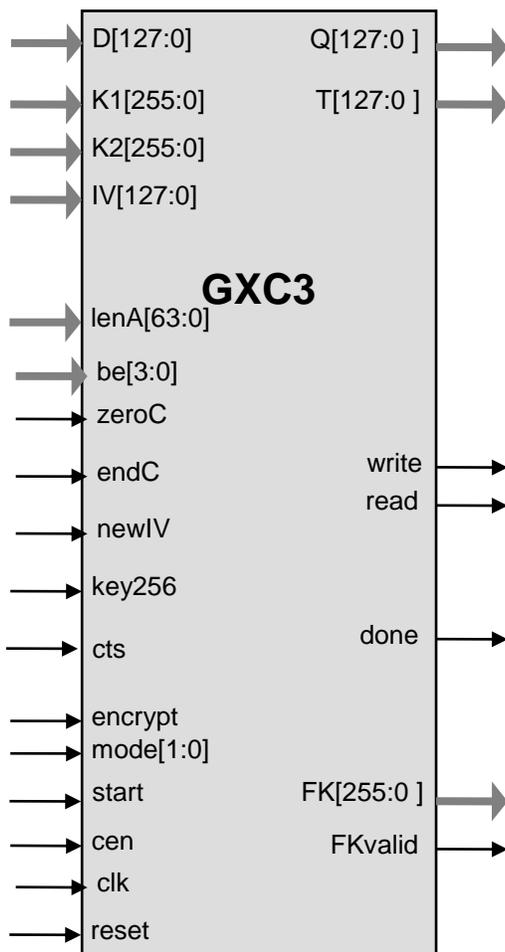## General Description

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/CBC core is not much larger than a dedicated core for either of the modes.

The GXC3 core is tuned for mid-performance P1619 and 802.1ae applications at the data rates up to 10 Gbps. 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

```
        D[127:0]          Q[127:0 ]
        K1[255:0]         T[127:0 ]
        K2[255:0]
        IV[127:0]

                 GXC3

        lenA[63:0]
        be[3:0]
        zeroC
        endC                 write
        newIV                read
        key256
        cts                  done
        encrypt
        mode[1:0]
        start             FK[255:0 ]
        cen               FKvalid
        clk
        reset
```

Key Features

Small size:
   From 70K ASIC gates (at throughput of 18.2 bits per clock)

500 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) , XEX-based Tweaked CodeBook mode (TCB) with Cipher Text Stealing (CTS) (abbreviated as XTS) mode per IEEE P1619, and Cipher Block Chaining (CBC) mode with 128 and 256-bit AES keys

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.
mode[1:0]	Input	Encryption mode. GCM mode if 01, XTS mode if 00, CBC mode if 10
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
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 and CBC, plain or cipher text
K1[255:0]	Input	256 bit or 128 bit AES key (128-bit key uses K1[255:128] pins)
K2[255:0]	Input	(XTS mode only) Tweak key (K_2) (128-bit key uses K2[255:128] pins)
IV[127:0]	Input	In GCM mode: initial counter value (Y_0, IV $\|$ $0^{31}1$) In CBC mode: initial value (IV) In XTS mode: location (IV)
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 (GCM and XTS modes only) in bytes minus 1 0 – corresponds to 1 byte 1 – corresponds to 2 bytes … 15 – corresponds to 16 bytes
FK[255:0]	Output	256 bit or 128 bit final round key (128-bit key uses FK[255:128] pins)
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 GXC3 implementation fully supports the AES algorithm for 128 and 256 bit keys in Galois Counter Mode (AES-GCM) as required by the 802.1ae IEEE standard, in AES-XTS mode as required by the IEEE P1619 (SISWG) standard, a the CBC-AES mode per NIST specification SP800-38A.

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. GXC3 supports both encryption and decryption modes.

Export Permits

The core can be a subject of the US export control. the IP Cores, Inc. licensing basics page, http://ipcores.com/export_licensing.htm, for links to US government sites and more 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