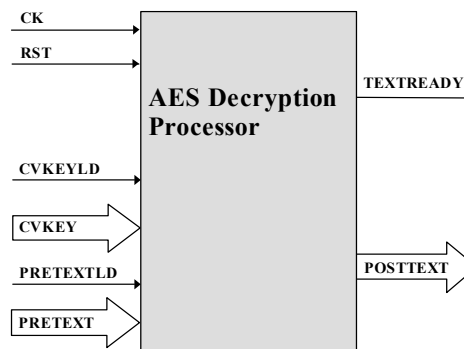
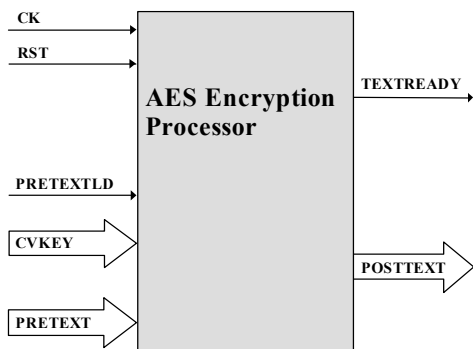


## Product Brief

# AES

Advanced Encryption Standard



### IP Core Names

R3AES-EDL – full-duplex AES encryption/decryption engine optimized for area

R3AES-EDH – full-duplex AES encryption/decryption engine optimized for speed

### Features

- AES (RIJNDael) encryption/decryption algorithm implementation (128-bit key)
- Synchronous single phase design
- Convenient external interface
- Convenient interface to synchronous 256x8 ROM cells
- Small area and lower performance or higher area and higher performance versions available
- Encryption/Decryption Processors are also available separately

### Deliverables

- Synthesizable RTL source code in VHDL or Verilog

- Comprehensive verification test bench and vectors in VHDL or Verilog
- Integration documentation and user guide

### Overview

This AES engine implements the RIJNDael algorithm.

The design targets use in ASICs and FPGAs.

The 128-bit wide input data (plaintext/ciphertext) is processed as a block by the AES core and the resultant 128-bit output data (ciphertext/plaintext) is generated.

A convenient interface is provided to synchronous 256x8 ROM cells.

The R3AES-EDL and R3AES-EDH both have the same interfaces and handshaking. The only differences are in execution speed and in area.

# RAD3 IP Cores Series: Cryptography

## Performance

### R3AES-EDH

High throughput AES engine

This high performance AES core executes one AES round per cycle and has 930 Mbps throughput at 80 MHz. It is scalable to higher frequencies and requires 40 synchronous 256x8 ROM cells.

The R3AES-EDH can be configured to have a pipeline in its decryption engine which may help some applications meet timing requirements.

Mode	Processing Rate	Initialization (when new key loaded)
Encrypt	128 bits/11 cycles	0 cycles
Decrypt w/pipeline	128 bits/11 cycles	11 cycles
Decrypt w/o pipeline	128 bits/12 cycles	12 cycles

#### ASIC implementation (0.18 TSMC process)

Gates (2-input NAND equivalent)	256x8 ROMs	Maximum Clock Speed
47,396 (Note 1)	40	100 MHz
50,654 (Note 1)	40	200 MHz

#### Xilinx Virtex implementation

	LUTs	Block RAM	Maximum Clock Speed
w/pipeline	2883	20	80+ MHz
w/o pipeline	2833	20	60+ MHz

**Note 1.** Gate count figures include 256X8 ROMs implemented as LUTs and includes key scheduling. Actual gate counts may vary depending on synthesis constraints. Contact RAD3 for a detailed gate count summary.

### R3AES-EDL

Area-optimized AES engine

This efficient AES core trades off execution speed for reduced area. The core executes one AES round per four cycles and has 222 Mbps throughput at 80 MHz. It requires 16 synchronous 256x8 ROM cells.

The R3AES-EDL can be configured to have a pipeline in its decryption engine which may help some applications meet timing requirements.

Mode	Processing Rate	Initialization (when new key loaded)
Encrypt	128 bits/44 cycles	0 cycles
Decrypt w/pipeline	128 bits/46 cycles	44 cycles
Decrypt w/o pipeline	128 bits/47 cycles	44 cycles

#### ASIC implementation (0.18 TSMC process)

Gates (2-input NAND equivalent)	256x8 ROMs	Maximum Clock Speed
23,361 (Note 1)	16	100 MHz
23,491 (Note 1)	16	200 MHz

#### Xilinx Virtex implementation

	LUTs	Block RAM	Maximum Clock Speed
w/pipeline	1490	8	80+ MHz
w/o pipeline	1491	8	60+ MHz

Specifications subject to change without notice. Information furnished by RAD3 is believed to be accurate and reliable. However, no responsibility is assumed by RAD3 for its use. All company and product names are trademarks or registered trademarks of their respective owners. All rights reserved. © 2009 RAD3 Communications Inc.