



## Overview

The **JetGCM<sup>TM</sup>-Fast and Ultra Fast** cores implement the AES-GCM (Galois Counter Mode) to provide both authentication and privacy. The ultra fast version supports very high throughput by pipelining and parallel processing techniques. Typical applications of AES-GCM are high-speed network security and storage data protection.

JetGCM<sup>TM</sup> cores integrate a Galois Field Multiplier with a high performance fully verified JetAES<sup>TM</sup> cryptographic core in counter mode to provide authenticated encryption. The cores support encryption, decryption, authentication, and verification functionalities and can be used with all or any of key sizes (128, 192, 256-bit). There are three JetGCM<sup>TM</sup> cores of different data rates to meet your project needs. The cores are available for licensing in both source and netlist form.

## Applications

- IPsec, SSL, Virtual Private Networks (VPN)
- Storage Area Networks (SAN)
- Optical transmission networks
- Voice over IP (VoIP)
- MACsec Ethernet security (IEEE 802.1ae)
- Security in data storage

## Features

- Fully compliant with AES-GCM mode as specified in
  - IEEE standard 802.1ae
  - IETF RFC-4106
  - Fibre Channel Security Protocol
  - IEEE draft standard P1619.1
- Simple interface
- Fully synchronous design
- Flow-through design
- Three cores
  - JetGCM<sup>TM</sup>-Fast  
128-bit wide data path processes each round in single clock cycle
  - JetGCM<sup>TM</sup>-Ultra Fast 2C  
process 128-bit block per 2 cycles
  - JetGCM<sup>TM</sup>-Ultra Fast 1C  
process 128-bit block per clock cycle
  - Other speed / size combinations are also available
- Combine both AES-GCM encryption-authentication and decryption-verification
- User programmable key size of 128, 192 or 256-bit change dynamically
- Cores with reduced gate count are also available for specific key size
- On-the-fly hardware key expansion
- Key expansion can also be done in software to reduce gate count
- Available as synthesizable Verilog source code, or as a netlist
- Self-checking test bench

## General Description

Advanced Encryption Standard (AES), also known as Rijndael, is a block cipher adopted as an encryption standard by NIST to replace DES. DES is now considered to be insecure for many applications.

GCM mode (Galois/Counter Mode) is a mode of operation for block ciphers such as AES. It combines the counter mode of encryption with the Galois mode of authentication to provide both authentication and privacy. Its main feature is the Galois Field Multiplication used for authentication can be processed in parallel to gain higher throughput than the authentication algorithms that use feedback, such as AES-CBC mode.

JetGCM<sup>TM</sup> cores implement AES-GCM mode as specified in the following applications:

- IEEE P1619.1 – *tape storage privacy and integrity*  
P1619.1 specifies an architecture for protection of data in variable-length block storage media such as tape cartridge. It utilizes AES-GCM with the 256-bit key size for privacy and integrity of data stored on tape.
- IEEE standard 802.1ae – *MACsec Ethernet security*  
Media Access Control security (MACsec) defines layer 2 security protocols for protecting data traversing Ethernet LANs on a hop-by-hop basis. It identifies and excludes unauthorized LAN connections from the network. MACsec utilizes a 128-bit key size AES-GCM in the mandatory cipher suite. Additional cipher suites may have key lengths longer than 128-bits.
- IETF RFC-4106 – *GCM in IPsec encapsulating security payload*  
IPsec defines security infrastructure to provide data confidentiality, data integrity and data authentication for Internet Protocol (IP) communications. IPsec secures network operation by protecting traffic on an end-to-end basis. IPsec security payload that utilizes AES-GCM may have 128, 192 or 256-bit key sizes.
- Fibre Channel Security Protocols – *ANSI (INCITS) draft FC-SP*  
FC-SP defines the security architecture for Fibre Channel networks. The security architecture has a mandatory 128-bit key size AES-GCM. Key lengths longer than 128-bits are optional.

The cores integrate a binary Galois Field Multiplier and a fully verified JetAES<sup>TM</sup> Fast cryptographic module to perform encryption, authentication, decryption, and verification functionalities. They support 128, 192 and 256-bit key sizes. The cores are implemented for flow-through operation. The design is fully synchronous for portability.

JetGCM<sup>TM</sup>-Fast core, with throughput up to 3 Gbps, is implemented with a 128-bit wide data path and 128-bit wide data interfaces. Therefore, each round takes 1 clock cycle. The number of cycles required to encrypt and authenticate 128-bit plain text is a function of the input key size:

