www.ipcores.com

CCM2-128-CMAC

Generic CCM AES Core with CMAC Option

General Description

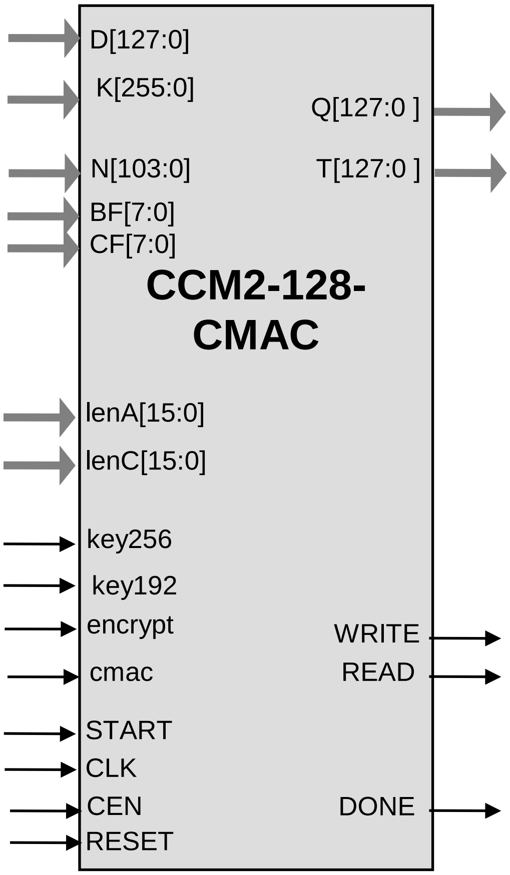
The CCM2 cores are tuned for mid-performance generic AES-CCM applications per NIST SP 800-38C.

CCM2 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

Completely self-contained: does not require external memory

Supports encryption and decryption,

Includes key expansion (scheduling)

Support for CCM mode of the AES cipher per NIST SP800-38C

Support for 128-bit, 192-bit and 256-bit AES keys

Support for CMAC (OMAC1) mode per NIST SP800-38B

Throughput of 9.1 bits per clock with 256-bit AES key

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
cmac	Input	When HIGH, core is is performing the CMAC operation, **encrypt** is ignored
key256	Input	When HIGH, 256 bit AES key is used
key192	Input	When HIGH, 192 bit AES key is used. Cannot be asserted simultaneously with **key256**
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) • associated data (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 associated data in bytes (should be a multiple of 16)
lenC[15:0]	Input	Length of plain or cipher text in bytes (“payload length”)
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

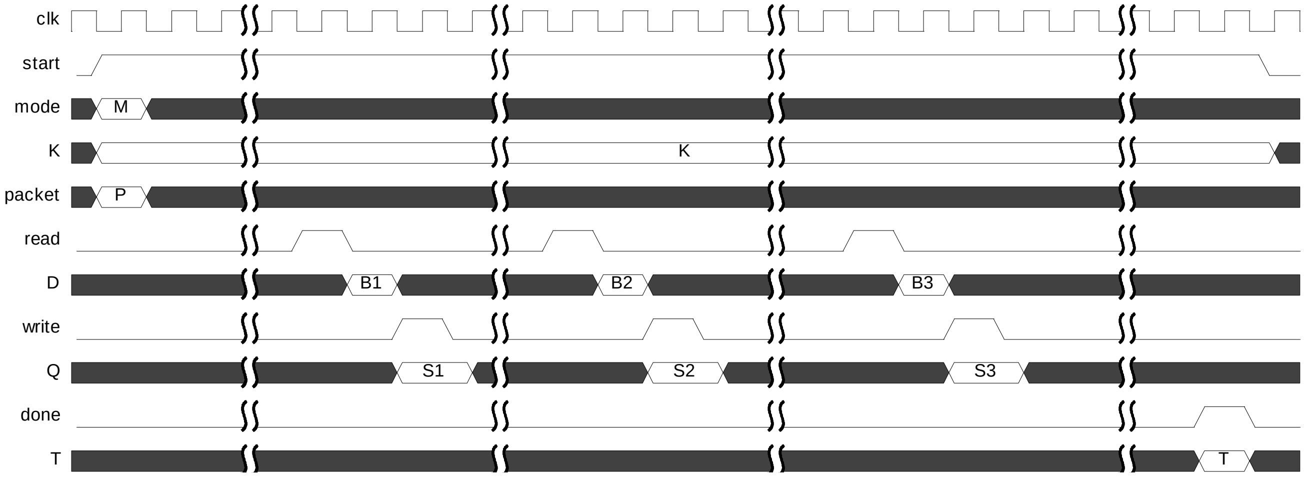
The Advanced Encryption Standard (AES) algorithm is a new NIST data encryption standard as defined in the http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf .

