X_DES Cryptoprocessor

March 14, 2000

Product Specification

300-2908 South Sheridan Way
Oakville, ON
Canada, L6J 7J8
Phone: +1 905 829 8889
Fax: +1 905 829 0888
E-mail: sales@xentec-inc.com
URL: www.xentec-inc.com

Features

- Supports Spartan™-II, Virtex, and Virtex™-E devices
- Fully compliant 64-bit DES implementation
- Both encryption and decryption supported
- Encryption and decryption performed in 16 clock cycles
- No dead cycles for key loading or mode switching
- Suitable for triple DES implementations
- Suitable for ECB, CBC, CFB and OFB implementations
- Sustained bit rate is 4 x clock speed
- High clock speed and low gate count
- Fully synchronous design
- Also available as fully functional and synthesizable VHDL or Verilog soft-core at extra cost
- Test benches provided

Export and Usage Restrictions

Encryption commodities, software, and technology are subject to US Government Export restrictions. **The user is advised to check current government policies on the export of these commodities, software, and technology**

AllianceCORE™ Facts

Core Specifics	
See Table 1	
Provided with Core	
Documentation	Core documentation
Design File Formats	EDIF Netlist, VHDL, Verilog RTL Source Available Extra
Constraints File	des.ucf
Verification	VHDL/Verilog test benches, test vectors
Instantiation Templates	VHDL, Verilog
Reference Designs & Application Notes	None
Additional Items	None
Simulator Tool Used	
1076 Compliant VHDL, Verilog Simulator	
Support	
Support provided by Xentec, Inc.	

Applications

- Electronic financial transactions
- Secure communications
- Secure video surveillance systems
- Encrypted data storag

Table 1: Core Implementation Data

Supported Family	Device Tested	CLB Slices	Clock IOBs[1]	IOBs[1]	Performance (MHz)	Xilinx Tools	Special Features
Spartan-II	2S100-6	235	1	188	94	M2.1i	None
Virtex-E	V300E-8	235	1	188	120	M2.1i	None
Virtex	V150-6	255	1	188	101	M1.5i	None

Notes:
1. Assuming all core I/Os are routed off-chip

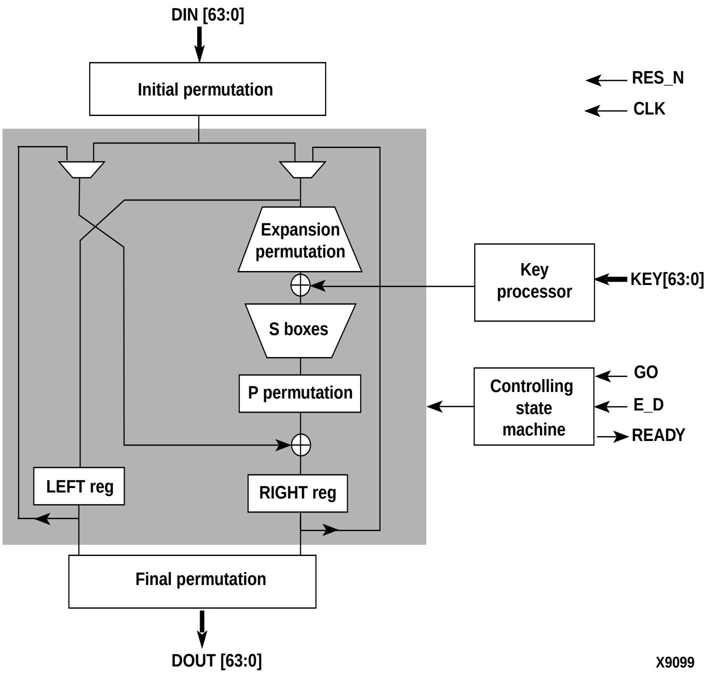

Figure 1: X_DES Cryptoprocessor Block Diagram

General Description

The X_DES core is a fully compliant hardware implementation of the DES encryption algorithm, suitable for a variety of applications.

