General Description

The CCM1 cores are tuned for mid-performance generic AES-CCM applications per NIST SP 800-38C. Specific protocol implementations are available in integrated cores:

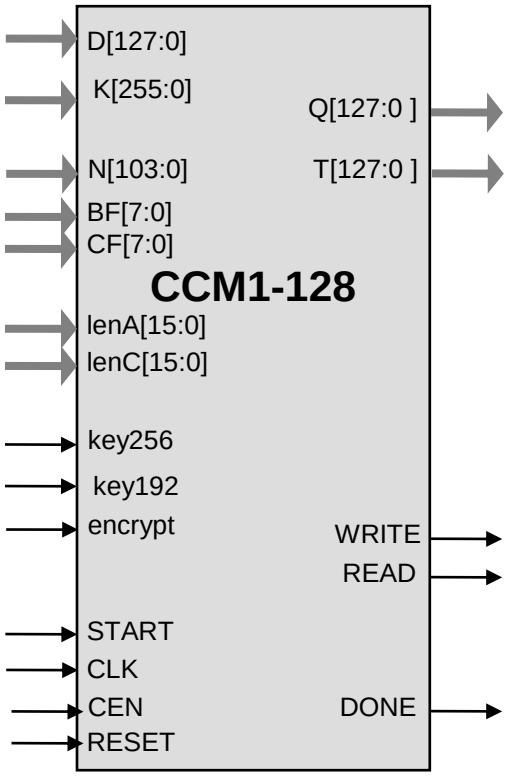
- WPA2 for IEEE 802.11i (Wi-Fi)
- CCM3 for IEEE 802.15.3 (UWB)
- CCM3M for MBOA
- CCM6 for IEEE 802.16e (WiMAX)
- CCMZ1/2 for IEEE 802.15.4 (Zigbee)

CCM1 core uses flow-trough design with dedicated inputs for key and nonce.

Cores contain the base AES core AES1 and are available for immediate licensing.

The design is fully synchronous and available in both source (Verilog or VHDL) and netlist form.

Symbol



Key Features

Small size:

- From 10,000 ASIC gates for CCM1-8 configuration with 0.8 bits per clock throughput with 128-bit key
- From 22,000 ASIC gates for CCM1-128 configuration with 12.8 bits per clock throughput with 128-bit key

Completely self-contained: does not require external memory

Supports encryption and decryption,

Includes key expansion (scheduling)

Support for CCM mode of the AES cipher

Test bench provided

Applications

- Generic CCM-AES applications

Pin Description

Name	Type	Description
CLK	Input	Core clock signal
RESET	Input	Core reset signal
CEN	Input	Synchronous enable signal. When LOW the core ignores all its inputs and all its outputs must be ignored.
Encrypt	Input	When HIGH, core is encrypting, when LOW core is decrypting
key256	Input	When HIGH, 256 bit AES key is used
key192	Input	When HIGH, 192 bit AES key is used
START	Input	HIGH level starts the input data processing
READ	Output	Read request for the input data byte
WRITE	Output	Write signal for the output interface
D[127:0]	Input	Input Data (other data bus widths are also available) • additional authenticated data (AAD, A), followed by the plain or cipher text
K[255:0]	Input	AES key. K[255:128] used for 128 bit key, K[255:64] used for 192 bit key
N[103:0]	Input	Nonce
BF[7:0]	Input	B_0 flag byte
CF[7:0]	Input	Counter flag byte
lenA[15:0]	Input	Length of additional authenticated data in bytes
lenC[15:0]	Input	Length of plain or cipher text in bytes
Q[127:0]	Output	Output plain or cipher text
T[127:0]	Output	Computed MAC (tag, T)
DONE	Output	HIGH when data processing is completed

Function Description

The Advanced Encryption Standard (AES) algorithm is a new NIST data encryption standard as defined in the http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf .

The CCM1 implementation fully supports the AES-CCM algorithm for 128, 192, and 256 bit keys per NIST SP800-38C (http://csrc.nist.gov/publications/nistpubs/800-38C/SP800-38C_updated-July20_2007.pdf).

The core is designed for flow-through operation, with configurable input and output interfaces.

Throughput

The core can sustain the following peak throughput; depending on the configuration (performance is lower on shorter packets):

- 0.8 to 12.8 bits per clock with a 128-bit key (e.g., 6.4 Gbps at 500 MHz clock)
- 0.57 to 9.1 bits per clock with a 256-bit key (e.g. 4.5 Gbps at 500 MHz clock)

If higher throughput is required, use the CCM2 core, which if two times faster, yet is larger and has a lower maximum frequency.

Export Permits

US Bureau of Industry and Security has assigned the export control classification number 5E002 to our AES1 core. The core is eligible for the license exception ENC under section 740.17(A) and (B)(1) of the export administration regulations. See the IP Cores, Inc. licensing basics page, http://ipcores.com/exportinformation.htm, for links to US government sites and more details.

Deliverables

HDL Source Licenses

- Synthesizable Verilog RTL source code
- Testbench (self-checking)
- Vectors for testbenches
- Expected results
- User Documentation

Netlist Licenses

- Post-synthesis EDIF
- Testbench (self-checking)
- Vectors for testbenches
- Expected results

Contact Information

IP Cores, Inc.
3731 Middlefield Rd.
Palo Alto, CA 94303, USA
Phone: +1 (650) 815-7996
E-mail: info@ipcores.com
www.ipcores.com