# ES4001 – AES Core

## Introduction

The es4001 AES core implements the Advanced Encryption Standard (Rijndael Algorithm FIPS 197) encoder and decoder. The core encrypts and decrypts in blocks of 128 bits. It supports key length of 128, 192 and 256.

## Features

.

- ✓ Supports AES FIPS 197 encryption and decryption.
- ✓ High speed operation. 1 clock per 1 step of operation. AES encryption is computed in 10, 12 and 14 clock cycles depending on the key length and decryption is computed in 20, 24 and 28 clock cycles.
- ✓ Simple external interface.
- ✓ Simple flow control.
- ✓ Minimal gate count.
- ✓ Support up to 64 Gbps of encryption and 48 Gbps of decryption.
- ✓ Supports upto 6.4Gbps in CBC and other feedback modes
- ✓ Available in ASIC and FPGA Technologies.

## Applications

- Secure corporate communications

  - 802.11i (Wi-Fi)
  - 802.16 (WiMax)
  - Virtual Private Networks (VPN)
  - Storage Area Networks (SAN)
  - Video conferencing
  - Voice services

- Secure electronic transactions

  - Smart Cards
  - Securities exchange
  - eCommerce

- Personal mobile communications

  - Video phones
  - PDA
  - Point-to-Point Wireless

## Pin Description

| Name | I/O | Width | Description |
|---|---|---|---|
| clk | Input | 1 | System Clock input |
| rst_n | Input | 1 | Asynchronous active low reset |
| aesIn | Input | 128 | 128 bit input plain text or cipher text data depending on the aesEncryptionMode. |
| aesInValid | Input | 1 | aesIn is valid only when this signal is asserted |
| aesKeyIn | Input | 256 | Key input is either 128, 192 or 256 depending on aesKeyType |
| aesKeyType | Input | 2 | aesKeyType defines the width of the aes key 00: 128 bits, 01:192 bits and 10: 256 key. 11: is invalid and the code will replace this with 00 option. |
| aesEncryptionMode | Input | 1 | Defines the encryption(0) and decryption(1) mode |
| aesOut | Output | 128 | Encrypted or decrypted data output. In case of the encryption mode, this bus gives the cipher text and in decryption it gives out the 128 bit plain text. |
| aesOutValid | Output | 1 | Asserted when the aesOut is valid. |
| aesBusy | Output | 1 | Asserted to indicate that the AES engine is busy and cannot accept any new inputs. The current encryption/decryption needs to be discarded by asserting the rst_n signal only. |

