CS5331-32

High Performance OCB-AES Simplex Encryption/Decryption Cores

AMPHION™ Virtual Components for the Converging World

The CS5331 and CS5332 OCB-AES Simplex Encryption/Decryption cores[1] are designed to provide simultaneous data privacy and authenticity in digital broadband, wireless, and multimedia systems. These high performance application specific silicon cores combine the efficiency of OCB authentication with the high security of Rijndael encryption algorithms, offering a state-of-the-art authenticated-encryption scheme. The CS5331 and CS5332 cores provide the high security functionality of OCB-AES for different applications based on the importance of required speed and size. The CS5331 is a Compact OCB-AES core and is suitable for applications like PDAs and wireless LANs where small size is crucial. The CS5332 is a High Speed OCB-AES core and is appropriate for applications such as wireless LAN high speed network servers where speed of operation is more critical. The Amphion CS5331 and CS5332 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.

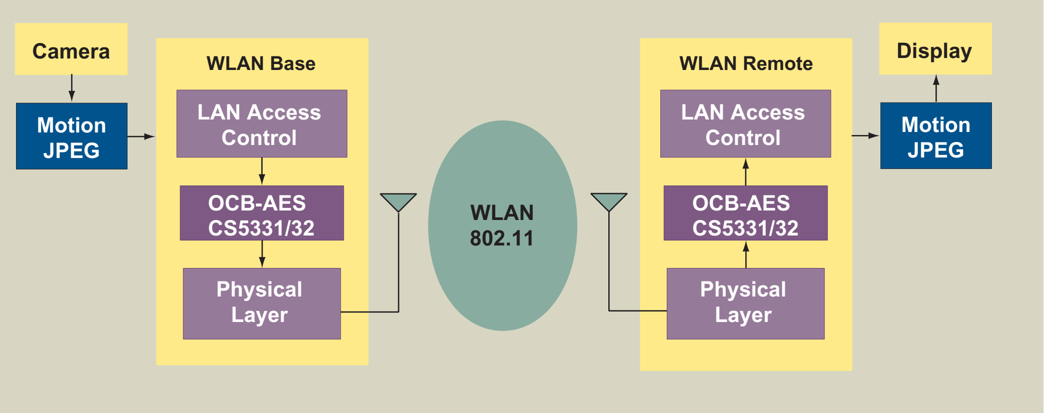

Figure 1: Example of a Secure Wireless Surveillance System Using OCB-AES Cores

FEATURES

- **Encryption/Decryption on the same device**
- **Fully compliant with Rijndael AES NIST FIPS 197**
- **Offset Codebook Mode (OCB)**
- **On-the-fly key generation**
- **128-bit data block**
- **128-bit keys only**

APPLICATIONS

- **Secure electronic transactions**
  - Medical files
  - Financial files
  - Securities exchange
  - eCommerce
  - Point-of-Sale
- **Secure corporate communications**
  - Virtual Private Networks (VPN)
  - Video conferencing
  - Voice services
- **Personal mobile communications**
  - Video phones
  - PDA
  - Point-to-Point Wireless
- **Secure distance learning**
  - Corporate Training
  - Universities

[1] Patent Pending

CS5330 SYMBOL AND PIN DESCRIPTION

Table 1 describes the input and output ports (shown graphically in Figure 2) of the CS5331/32 OCB-AES Simplex Encryption/Decryption cores. Unless otherwise stated, all signals are active high and bit (0) is the least significant bit.

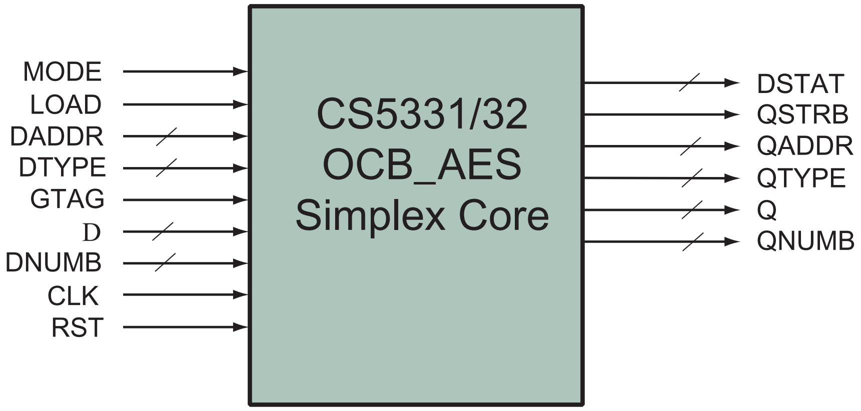

Figure 2: CS5331-32 Symbol

Table 1: CS5331-32 OCB-AES Simplex Encryption/Decryption Core Interface Signal Definitions

