CS5010-40

DES/3DES Encryption/Decryption Cores

AMPHION™
Virtual Components for the Converging World

The CS5010-CS5040 DES/3DES Encryption/Decryption cores are designed to achieve data privacy in digital broadband, wireless, and multimedia systems. These high performance application specific silicon cores support the Data Encryption Standard (also referred as Data Encryption Algorithm) as described in the NIST Federal Information Processing Standard 46-3. They offer an efficient means of providing both DES and Triple DES encryption and decryption in one core in order to rapidly construct complete security solutions. The DES/3DES 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.

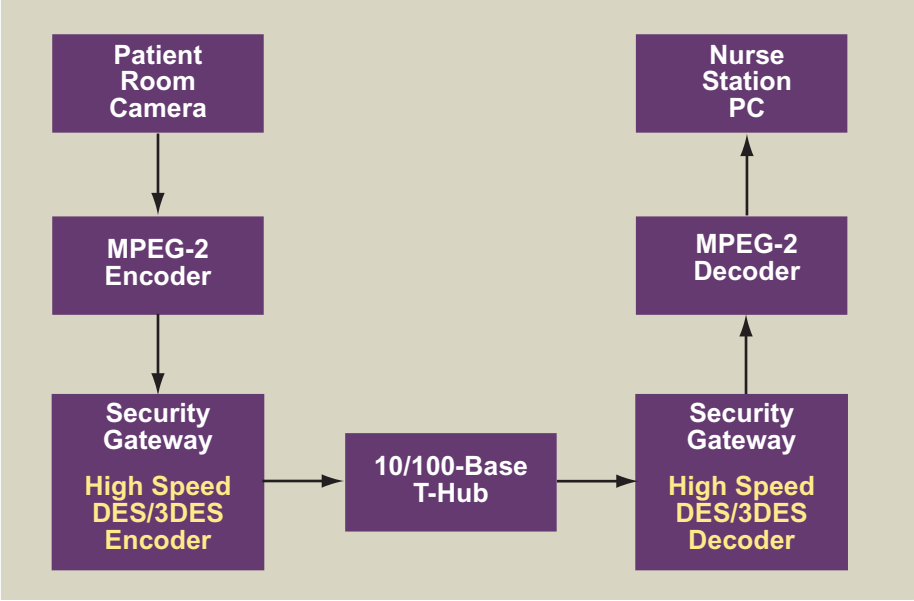

Figure 1: Example of a Secure Audio/Video Based Remote Patient Monitoring System Using DES/3DES

ENCRYPTION CORE FEATURES

Table 1: CS5010-40 Features at a Glance

	CS5010 Ultra Compact	CS5020 Compact	CS5030 High Speed	CS5040 Ultra HIgh Speed
Fully compliant with DES NIST FIPS 46-3	•	•	•	•
DES and Triple DES Support	•	•	•	•
32-bit I/O	•	•	•	
128-bit I/O				•
28-bit Key Input Port	•	•	•	
56-bit Key Input Port				•
EDE2 and EDE3 Triple DES (112- or 168-bit key length)	•	•	•	•

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

DATA ENCRYPTION ALGORITHM

The Data Encryption Algorithm is an iterated block cipher with a Feistel structure that encrypts and decrypts data in 64-bit data blocks using a 56-bit key. The algorithm consists of:

- An initial permutation of the input data
- Sixteen rounds of the same process - the DES round
- A final inverse initial permutation of the data

Figure 2 represents a block diagram of the Data Encryption Algorithm. A DES round transforms the data using permutations, additions and non-linear substitutions. The DES key schedule consists of three parts:

1. Key Permutation - to remove the eight redundant parity bits within the 64-bit key, and to permute the key
2. Scheduled Circular Shifting - the permuted key is circularly shifted according to a schedule by either 1 or 2 bits, to the left or right.
3. Key Compression - the 56-bit shift key is compressed using another permutation, or rearrangement, to obtain a 48-bit subkey.

