



AES Cores (AES)

Technical Data Sheet

Part Number: T-CS-EN-0010-100 (AES_HP)
T-CS-EN-0009-100 (AES_128)
T-CS-EN-0012-100 (AES_192)
T-CS-EN-0013-100 (AES_256)

Document Number: I-IPA01-0121-USR Rev 04

June 2003

AES Cores (AES)

©2000 Cadence Design Foundry (UK) Ltd. All rights reserved

Proprietary Notice

In the U.S. and numerous other countries, Cadence and the Cadence logo are registered trademarks and Cadence Design Foundry is a trademark of Cadence Design Systems, Inc. All other products or services mentioned herein may be trademarks of their respective owners.

Neither the whole nor any part of the information contained in, or the product described in this document may be adapted or reproduced in any material form except with the prior written permission of the copyright owner.

The product described in this document is subject to continuous developments and improvements and is supplied "AS IS". All warranties implied or expressed including but not limited to implied warranties or merchantability, or fitness for purpose, are excluded. Cadence Design Foundry, Inc shall not be liable for any loss or damage arising from the use of any information in this document, or any error or omission in such information, or any incorrect use of the product. Cadence Design Foundry products are not authorized for use as critical components in life support devices or systems without the express written approval of an authorised officer of Cadence Design Foundry, Inc. As used herein:

1. Life support devices or systems are devices or systems that are (a) intended for surgical implant into the body or (b) support or sustain life, and whose failure to perform, when properly used in accordance with instructions for use provided in the labeling, can be reasonably expected to result in a significant injury to the user.
2. A critical component is any component of a life support device or system or system whose failure to perform can reasonably be expected to cause the failure of the life support device or system, or to affect its safety or effectiveness.

AES Cores (AES)

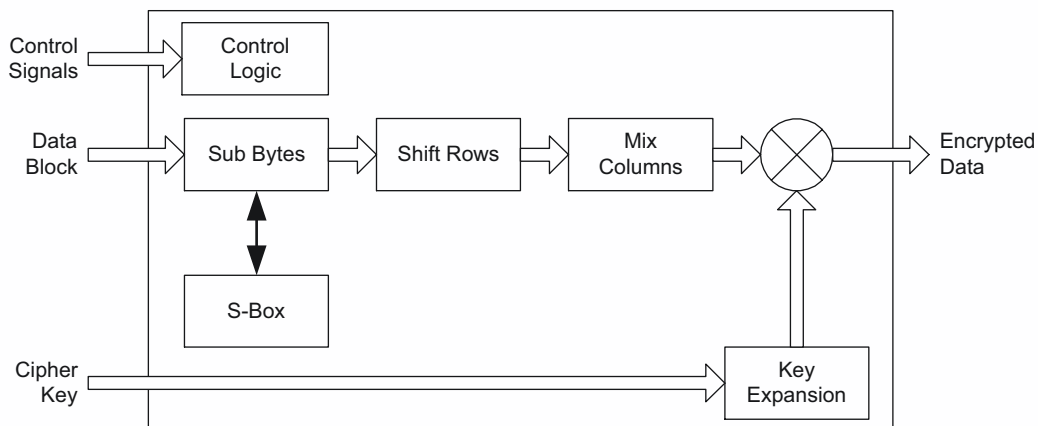
Features

- Conforms to the Advanced Encryption Standard as specified in the NIST FIPS 197
- 128 bit block size with programmable key sizes of 128 bit, 192 bit or 256 bit
- Cipher modes of operation - electronic codebook (ECB); cipher block chaining (CBC); output feedback (OFB); cipher feedback (CFB); counter mode CBC-MAC (CCM); counter mode (CTR)
- Four different implementations available:
 - Single high performance version with 960 Mbit/s throughput at 83 MHz for use with all three key sizes of 128 bit, 192 bit or 256 bit
 - Three low power versions with 260 Mbit/s throughput at 83 MHz for use with each of the different key sizes of 128 bit, 192 bit or 256 bit

Description

The AES Core is a hardware implementation of the Rijndael Block Cipher Algorithm, which was chosen for the Advanced Encryption Standard (AES) as specified in the Federal Information Processing Standards 197 (FIPS PUB 197) (<http://www.itl.nist.gov/fipspubs>). It supports the most commonly used cipher modes ECB, CBC, OFB, CFB, and CTR detailed in NIST Special Publication 800-38A. Counter mode with CBC-MAC (CCM) is also an operation mode that is supported since the building blocks of this mode, CTR and CBC, are available in the modes wrapper. A single high performance and three low power versions of the AES Core make it suitable for a wide range of SoC encryption applications.

