CBC-mode Triple DES Cryptographic Smart Processor Core

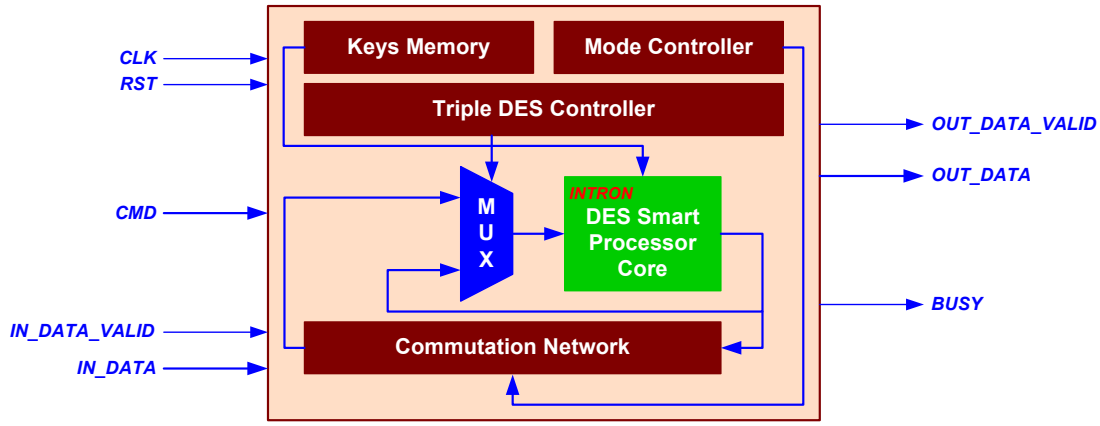
General information

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. Dynamic key changing is provided. Three keys processing is applied. Low equipment volume is achieved due to fully iterative CORE's structure. 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;*
- *Low gate count;*
- *Iterative structure, 56 clocks per encryption/decryption;*
- *Vendor independent VHDL model, netlist for target device.*

CBC-mode Triple DES Cryptographic Smart 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						
EP20K60EBC356	-01X	1669 LEs	73.529 MHz	84.03 Mbits/s	Synplify, Altera [1)]	***Now***, ver_2_1_1
EP2S15F484C3	3	1286 ALUTs	**330.03** MHz	**377.17** Mbits/s	Altera [2)]	***Now***, ver_2_1_2 [3)]
EP2S15F484C3	3	**675** ALUTs	221.93 MHz	253.63 Mbits/s	Altera [2)]	***Now***, ver_2_1_3 [4)]

1) Altera –Altera Quartus II version 1.1 build 155;
2) Altera – Altera Quartus II, ver 5.1;
3) – Speed optimized;
4) – Area optimized.

Synplify – Synplicity Synplify Pro VHDL Compiler, version 7.0.1.

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