

The Galois/Counter Mode (GCM) algorithm has been proposed to provide for high-speed (20/40 Gbps and beyond) encryption and authentication. GCM uses a block cipher in counter mode together with Galois Field based authentication to get past the performance limitations of using block ciphers for authentication (e.g. AES-CBC-MAC). Elliptic's AES-GCM core uses a binary Galois Field Multiplier (GFM) for authentication, together with a high-performance AES-CTR mode cipher to provide high-speed encryption and authentication. It provides both AES-GCM and GMAC-AES functionality.

### Key Features:

- Throughput up to 40 Gbps
- Implements AES-GCM as specified in draft IEEE standard 802.1AE
- Multiple message authentication modes
  - Stand-alone
  - Authentication without encryption
  - Incremental authentication of header data
- Test bench and synthesis scripts provided

### Applications:

- WAN Security - OC-48, OC-192 and OC-768
- EPON – Passive Optical Networking
- Ethernet link security such as 802.1AE
- IPsec
- SAN/NAS

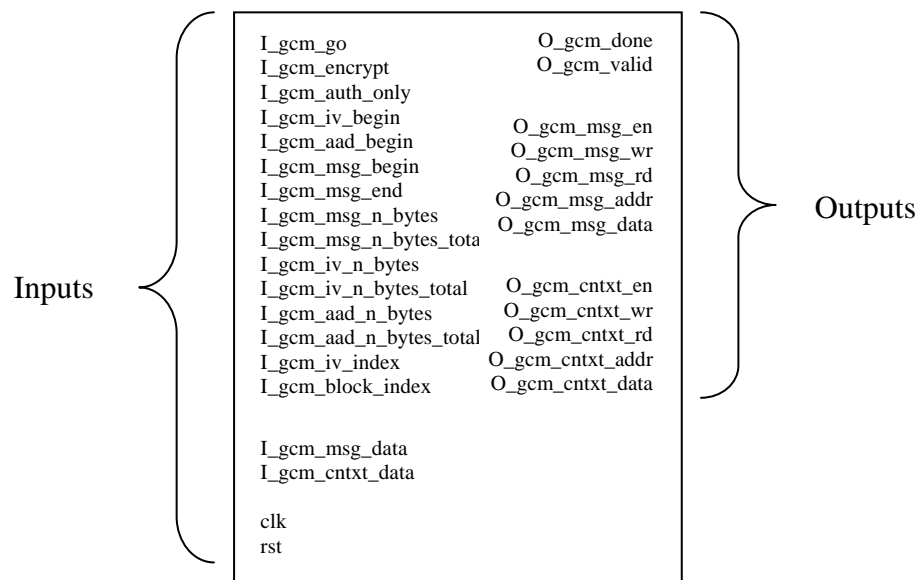


Figure 1 CLP-15 Block Diagram

## Pin Description

Signal Name	Bit Width	Direction	Description
<i>System Pins</i>			
clk	1	input	System clock. All inputs are sampled upon the rising edge of the clock.
rst	1	input	Asynchronous reset. Internal state returns to default value upon assertion (active high).
<i>Control pins</i>			
I_gcm_go	1	input	Asserted to start operation; hold until done is asserted
O_gcm_done	1	output	Indicates engine has finished processing; de-asserted upon de-assertion of I_aes_go
O_gcm_valid	1	output	Indicates decrypted message was successfully authenticated
I_gcm_encrypt	1	input	Controls encryption/decryption mode.
I_aes_gcm_auth_only	1	input	Authenticate only
I_gcm_msg_begin	1	input	Assert to indicate start of message
I_gcm_msg_end	1	input	Assert to indicate end of message
I_gcm_iv_begin	1	input	Assert to indicate start of initial vector (IV)
I_gcm_aad_begin	1	input	Assert to indicate start of additional authenticated data (AAD).
I_gcm_msg_n_bytes	16	input	Current number of bytes of message to encrypt/decrypt; must be a multiple of 16 bytes (AES block-size)

Signal Name	Bit Width	Direction	Description
I_gcm_aad_n_bytes	16	input	Current number of additional authenticated (AAD) bytes to hash
I_gcm_iv_n_bytes	16	input	Current number of IV bytes to hash
I_gcm_msg_n_bytes_total	39	input	Total number of message bytes to process
I_gcm_aad_n_bytes_total	64	input	Total number of AAD bytes to process
I_gcm_iv_n_bytes_total	64	input	Total number of IV bytes to process
I_gcm_iv_index	3	input	Context page number
I_gcm_block_index	7	input	First block page number
<b>Memory I/O pins</b>			
O_gcm_msg_addr	9	output	Address to write data word to
O_gcm_wr	1	output	Write signal to unload ciphertext, if encrypting, or plaintext, if decrypting
O_gcm_msg_en	1	output	Enable signal to message memory
O_gcm_msg_data	128	output	Data word to write ciphertext, if encrypting, or plaintext, if decrypting
O_gcm_msg_rd	1	output	Read signal to load plaintext, if encrypting, or ciphertext, if decrypting
I_gcm_msg_data	128	input	Data word to read plaintext, if encrypting, or ciphertext, if decrypting
O_gcm_cntxt_addr	9	output	Address to write context word to
O_gcm_cntxt_wr	1	output	Write signal to unload context word
O_gcm_cntxt_en	1	output	Enable signal to context memory

Signal Name	Bit Width	Direction	Description
O_gcm_cntxt_data	32	output	Data word to write context
O_gcm_cntxt_rd	1	output	Read signal to load context
I_gcm_cntxt_data	32	input	Data word to read context

**Table 1: Pin description table.**

## General Description

The implementation of a secure communications design requires the ability to do both cipher operations and message authentication. The Advanced Encryption Standard (AES) algorithm is a proven cipher capable of performing hardware encryption and decryption at speeds up to 40 Gbps or more. Current authentication modes however have drawbacks either in throughput or have intellectual property issues that restrict their use.

