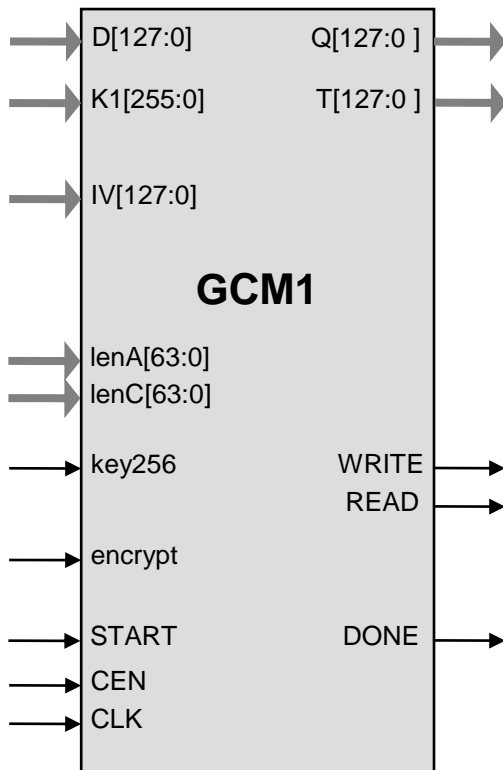


### General Description

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 midrange data rates of 100 Mbps to 500 Mbps (see the GCM2/GCM3/GCM5/GCM10 families for higher throughputs). 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 combined with high performance, starting at less than 6K Actel tiles

Completely self-contained: does not require external memory

Supports encryption and decryption

Includes key expansion

Support for Galois Counter Mode Encryption and authentication (GCM), Galois Message Authentication (GMAC)

Optional countermeasures against SPA and DPA attacks

Flow-through design

Test bench provided

Deliverables include test benches and optional NIST algorithm validation

### Applications

- NSA Suite B applications
- WLAN 802.1ae MACsec
- RFC 4869

### 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) <ul style="list-style-type: none"> <li>• additional authenticated data (AAD, A), followed by the plain or cipher text</li> </ul>
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 and NIST publication SP800-38D <http://csrc.nist.gov/publications/nistpubs/800-38D/SP-800-38D.pdf> .

The core is designed for flow-through operation. GCM1 supports encryption and decryption modes.

## Implementation Results

### Area Utilization and Performance

Representative area/resources figures are shown below.

Technology	Area / Resources	Frequency	Throughput
Actel ProAsic-3	5,816 tiles	44 MHz	100 Mbps (256 bit key)
Actel ProAsic-3	10,981 tiles	44 MHz	560 Mbps

## Power Attack Countermeasures

A power attack countermeasure option –DPA is available to protect the core from simple power analysis (SPA) and differential power analysis (DPA) attacks. This option is available to Actel customers on selected Actel FPGA devices without a separate license from Cryptography Research, Inc.

## 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 IP Cores, Inc. licensing basics page <http://ipcores.com/exportinformation.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
- Expected results
- User Documentation
- Optional GCMVS NIST validation

### Netlist Licenses

- Post-synthesis EDIF
- Testbench (self-checking)
- Vectors for testbenches
- Expected results



[www.ipcores.com](http://www.ipcores.com)

# GCM1 Core

## 802.1ae (MACSec) GCM/AES Core

---

### Contact Information

IP Cores, Inc.  
3731 Middlefield Rd.  
Palo Alto, CA 94303, USA  
Phone: +1 (650) 815-7996  
E-mail: [info@ipcores.com](mailto:info@ipcores.com)  
[www.ipcores.com](http://www.ipcores.com)