Dillon Engineering, Inc.

3925 West 50th Street, Suite 202, Edina, MN 55424
Tel.: 952-836-2413 Fax: 952-927-6514
www.dilloneng.com

AES (Rijndael) Library IP Core

1 Features

- Complies with Federal Information Processing Standard (FIPS) 197
- Data throughput up to 12.8 Gb/s
- Several configurations available to trade throughput for area
- Key can be changed dynamically with no throughput penalty
- Cores available for encryption, decryption, or combined encryption/decryption
- Available in generic HDL or EDIF formats
- Full test bench supplied
- Supports ECB, CBC, CFB, OFB, and CTR modes (NIST special publication 800-38A)

2 General Core Description and Background

The Dillon Engineering (DE) AES Library IP Core performs data encryption and/or decryption as specified by the Federal Information Processing Standard (FIPS) 197, Advanced Encryption Standard (AES). The HDL for the core is designed so it can be targeted toward FPGAs or ASICs. The AES Library IP Core addresses a wide range of throughput requirements by providing various levels of parallelism which trade throughput for area.

2.1 Background

AES was designed to replace the Data Encryption Standard (DES) which was developed in the 1970s. Following the submission of 15 candidate algorithms in 1998, five finalists were chosen in 1999, and the Rijndael algorithm was chosen as the Advanced Encryption Standard in 2000. AES is a *symmetric key block* cipher algorithm. A *symmetric key* cipher uses the same key for encryption and decryption, which is in contrast to public-key block ciphers, where separate public and private keys are used for encryption and decryption. A *block* cipher operates on data in blocks. Specifically, AES operates on 128-bit blocks of data, as described in the next section.

2.2 AES Algorithm Information

The inputs to the AES algorithm are a 128-bit block of plaintext and a key which is 128, 192, or 256 bits, and the output is a 128-bit block of ciphertext. The National

Institute for Standards and Technology (NIST) website provides a complete description of how the plaintext block and key are used to compute the ciphertext block at http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf.

2.3 Modes of Operation

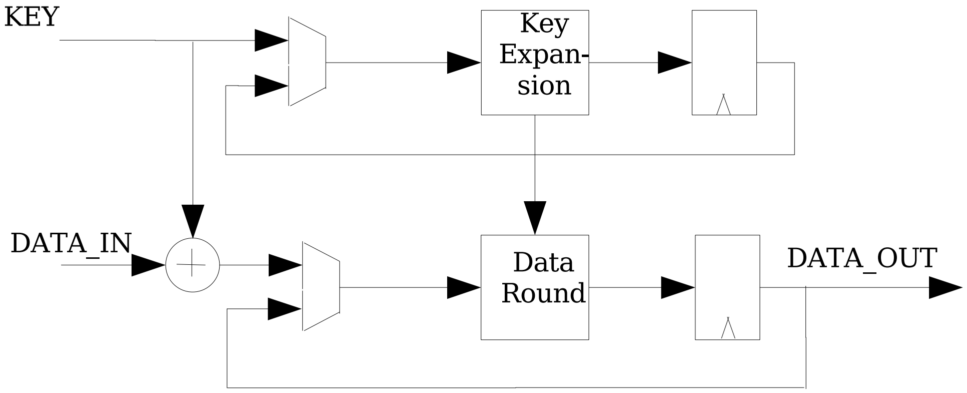
The DE AES Library IP Core supports the ECB, CBC, CFB, OFB, and CTR modes of operation. A mode of operation is an algorithm that features the use of a symmetric key block cipher algorithm (such as AES). The modes of operation are described by NIST at http://csrc.nist.gov/CryptoToolkit/modes/.

3 Theory of Operation

The DE AES Core is a ParaCore Architect™ IP Core, making configuration option specification at compile time via parameters. A highly efficient Core is created as logic required for modes of operation not needed by this application aren't included in the Core. As an example, if the key length of 192 bits isn't required, the core created would contain no logic pertaining to the 192-bit key, even though the version that supports 128-bit and 256-bit keys is generated from the same source code.