**Table 1. ES4001 interface.**

# Functional Description

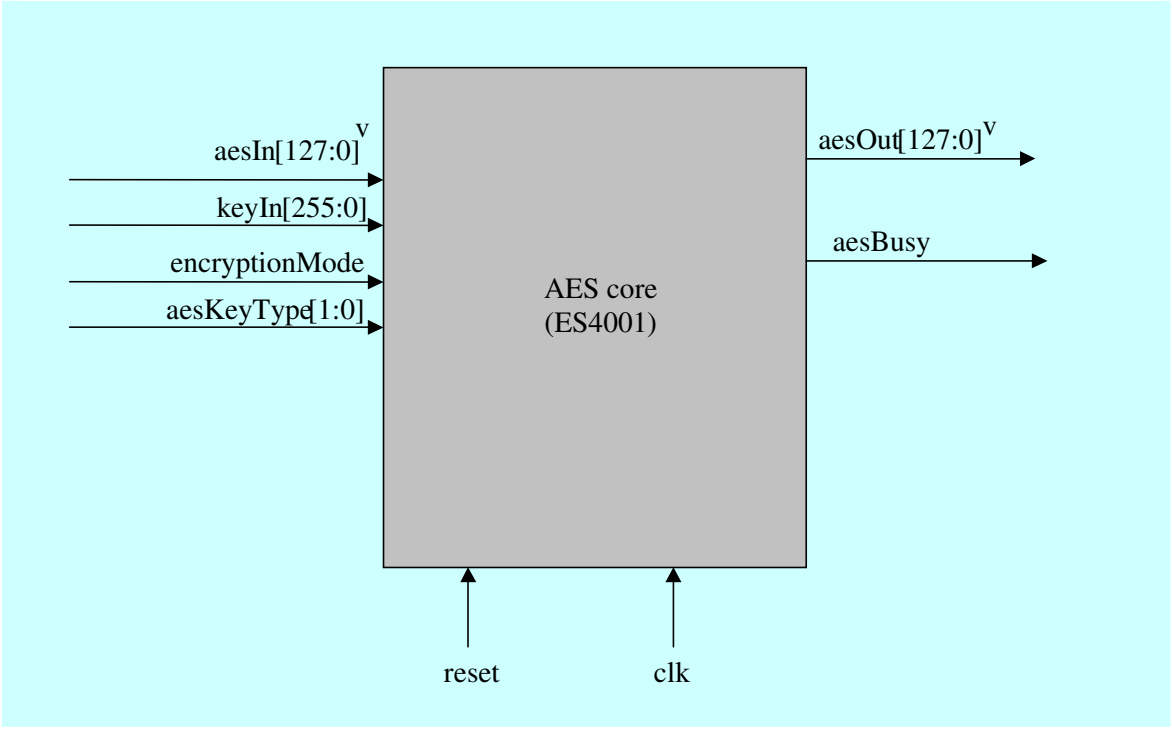


**Figure 1. ES4001 Symbol**

As shown in the block diagram, ES4001 has a very simple I/O interface. The aesIn and aesKeyIn data is latched by the block when aesInValid is high and aesBusy is not asserted. The delay of AES encryption is approximately
.

| *Mode* | *Rounds* | *Clocks* | *Throughput in Mbps (assuming 100MHz clk)* |
|---|---|---|---|
| AES 128 encryption | 10 | 10 | 1200* |
| AES 192 encryption | 14 | 14 | 914* |
| AES 256 encryption | 16 | 16 | 800* |
| AES 128 decryption | 10 | 10 | 1200* |
| AES 192 decryption | 14 | 14 | 914* |
| AES 256 decryption | 16 | 16 | 800* |

