ALDES Core
Application Note

Rev. [6/2012]

6-19-2012

Table of Contents

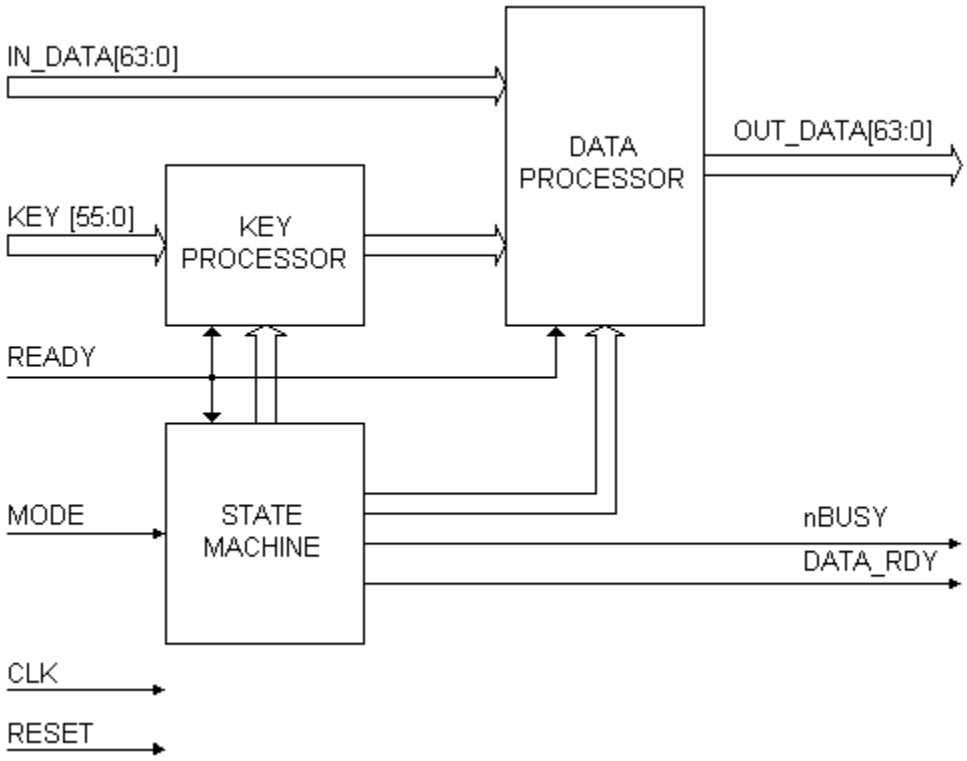
General Information

The ALDES core is the VHDL model of the processor, that performs DES encryption and decryption. The model is fully compliant with FIPS46-2.

Features

- Fully compliant 56-bit key DES implementation
- Single DES operation
- Encryption and decryption are performed in 16 clock cycles
- Suitable for ECB, CBC, CFB and OFB implementations
- Suitable for Triple-DES implementation
- No dead clock cycles
- Simple interface and timing
- Fully synchronous design

Block Diagram



The basic structure of the ALDES core is shown below:

Contents

Synthesizable

See the Deliverables section of this document for further details.

Test Vectors

See the Deliverables section of this document for further details.

Interface

The pinout of the ALDES core has not been fixed to specific FPGA I/O, allowing flexibility with a user's application. Signal names are shown in the table.

Signal Name	Signal Direction	Polarity	Description
CLK	IN	-	Clock input
RESET	IN	HIGH	Asynchronous reset
MODE	IN	-	Mode: 0 - encryption, 1 - decryption
KEY[55:0]	IN	-	Key
IN_DATA[63:0]	IN	-	Input data
READY	IN	HIGH	Data ready signal, 1 - operate, 0 - pause in processing
nBUSY	OUT	-	Busy signal, 0 - processor is busy, 1 - data can be loaded
OUT_DATA[63:0]	OUT	-	Output data
DATA_RDY	OUT	-	Output data ready, 1 – data on OUT_DATA are valid

Data processing may be paused using the READY signal. If this signal is HIGH, then the processor operates. If this signal is LOW, the processor will wait and data processing will be paused.

nBUSY signal is used to indicate that the processor is busy. If set HIGH, then the input data signal IN_DATA can be changed, when set LOW, the processor will not load input data to itself.

Implementation Data

The core has been synthesized and implemented to different types of reprogrammable devices. The model has been verified using the simulation environment and tested on the real hardware.

Software					
Synthesis Tool	Synplify VHDL Compiler, version 5.1.2, built Apr 14 1999				
Implementation Tools	Xilinx Foundation™ 2.1i SP2, Altera MAX+plusII™ 9.21, Quartus™ 1.0 A				
Verification Tool	Active-HDL™ 3.5 build 437				
Hardware					
Vendor	Xilinx			Altera	
Device Family	4K	Virtex™	Spartan	FLEX™ 10K	FLEX™ 8000
Target Device	XC4013XL-08	XC V150-6	XLC30-3	EPF10K50V-1	EPF81500-2
Area	259CLBs	283Slices	255CLBs	656LCs	750LCs
System Clock fmax	55MHz	104MHz	26MHz	49MHz	34MHz

Deliverables

After you request the desired compiled synthesizable core, Aldec delivers the following files:

- Technology-dependent EDIF (ALDES.EDF) and VHDL (ALDES.VHD) netlists
- Test vectors and patterns
- User-Guide and Application Notes
- Sample designs
- Software emulator of ALDES core

Usually Aldec delivers both EDIF and VHDL netlists for customers who order the synthesizable model. The EDIF netlist is used for the place and route process and VHDL is the post-synthesis netlist used for the simulation only. Of course, both netlists are technology-dependent, because they are created after the synthesis where the customer needs to specify a vendor, target family, etc.

Software emulator of ALDES core is intended to use as «golden» source for patterns from user-provided set of data.

Aldec can provide also a set of VHDL test benches for their cores. Usually they are sold at the additional charge.

Source codes are sold on a case-by-case basis.