Signal	I/O	Width (Bits)	Description
MODE	I	1	OCB Mode select; 0: Encryption, 1: Decryption
LOAD	I	1	Load OCB data enable
DADDR	I	2	OCB data block address
DTYPE	I	2	OCB data block type; 0: Key, 1: Nonce, 2: Plaintext, 3: Last Plaintext
GTAG	I	1	Generate Tag
D	I	32	OCB input data – Key, Nonce or Plaintext
DNUMB	I	4	Number of valid bytes, 0 for 16, applied to the last plaintext block only
CLK	I	1	System clock, rising edge active
RST	I	1	Asynchronous reset
DSTAT	O	2	OCB input data port status; DSTAT[1]: Core loading indicator, DSTAT[0]: Core ready indicator. The data port status indicator has a 2 cycle latency
QSTRB	O	1	OCB output strobe indicating the ciphertext/tag word Q is valid
QADDR	O	2	OCB output data address; 0: the lowest 32-bit word
QTYPE	O	2	OCB output block type; 0: Ciphertext, 1: Last Ciphertext, 2: Tag
Q	O	32	OCB output data – Ciphertext or Tag
QNUM	O	4	Number of valid output bytes, 0 for 16, applied to the last ciphertext block only

FUNCTIONAL DESCRIPTION

Offset Codebook Mode (OCB) is a parallelizable block cipher mode of operation that provides both authenticity and privacy when combined with encryption algorithms. OCB is contained in the draft NIST FIPS for the modes of operation for symmetric key block ciphers and OCB-AES has been implemented in the IEEE wireless LAN standard 802.11i. The Amphion CS5331 and CS5332 combine the OCB mode with the Rijndael AES algorithm to provide efficient high security functionality for a wide range of operations. These cores integrate the Amphion CS5265 / CS5275 Simplex AES Encryption/Decryption cores with the CS5330 Simplex OCB Controller core.

The CS5331 and CS5332 OCB-AES simplex Encryption/Decryption cores are excellent compliments to other Amphion cores. For example, they can be combined with the CS6750 MPEG-4 decoder to rapidly construct a secure duplex video conferencing system, or they can be combined with the CS3500/CS3600 family of Turbo Coders to achieve secure, error free data transmission. Figure 3 represents an overview diagram of the CS5331/CS5332.

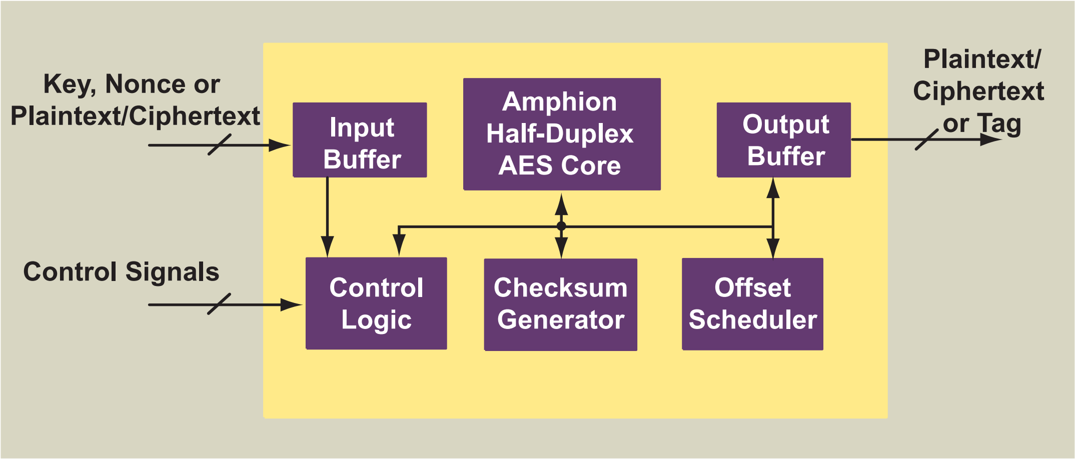

Figure 3: Block Diagram of the CS5331/CS5332 Simplex OCB-AES Encryption/Decryption Cores

AVAILABILITY AND IMPLEMENTATION INFORMATION

Hardware accelerated AES technology is governed internationally by export regulations. The Amphion OCB-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.

OCB cores contain technology that is patent pending to Philip Rogaway of the University of California, Davis. Vendors are obliged to contact Mr. Rogaway in order to license the 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: CS5331-32 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)[a]
CS5331TK	37K	44	200	581
CS5332TK	70K	11	200	2327

[a] Sustained data rate refers to the maximum throughput of the plaintext/ciphertext.

Table 3: CS5331-32 ASIC Cores Using TSMC 130 nm Process and Standard Cell Libraries

PRODUCT ID	LOGIC GATES	CYCLES PER OPERATION	TIMING CONSTRAINT (MHz)	DATA RATE (MBITS/SEC)[a]
CS5331TM	39K	44	300	872
CS5332TM	84K	11	300	3490

[a] Sustained data rate refers to the maximum throughput of the plaintext/ciphertext.