The CCM2 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). Authentication block B_0 is assembled inside the core from the value on the dedicated input pins, subsequent blocks B are read by the core from the D input. The encryption results are output by the core on the Q output.

The CMAC implementation is per NIST SP 800-38B (http://csrc.nist.gov/publications/nistpubs/800-38B/SP_800-38B.pdf). Blocks M are read by the core from the D input.

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

CCM Operation



start signal marks the beginning of the operation of the core. **mode** (a combination of **encrypt**, **key192**, **key256**) is sampled on the first clock that samples **start** HIGH. **cmac** shall be LOW.

packet information (a combination of **lenA**, **lenC**, **N**, **BF**, **CF**) is also sampled on the first clock that samples **start** HIGH.

AES key **K** is sampled by the core on the same edge of **clk** that samples start signal HIGH and re-sampled during the processing.

Input data **D** is sampled 14 clocks after **start** is sampled HIGH and re-sampled every 14 clocks. Core generates **read** signal when it ready to accept the new word of data. Input data should be advanced on the next clock after each **read** pulse. Associated data on the input precedes the input text (plaintext or ciphertext), except for the block B_0. B_0 is assembled inside the core from **BF**, **N** and payload length **lenC** per Appendix A of NIST SP800-38C.

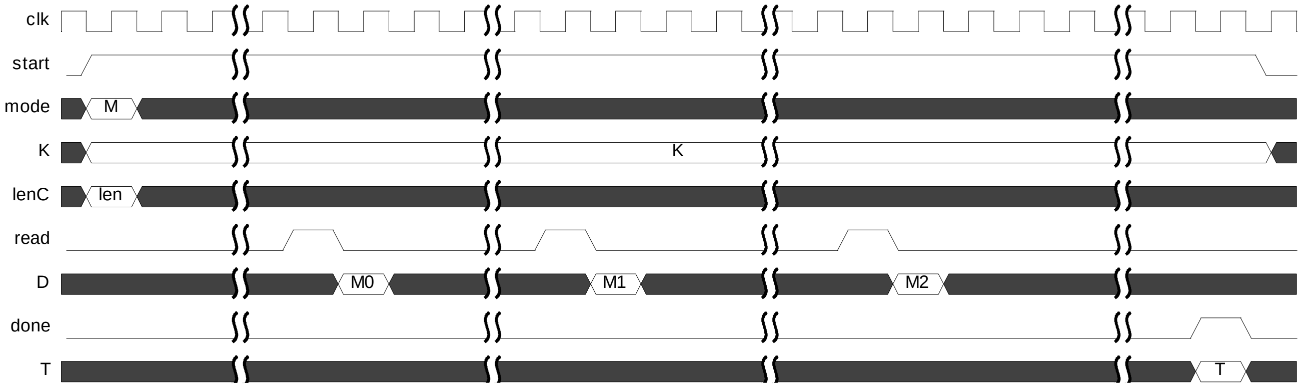
Core generates **write** signal when **Q** output contains a valid encryption or decryption result. **Q** can be sampled by the receiver of the core data on the same edge of **clk** that samples **write** signal HIGH and remains valid until next **write** signal.

Core generates **done** signal when it completes the encryption or decryption operation. **done** will stay HIGH for one clock period.

T should be sampled by the receiver of the core data on the same edge of **clk** that samples **done** signal HIGH.

start should be held HIGH at least until **done** signal would be generated by the core. **start** going LOW will abort the operation of the core.

CMAC Operation



start signal marks the beginning of the operation of the core. **mode** (a combination of **key192** and **key256**) is sampled on the first clock that samples **start** HIGH. **cmac** shall be HIGH.

lenC is also sampled on the first clock that samples **start** HIGH.

AES key **K** is sampled by the core on the same edge of **clk** that samples start signal HIGH and re-sampled during the processing.

Input data **D** is sampled 14 clocks after **start** is sampled HIGH and re-sampled every 14 clocks. Core generates **read** signal when it ready to accept the new word of data. Input data should be advanced on the next clock after each **read** pulse.

Core generates **done** signal when it completes the CMAC operation. **done** will stay HIGH for one clock period.

T should be sampled by the receiver of the core data on the same edge of **clk** that samples **done** signal HIGH.

start should be held HIGH at least until **done** signal would be generated by the core. **start** going LOW will abort the operation of the core