OFB-mode Triple DES Cryptographic Processor Core

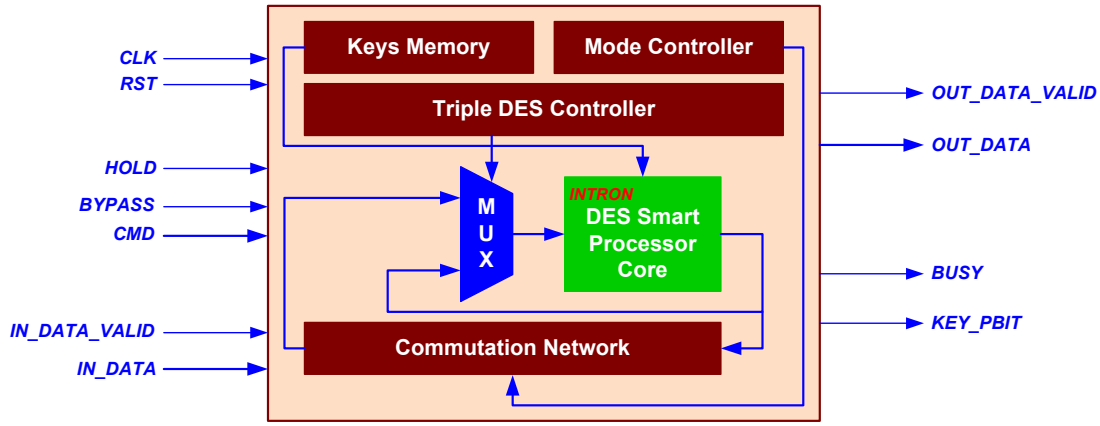
General information

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 – 64 bits;*
- *Encryption and decryption are supported;*
- *Transparent mode is supported;*
- *Hold / Valid interface is supported;*
- *Simple interface and timing;*
- *Low gate count;*
- *Iterative structure, 53 clocks per encryption/decryption;*
- *Vendor independent VHDL model, netlist for target device.*

OFB-mode Triple DES Cryptographic 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
HOLD	HIGH	Signal to stall the processing
BYPASS	HIGH	Signal to switch the Processor into transparent (test) mode
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
KEY_PBIT	HIGH	Key parity bit

Sample implementation

Device	Speed grade	Utilization	Clock rate	Performance	Synthesis and implementation tools	Availability
XILINX VIRTEX DEVICE						
XCV1000BG560	-04	1,120 Clices	39.612 MHz	47.833 Mbits/s	Synplify, Xilinx	***Now***, ver_1_1_1
ALTERA STRATIX II DEVICE						
EP2S15F484C3	3	1599 LEs	**219.93** MHz	**265.57** Mbits/s	Altera	***Now***, ver_1_1_2 ***1)***
EP2S15F484C3	3	**1371** LEs	184.26 MHz	222.50 Mbits/s	Altera	***Now***, ver_1_1_3 ***2)***

Synplify – Synplicity Synplify Pro VHDL Compiler, version 6.2.4; ***Xilinx*** – Xilinx Foundation, version 3.1i; ***Altera*** – Altera Quartus II, ver 5.1.
1) – Speed optimized; ***2)*** – Area optimized.

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