CBC-mode DES Cryptographic Fast Processor Core

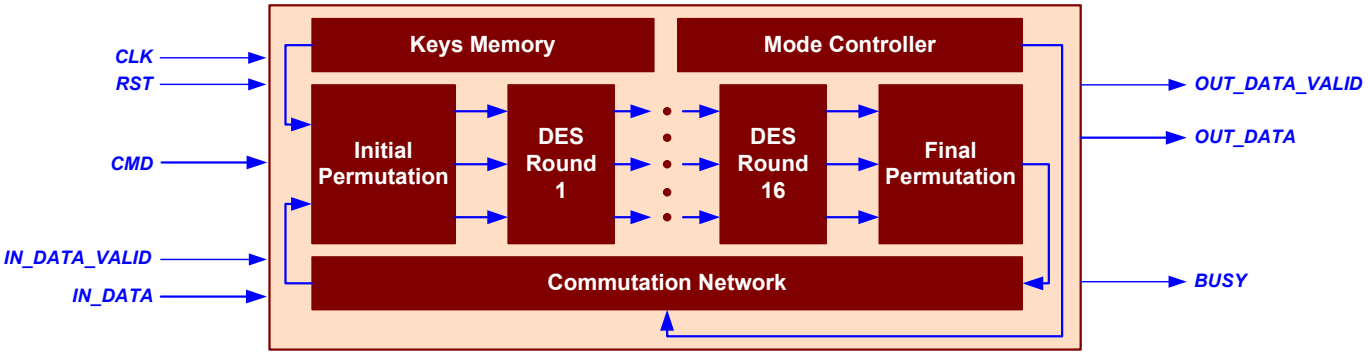
General information

*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 **for decryption** 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 for decryption;*
- *Encryption and decryption are performed in 17 clock cycles;*
- *Vendor independent VHDL model, netlist for target device.*

CBC-mode DES Cryptographic Fast Processor Core pinout



Interface description

Pin	Activity	Description
CLK	Positive clock edge	Clock
RST	HIGH	Asynchronous reset
CMD [2 - 0]	-	Input command
IN_DATA_VALID	HIGH	Input data validation flag
IN_DATA [63 - 0]	-	Input data bus
OUT_DATA_VALID	HIGH	Output data validation flag
OUT_DATA [63 - 0]	-	Output data bus
BUSY	HIGH	Processor's business flag

Sample implementation

Device	Speed grade	Utilization	Clock rate	Performance	Synthesis and implementation tools	Availability
ALTERA						
EP20K200EBC356	-01X	7235 LEs	64 MHz	E [1]: 240.9 Mbits/s D [2]: 4096 Mbits/s	Synplify, Altera [3]	***Now***, ver_2_1_1
EP2S15F484C3	3	4060 ALUTs	**343.88** MHz	E [1]: 1294.6 Mbits/s D [2]: **22008.32** Mbits/s	Altera [4]	***Now***, ver_2_1_2

1) E – Encryption;
2) D – Decryption;
3) Altera – Altera Quartus II, version 1.1 build 155;
4) Altera – Altera Quartus II, ver 5.1.

Synplify – Synplicity Synplify VHDL Compiler, version 7.0.1.

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