

AES encryption and decryption

BA411AES Factsheet

Features

Iterative Encryption / Decryption Core :

- 128-bit data block encryption and decryption in ECB mode
- 128-bit key (192 and 256 bits available in separate cores)
- encryption performed in 11 cycles, decryption in 21 cycles (another version is available, with encryption performed in 10 cycles and decryption in 20 cycles)
- 128-bit data input, data output and key input buses
- 1 clock signal (positive edge), 1 asynchronous reset
- validated with reference AES test vectors

Iterative Encryption Core :

- 128-bit data block encryption in ECB mode
- 128-bit key (192 and 256 bits available in separate cores)
- encryption performed in 11 cycles
- 128-bit data input, data output and key input buses
- 1 clock signal (positive edge), 1 asynchronous reset
- validated with reference AES test vectors

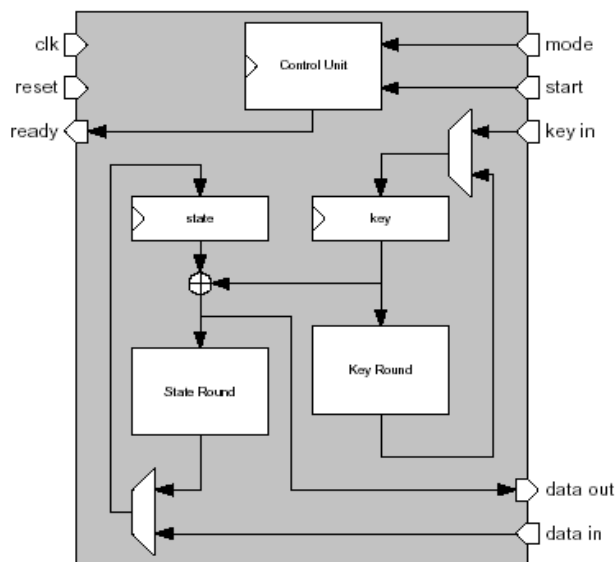


Figure 1 - Iterative Encryption/Decryption

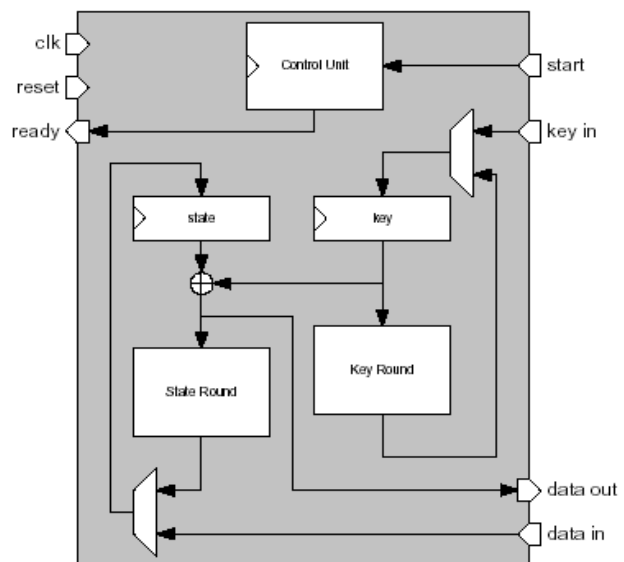


Figure 2 - Iterative Encryption

General description

The AES cores implements the Advanced Encryption Standard as specified in the Federal Information Processing Standards publication 197 (FIPS-197) of the National Institute of Standards and Technology.

Implementation data

The following tables show the cost and performance for iterative AES encryption/decryption and encryption cores targeting several technologies: ATMEL, EPSON and XILINX. For each core, two versions are available: small and fast. The small version has been optimized for space and the fast version has been optimized for speed.

Using FPGA (Virtex) the cores can be implemented with the SBox tables either in LUT or in block rams, depending on the available resources.

