

CAST



AES-P

Programmable AES Encryption - Decryption, Core

The AES-P core implements hardware data encryption and decryption using Rijndael encoding in compliance with the FIPS-197 Advanced Encryption Standard (AES).

The versatile core can be run-time programmed to: perform either encryption or decryption; run in any of the common block-cipher modes (ECB, CBC, CFB, OFB, and CTR); and use a 128-bit, 192-bit or 256-bit cipher key.

Two architectural versions are available to suit system requirements. The Standard version (AES32-P) is more compact, using a 32-bit datapath and requiring 44/52/60 clock cycles for each data block (128/192/256-bit cipher key, respectively). The Fast version (AES128-P) achieves higher throughput, using a 128-bit datapath and requiring 11/13/15 clock cycles for each data block. The Fast version can achieve rates of 2.8 Gbps or more in FPGAs, and 5 Gbps or more in ASICs.

The core includes an internal round key table in which expanded AES encryption and decryption key values are stored. An optional Key Expander module can automatically generate the round keys and fill the table, or this can be handled externally by the user.

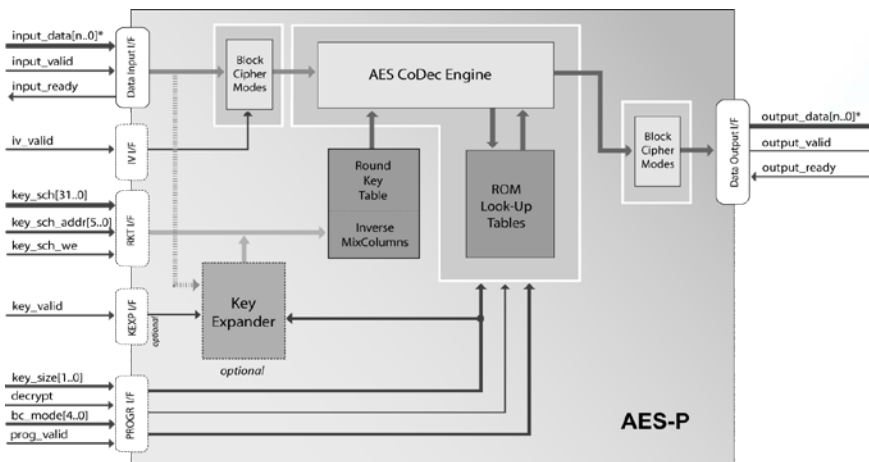
Fully-stallable input and output interfaces simplify AES integration for different applications. These enable system software to stop the input stream according to a specific data arrival rate, or to stop the output stream when the core is not able to receive data.

The core has been verified against the AES FIPS 197 standard using the NIST AES Algorithm Validation Suite (AESAVS), NIST document SP800-38A, and additional random test vectors. Deliverables include all these tests, plus a bit-accurate model (BAM) for generating additional test vectors. The AES-P core has been evaluated in a variety of technologies, and is available optimized for ASICs or FPGAs.

Applications

The AES-P core is suitable for a variety of applications, including: secure networking routers; wireless communications; encrypted data storage; secure video surveillance systems; and electronic financial transactions.

Block Diagram



* n = 127 for AES128-P core.
n = 31 for AES32-P core.

Features

- Conforms to the Advanced Encryption Standard (AES) standard (FIPS PUB 197)
- Single module efficiently integrates multiple AES functions and modes
- Run-time programmable for:
 - Encryption or Decryption
 - Cipher Key length: 128- 192- or 256-bits
 - Cipher Mode: ECB (Electronic Codebook) CBC (Cipher Block Chaining) CFB (Cipher Feedback) OFB (Output Feedback) CTR (Counter)
- Two architectural versions available:
 - Standard is more compact: 32-bit data path size Processes each 128-bit data block in 44/52/60 clock cycles for 128/192/256-bit cipher key, respectively
 - Fast yields higher transmission rates: 128-bit data path Processes each 128-bit block in 11/13/15 clock cycles for 128/192/256-bit cipher key, respectively
- Optional Key Expander automatically generates and stores Round Keys for AES processing
- Optimized design for ASIC or FPGA implementations
- Verified against the AES FIPS 197 standard using:
 - Known Answer Tests (KAT) of the NIST AES Algorithm Validation Suite (AESAVS)
 - Block cipher modes tests of NIST document SP800-38A
 - Additional random test vectors
- Fully-stallable input and output interfaces, ideal for streaming applications, e.g. system software can:
 - pause input processing to match slow transmission, or
 - pause output processing to allow a slower application to catch up with decrypted data
- Deliverables include bit-accurate software model (BAM) for easy user-generation of tests

Functional Description

The core performs standard AES processing, efficiently combining some steps into a single look-up table operation.