The Triple Data Encryption Algorithm offers increased security by extending the DES key to 112 or 168 bits, thus greatly reducing the effectiveness of exhaustive key searches or "brute-force" attacks. Triple DES is simply three successive DES operations in the sequence of encrypt-decrypt-encrypt, or decrypt-encrypt-decrypt if decrypting data.

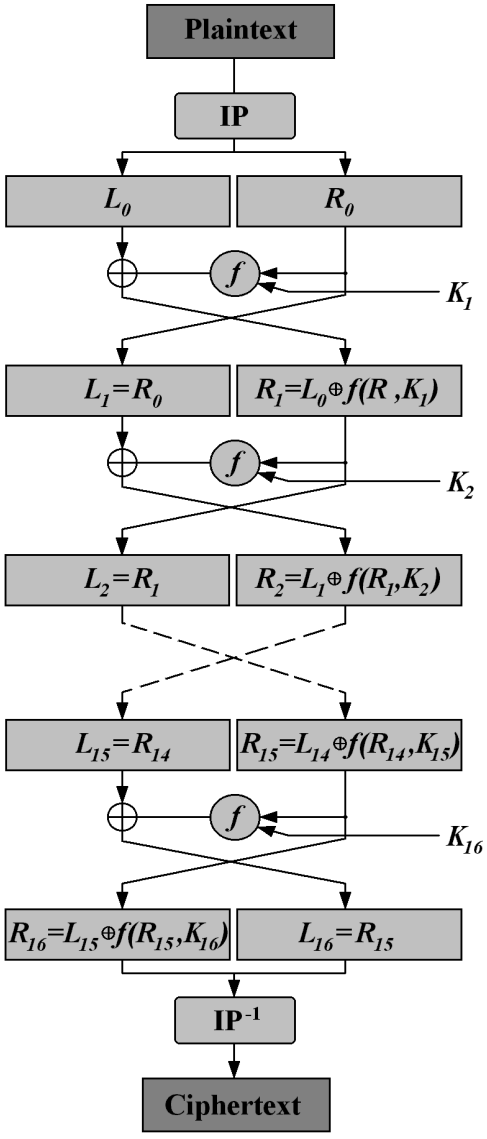

Figure 2: DES Algorithm Structure

FUNCTIONAL DESCRIPTION

The Amphion series of DES/3DES cores offer a complete solution to maintaining legacy DES functionality for modern data encryption needs, offering a simple interface, no internal or external memory usage, no external keyspace processing, and a highly efficient design offering unparalleled performance.

The CS5010 Ultra Compact DES/3DES and the CS5020 Compact DES/3DES Cores are designed to offer an efficient yet high performance means of both DES and Triple DES encryption/decryption, with the emphasis on reduced resource usage.

The CS5030 High Speed DES/3DES Core offers an increased data throughput in comparison to the Compact Cores, while still achieving a highly efficient hardware implementation.

The CS5040 Ultra High Speed DES/3DES Core is designed to provide a high performance solution while still achieving a relatively low resource usage.

The Ultra Compact DES/3DES Core is capable of all DES standard modes of operation. The use of these added modes of operation on Compact, High Speed and Ultra High Speed DES/3DES Cores is subject to conditions. For example, it is impractical to use a fully pipelined DES core to perform CBC mode, as the data throughput of the hardware would have to be substantially reduced in order to support the feedback XOR operation between output and input of the DES core.

All versions of the Amphion DES/3DES cores follow the block diagram shown in Figure 3.

The DES/3DES cores are excellent complements to other Amphion cores. For instance they can be combined with the CS6650 MPEG-2 Decoder to rapidly construct a secure patient monitoring system, 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.

