CCMZ1/CCMZ2

IEEE 802.15.4 CCM AES Cores

General Description

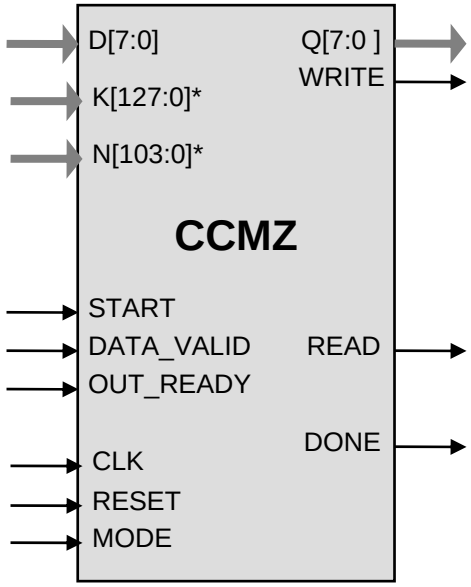
IEEE 802.15.4 is the low-power wireless standard that is used by ZigBee Alliance as a base of its ZigBee™ specification. It uses the CCM* mode of the AES cipher for encryption and message authentication. The CCMZ cores are tuned for low-power IEEE 802.15.4 applications.

CCMZ1 core is slightly larger and uses flow-trough design with key and nonce in the data stream; CCMZ2 core has 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 and netlist form.

Symbol



* CCMZ2 only

Key Features

Small size:
From 6,000 ASIC gates at IEEE 802.15.4 data speeds

Completely self-contained: does not require external memory

Supports encryption and decryption,

Includes key expansion (scheduling)

Support for CCM* mode of the AES cipher

Flow-through design with frame header parsing

Test bench provided

Applications

- IEEE 802.15.4 (ZigBee)

Pin Description

Name	Type	Description
CLK	Input	Core clock signal
RESET	Input	Core reset signal
MODE	Input	Core operational mode
START	Input	HIGH starting input data processing
READ	Output	Read request for the input data byte
DATA_VALID	Input	HIGH when valid data byte present on the input
WRITE	Output	Write to the output interface
OUT_READY	Input	HIGH when output interface is ready to accept data byte
D[7:0]	Input	Input Data
K[127:0]	Input	AES key (CCMZ2 only)
N[103:0]	Input	CCM* Nonce (CCMZ2 only)
Q[7:0]	Output	Output Data
DONE	Output	Data processing 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 CCMZ implementation fully supports the AES algorithm for 128 bit keys in Counter Mode (CTR) method of encryption with CBC message integrity check of all sizes required by the CCM* protocol of the IEEE 802.15.4 standard.

The core is designed for flow-through operation, with byte-wide input and output interfaces. For CCMZ1, CCM key and nonce material precede the frame in the flow of data. Both CCMZ1 and CCMZ2 support encrypt/decrypt modes and includes on-the-fly key expansion (scheduling).

Implementation Results

Area Utilization and Performance

Representative area/resources figures are shown below.

Core	Technology	Area / Resources
CCMZ1	TSMC 0.18 µ	8K gates
CCMZ2	TSMC 0.18 µ	6K gates

.

Export Permits

US Bureau of Industry and Security has assigned the export control classification number 5E002 to our AES 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 licensing basics page, http://ipcores.com/export_licensing.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) 814-0205
E-mail: info@ipcores.com
www.ipcores.com