www.ipcores.com

GXM2 Core

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

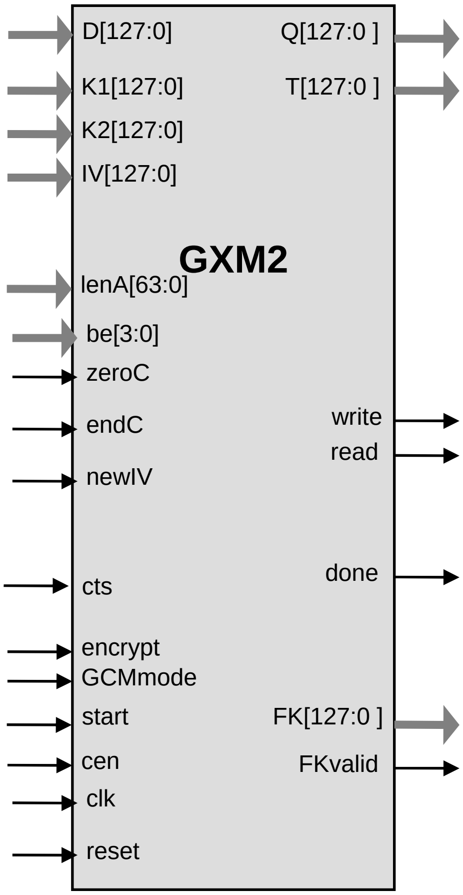
General Description

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

The GXM2 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:
From 60K ASIC gates (at throughput of 25.6 bits per clock)

487 MHz frequency in 90 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 XTS mode per P1619 with 128-bit keys

Cipher Text Stealing (CTS) mode included

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
Reset	Input	Core reset signal (active HIGH)
Cen	Input	Synchronous enable signal. When LOW the core ignores all its inputs and all its outputs must be ignored.
GCMmode	Input	When HIGH, GXM2 mode is GCM, when LOW mode is XTS
Encrypt	Input	When HIGH, core is encrypting, when LOW core is decrypting
endC	Input	(GCM mode only) Marks last data block
zeroC	Input	(GCM mode only) Marks the block with zero length of plaintext/ciphertext field
newIV	Input	(XTS mode only) Marks the last block of the data unit if followed immediately by the first block of the next data unit with different IV.
cts	Input	(XTS mode only) Marks the last full 128-bit block of the data unit in case that the next block of this data unit is less than 128 bit (CTS mode)
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 XTS, plain or cipher text
K1[127:0]	Input	128 bit AES key
K2[127:0]	Input	(XTS 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
be[3:0]	Input	Byte length of the last data block in bytes minus 1
FK[127:0]	Output	128 bit final round key
FKvalid	Output	HIGH when FK is valid
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 GXM2 implementation fully supports the AES algorithm for 128 bit keys in Galois Counter Mode (GCM) as required by the 802.1ae IEEE standard and in XTS mode 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. GXM2 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	70,543 gates	207 MHz	3.7 Gbps
TSMC 0.09 µ LV	85,961 gates	348 MHz	6.3 Gbps
TSMC 0.09 µ LV	119,493 gates	487 MHz	8.9 Gbps

Core can be easily synthesized for higher throughputs with slightly increased gate count. Few GXM2 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