

Features

Signali's family of Advanced Encryption Standard (AES) cores are FIPS-197 compliant, and designed to meet an application-appropriate balance between high throughput, low power, and minimal area in accordance with the product requirements and schedule. These cores are available for FPGA and ASIC designs. This product brief describes the 128-bit version of the cores.

- ◆ Stand-alone AES 128-bit encryption with integrated on-the-fly key expansion
- ◆ All standard modes of operation supported
- ◆ A large variety of configurations, with optimizations in the areas of:
 - ▶ Resource utilization (LUT/gate count and Block RAM usage)
 - ▶ Latency, Data rate (bits/cycle) and Datapath width

AES is used to secure data-in-transit and data-at-rest for many common applications, including:

- ◆ Wired and wireless communications
- ◆ Encrypted storage: network-attached storage, storage-area network, iSCSI
- ◆ Electronic financial transactions
- ◆ Digital Rights Management

Example Configurations

Example performances and resource benchmarks are shown in the following table for the AES 128-bit core in ECB mode. All cores shown have a datapath width of 128 bits, except for the AES_16 core, having a datapath width of 16 bits.

IP Core	Platform	Resources		Latency (cycles)	Rate (bits/cycle)	Fmax (Mhz)	Throughput (Gbps)
		LUTs	Block RAM				
AES_Ultra	Achronix Speedster	19,100	100	55	128	950	120
	Xilinx Virtex-5	11,800	100	55	128	425	54
AES_Std	Xilinx Virtex-5	3,100	100	11	128	320	40
AES_16	Achronix Speedster	4,722	20	92	16	684	11
AES_Tiny	Xilinx Virtex-5	2,100	0	11	11.6	200	2

Deliverables

All Signali cores are delivered with the following:

- ◆ Fully synthesizable RTL (Verilog or VHDL) or netlist
- ◆ Test harness (test vectors, scripts, expected results)
- ◆ Complete documentation
- ◆ Technical support

Licensing

AES cores are licensed as soft (RTL) or firm (netlist) IP cores from Signali Corp. Special licensing arrangements are also available through our partners.

For more information about this product, or additional products and services, contact us at:

503-808-7199
info@signalicorp.com

Signali Corporation
421 SW 6th Avenue
Suite 300
Portland, OR 97204