CBC-mode Triple DES Cryptographic Fast Processor Core

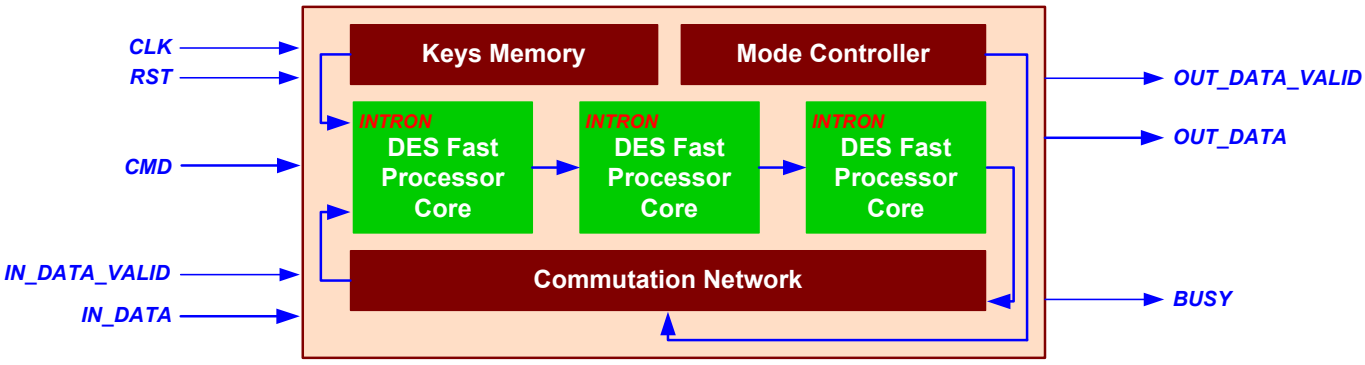
General information

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. Dynamic key changing is provided. Three keys processing is applied. High performance is achieved ***for decryption*** *due to fully pipelined 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;*
- *Simple interface and timing;*
- *Fast chip operation for decryption;*
- *No dead clock cycles;*
- *Encryption and decryption are supported;*
- *Processing time – 51 clock cycles;*
- *Vendor independent VHDL model, netlist for target device.*

CBC-mode Triple 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						
EP20K600EBC652	-01X	20678 LEs	52 MHz	E [1]: 65.25 Mbits/s D [2]: 3328 Mbits/s	Synplify, Altera [3]	***Now***, ver_2_1_1
EP2C35F484C6	6	20390 LEs	**195.39** MHz	E [1]: 245.19 Mbits/s D [2]: **12504.96** 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 Pro VHDL Compiler, version 7.0.1.

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