Device	Logic	# of Clk	Performance (MHz)	Data throughput (encrypt/decrypt)	Data latency (encrypt/decrypt)
Atmel 58K, 0.18µ Iterative E/D small	26.4k gates	1	62	721 / 377 Mbit/s	178/399 ns
Atmel 58K, 0.18µ Iterative E/D fast	32.1k gates	1	103	1198 / 627 Mbit/s	107/204 ns
Atmel 58K, 0.18µ Iterative E small	19.7k gates	1	91.1	1060 Mbit/s	121 ns
Atmel 58K, 0.18µ Iterative E fast	28.2k gates	1	162	1885 Mbit/s	67.9 ns
Epson S1L60k, 0.25µ Iterative E/D small	27.4k gates	1	52.9	615 / 322 Mbit/s	208 / 397 ns
Epson S1L60k, 0.25µ Iterative E/D fast	30.7k gates	1	96.5	1122 / 588 Mbit/s	114 / 218 ns
Epson S1L60k, 0.25µ Iterative E small	21.0k gates	1	103	1198 Mbit/s	107 ns
Epson S1L60k, 0.25µ Iterative E fast	22.6k gates	1	125	1454 Mbit/s	88 ns
Xilinx XCV400E-8 Iterative E/D, LUT	4400 LUT 289 FF	1	36.3	422 / 221 Mbit/s	304 / 579 ns
Xilinx XCV400e-8 Iterative E/D, LUT	1672 LUT 175 FF	1	50.2	584 / 305 Mbit/s	220 / 419 ns

Pinout description

Table 1: Iterative Encryption / Decryption core

Signal	Size	I/O	Description
Clk	1	I	Core main clock. All registers are triggered on the rising edge of the clock.
Reset	1	I	Asynchronous reset. This signal is active high.
Start	1	I	The start 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 signal is ignored when the core is already processing data.
Mode	1	I	Encryption / decryption mode selection. This signal is sampled on the rising edge of the clk signal when a start command is issued. It is ignored when the core is processing data.
Ready	1	O	The ready flag is active high when the core has finished the data encryption or decryption, and when the data out bus contains the result. This signal is only active during one cycle, it can be used as a register enable input to latch the result. There is no guarantee that the data out bus is valid when the ready flag is not active.
key in	128	O	Encryption / decryption key input bus. The key is sampled on the rising edge of the clk signal when a start command is issued. It is ignored when the core is processing data.
data in	128	I	Input data bus. The input data is sampled on the rising edge of the clk signal when a start command is issued. It is ignored when the core is processing data.
Data out	128	O	Output data bus. The data is only valid when the signal ready is active.

Table 2: Iterative Encryption core

Signal	Size	I/O	Description
Clk	1	I	Core main clock. All registers are triggered on the rising edge of the clock.
Reset	1	I	Asynchronous reset. This signal is active high.
Start	1	I	The start signal indicates that the data, mode and key inputs are valid and that the encryption processing can start. This signal is sampled on the rising edge of the clk signal. The start signal is ignored when the core is already processing data.
Ready	1	O	The ready flag is active high when the core has finished the data encryption, and when the data out bus contains the result. This signal is only active during one cycle, it can be used as a register enable input to latch the result. There is no guarantee that the data out bus is valid when the ready flag is not active.
key in	128	I	Encryption key input bus. The key is sampled on the rising edge of the clk signal when a start command is issued. It is ignored when the core is processing data.
data in	128	I	Input data bus. The input data is sampled on the rising edge of the clk signal when a start command is issued. It is ignored when the core is processing data.
data out	128	O	Output data bus. The data is only valid when the signal ready 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: **BA411AES**

For additional information and other IP products contact:

Barco – Silex

e-mail: barco-silex@barco.com

<http://www.barcodesignservices.com>

or the local Barco Silex design centers:

Belgium

Scientific Park
Rue du Bosquet 7
1348 Louvain-la Neuve
+32(0)10/45.49.04

France

ZI Peynier- Rousset
Route de Trets Imm CCE
13790 Peynier
+33(0)44/216.41.06