GLM2 Core

P1619 / 802.1ae (MACSec) GCM/LRW-AES Core

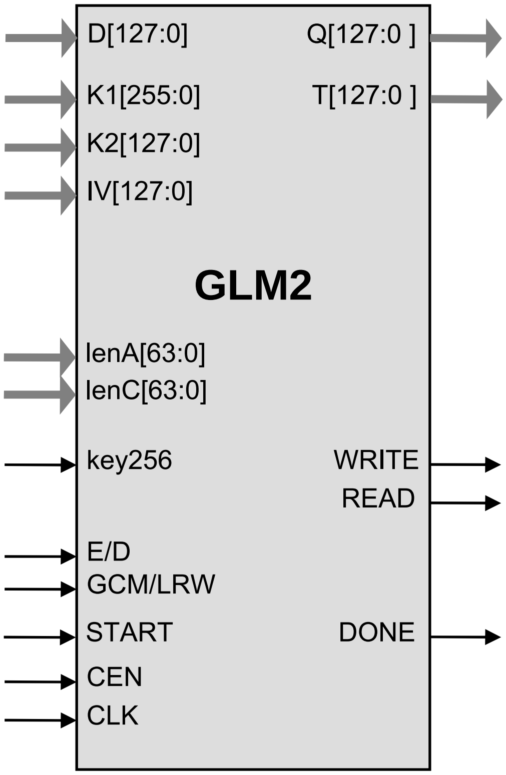
General Description

LAN security standard IEEE 802.1ae (MACSec) uses AES cipher in the GCM mode, while the disk/tape encryption standard IEEE P1619 uses the LRW mode. Since GCM and LRW share some of their basic components, a combo GCM/LRW core is not much larger than a dedicated core for either of the modes.

The GLM2 core is tuned for mid-performance P1619 and 802.1ae applications at the data rates of 2-3 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:
58K ASIC gates (at throughput of 25.6 bits per clock)

400 MHz frequency in 130 nm process

Easily parallelizable to achieve higher throughputs

Completely self-contained: does not require external memory. Includes encryption, decryption, key expansion and data interface

Support for Galois Counter Mode Encryption and authentication (GCM) and Liskov, Rivest, and Wagner Mode (LRW)

Flow-through design

Test bench provided

Applications

- IEEE 802.1ae

  LAN switches, routers, NICs

- IEEE P1619

  Hard drive and tape encryption, SAN, NAS

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.
GCM/LRW	Input	When HIGH, GLM2 mode is GCM, when LOW mode is LRW
E/D	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) • For GCM, additional authenticated data (AAD, A), followed by the plain or cipher text • For LRW, plain or cipher text
K1[255:0]	Input	AES key (128-bit key option is also available)
K2[127:0]	Input	(LRW mode only) Tweak key (K_2)
IV[127:0]	Input	(GCM mode only) Initial counter value (Y_0, IV || $0^{31}1$)
lenA[63:0]	Input	(GCM mode only) Length of additional authenticated data in bits
lenC[63:0]	Input	(GCM mode only) Length of plain or cipher text in bits
Q[127:0]	Output	Output plain or cipher text
T[127:0]	Output	(GCM mode only) 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 GLM2 implementation fully supports the AES algorithm for 128 and 256 bit keys in Galois Counter Mode (GCM) as required by the 802.1ae IEEE standard and in Liskov, Rivest, and Wagner Mode (LRW) as required by the IEEE P1619 standard.

The core is designed for flow-through operation, with input and output interfaces of flexible width. GCM additional authentication data precede the plaintext in the flow of data. GLM2 supports both encryption and decryption modes.

Synthesis Results

Device Area Utilization and Performance

Representative area/resources figures are shown in the table below.

Technology	Area / Resources	Max Frequency	Throughput
TSMC 0.13 µ LV	58,000 gates	200 MHz	5.1 Gbps
TSMC 0.13 µ LVOD	100,000 gates	400 MHz	10 Gbps

Few GLM2 cores can be easily paralleled to achieve 10 Gbps or higher throughput.

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 export or 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
- 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