3.1 Block Diagram

The block diagram shows the basic DE AES architecture for encryption. A similar architecture is used for the decryption core and the combined encryption/decryption core.



3.1.1 Key Expansion

The key expansion block performs four iterations of the key expansion algorithm described in the FIPS197 specification. The 128-bit input is the round key for round i, and the 128-bit output is the round key for round i+1. Internally, for a 128-bit key, the block contains five 32-bit 2-input XORs, one RotWord transformation, and one SubWord transformation, where the RotWord and SubWord transformations are defined in the FIPS197 specification. The key expansion block for 192-bit and 256-bit keys use the same internal functions in a slightly different way due to the larger key sizes.

3.1.2 Data Round

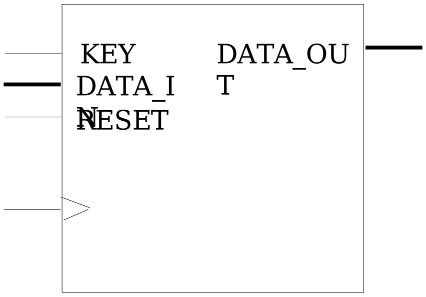
The data round block performs the data processing for a single round. The input and output each represent the 128 bits of the state matrix. Internally, the block contains 16 S-box substitutions, wiring for the ShiftRows transformation, four MixColumns operations (one for each column of the state matrix), and a 128-bit 2-input XOR for the AddRoundKey transformation, where the S-box and the ShiftRows, MixColumns, and AddRoundKey transformations are defined in the FIPS197 specification. The data round block is independent on the key length.

4 Interface

All interface to the AES IP module is synchronous CLK input and defined in the following sections.

4.1 Schematic Symbol

The AES schematic symbol:



A_<inputs> is actually a series of ports, based upon the *inputs* parameter. If *inputs* == 1, then A_0 is the only input port, otherwise A_0, A_1, ... A_N are the input ports, where N == *inputs* -1. Real data is on the most significant half of the port and imaginary data in on the least significant half of the port.

X_<inputs> is actually a series of ports, based upon the *outputs* parameter. If outputs == 1, then X_0 is the only input port, otherwise X_0, X_1, ... X_N are the input ports, where N == outputs -1. Real data is on the most significant half of the port and imaginary data in on the least significant half of the port.

4.2 Signals Defined

Signal definition table:

Signal	***Direction***	***Description***
DATA_IN	IN	Input data to module, valid one clock cycle after SYNC_IN.
SYNC_IN	IN	Synchronize incoming data to module. Active for one clock to indicate new set of data to process.
KEY	IN	KEY input, new can is applied with each SYNC_IN and data set.
RESET	IN	Synchronous reset, should be applied for a one clock cycle minimum before using IP after configuration.
CLOCK		
DATA_OUT	OUT	Output data from the module, valid one clock cycle after the SYNC_OUT.
SYNC_OUT	OUT	Indicates result is ready and will begin streaming out on the next clock cycle.

5 Area and Performance

The DE AES Library IP Core can be configured for a variety of throughput requirements. The following table shows three of these configurations along with throughput information and area usage on a Xilinx Virtex II FPGA. The data in the table refers to an AES encryption-only engine with a 128-bit key which can be changed with every 128-bit input data block.

Configuration (round/S-box)	***Throughput (Mbps)***	***18Kbit Block RAM***	***Slices***
Serial/Serial	128 * frequency	2	TBD
Serial/Parallel	12.8 * frequency	10	TBD
Parallel/Parallel	12.8 * frequency / 8	90	TBD

As the first column of this table shows, the DE AES Core can be configured for parallelism at the round level and at the S-box level. Parallel rounds imply that all Nr rounds (Nr = 10 for 128-bit key, Nr = 12 for 192-bit key, Nr = 14 for 256-bit key) can be operated in parallel during a single clock cycle, while Serial rounds mean that the Nr rounds require Nr clock cycles. Parallel S-box means that all 16 S-box substitutions within a round are performed in parallel, while serial S-box means that the 16-Sbox substitutions within a round require 8 clock cycles, where 2 S-box substitutions are performed during each of the 8 clock cycles.