Advanced technologies for your success

ECB-MODE DES CRYPTOGRAPHIC FAST PROCESSOR CORE DATASHEET

VERSION 2.0.1
LAST TIME MODIFIED 08.02.2008

ECB-mode DES Cryptographic Fast Processor Core

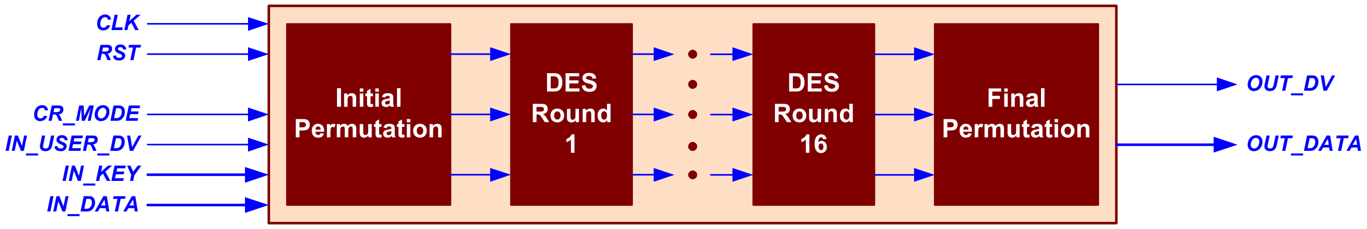
General information

The CORE is fully compatible with the Data Encryption Standard according to the Federal Information Processing Standards Publication 46-3 (FIPS 46-3) of the National Institute of Standards and Technology. High performance is achieved due to its fully pipelined structure. Dynamic key changing is provided. The CORE is intended to be used in PC market files encryption, electronic commerce, financial applications, computer and telecommunication networks, pay TV etc.

Features

- ❑ *Input data word size – 64 bits;*
- ❑ *Output data word size – 64 bits;*
- ❑ *Input key size – 56 bits;*
- ❑ *Encryption and decryption are supported;*
- ❑ *Simple interface and timing;*
- ❑ *No dead clock cycles;*
- ❑ *Fast chip operation;*
- ❑ *Pipeline delay 17 clock cycles;*
- ❑ *Vendor independent VHDL model, netlist for target device.*

ECB-mode DES Cryptographic Fast Processor Core Interface pinout



Interface description

Pin	Activity	Description
CLK	Positive clock edge	Clock
RST	HIGH	Asynchronous reset
CR_MODE	HIGH	Encipherment direction ('0' - encryption)
IN_USER_DV	HIGH	Input data validation flag
IN_DATA [63 - 0]	-	Input data bus
IN_KEY [55 - 0]	-	Input key
OUT_DV	HIGH	Output data validation flag
OUT_DATA [63 - 0]	-	Output data bus

Sample implementation

Device	Speed grade	Utilization	Clock rate	Performance	Synthesis and implementation tools	Availability
ALTERA						
EP20K160EBC356	-01X	5449 LEs	92.75MHz	5936 Mbits/s	Synplify, Altera[1]	***Now***, ver_2_1_1
EP2S15F484C3	3	2669 ALUTs	**367.38** MHz	**23512,32** Mbits/s	Altera [2]	***Now***, ver_2_1_2

1) Altera – Altera Max+Plus II version 10.1;
2) Altera – Altera Quartus II, ver 5.1.

Synplify – Synplicity Synplify Pro VHDL Compiler, version 7.0.1.

http://www.intron-innovations.com
info@intron-innovations.com