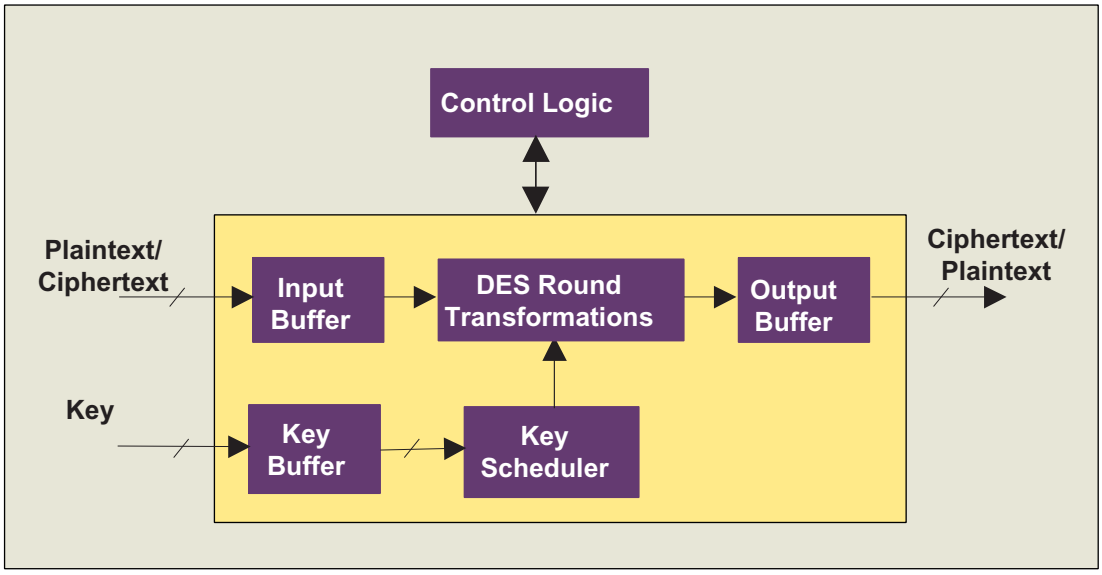

Figure 3: Block Diagram of DES/3DES Cores

CS5210-40 SYMBOL AND PIN DESCRIPTION

Table 2 describes the input and output ports (shown graphically in Figure 4) of the CS5010-40 series of DES/3DES encryption cores. Unless otherwise stated, all signals are active high and bit(0) is the least significant bit.