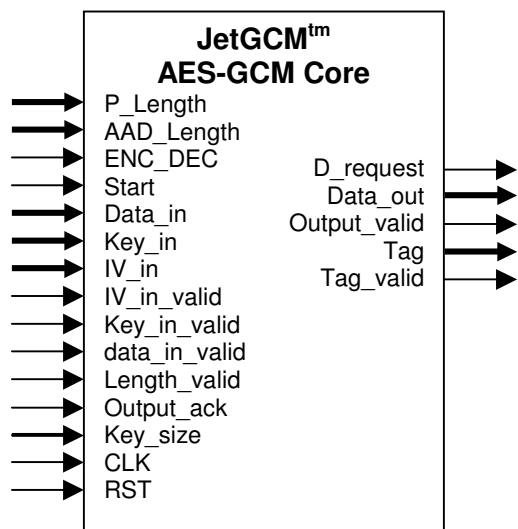
- 128-bit key → 11 cycles

- 192-bit key → 13 cycles
- 256-bit key → 15 cycles

JetGCM<sup>™</sup>-Ultra Fast 1C core, integrates a binary Galois Field Multiplier and a fully verified JetAES<sup>™</sup> Ultra Fast 1C cryptographic module to perform encryption, authentication, decryption, and verification functionalities. The core is implemented with a 128-bit wide pipelined data path and 128-bit wide data interface. After an initial latency of 11 cycles (13 cycles for 192-bit keys, 15 cycles for 256-bit keys) the core performs authentication and outputs 128-bit cipher text every clock cycle, thus, achieving ultra high throughput. Similarly, JetGCM<sup>™</sup> Ultra Fast 2C performs authentication and outputs 128-bit cipher text every 2 clock cycles.

The key expansion logic inside the core works as a standalone block which can generate the AES roundkeys on-the-fly. If the input key does not change frequently, then the roundkeys can be pre-expanded and stored in memory by the Key Expansion Logic. Alternatively, the roundkeys can also be generated and stored in memory by an embedded processor. Thus, these options can further reduce gate count.

**Core I/O**



The core I/O signals of the JetGCM<sup>™</sup> core are described in the table below.

Signal	I/O	Width	Description
CLK	Input	1	Master clock
RST	Input	1	Master reset, 1 = reset
P_Length	Input	64	Length of plain or cipher text data in bits
AAD_Length	Input	64	Length of additional authentication data in bits
ENC_DEC	Input	1	Encrypt when low, Decrypt when high
Start	Input	1	Start process

Data_in	Input	128	Input data (AAD followed by plain or cipher text)
Key_in	Input	128	AES-key in 128-bit (other sizes also supported)
IV_in	Input	128	Initialization vector (96-bit followed by 32 zeros)
IV_in_valid	Input	1	Initialization vector valid
Key_in_valid	Input	1	Key valid
Data_in_valid	Input	1	Input data valid
Length_valid	Input	1	Length valid
Output_ack	Input	1	Output acknowledgement
Key_size	Input	2	Select 128-bit, 192-bit or 256-bit key
Data_out	Output	128	Output cipher text or plain text
D_request	Output	1	Data input request
Output_valid	Output	1	Cipher or plain text output valid
Tag	Output	128	MAC (message authentication code)
Tag_valid	Output	1	Process done and Tag output valid

## Implementation Results

Example ASIC implementation statistics for the JetGCM<sup>tm</sup>-Fast core (for 128,192 or 256 bit key are shown below

Technology	Gate Count
TSMC 0.18 $\mu$ m	60,000

Example implementation statistics for the JetGCM<sup>tm</sup>-Fast core are shown below.

Xilinx Family	Device	Slices	BRAM	GCLK	I/O	FMax(MHz)	Throughput
Virtex-5 <sup>tm</sup>	XC5VLX30	924	10	1	782	256	2.9 Gbps
Virtex-4 <sup>tm</sup>	XC4VLX25	2090	10	1	782	233	2.7 Gbps
Virtex-II <sup>tm</sup>	XC2V8000	2041	10	1	782	148	1.7 Gbps
Virtex-II Pro <sup>tm</sup>	XC2VP40	1966	10	1	782	269	3.1 Gbps
Spartan-3 <sup>tm</sup>	XC3S4000	2143	10	1	782	130	1.5 Gbps

### Support

Sixty days of phone and email technical support are included. Additional maintenance and support options are available.

### Verification

The JetGCM<sup>™</sup> cores have been thoroughly simulated and verified on Xilinx FPGA hardware using the NIST test vectors and additional software-generated test vectors.

### Deliverables

The cores are available in soft IP form, either as a Netlist or HDL Source. The deliverables include:

- For **Netlist Licenses** : Target specific net list
- For **HDL Licenses** : Fully synthesizable RTL Verilog source
- Self-checking test bench
- Simulation script, test vectors and expected results
- User documentation

### Export Permits

Jetstream Media Technologies' security products are subject to the export control under the United States Bureau of Industry and Security (BIS) ([www.bis.doc.gov](http://www.bis.doc.gov)). Customers must reference the U.S. rules governing exports and re-exports of encryption items specified in the Export Administration Regulations (EAR) (<http://www.access.gpo.gov/bis/index.html>), and consult with their legal advisors to determine if licenses are required. Please also refer to the export information page in our web site.

### More Information

For more detailed information on this or any of our other products and services, please contact us and we will be pleased to discuss how we can assist with your individual requirements.

[www.security-cores.com](http://www.security-cores.com)  
or  
[www.jetsmt.com](http://www.jetsmt.com)

Jetstream Media Technologies  
800 W. 5th Ave.  
Naperville, IL 60563 U.S.A.  
Tel: 1 (630)-301-4778  
Email: [sales@jetsmt.com](mailto:sales@jetsmt.com)