The DES algorithm is the result of a joint effort between IBM and the NSA and was adopted as a federal standard in November 1974

Functional Description

Encryption or decryption behavior is selected by the E_D input port. If this input is high, the core performs encryption, otherwise decryption is performed.

A transition to high on the GO port triggers the beginning of a cryptographic operation on DIN using KEY as key data. The operation can be aborted at any time by turning GO to low. Sixteen clock cycles are required to complete a cryptographic operation.

The X_DES core is partitioned into modules as shown in Figure 1 and as described below.

Initial Permutation

After an initial permutation, the input data is split into two 32-bit words, left and right. This initial permutation changes the order of the bits of the input data.

Expansion Permutation

The right word is processed with an expansion permutation and XORed with the processed key. This operation is known as expansion permutation, as it expands the number of bits from 32 to 48 by changing the order of some bits as well as by repeating the values of others.

S Boxes

The S boxes are look up tables with six input bits and four output bits. There are eight S boxes that transform the 48-bit input into a 32-bit output. The content of the S boxes was initially defined by IBM and later modified by the NSA.

P Permutation

The output of the S boxes is permuted in the P permutation block and then XORed with the left word. The P permutation is a straight permutation. None of the input bits are used twice or ignored.

Registers (LEFT reg and RIGHT reg)

The right word register is updated on the rising edge of CLK with the results of the P permutation block XORed with the left word. Also, the previous right word is stored in the left word register.

Final Permutation

At the end of the each encryption or decryption operation (16 clocks), the left and right words are reassembled together and passed through the final permutation. The final permutation is the inverse of the initial permutation.

Key Processor

The key processor reduces the 64-bit input key to 56 bits by ignoring every eighth bit. At each rising edge of CLK the 56-bit key is divided into two 28-bit words. Depending on the current state of encryption, each word is circularly shifted by one or two bits. A 48-bit subkey is extracted at each clock and XORed with the result of the expansion permutation, as explained above.

Controlling State Machine

The controlling state machine controls all the operations and generates the READY signal.

Core Modifications

Please contact Xentec, Inc. directly for any required modifications.

Pinout

The pinout of the X_DES core has not been fixed to specific FPGA I/O, allowing flexibility with a user's application. Signal names are shown in the block diagram in Figure 1, and in Table 2.

Verification Methods

The X_DES core's functionality has been extensively tested with an HDL testbench and a large number of test patterns.

Recommended Design Experience

The user must be familiar with HDL design methodology as well as instantiation of Xilinx netlists in a hierarchical design environment.

Ordering Information

The X_DES core is available from and is licensed from Xentec, Inc. Please contact Xentec, Inc. directly for pricing and additional information.

Related Information

The core is approved by the National Institute of Standards and Technology (NIST) and conforms to the Data Encryption Algorithm as specified in Federal Information Processing Standard Publication FIPS 46-3 and ANSI X9.52. See http//csrc.nist.gov/cryptval/des/desval.htm.

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

Table 2: Core Signal Pinout

Signal	Signal Direction	Description
DIN[63:0]	Input	Input data
DOUT[63:0]	Output	Output data
RES_N	Input	Reset, active low
CLK	Input	Clock signal
KEY[63:0]	Input	Input key
GO	Input	Activates encryption or decryption
E_D	Input	Selects encryption or decryption
READY	Output	Ready to operate and output data valid

Availability

Encryption commodities, software, and technology are subject to US Government Export restrictions. **The user is advised to check current government policies on the export of these commodities, software and technology.**

The core is available from Australia for export to the following countries:

Belgium-Luxembourg
Brazil
Canada
China
Denmark
Germany
Finland
France
Italy
Japan
Netherlands
Norway
South Korea
Singapore
Spain
Sweden
Taiwan
United Kingdom
United States of America

It is the customer's responsibility to check with the relevant authorities regarding the re-export of components containing encryption technology.