- AES High Performance (AES_HP), Part number T-CS-EN-0010-100, for use with all three key sizes of 128 bit, 192 bit or 256 bit
- AES Low Power 128 bit Key (AES_128), Part number T-CS-EN-0009-100, for use with a key size of 128 bit
- AES Low Power 192 bit Key (AES_192), Part number T-CS-EN-0012-100, for use with a key size of 192 bit
- AES Low Power 256 bit Key (AES_256), Part number T-CS-EN-0013-100, for use with a key size of 256 bit



Area Speed Trade-off

There are four different implementations of the AES as follows:

- Single high performance version with large area, high throughput running at 960 Mbit/s requiring approximately 69000 gates
- Three low power versions with small area, low throughput running at up to 260 Mbit/s requiring up to 40000 gates.

| | AES_128 | AES_192 | AES_256 | AES_HP |
|--|---------|---------|---------|--------|
| Total area (gates) | 36000 | 42000 | 40000 | 69000 |
| Estimated throughput (Mbit/s) based on 83 MHz | 260 | 175 | 150 | 960 |

Cycles Per Operation

| AES Type | Encrypt | Initial Decrypt | Decrypt |
|----------|---------|-----------------|---------|
| AES_128 | 42 | 54 | 43 |
| AES_192 | 50 | 64 | 51 |
| AES_256 | 58 | 75 | 59 |
| AES_HP | 12 | 24 | 12 |

Signal Interfaces

| Signal Name | I/O | Description |
|---|-----|--|
| clk | I | Clock |
| n_reset | I | Asynchronous reset |
| soft_n_reset | I | Synchronous reset by software control |
| aes_in[127:0] | I | Input data to be ciphered with AES |
| aes_out[127:0] | O | The encrypted/decrypted data output from AES |
| encrypt | I | 1 = encrypt; 0 = decrypt |
| start | I | Enables the AES algorithm and starts the encrypt/decrypt process. |
| new_key | I | 1 = indicates a new key being used or initial decrypt. |
| key_in[127:0] key_in[191:0] key_in[255:0] | I | Cryptographic key size that can be one of the three sizes shown. |
| valid_data | O | Asserted when valid data is at aes_out |
| key_size | I | Size of encryption keys to be used: 00 : 128-bit 01 : 192-bit 10 : 256-bit 11 : unused |

Wrapper Logic

The following additional signals are required when wrapper logic is used:

| Signal Name | I/O | Description |
|-------------|-----|---|
| cbc | I | 1 = CBC; 0 = ECB |
| ofb | I | 1 = OFB used; 0 = not used |
| cfb | I | 1 = CFB mode; 0 = not used |
| ctr | I | 1 = CTR; 0 = not used |
| iv[127:0] | I | Initialization vector for CBC mode, or initial authentication block (B ₀) during CCM mode |
| width[1:0] | I | 00 = 1 bit mode; 01 = 8 bit mode; 10 = 128 bit mode; 11 = not used |
| first | I | Indicates first round of encryption |

Physical Estimates

| | AES_128 | AES_192 | AES_256 | AES_HP |
|-------------------------|---------|---------|---------|--------|
| Gate count | 36000 | 42000 | 40000 | 69000 |
| FF count | 1119 | 1373 | 1280 | 1166 |
| SOC internal pins (in) | 395 | 459 | 523 | 526 |
| SOC internal pins (out) | 129 | 129 | 129 | 129 |

Verification

IP modules from Cadence Design Foundry are verified to one of the following levels:

| | |
|-----------------------|--|
| Gold | IP has been to target silicon |
| Silver | IP has been to silicon in FPGA |
| Bronze | IP has been verified in simulation with logical timing closure |
| In development | IP has not yet been verified |

Please contact the IP Gallery™ (ipgallery@cadence.com) for the latest verification information.

Deliverables

The full IP package comes complete with:

- Verilog HDL
- Cadence BuildGates and Synopsys Design Compiler synthesis scripts
- Verilog testbench
- *AES User Guide* with full description and operation, synthesis and integration instructions

Cadence Design Foundry

Cadence Design Foundry, a division of Cadence Design Systems, Inc. (NYSE:CDN), is a leading provider of electronic design and supply chain management services. Leading and emerging technology companies around the globe leverage Cadence Design Foundry's engineering services and intellectual property for the design of complex integrated circuits and systems-on-chip (SoC). Cadence is head quartered in San Jose, California. For more information, please contact us: North America 1 877 473 2924, Europe +44 (0) 1506 595955, Asia +81 (0) 454 757756, by e-mail IPGallery@cadence.com, or visit us on the World Wide Web at: <http://www.cadence.com>.