XF-DES Data Encryption Standard Engine Core

September 16, 1999 Product Specification

7810 South Hardy Drive, Suite 104
Tempe, Arizona 85284 USA
Phone: +1 888-845-5585 (USA)
+1 480-753-5585
Fax: +1 480-753-5899
E-mail: info@memecdesign.com
URL: www.memecdesign.com

Features

- Single- and triple-DES operation
  - Configurable to support all DES options and configurations
- NIST Certificate Number 31
- Suitable for implementation in ECB, CBC, CFB, and OFM operating modes
- 56-bit key (United States only)
- Simple interface and timing
- Bit-rate is 4 times clock frequency (DC-172 Mbits/sec, single-DES)
  - Supports OC3 applications

Applications

- Secure internet applications
- Remote access servers
- Cable modems
- Satellite modems
- Hardware-based RSA challenges

Export and Usage Restrictions

Cryptographic equipment and algorithms are subject to US Government export restrictions. **The user is advised to check current government policies on export of devices containing cryptographic algorithms.**

AllianceCORE™ Facts

Core Specifics		
Device Family	XC4000E/XL	Spartan
CLBsUsed Core Core+Ext Logic	 316 316	 316 316
IOBs Used Core[1] Core+Ext logic	 200 200	 200 200
System Clock f_{max}	43 MHz	25 MHz
Device Features Used	Embedded ROM	
Provided with Core		
Documentation	User's Guide Example Implementation Implementation Instructions	
Design File Format	Verilog or VHDL RTL	
Constraint Files	TimeSpecs	
Verification Tool	Testbench and Vectors	
Symbols	None	
Evaluation Model	None	
Reference Designs & Application Notes	Example Implementation	
Additional Items	Warranty by MDS	
Design Tool Requirements		
Xilinx Core Tools	Alliance/Foundation 1.5	
Entry/Verification Tools	Verilog/ VHDL Synthesis Tools Model Technology ModelSim	
Support		
Support provided by Memec Design Services.		

Notes:
1. Assuming all core signals are routed off-chip. Implementations for I/O limited devices require an additional bus interface module.

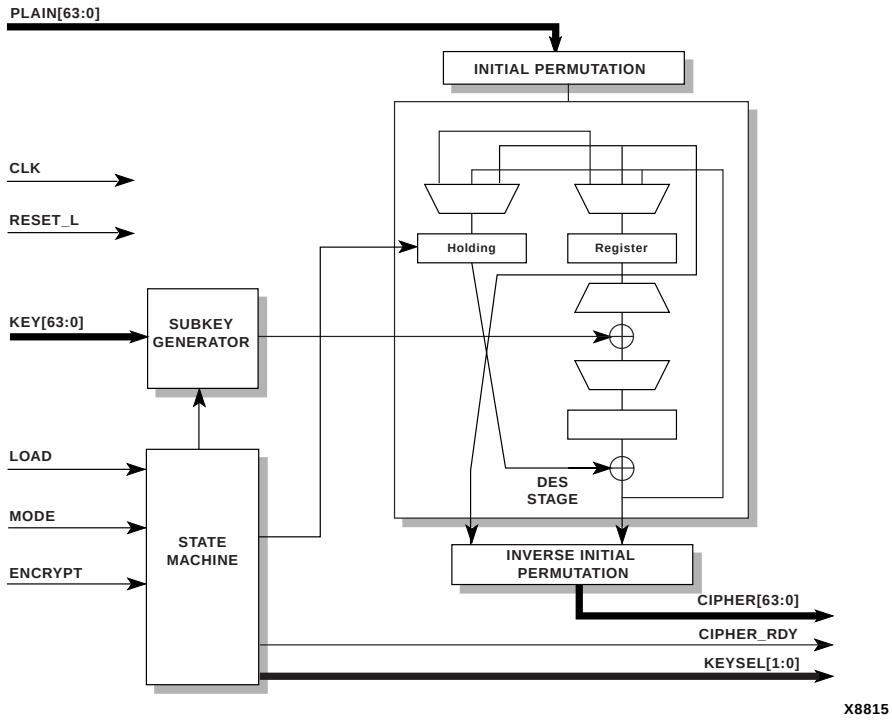

Figure 1: XF-DES Block Diagram

General Description

The XF-DES Core provides a scalable hardware implementation of the Data Encryption Standard (DES). Its ease of use and high performance makes it a cost competitive solution to dedicated hardware or software alternatives.

DES is a block-oriented encryption algorithm. Plaintext data is loaded 64-bits at a time along with the encryption key. Encrypted ciphertext is available 16 clock cycles later for Single-DES operation.