PROGRAMMABLE LOGIC CORES

For ASIC prototyping or for projects requiring fast time-to-market, Amphion programmable logic cores 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: CS5331-32 Family Programmable Logic Core Using Xilinx Virtex2-5

PRODUCT ID	LOGIC USED (Slices)	MEMORY USED (BRAM)	CYCLES PER OPERATION	CLOCK SPEED (MHz)	DATA RATE (MBITS/Sec)[a]
CS5331X2	1826	6	44	75	220
CS5332X2	2184	18	11	75	875

a. Sustained data rate refers to the maximum throughput of plaintext/ciphertext

Table 5: CS5331-32 Family Programmable Logic Core Using Altera APEX20KE-1

PRODUCT ID	LOGIC USED (LE)	MEMORY USED (ESB)	CYCLES PER OPERATION	CLOCK SPEED (MHz)	DATA RATE (MBITS/Sec)[a]
CS5331AA	4511	12	44	44	128
CS5332AA	5081	36	11	39	461

a. Sustained data rate refers to the maximum throughput of plaintext/ciphertext

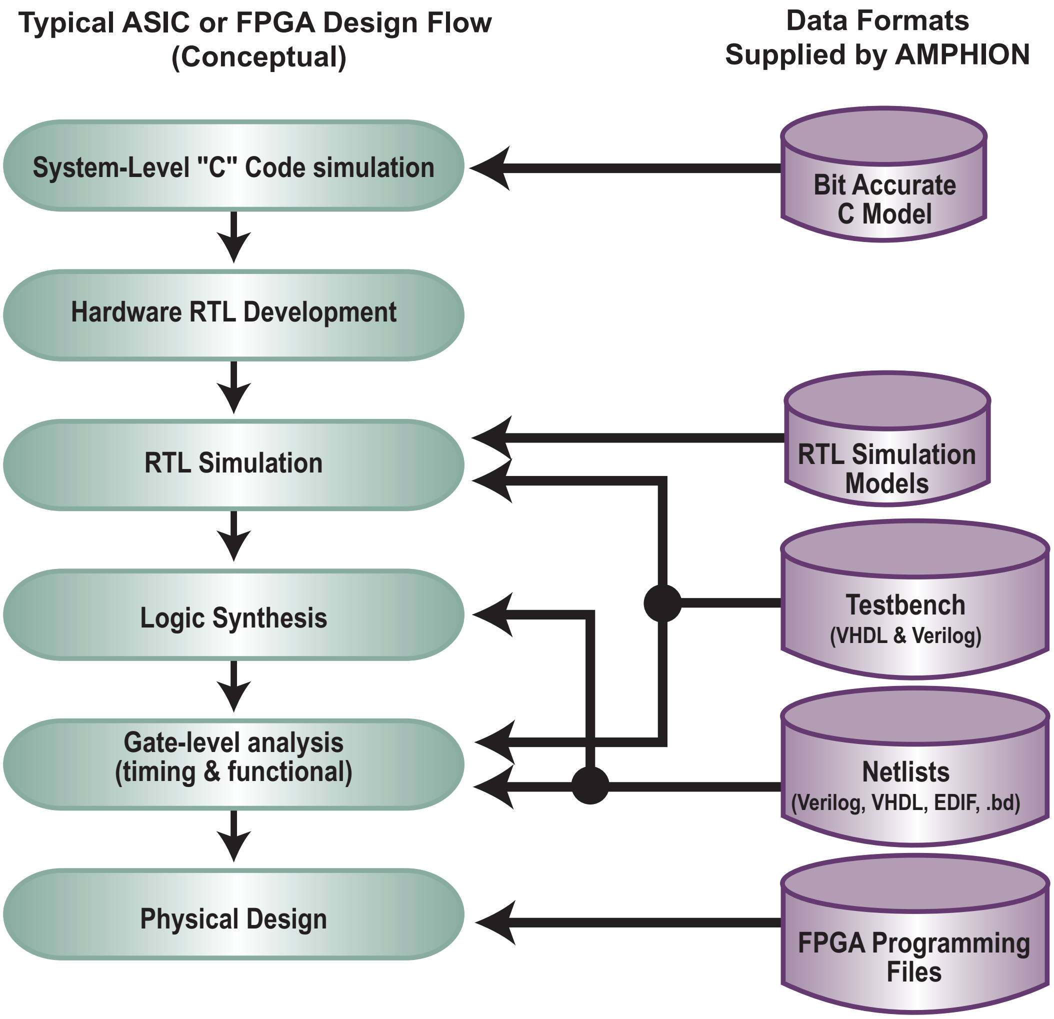

Figure 4: Design Data Formats Supplied by Amphion

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

1 Rue Holiday
Tour Est, Suite 501
Point Claire, Quebec
Canada H9R 5N3

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

JASONTECH, INC

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

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

Phoenix Technologies Ltd

3 Gavish Street
Kfar-Saba, 44424
Israel

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

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

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