CMAC1

CMAC and XCBC AES Core

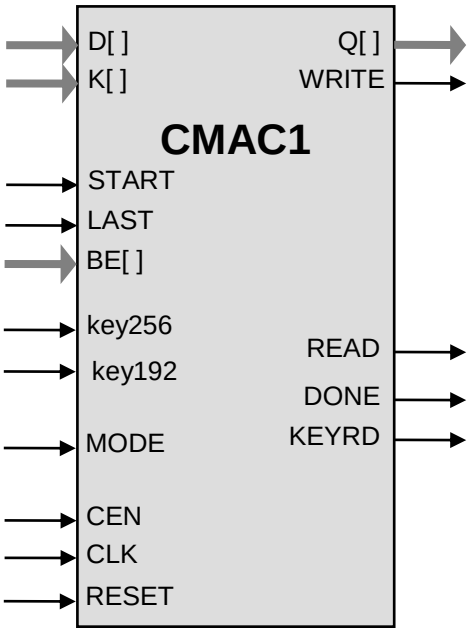
General Description

The CMAC1 core provides implementation of cryptographic hashes AES-CMAC per NIST SP 800-38B and AES-XCBC.

The cores utilize “flow-through” design that can be easily included into the data path of a communication system or connected to a microprocessor: the core reads the data via the D input, key from the K input and outputs the hash result via its Q output. Data bus widths for D, K, and Q are parameterized.

The design is fully synchronous and is available in both source and netlist form.

Symbol



Key Features

Completely self-contained; does not require external memory

CMAC algorithm per NIST SP800-38B and RFC 4493, AES-XCBC per CBC MAC submissions to NIST and RFC 3566.

Supports 128, 192, and 256 bit AES keys.

Flow-through design; flexible data bus width.

Self-checking test bench provided

Applications

- Message digest calculation
- AES-CMAC-96
- AES-XCBC-96
- AES-CMAC-PRF-128
- AES-XCBC-PRF-128
- IPsec
- TLS

Pin Description

Name	Type	Description
CLK	Input	Core clock signal
CEN	Input	Synchronous enable signal. When LOW the core ignores all its inputs and all its outputs must be ignored.
START	Input	HIGH starting input data processing
READ	Output	Read request for the input data word
DONE	Output	HIGH after the completion of the operation. Brought LOW by de-assertion of the **start**
RESET	Input	Asynchronous reset (for simulation purposes). Core will operate correctly if **reset** is never asserted.
LAST	Input	Marks the last byte of data
WRITE	Output	Write to the output interface
KEYRD	Input	Key read signal
MODE	Input	Mode of operation: LOW selects CMAC operation, HIGH – XCBC. Value on the **mode** input can only be changed while the **start** is low
D[ ]	Input	Input Data
K[ ]	Input	Input Key
BE[ ]	Input	Specifies the number of bytes in the last word; unused if the input bus width is 8 bits
Q[ ]	Output	Output Hash Data
key256	Input	When HIGH, 256 bit AES key is used
key192	Input	When HIGH, 192 bit AES key is used

Function Description

The CMAC and XCBC algorithms process data in 128-bit blocks and produce message digests consisting of 128 bits and are defined in NIST SP 800-38B (http://csrc.nist.gov/publications/nistpubs/800-38B/SP_800-38B.pdf) and Black-Rogaway submission to NIST (http://www.cs.ucdavis.edu/~rogaway/papers/xcbc.pdf) together with RFC 3566.

The core is designed for flow-through operation, with I/O interface of parameterizable width. The input data can contain any number of bytes (data padding is performed inside the core). The output data is the 128-bit MAC value.

Throughput Options

The throughput of the core on long data packets depends on the core configuration and ranges

- from 0.8 bit to 12.8 bits per clock for the 128-bit key
- from 0.57 to 9.1 bits per clock for the 256-bit key

On short packets, performance is up to two times lower.

CMAC2 provides two times the performance of CMAC1 at the expense of larger size and lower maximum frequency.

Deliverables

HDL Source Licenses

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

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