



# AES-P

## Programmable AES Encrypt/Decrypt Megafunction

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

The versatile megafunction 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 is more compact, using a 32-bit datapath and requiring four clock cycles for each data block. The Fast version achieves higher transmission bit rates (throughput), using a 128-bit datapath and requiring one clock cycle to for each data block. The Fast version can achieve throughput rates of 2 Gbps or more in FPGAs, and 5 Gbps or more in ASICs.

The megafunction 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.

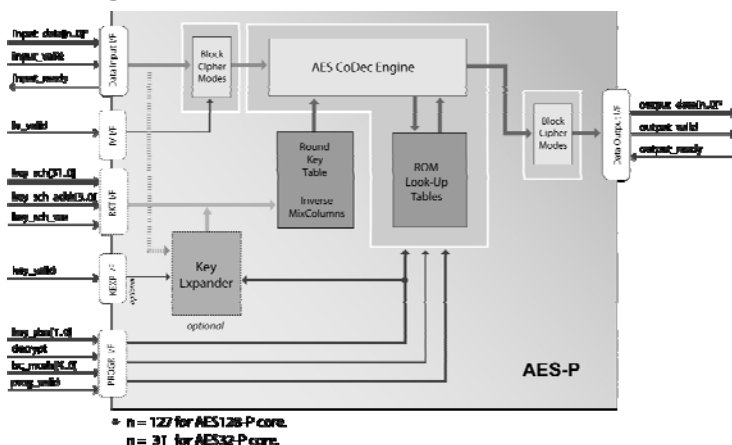
Fully-stallable input and output interfaces simplify AES integration for different applications. These enable system software to stop the input stream according to a specific data arrival rate, or to stop the output stream when the megafunction is not able to receive data.

The megafunction 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 megafunction has been evaluated in a variety of technologies, and is available optimized for ASICs or FPGAs.

### Applications

The AES-P megafunction 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



### 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 keys, 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 keys, respectively
- 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
- 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
- Deliverables include bit-accurate software model (BAM) for easy user-generation of tests
- Scan-ready design architecture

## Functional Description

The megafunction 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 megafunction 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 megafunction 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 megafunction. The application receiving the output of the megafunction 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 megafunction. The megafunction can also stall the application feeding its input, when the megafunction is busy processing, or when the output cannot receive any more processed data.

## Export Permits

Strong encryption technology is governed internationally by export regulations. Immediate export of the megafunction is permitted to the following countries for non-military applications:

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 or military applications; 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.

## Implementation Results

AES-P reference designs have been evaluated in a variety of technologies. The following are sample Altera results for the fast version running ECB mode, with the round key table, no key expander, and optimized for speed.

Altera Device	LEs/ALUTs	Memory	I/Os	Fmax (MHz)	Throughput (Gbps)	Quartus
Arria EP1AGX50-6	2110	36 M4Ks	275	102	1.18	8.0
Cyclone EP1C20-6	2365	36 M4Ks	275	90	1.11	8.0
Cyclone-II EP2C20-6	2296	36 M4Ks	275	112	1.30	8.0
Cyclone-III EP3C40-6	2288	20 M9Ks	275	140	1.63	8.0
Stratix EP1S10-5	2365	36 M4Ks	275	102	1.19	8.0
Stratix-II EP2S30-3	2186	36 M4Ks	275	162	1.88	8.0
Stratix-III EP3S50-2	2133	22 M9Ks	275	186	2.16	8.0

## Support

The AES-P megafunction 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 AES-P megafunction has been verified through extensive simulation and rigorous code coverage measurements. It has also been verified in a prototyping FPGA board platform.

## Deliverables

The AES-P is available as a soft megafunction (synthesizable HDL) for ASIC technologies and as a firm megafunction (netlist) for FPGA technologies, and includes everything required for successful implementation. The Altera version includes:

- Post-synthesis EDIF netlist
- Place and route script
- Simulation script, vectors and expected results.
- Sophisticated self-checking Testbench (Verilog versions use Verilog 2001).
- Software (C++) Bit-Accurate Model.
- Comprehensive user documentation, including detailed specifications and a system integration guide.

## Related IP Megafunctions

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

**CAST**  
info@cast-inc.com  
www.cast-inc.com

CAST, Inc. 11 Stonewall Court  
Woodcliff Lake, NJ 07677 USA  
tel 201-391-8300 fax 201-391-8694

Copyright © CAST, Inc. 2008, All Rights Reserved.  
Contents subject to change without notice.  
Trademarks are the property of their respective owners.



This megafunction developed by the encryption experts at Alma Technologies S.A.

