AES-CCM

Advanced Encryption Standard Core

The AES-CCM encryption IP core implements Rijndael encoding and decoding in compliance with the NIST Advanced Encryption Standard. It processes 128-bit blocks, and is programmable for 128-, 192-, and 256-bit key lengths.

Two architectural versions are available to suit system requirements. The Standard version (AES-CCM-S) 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 (AES-CCM-F) achieves higher throughput, using a 128-bit datapath and requiring 11/13/15 clock cycles for each data block.

CCM stands for Counter with CBC- MAC mode. CCM is a generic authenticate-and-encrypt block cipher mode. CBC-MAC is utilized to generate an authentication string while CTR mode is used to encrypt.

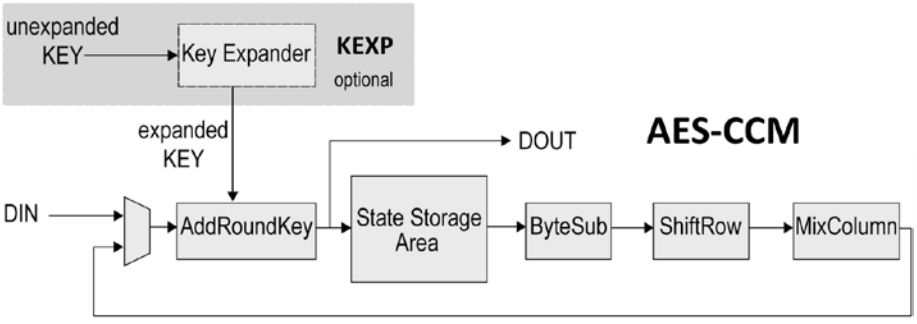
The AES-CCM core is a fully synchronous design and has been evaluated in a variety of technologies, and is available optimized for ASICs or FPGAs.

Applications

The AES-CCM can be utilized for a variety of encryption applications including:

- Protected network routers
- Electronic financial transactions
- Secure wireless communications
- Secure video surveillance systems
- Encrypted data storage

Block Diagram



Features

- Encrypts and decrypts using the AES Rijndael Block Cipher Algorithm
- Satisfies Federal Information Processing Standard (FIPS) Publication 197 from the US National Institute of Standards and Technology (NIST)
- Processes 128-bit data in 32-bit blocks
- Employs user-programmable key size of 128, 192, or 256 bits
- 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
- Works with a pre-expended key or can integrate the optional key expansion function
- Simple, fully synchronous, reusable design
- Available as fully functional and synthesizable VHDL or Verilog, or as a netlist for popular programmable devices
- Complete deliverables include test benches, C model and test vector generator

Functional Description

An AES encryption operation transforms a 128-bit block into a block of the same size. The encryption key can be chosen among three different sizes: 128, 192, or 256 bits. The key is expanded during cryptographic operations.

The AES algorithm consists of a series of steps repeated a number of times (rounds). The number of rounds depends on the size of the key and the data block. The intermediate cipher result is known as state.

	KSIZE = 00	KSIZE = 01	KSIZE = 10
Rounds	• 10	• 12	• 14

Number of rounds as a function of key size

Initially, the incoming data and the key are added together in the AddRoundKey module. The result is stored in the State Storage area.

The state information is then retrieved and the ByteSub, Shiftrow, MixColumn and AddRoundKey functions are performed on it in the specified order. At the end of each round, the new state is stored in the State Storage area. These operations are repeated according to the number of rounds.

The final round is anomalous as the MixColumn step is skipped. The cipher is output after the final round.

CCM mode

During encryption, CBC-MAC is used to process the message data and additional data to produce an authentication value T. This is then encrypted using CTR mode. CTR mode is also used to encrypt the message. The output is an encrypted message and an encrypted authentication string U.

During decryption, the above steps are reversed. The message is decrypted first with CTR mode. The resulting decrypted message is processed, together with the additional data with CBC-MAC in order to produce the encrypted authentication string U. If the latter is different from the original U, the authentication has failed. In this case no other information (i.e. no decrypted data or the value of the authentication string) should be revealed except the failure itself.

Key Expansion

The AES algorithm requires an expanded key for encryption or decryption. The CAST KEXP AES key expander core is available as an AES-CCM core option.

During encryption, the key expander can produce the expanded key on the fly while the AES core is consuming it. For decryption, though, the key must be pre-expanded and stored in an appropriate memory before being used by the AES core.

This is because the core uses the expanded key backwards during decryption.

In some cases a key expander is not required. This might be the case when the key does not need to be changed (and so it can be stored in its expanded form) or when the key does not change very often (and thus it can be expanded more slowly in software).

Related Products

AES in ECB, CFB, CBC, OFB, CTR, GCM and LRW modes are also available as stand-alone cores.

AES-P: run-time programmable AES core supporting ECB, CFB, CBC, OFB, and CTR modes.

Export Permits

This core implements encryption functions and as such it is subject to export control regulations. Export to your country may or may not require a special export license. Please contact CAST to determine what applies in your specific case.

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 (RTL) or FPGA (netlist) forms, and includes everything required for successful implementation. The ASIC version includes

- HDL RTL source
- Sophisticated HDL Testbench (self checking)
- C Model & test vector generator
- Simulation script, vectors & expected results
- Synthesis script
- User documentation

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

CAST, Inc. 50 Tice Blvd, Suite 340
Woodcliff Lake, NJ 07677 USA
tel 201-391-8300 fax 201-391-8694

The AES-CCM core is sourced from Technology Partner Ocean Logic.