449	8	44[a] 52[b] 60[c]	36.36	105[a] 133[b] 154[c]
CS5260RQ	APA450	2485	8	44	39.73	116[a]
CS5270RQ	APA300	3167	20	11	31.08	361[a]
CS5280RQC	N/A	N/A	N/A	N/A	N/A	N/A

a. Implementation of 128-bit key length
b. Implementation of 192-bit key length
c. Implementation of 256-bit key length

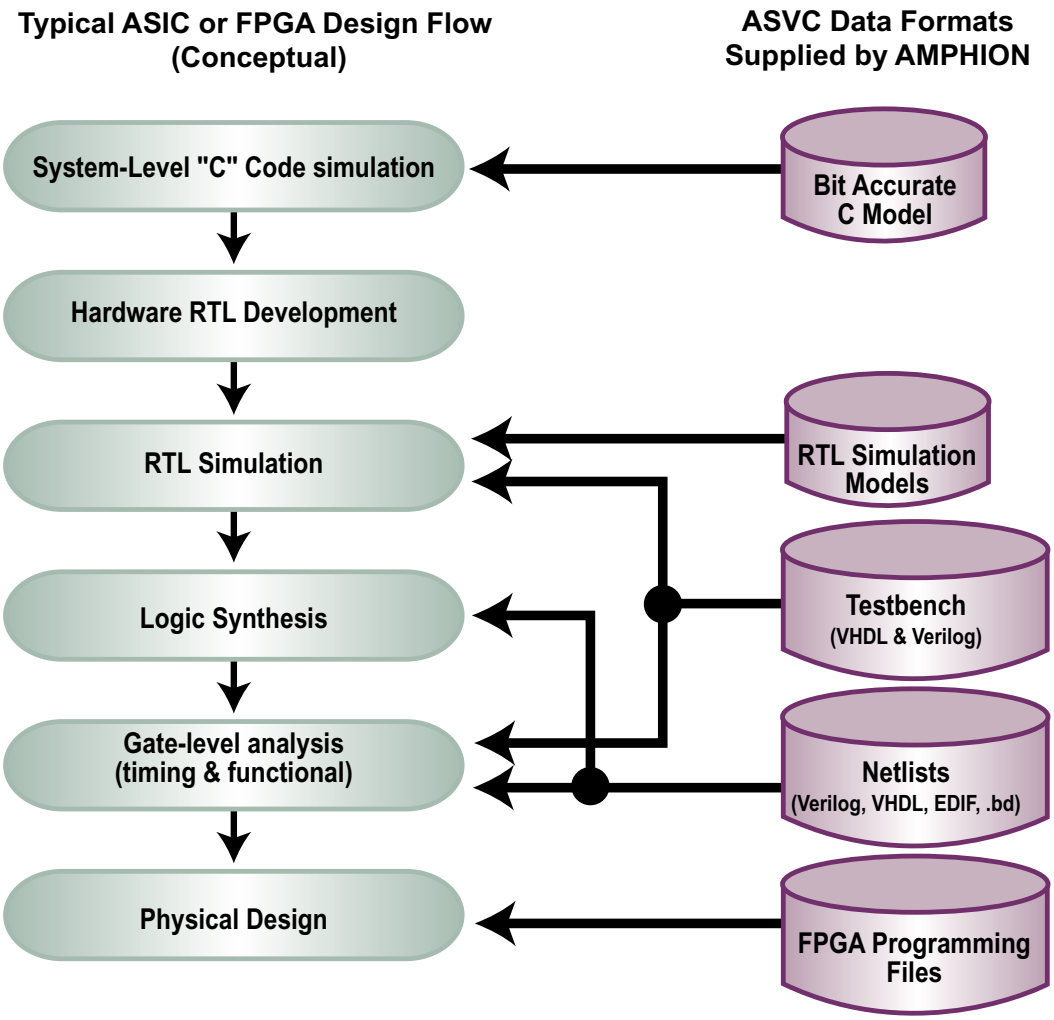

Figure 4: Design Data Formats Supplied by Amphion

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

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

WORLDWIDE SALES & MARKETING
Amphion Semiconductor, Inc
2001 Gateway Place, Suite 130W
San Jose, CA 95110

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

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
6205 Airport Road
Building A, Suite 300
Toronto, Ontario
Canada L4V1E1

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 Park II
Singapore 117628

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

© 2001-02 Amphion Semiconductor Ltd. All rights reserved.
Amphion, the Amphion logo and "Virtual Components for the Converging World" are trademarks of Amphion Semiconductor Ltd. All others are the property of their respective owners.