**Table 2. ES4001 performance**

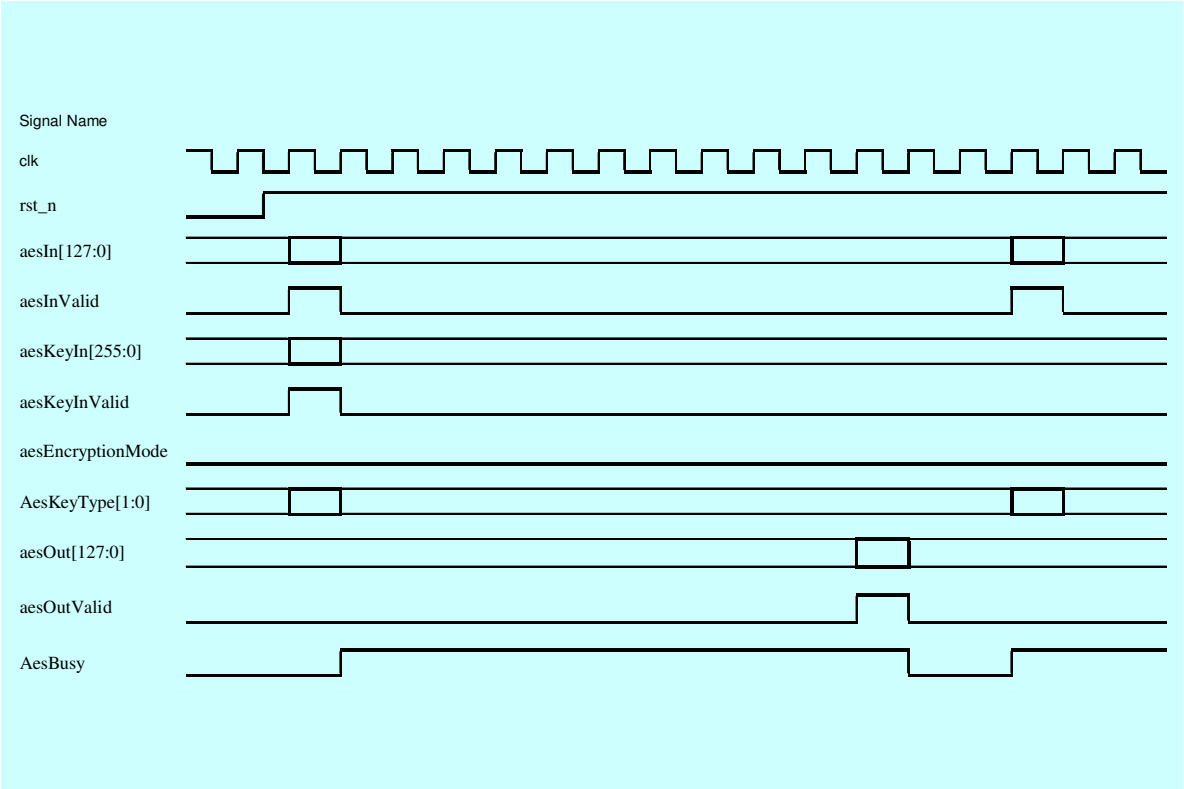


**Figure 2.** ES4001 Encryption Timing Diagram

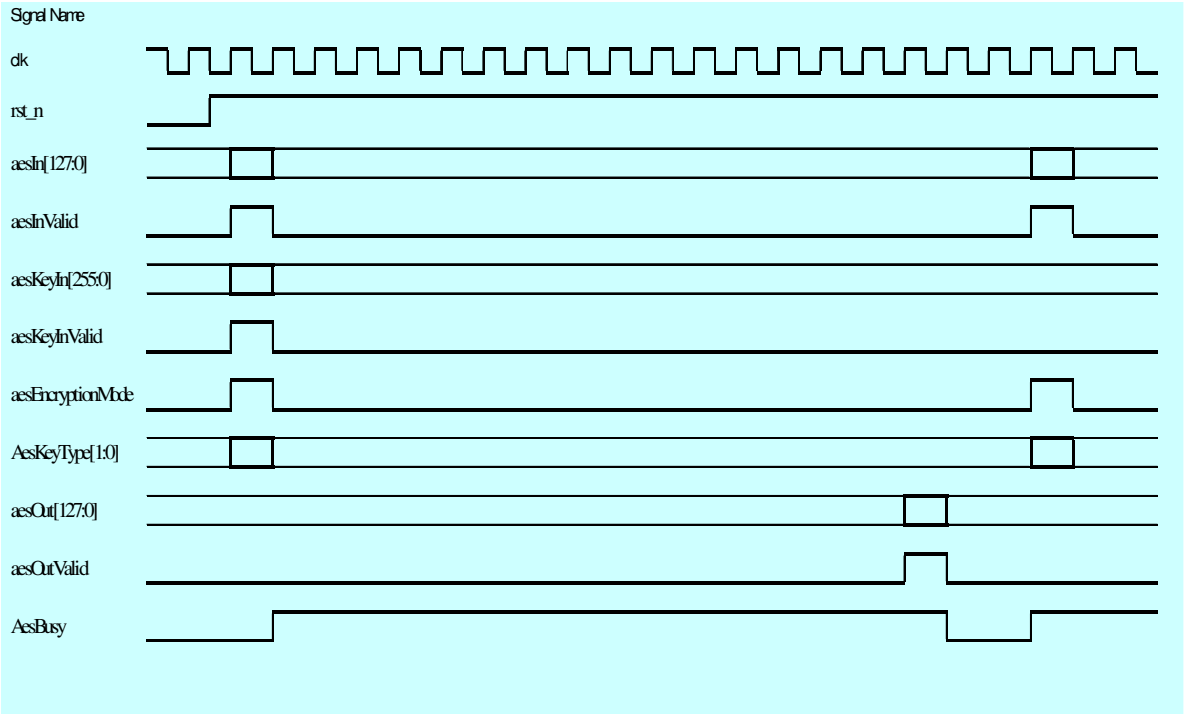


**Figure 3.** ES4001 Decryption Timing Diagram

## Deliverables

- ✓ Synthesizable Verilog RTL source code
- ✓ Simulation scripts
- ✓ Self-checking Test environment
  - ➢ Test-bench
  - ➢ Test-vectors
  - ➢ Expected results
- ✓ Synthesis scripts
- ✓ User Documentation

## Sales Representatives

For pricing information:

Esencia Technologies Inc.
2041 Mission College Blvd., Suite #100
Santa Clara CA, 95054
Tel: (408) 736-8284
Web: www.esenciatech.com
E-mail: sales@esenciatech.com

## About Esencia

Esencia Technologies is a leading provider of pre-verified virtual components for consumer electronics and communication markets at competitive prices.