The round key values for the current cipher key must be calculated prior to any encryption or decryption operation, by system software, or with the optional Key Expander to save processing time. The values are stored in the Round Key Table and accessed by the AES CoDec Engine. Both the round key for encryption and the inverse round key for decryption are stored; the inverse round key is obtained by using the Inverse MixColumns function.

The core can encrypt or decrypt a stream of 128-bit blocks of data until a new cipher key has to be used and the round key values recalculated. The cipher key size and whether the core will encrypt or decrypt the data block are controlled by the state of input control signals, and may be changed on the beginning of each block without any performance penalty.

A powerful input/output interface permits fully-stallable data streaming through the core. The application receiving the output of the core can arbitrarily pause the generation of output data. In a similar way, the application that feeds data to the input can arbitrarily pause the data stream to the core. The core can also stall the application feeding its input, when the core is busy processing, or when the output cannot receive any more processed data.

Implementation Results

AES-P reference designs have been evaluated in a variety of technologies. The following are sample Xilinx results for the core, including the Key Expander, and optimized for speed. Throughput figures are given for 128-bit cipher key in ECB block-cipher mode.

STANDARD Version (AES32-P)

Xilinx Device	Slices	Fmax (MHz)	Throughput (Mbps)	BRAM	ISE
Spartan-3 3S1000-5	1,494	106	308	5 RAMB16	12.2
Spartan-6 6SLX9-3	790	140	407	5 RAMB16	12.2
Virtex-5 5VLX30-3	714	239	695	3 RAMB36 1 RAMB18	12.2
Virtex-6 6VLX75T-3	715	270	785	3 RAMB36 2 RAMB18	12.2

FAST Version (AES128-P)

Xilinx Device	Slices	Fmax (MHz)	Throughput (Mbps)	BRAM	ISE
Spartan-3 3S1000-5	1,992	83	965	12 RAMB16	12.2
Spartan-6 6SLX9-3	855	148	1,722	12 RAMB16	12.2
Virtex-5 5VLX30-3	984	212	2,466	10 RAMB36 1 RAMB18	12.2
Virtex-6 6VLX75T-3	1,046	243	2,827	10 RAMB36 2 RAMB18	12.2

Export Permits

This encryption technology is governed internationally by export regulations. Immediate export of the core is permitted to the following countries for uses not related to weapons of mass destruction:

Argentina	Japan	South Korea
Australia	New Zealand	Switzerland
Canada	Norway	Turkey
European Union Member States	Russia	Ukraine
		United States

Please contact CAST to discuss delivery to other destinations; approval is subject to the applicable export licenses being granted. The license can be generated from either the EU or the USA. Please note that licensees are responsible for complying with the applicable requirements for re-export of electronics containing strong encryption technology.

Support

The core as delivered is warranted against defects for ninety days from purchase. Thirty days of phone and email technical support are included, starting with the first interaction. Additional maintenance and support options are available.

Verification

The core has been verified through extensive synthesis, place and route and simulation runs. It has also been embedded in several products, and is proven in FPGA technologies.

Deliverables

The core is available in ASIC (synthesizable HDL) and FPGA (netlist) forms, and includes everything required for successful implementation. The Xilinx version includes:

- Post-synthesis EDIF or NGC netlist
- Sophisticated self-checking Testbench (Verilog versions use Verilog 2001)
- Software (C++) Bit-Accurate Model and test vector generator
- Simulation scripts
- NIST KAT test vectors, SP800-38A test vectors, additional vectors for block cipher modes
- Place and route scripts
- Comprehensive user documentation, including detailed specifications and a system integration guide.

Related Cores

The CAST AES-C core executes just a single AES mode (selected prior to synthesis) for an encryption and decryption implementation that is typically smaller and faster.