The same hardware can be used to decrypt a block of data. With decryption selected, a block of ciphertext is loaded along with the encryption key and 16 clocks later the plaintext is available.

Triple-DES consists of applying the DES algorithm on the data three times. Encryption in Triple-DES is performed by encrypting the data with key number 1, decrypting the resulting ciphertext with key number 2, and encrypting that result with key number 3. The process is reversed for decryption. The state machine within the core controls selection of the key. The user must provide a multiplexing function specific to the end application.

XF-DES Core supplies the base engine on which an encryption application can be built. The CBC, CFB, and OFM modes are realized by surrounding the XF-DES Core with multiplexers and XOR functions.

Functional Description

The XF-DES core is made of three main blocks: the State Machine, the SubKey Generator, and the DES-Stage. Refer to XF-DES Data Encryption Standard Engine User's Guide for detailed technical information. The User's Guide is available, directly from MDS.

General Operation

When new data is presented to the core and the LOAD input is high, data is clocked into the DES-Stage holding registers. The outputs of the DES-Stage are fed back to its input. Data is cycled through the stage 16 times during a Single-DES process. Each pass through the stage consists of the following steps.

1. The data word is split into a right half and a left half.
2. The right 32 bits are expanded to 48 bits by replicating some of the bits.
3. These 48 bits are XOR'd with a 48-bit subkey. The subkey changes each pass through the stage.

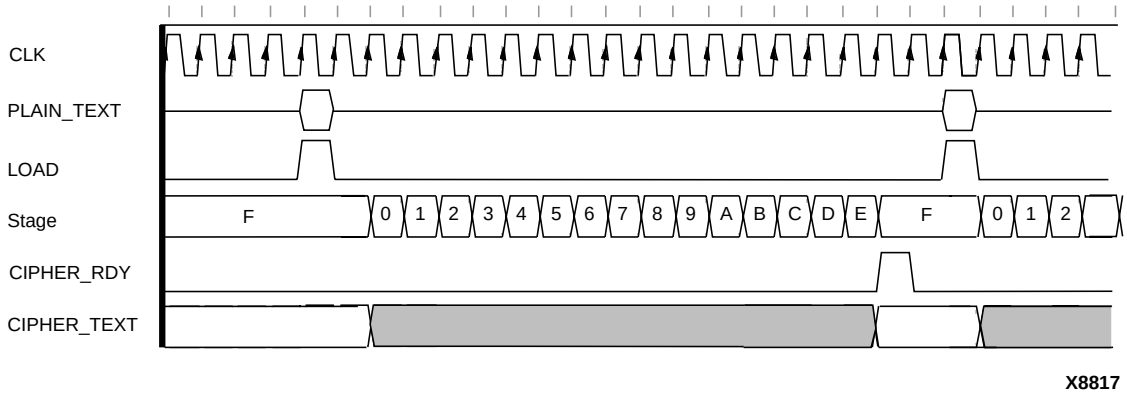

Figure 2: DES Core Interface Timing Diagram

4. The 48-bit result is fed to 8 substitution boxes (Sbox). Each Sbox is unique and the substitution is non-linear. A 6-bit input is converted to a 4-bit output.
5. The order of the Sbox output is permutated and the 32-bit result is XOR'd with the left 32 bits from the holding register.
6. The resulting 32 bits are fed to the right half of the holding register. Data from the right half is fed to the left half of the register.

SubKey Generator

The SubKey Generator has a 56-bit holding register for the KEY input. Although the interface for the KEY is 64 bits, every eighth bit is a parity bit and is not used for encryption.

Initial Permutation

The order of the KEY value is permutated before it is loaded into a holding register. Like the DES-Stage, the KEY word is split into a right half and a left half. These halves are shifted right or left in a circular fashion depending on the state of the ENCRYPT input. The halves may be shifted 0, 1, or 2 bits depending on the cycle of the algorithm.

State Machine

The state machine provides control timing. It controls the cycles and operation of the core.

Encryption applications often have very specific needs. For example, when operating in CBC mode, the incoming data will be XOR'd with either the output of the previous encryption cycle or with an initial value that is provided as an additional input to the encryption engine. These types of changes and decisions require the state machine to be modified to control a multiplexer in the feedback path.

Interface Timing

The waveform in Figure 2 shows the interface timing for the XF-DES core. Data is presented to the core on the PLAINTXT 64-bit parallel input. The LOAD signal is active for one clock cycle and causes the data to be clocked into the DES-Stage holding register. It also causes the state machine to begin stepping through the stages.

