GCE1 Core

AES-GCM/CCM/CCM*/EAX' Core

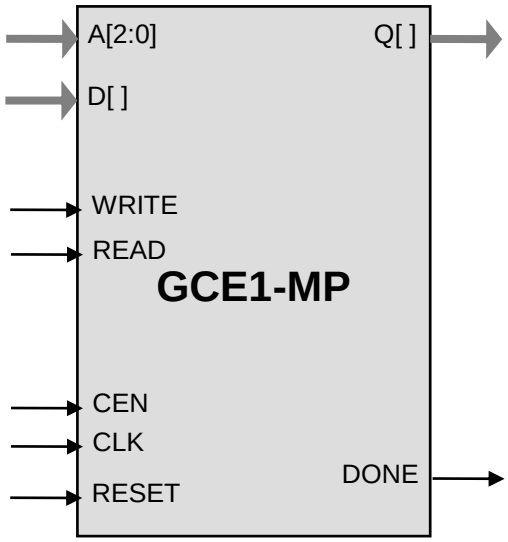
General Description

The GCE1-MP core implements Rijndael encoding and decoding in compliance with the NIST Advanced Encryption Standard and encryption/authentication modes GCM, CCM, CCM*, and EAX'. It processes 128-bit blocks using 128-bit keys.

GCE1-MP core is a configuration of the GCE1 core that includes a 128-bit internal key. The register-based interface of the core of the core allows its easy integration into a microprocessor system.

The design is fully synchronous and is immediately available in Verilog (optional VHDL).

Symbol



Key Features

Scalable throughput from 0.8 bits per clock (GCE1-8MP) to 12.8 bits per clock (GCE1-128MP)

Completely self-contained: does not require external memory

Supports both encryption and decryption

Includes AES key expansion and mode processing.

128 bit AES key, IV, counter, tag storage

SRAM-like interface design for 8-bit and 32-bit buses

Test bench provided

Applications

- IEEE 802.3ae (MACsec)
- Zigbee, IEEE 802.15.4
- ANSI C 12 22
- IPsec RFC 4106, RFC 4543

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.
RESET	Input	HIGH level asynchronously resets the core
A[2:0]	Input	Address bus. Selects the internal registers: 0 – Command/status, 1 – Data, 2 – IV / Tag, 3 – Counter, 4 – Key
READ	Input	Read register request
WRITE	Input	Write register request
DONE	Output	HIGH level indicates a completion of an encryption step
D[ ]	Input	Input Data
Q[ ]	Output	Output Data

Function Description

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

GCE1 supports five AES encryption modes: ECB encryption per NIST SP800-38B (http://csrc.nist.gov/publications/nistpubs/800-38D/SP-800-38B.pdf) GCM per NIST SP800-38D (http://csrc.nist.gov/publications/nistpubs/800-38D/SP-800-38D.pdf), CCM per NIST SP800-38C (http://csrc.nist.gov/publications/nistpubs/800-38D/ SP800-38C_updated-July20_2007.pdf), CCM* per Zigbee specification, and EAX' per ANSI C 12 22.

Export Permits

US Bureau of Industry and Security has assigned the export control classification number 5E002 to the 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 the US government sites and more details.

Deliverables

HDL Source Licenses

- Synthesizable Verilog RTL source code
- Verilog testbench (self-checking)
- Vectors for testbench
- Firmware samples for complete GCM, CCM, CCM*, and EAX' implementations
- Expected results
- User Documentation

Netlist Licenses

- Post-synthesis EDIF
- Testbench (self-checking)
- Vectors for testbench
- 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