GCM2 Family of Cores

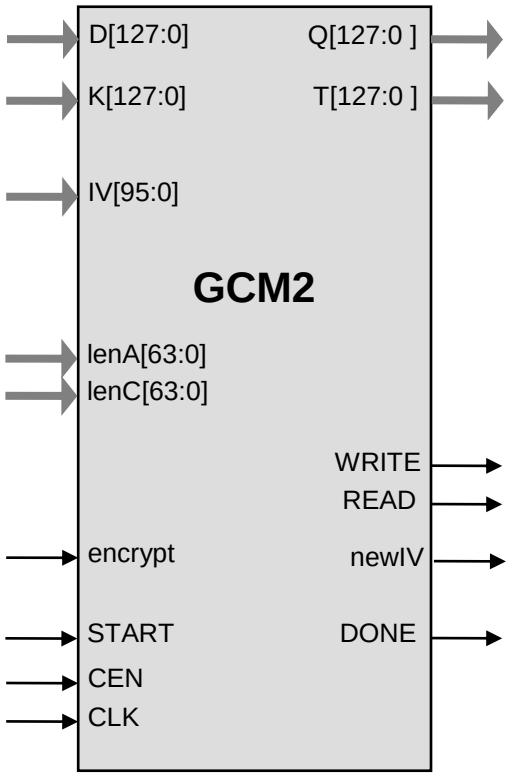
802.1ae (MACSec) GCM/AES Cores

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 GCM2 family of cores covers a wide range of area / throughput combinations, allowing the designer to choose the smallest core that satisfies the desired clock/throughput requirements. Each 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:GCM2-25.6 starts at less than 40,000 ASIC gates at throughput of 25.6 bits per clock

Completely self-contained: does not require external memory

Supports both encryption and decryption

128 bit AES keys supported.

Easily parallelizable for even higher data rates

Includes key expansion

Support for Galois Counter Mode Encryption and authentication (GCM)

Flow-through design

Test bench provided

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
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
newIV	Output	Request for IV (and key) for the new data packet
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
K[127:0]	Input	AES key
IV[95:0]	Input	96 msb of the initial counter value
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 GCM2 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, with 128-bit wide input and output interfaces. GCM2 supports both encryption and decryption modes.

Implementation Results

Area Utilization and Performance

Representative area/resources figures are shown below.

Core	Technology	Area / Resources	Frequency	Throughput
GCM2-64	TSMC 0.09 µm LV	110,000 gates	410 MHz	26 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