CoreTex Systems, LLC
2851 S Ocean Blvd, Suite 5L
Boca Raton, FL 33432

Phone: (561) 208-5550
Fax: (877) 840-1047
E-mail: **info@coretexsys.com**
URL: **www.coretexsys.com**

Core Facts	
Core Specifics	
See Table 1	
Provided with Core	
Documentation	Core documentation
Design File Formats	VHDL Source RTL
Constraints File	Core user constraints file
Verification Tool	VHDL Testbench: Test Vectors
Instantiation Templates	VHDL
Reference designs & application notes	None
Additional items	None
Simulation Tool Used	
Xilinx ISE Simulator	
Support	
Support provided by CoreTex Systems, LLC (**support@coretextsys.com**)	

Features

- Supports Spartan™-3, Spartan™-IIE, Virtex™, Virtex-E, Virtex-II and Virtex-II Pro™ devices
- Compliant with Triple-DES specification from NIST FIPS 46-3 (1999) standard [1]
- Three 64-bit DES keys
- Fully synchronous design
- Stand-alone operation
- High Performance

Applications

- Secure communication applications:
  - Teleconferencing
  - Electronic commerce transactions:
    - ATM machines
    - Secure data/multimedia transmission
    - Wireless communication,
    - Virtual Private Networks (VPN)
  - Secure Storage Applications
  - Major security protocols:
    - IPSec
    - SSL

Table 1: Core Implementation Data

	Xilinx Family	Tested Device	Fmax (MHz)	Slices	IOB	GCLKs	BRAM	DCM	BW (Mbs)	Design Tool
Open Cores	Virtex-II	2V6000FF1517-6	134	1738	302	1	0	1	481	ISE 8.1i
	Spartan-3	XC3S4000L-4FG900	82	1790	302	1	0	1	294	ISE 8.1i
	Virtex-4	XC4VLX200-11FF1513	162	1742	302	1	0	1	581	ISE 8.1i

Note: Results are generated for ECB mode of operation. *The BW for fast version is based on a sustained feed of input data, which makes full use of the pipelined architecture.

General Description

The core complies with the Triple-DES 64-bit block cipher defined in FIPS 46-3 NIST standard and operates with three 64-bit keys.

Functional Description

Triple-DES Specification

Triple-DES is an extension of Data Encryption Standard (DES) that results in a more complex but more secure block cipher. Standard DES represents a component in Triple-DES architecture. If $E_K(I)$ and $D_K(I)$ denote the DES encryption and decryption of I using DES key K, respectively, then Triple-DES encryption and decryption is performed as follows:

Encryption: $E_{K3}(D_{K2}(E_{K1}(I))) = O$

Decryption: $D_{K1}(E_{K2}(D_{K3}(O))) = I$

Initialization and Setup

Upon reset, the core captures status of FUNCTION_SELECT pin, which determines cores functionality. The activation of LDKEY signal indicates that the key is ready for input. The key is supplied as three separate 64-bit words (KEY1_IN, KEY2_IN and KEY3_IN). Once the keys are loaded the core is ready to accept blocks of data for encryption/decryption. LDDATA pin should be set to high to indicate that a 64-bit block of data is ready at DATA_IN port. To load new key values a reset of the core has to be performed.

Triple-DES Encryption/Decryption process

The encryption/decryption process is equivalent to performing three standard DES encryption/decryption sequences.
The Standard Triple-DES core iteratively performs the DES encryption/decryption process. Fast Triple-DES implementation contains three DES modules arranged in a pipelined architecture. Thus, the first output block is obtained in three times the time needed by a single DES core. However, each subsequent input block can be fed to the core in the time needed for a single DES encryption/decryption. If the input feed to the core is maintained constant in this respect, each output block, save the first, is obtained after time needed to perform single DES processing.

A typical sequence diagram of the pipelined Fast Triple-DES core is shown in Figure 2. The diagram shows the signals for the loading key and first data block in the encryption/decryption sequence

Output

Upon completion of all rounds the core sets OUT_READY pin to 1. At that point the output is available at DATA_OUT port for further processing.

Pinout

Port names for the core input and output are shown in Figure 1 and described in Table 2.

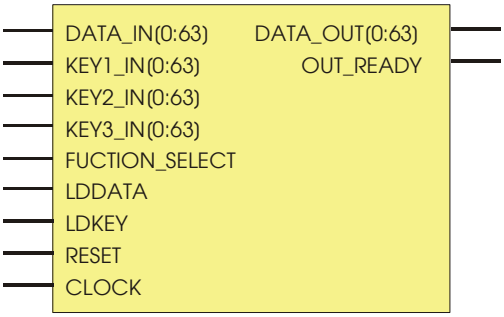

Figure 1: Core Schematic Symbol

Table 2: Core Signal Pinout

Signal	Direction	Description
KEY1_IN[0:63]	IN	**Key #1:** the first 64-bit encryption key.
KEY2_IN[0:63]	IN	**Key #2:** the second 64-bit encryption key.
KEY3_IN[0:63]	IN	**Key #3:** the third 64-bit encryption key.
DATA_IN[0:63]	IN	**Data Input:** 64-bit block of data to be encrypted.
FUNCTION_SELECT	IN	**Function Select:** sets the function to encryption.
LDKEY	IN	**Load Key:** key ready to be read from the input.
LDDATA	IN	**Load Data:** data ready to be read from the input.
RESET	IN	**Reset:** forces module to go to the initial state.
CLOCK	IN	**Clock:** all operations of the core synchronous with the rising edge of the clock.

DATA_OUT[0:63]	OUT	**Data Output:** synchronous output of the encrypted/ decrypted data.
OUT_READY	OUT	**Data Output Ready:** signals that the output data is ready.

Key Bus – KEY_INn[0:63]; n=1, 2, 3

The key bus is used to input three 64-bit keys for Triple-DES encryption/decryption. The input is synchronous with the rising edge of the clock and controlled by the ldkey signal.

Data-In Bus – DATA_IN[0:63]

The DATA_IN bus provides a 64-bit block of input data to be encrypted or decrypted. The input is synchronous with the rising edge of the clock and controlled by the LDDATA signal.

Function Select – FUNCTION_SELECT

Function Select is used to set the functionality of the core to encryption (FUNCTION_SELECT = 1) or decryption (FUNCTION_SELECT = 0).

Load Key – LDKEY

Indicates that key is ready on KEY1_IN, KEY2_IN and KEY3_IN ports. It is active high.

Load Data – LDDATA

Indicates that there is valid data on DATA_IN port. It is active high.

Reset – RESET

Reset forces module to go to the initial state, enter the key load mode of operation and expect the input of the key and FUNCTION_SELECT. By default the RESET pin is active high.

Clock – CLOCK

All operations of the core are synchronous with the rising edge of the clock input. All input pins have setup time referenced to the port clock pin.

Data Output Ready – OUT_READY

Indicates that the core output is available. When OUT_READY=1, data is ready at port DATA_OUT.

Data-Out Bus – DATA_OUT[0:63]

The DATA_OUT bus is used to output a block of encrypted or decrypted data.

Verification Methods

A large set of test vectors has been used to verify the correct operation of the core, along with the standard NIST Triple-DES test vectors.

Figure 2: Timing diagram for Triple-DES IP