CCM3

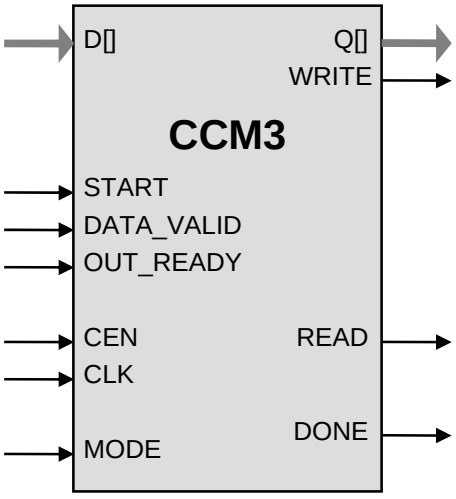
802.15.3 AES Core

General Description

Implementation of the new WPAN security standard (802.15.3) requires the NIST standard AES cipher in CTR and CBC modes (a.k.a. CCM) for encryption and message authentication. The CCM3 AES core is tuned for 802.15.3 applications and as such requires much smaller gate count than a full implementation. The core contains the base AES core AES1 and is available for immediate licensing.

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

Symbol



Key Features

Small size:
From 9,500 ASIC gates at 802.15.3 data speeds

Completely self-contained: does not require external memory

Includes encryption, decryption, key expansion and data interface

Support for Counter Mode Encryption (CTR) operation and CCM extensions (Counter Mode with CBC MAC)

Automatic generation of key context from key data

Flow-through design

Test bench provided

Applications

- IEEE 802.15.3

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.
MODE	Input	Mode. When HIGH, transmit, when LOW receive
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[]	Input	Input Data
Q[]	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 CCM3 implementation fully supports the AES algorithm for 128 bit keys in Counter Mode (CTR) method of encryption with CBC message integrity check as required by the CCM protocol of the 802.15.3 standard.

The core is designed for flow-through operation, with byte-wide input and output interfaces. CCM key and nonce material precedes the frame in the flow of data. CCM3 supports encrypt and decrypt modes

Implementation Results

Device Utilization and Performance

Representative area/resources figures are shown below.

Technology	Area / Resources
TSMC 0.18 **u**	9500 gates

.

Export Permits

US Bureau of Industry and Security has assigned the export control classification number 5E002 to the 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 site of US Department of Commerce http://www.bxa.doc.gov/Encryption/ for details.

Deliverables

HDL Source Licenses

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

Netlist Licenses

- Post-synthesis EDIF
- Testbench (self-checking)
- Vectors for testbenches
- Expected results
- Place & Route script
- Simulation script

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