GCM1 Core

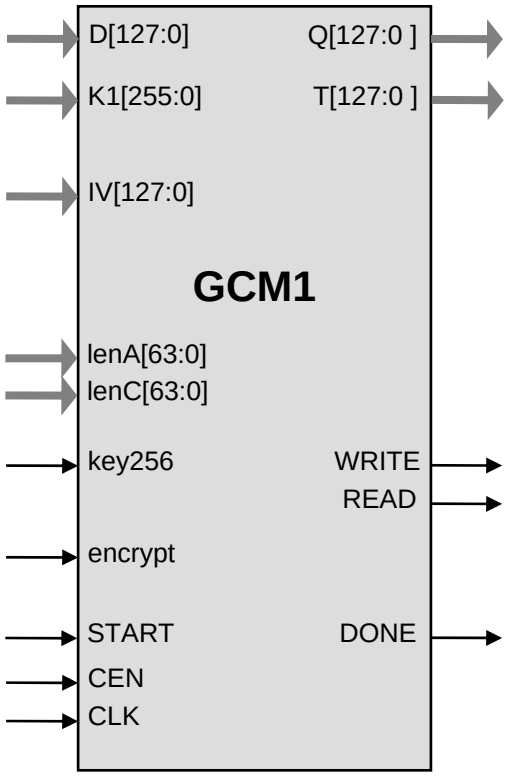
802.1ae (MACSec) GCM/AES Core

General Description

Implementation of the new LAN security standard 802.1ae (MACSec) requires the NIST standard AES cipher in the GCM mode for encryption and message authentication. The GCM1 AES core is tuned for 802.1ae applications at the data rates of 1 Gbps and higher. 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:
25K ASIC gates at 1 Gbps and above data speeds (at throughput of 6.4 bits per clock)

Completely self-contained: does not require external memory

Supports encryption and decryption

Includes key expansion

Support for Galois Counter Mode Encryption and authentication (GCM)

Flow-through design

Test bench provided

Deliverables include test benches

Applications

- WLAN 802.1ae

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.
encrypt	Input	When HIGH, core is encrypting, when LOW core is decrypting
key256	Input	When HIGH, 256 bit AES key is used, when LOW – 128 bit AES key
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) • additional authenticated data (AAD, A), followed by the plain or cipher text
K1[255:0]	Input	AES key (128-bit key only option is also available)
IV[127:0]	Input	Initial counter value (Y_0, IV || $0^{31}1$)
lenA[63:0]	Input	Length of additional authenticated data in bits
lenC[63:0]	Input	Length of plain or cipher text in bits
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 GCM1 implementation fully supports the AES algorithm for 128 bit keys in Galois Counter Mode (GCM) as required by the 802.1ae IEEE standard.

The core is designed for flow-through operation. GCM key and nonce material precedes the frame in the flow of data. GCM1 supports encryption and decryption modes.

Implementation Results

Area Utilization and Performance

Representative area/resources figures are shown below.

Technology	Area / Resources	Frequency	Throughput
TSMC 0.13 µm LV	30,707 gates	250 MHz	3.2 Gbps
TSMC 0.13 µm LV	40,335 gates	500 MHz	6.4 Gbps
TSMC 90 nm LV	49,633 gates	824 MHz	10.54 Gbps

Export Permits

The core can be a subject of the US export control. It is the customer's responsibility to check with relevant authorities regarding the re-export of equipment containing the AES encryption technology. 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
- 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