To address this, the Galois/Counter Mode (GCM) algorithm has been introduced. The design integrates message authentication through a Galois binary field multiplication algorithm with a block cipher in counter mode. The Galois field authentication algorithm is very well suited to the target designs because it:

- Reaches throughput of 40 Gbps or higher using single clock cycle operations;
- Offers universal message authentication which can do incremental authentication of packet header information for example which can't be encrypted; and
- Is rendered very efficiently in hardware.

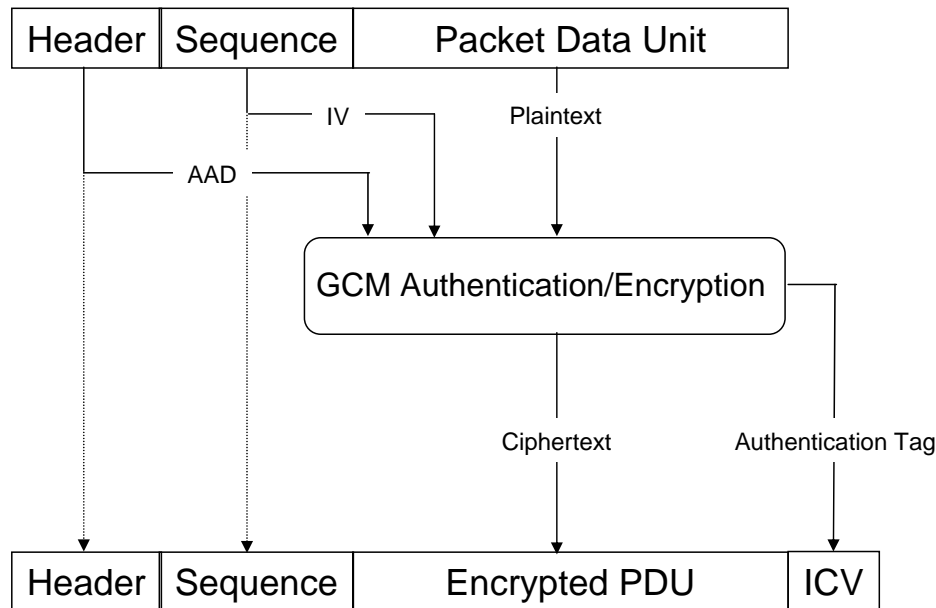
The CLP-15 integrates Elliptic's production proven AES core with the Galois field binary multiplication logic to offer a fully integrated solution. The resulting core has been thoroughly verified with internal and published reference test suites.

AES-GCM has been selected as a mandatory cipher for 802.1AE – the Ethernet link security standard currently under development by the IEEE. The current draft standard for 802.1AE specifies operation of the AES cipher with 128 bit keys and as such the CLP-15 is designed to support only that key size.

AES-GCM has also been nominated as an optional cipher for IPsec with all three key sizes specified i.e. 128, 192, and 256 bit keys. Variants of the CLP-15 are available to support these key sizes if required.

The use of AES-GCM is shown in Figure 2.

This diagram illustrates the benefit of a universal authentication design as the header of the packet cannot be encrypted as it is used in routing the packet but it is important to authenticate the entire message including the header. As such, the header is input to the AES-GCM core as Additional Authenticated Data (AAD) alongside the Sequence Number of the packet, which in this case is used as the Initialization Vector for the cipher operation, followed by the PDU itself which are all operated on to create the Authentication Tag. The Authentication Tag is then appended to the transmitted packet as the Integrity Check Value (ICV).



**Figure 2 AES-GCM Functional Diagram**

The core has two interfaces on it – a slave mode memory interface that is used to control the state and operation of the core. The control registers determine the way in which the core is used, the number of bytes of AAD, IV and data to be processed by the core and the end of an operation. The memory interface masters the bus to permit high speed transfer of plaintext into the core for message authentication and/or encryption and vice versa. The complete operation of the core is explained in the documentation available under NDA from Elliptic.

The CLP-15 has two throughput options as specified in the Table on page 5.

Authenticated Encryption Throughput	ASIC Gate Count (K gates)
20 Gbps	250
40 Gbps	400

The CLP-15 is available in soft IP form, either as a Netlist or HDL Source. The deliverable available are:

**Netlist Licenses:**

- Post synthesis netlist
- Testbench
- Sample simulation script
- Documentation

**HDL Source Licenses:**

- Verilog HDL
- Testbench
- Sample synthesis script
- Documentation

An FPGA load can be made available under license for evaluation purposes or the core can be made available on the Elliptic evaluation system – the ELP-01. For more information on pricing and a full data sheet, please contact:

Elliptic Semiconductor Inc.  
308 Legget Dr., Suite 202  
Kanata, ON, K2K 1Y6

Phone: +1 613 254-5456  
Fax: +1 613 254-7260  
Email: [info@ellipticsemi.com](mailto:info@ellipticsemi.com)