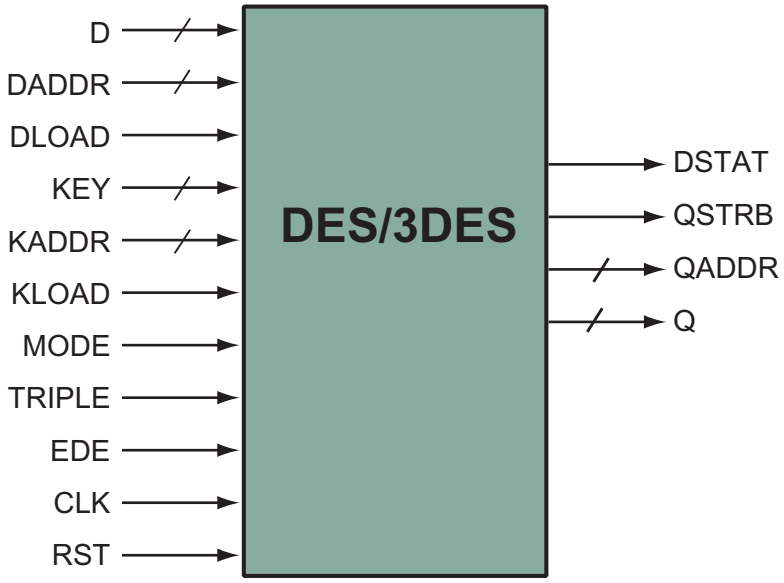

Figure 4: CS5010-40 DES/3DES Symbol

Table 2: CS5010-40 DES/3DES Cores Interface Signal Definitions

Signal	I/O	Width (Bits)	Description
D	I	32 (64 Ultra High Speed)	Input Plaintext/Ciphertext data
DADDR	I	1 (Ultra Compact) 2 (Compact) 3 (High Speed) 0 (Ultra High Speed)	Input Plaintext/Ciphertext data address, 0: the lowest 32-bit word
DLOAD	I	1	Load input Plaintext/Ciphertext enable
KEY	I	28 (56 Ultra High Speed)	Encryption key data
KADDR	I	2	Encryption key address, 0: the lowest 28-bit word
KLOAD	I	1	Load encryption key
MODE	I	1	Encryption/Decryption mode select, 0: Encryption. 1: Decryption
TRIPLE	I	1	DES/3DES mode select, 0: DES, 1:3DES
EDE	I	1	Triple DES key selection mode, 0:EDE2, 1: EDE3
CLK	I	1	System clock, rising edge active
RST	I	1	Asynchronous reset
DSTAT	O	1	Input port status This signal will be *Asserted* when the core is ready for loading the highest word of the next 64-bit data block, or the highest word of the multiple input DES blocks available in the Compact or High Speed cores. The lower 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	1 (Ultra Compact) 2 (Compact) 3 (High Speed) 0 (Ultra High Speed)	Output Plaintext/Ciphertext data address, 0: the lowest 32-bit word
Q	O	32 (64 Ultra High Speed)	Output Plaintext/Ciphertext data

AVAILABILITY AND IMPLEMENTATION INFORMATION

Hardware accelerated 3DES technology is governed internationally by export regulations. Amphion 3DES cores listed in this datasheet are available within the UK. License to export to the following countries is pending:

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 3DES cores are responsible for complying with applicable requirements for the re-export of electronics containing 3DES technology.

PROGRAMMABLE LOGIC CORES

For ASIC prototyping or for projects requiring the fast time-to-market of a programmable logic solution, Amphion programmable logic core 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: CS5010-40 DES/3DES Programmable Logic Cores using Actel Axcelerator

PRODUCT ID	SILICON VENDOR	DEVICE	MAX. FREQUENCY (MHz)	DATA RATE (MBits/Sec)		UTILIZATION		DEVICE UTIL	AVAILABILITY
				DES	3DES	R-CELLS	C-CELLS		
CS5010RR	Actel	AX500	71	284	94	545	1151	22%	Now
CS5020RR	Actel	AX500	63	504	168	735	1715	31%	Now
CS5030RR	Actel	AX500	57	912	304	1213	3116	54%	Now
CS5040RR	Actel	AX1000	56	3584	1194	4162	7179	63%	Now

Cycles per operation for the CS5010-40 cores are 16, 8, 4 and 1 respectively

Note: Speed grade = -3

Table 4: CS5010-40 DES/3DES Programmable Logic Cores using Actel ProASICPlus

PRODUCT ID	SILICON VENDOR	DEVICE	MAX. FREQUENCY (MHz)	DATA RATE (MBits/Sec)		UTILIZATION (Tiles)		DEVICE UTIL	AVAILABILITY
				DES	3DES	Combinatorial	Sequential		
CS5010RQ	Actel	APA150	27	108	36	1923	510	40%	Now
CS5020RQ	Actel	APA150	27	216	72	2830	712	58%	Now
CS5030RQ	Actel	APA300	21	336	112	5253	1192	79%	Now
CS5040RQ	Actel	APA600	26	1664	554	11331	3926	71%	Now

Cycles per operation for the CS5010-40 cores are 16, 8, 4 and 1 respectively

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
Shin-Yokohama Square Bldg. 11F, 2-3-12
Shin-Yokohama, Kouhoku-Ku
Yokohama 222-0033 Japan

Tel: +81 45 478 3803
Fax: +81 45 478 3809

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

Optimized for Actel
10/02 Publication #: DS5010/40ACT v1.2