

CAST

ALTERA

AES-C

AES Optimized Encrypt/Decrypt Megafunction

The AES-C megafunction implements hardware data encryption and decryption using Rijndael encoding in compliance with the FIPS-197 Advanced Encryption Standard (AES). It runs any one of the common block-cipher modes: ECB, CBC, CFB, OFB, or CTR.

The megafunction can be run-time programmed to perform either encryption or decryption, and to 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.

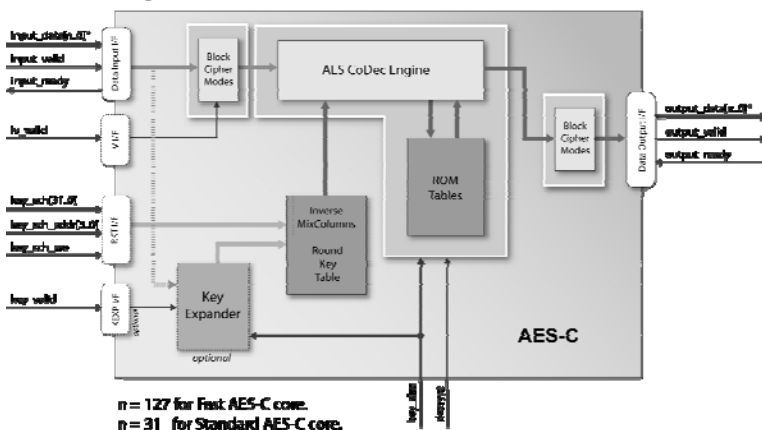
Fully-stallable input and output interfaces simplify AES integration for different applications. These enable system software to stop the input stream according to a specific data arrival rate, or to stop the output stream when the megafunction is not able to receive data.

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-C 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
- Run-time programmable for:
 - Encryption or Decryption
 - Cipher Key length: 128- 192- or 256-bits
- Executes one AES mode, configured prior to synthesis:
 - ECB (Electronic Codebook)
 - CBC (Cipher Block Chaining)
 - CFB (Cipher Feedback)
 - OFB (Output Feedback)
 - CTR (Counter)
- Two architectural versions:
 - 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
- Round key (encryption) and inverse round key (decryption) both stored internally
- 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. It operates in any one of the common block cipher modes (ECB, CBC, CFB, OFB, CTR) as selected before synthesis.

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.

Implementation Results

AES-C reference designs have been evaluated in a variety of technologies. The following are sample Altera results for the standard AES-C megafunction in ECB, without the optional Key Expander, and optimized for speed. All I/Os are assumed to be routed off-chip and I/O registers are included.

Family Device	LEs/ALUTs	Memory	I/Os	Fmax (MHz)	Throughput (Mbps)	Quartus
Cyclone EP1C12-6	792	10 M4K	115	111	321	7.2
Cyclone-II EP2C20-6	779	10 M4K	115	119	345	7.2
Cyclone-III EP3C120-6	789	6 M9K	115	136	394	7.2
Stratix EP1S10-5	760	10 M4K	115	113	327	7.2
Stratix-II EP2S15-3	632	10 M4K	115	192	556	7.2
Stratix-III EP3SE50-2	630	6 M9K	115	208	603	7.2

Note: key expander adds another 550 LEs

Export Permits

Strong encryption technology is governed internationally by export regulations. Immediate export of the megafunction is permitted to the following countries:

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.

Support

The 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 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-C 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
- Place & Route scripts
- Simulation script, vectors and expected results
- NIST KAT test vectors, SP800-38A test vectors, additional vectors for block cipher modes
- Sophisticated self-checking Testbench (Verilog versions use Verilog 2001)
- Software (C++) Bit-Accurate Model for additional test vector generation
- Comprehensive user documentation, including detailed specifications and a system integration guide