

# Triple DES

## BA412TripleDES Factsheet

### Features

- 64-bit data block encryption and decryption in ECB mode
- 56-bit key in DES mode, 56 / 112 / 168-bit key in 3DES mode
- Encryption or decryption performed in 16 cycles for DES, 48 cycles for 3DES
- 64-bit data input, data output and key input buses
- 1 clock signal (positive edge), 1 asynchronous reset
- Compliant with FIPS 800-17 and FIPS 800-20 test specifications

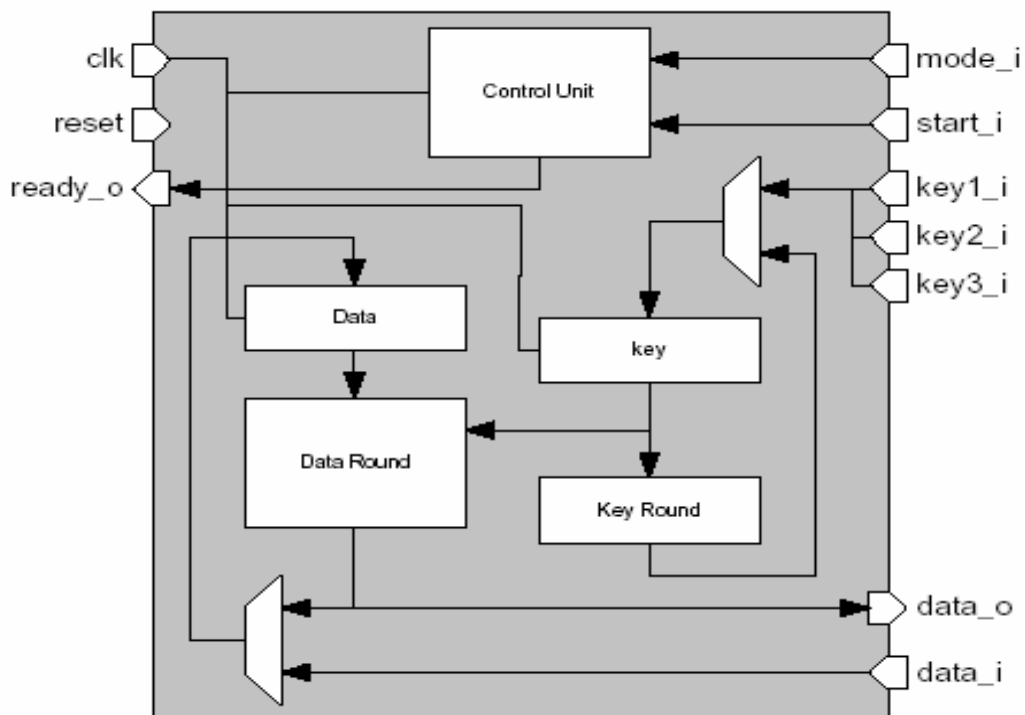


Figure 1

## General description

The DES/3DES core implements the Data Encryption Standard according to Federal Information Processing Standards Publication 46-3 the (FIPS 46-3) of the National Institute of Standards and Technology.

## Implementation data

Device	Logic	# of Clk	Performance (MHz)	Data throughput (DES/3DES)	Data latency (DES/3DES)
Atmel 58K, 0.18μ Iterative E/D small	4684	1	78	312 / 104 Mbit/s	206 / 616 ns
Atmel 58K, 0.18μ Iterative E/D fast	8604	1	165	660 / 220 Mbit/s	97 / 291 ns
Epson S1L60k, 0.25μ Iterative E/D small	4405	1	55.1	220 / 73 Mbit/s	291 / 872 ns
Epson S1L60k, 0.25μ	8193	1	145	580 / 193 Mbit/s	111 / 332 ns
Xilinx XCV400E-8FG676C Iterative E/D small	368 Slices	1	59.8	239 / 79 Mbit/s	268 / 803 ns
Xilinx XCV400E-8FG676C Iterative E/D fast	374 Slices	1	79.5	318 / 106 Mbit/s	202 / 604 ns

## Pinout description

Signal	Size	I/O	Description
clk	1	I	Core main clock. All registers are synchronized on the rising edge of the clock.
reset	1	I	Asynchronous reset. The polarity (active high or low) is a parameter.
Start_i	1	I	The start_i signal indicates that the data, mode and key inputs are valid and that the encryption/decryption processing can start. This signal is sampled on the rising edge of the clk signal. The start_i signal is ignored when the core is already processing data. When the start_i signal is active on the end of the last processing cycle, new data and key are processed immediately without wait state.
Mode_i	2	I	This signal is sampled on the rising edge of the clk signal when a start_i command is issued. It is ignored when the core is processing data. bit 0: Encryption (0) / decryption (1) mode selection. bit 1: DES (0) / 3DES (1) mode selection.
Ready_o	1	O	The ready_o flag is active high when the core has finished the data encryption or decryption, and when the data_o bus contains the result. There is no guarantee that the data_o bus is valid when the ready_o flag is not active.
Key1_i Key2_i Key3_i	64 64 64	I	Encryption / decryption key input bus. The keys are sampled on the rising edge of the clk signal when a start_i command is issued. They are ignored when the core is processing data. key1_i is used for single and triple DES. key2_i and key3_i are only used for triple DES.
Data_i	64	I	Input data bus. The input data are sampled on the rising edge of the clk signal when a start_i command is issued. They are ignored when the core is processing data.
Data_o	64	O	Output data bus. The data are only valid when the signal ready_o is active.

## Barco Silex overview

Barco Silex is a micro-electronic design house located in Belgium and France belonging to the Belgian Barco group.

Barco Silex offers a complete portfolio of high-end design services, from ASIC/FPGA design to advanced SoC/SoPC based system development, IP-core design and board design in the fields of:

- Image processing
- Communications
- Consumer electronics
- Industrial electronics.

## Barco Silex IP products

Barco Silex design expertise is also made available through a wide portfolio of IP products, with a strong focus on high performance, standardized image processing and encryption functions.

All these IP cores have been designed and fully validated by Barco Silex and are hardware proven, which guarantees high IP quality as well as best support during your integration phase.

Deliverables include:

- RTL Code or netlist (depending on license type)
- Functional simulation testbench
- Synthesis script
- Full documentation

For some of them, we can also provide you with simulation models and a design kit.

These "off the shelf", high quality IP cores provide you with the fastest and most efficient way of integrating complex functionalities on FPGAs or ASICs, while meeting short time to market constraints.

## More information

Order-reference: **BA412TripleDES**

For additional information and other IP products contact:

Barco – Silex

e-mail: [barco-silex@barco.com](mailto:barco-silex@barco.com)

<http://www.barcodesignservices.com>

or the local Barco Silex design centers:

<b>Belgium</b>	<b>France</b>
Scientific Park	ZI Peynier- Rousset
Rue du Bosquet 7	Route de Trets Imm CCE
1348 Louvain-la Neuve	13790 Peynier
+32(0)10/45.49.04	+33(0)44/216.41.06