

CFB-mode Triple DES Cryptographic Fast Processor Core

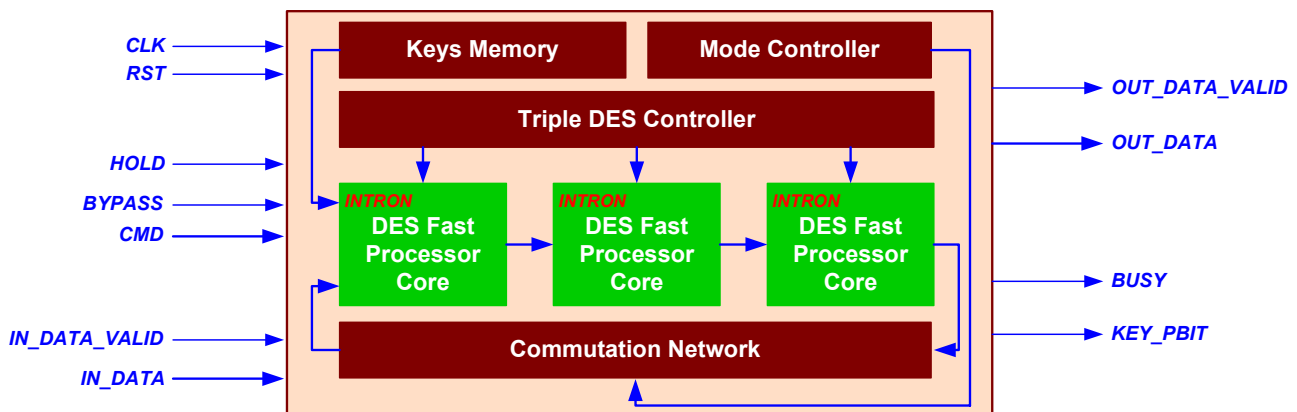
General information

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 – 64 bits;
- ❑ Simple interface and timing;
- ❑ Fast chip operation for decryption;
- ❑ No dead clock cycles;
- ❑ Encryption and decryption are supported;
- ❑ Transparent mode is supported;
- ❑ Hold / Valid interface is supported;
- ❑ Processing time – 55 clock cycles;
- ❑ Vendor independent VHDL model, netlist for target device.

CFB-mode Triple DES Cryptographic Fast Processor Core pinout



Interface description

| Pin | Activity | Description |
|-------------------|---------------------|---|
| CLK | Positive clock edge | Clock |
| RST | HIGH | Asynchronous reset |
| HOLD | HIGH | Signal to stall the processing |
| BYPASS | HIGH | Signal to switch the Processor into transparent (test) mode |
| 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 |
| 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 | 10248 Slices | 53.166 MHz | E ¹⁾ : 61.86 Mbits/s D ²⁾ : 3402.624 Mbits/s | Synplify, Xilinx | Now , ver_1_1_1 |
| ALTERA CYCLONE II DEVICE | | | | | | |
| EP2C35F484C6 | 6 | 18407 LEs | 205.93 MHz | E ¹⁾ : 239.62 Mbits/s D ²⁾ : 13179.52 Mbits/s | Altera | Now , ver_1_1_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) E – Encryption; 2) D – Decryption.