On the first clock-cycle of stage "F", CIPHER_RDY is asserted. This signal can be used as the clock enable to a register bank on the output or to signal another process that data is available. The output data will remain valid until a new data block is written to the core. New data can be written to the core on the same clock-cycle that data is read from the core.

Core Modifications

The state machine delivered with the core is a simple example that will operate the core in ECB mode. It operates in single and triple mode for encryption or decryption and can be used to demonstrate timing requirements of the core. Modification of the state machine can be done by the user or by Memec Design Services to the user's specifications. Memec Design Services can also design system interface modules specific to the user's requirements. Contact Memec Design directly to discuss any application requirements.

Table 1: Core Signal Pinout

Signal	Signal Direction	Description
PLAIN[63:0]	Input	Data input to core. Plaintext input in Encrypt mode, Ciphertext input in Decrypt mode. Data must be valid during “LOAD” signal.
CLK	Input	System Clock.
RESET_L	Input	Asynchronous Clear input to all registers for simulation; maps to dedicated GSR logic in FPGA.
KEY[63:0]	Input	Key input value. Key data must be valid for duration of the “LOAD” signal.
LOAD	Input	Active-high signal enables core data registers to capture KEY and input data. Signal initiates 16-stage block processing in Single-DES mode and 48-stage processing in Triple-DES mode.
MODE	Input	Mode Select - high selects Triple-DES mode; low selects Single-DES mode.
ENCRYPT	Input	Encrypt Select - high selects encrypt mode; low selects decryption in Single-DES mode. In Triple-DES mode an “EDE” sequence is selected when ENCRYPT is high. “DED” sequence is active when ENCRYPT is low.
CIPHER[63:0]	Output	Ciphertext output during encryption; Plaintext output during decryption. Data is valid from CIPHER_RDY active to LOAD active of next block.
CIPHER_RDY	Output	Active high pulse indicates block processing is complete and output is available on CIPHER outputs.
KEYSEL[1:0]	Output	State machine outputs for control of key multiplexer in Triple-DES modes.

Pinout

I/O signals for this core are shown in Figure 1 and described in Table 1.

Verification Methods

The XF-DES core has been simulated using ModelSim PE/Plus V4.b. Simulation results were accredited by:

InfoGard Laboratories
NVLAP Lab Code: 100432-0
669 Pacific Street, Suite F
San Luis Obispo, CA 93401
Phone: +1 805-783-0810
Fax: +1 805-783-0889
E-Mail: info@infogard.com
URL: www.infogard.com

Recommended Design Experience

Users should be familiar with HDL-based design techniques including synthesis and simulation design flows. Some exposure to cryptographic techniques and terminology is helpful.

Ordering Information

The XF-DES Data Encryption Standard Engine core is provided under license from Memec Design Services for use in Xilinx programmable logic devices and Xilinx HardWire gate arrays. Please contact Memec for pricing and more information.

Information furnished by Memec Design Services is believed to be accurate and reliable. Memec Design Services reserves the right to change specifications detailed in this data sheet at any time without notice, in order to improve reliability, function or design, and assumes no responsibility for any errors within this document. Memec Design Services does not make any commitment to update this information.

Memec Design Services assumes no obligation to correct any errors contained herein or to advise any user of this text of any correction, if such be made, nor does the Company assume responsibility for the functioning of undisturbed features or parameters.

Memec Design Services will not assume any liability for the accuracy or correctness of any support or assistance provided to a user.

Memec Design Services does not represent that products described herein are free from patent infringement or from any other third-party right. No license is granted by implication or otherwise under any patent or patent rights of Memec Design Services.

Memec Design Services products are not intended for use in life support appliances, devices, or systems. Use of a Memec Design Services product in such application without the written consent of the appropriate Memec Design Services officer is prohibited.

Related Information

Xilinx Programmable Logic

For information on Xilinx programmable logic or development system software, contact your local Xilinx sales office, or:

Xilinx, Inc.
2100 Logic Drive
San Jose, CA 95124
Phone: +1 408-559-7778
Fax: +1 408-559-7114
URL: www.xilinx.com

For general Xilinx literature, contact:

Phone: +1 800-231-3386 (inside the US)
+1 408-879-5017 (outside the US)
E-mail: literature@xilinx.com

For AllianceCORE™ specific information, contact:

Phone: +1 408-879-5381
E-mail: alliancecore@xilinx.com
URL: www.xilinx.com/products/logicore/alliance/tblpart.htm