



## Overview

The **JetCombo<sup>TM</sup>-3** core implements the AES-GCM (Galois Counter Mode), XTS-AES (XEX-based Tweaked codebook mode with ciphertext Stealing) and AES-CCM (Counter with CBC-MAC) mode to provide authentication and privacy. Typical applications of the core are high-speed network security, wireless security, authentication, and disk / tape storage data protection.

JetCombo<sup>TM</sup>-3 core integrates a Galois Field Multiplier, a high performance fully verified JetAES<sup>TM</sup> cryptographic core. The core supports authentication and verification for GCM/CCM modes, and supports encryption and decryption functionalities for all three modes. The core is available for licensing in both source and netlist form.

## Applications

- IPsec, Virtual Private Networks (VPN)
- Wireless network security
- Hard disk encryption (IEEE P1619)
- Tape storage encryption (IEEE P1619.1)
- Storage Area Networks (SAN)
- Optical transmission networks
- Voice over IP (VoIP)
- MACsec Ethernet security (IEEE 802.1ae)

## Features

- Fully compliant with both AES-GCM, XTS-AES and AES-CCM modes as specified in
  - IEEE standard 802.1ae
  - Wireless security standards
  - IETF RFC-4106, RFC4309
  - Fibre Channel Security Protocol
  - IEEE draft standard P1619
  - IEEE draft standard P1619.1
- Simple interface
- Fully synchronous design
- Flow-through design
- Throughput up to 3 Gbps
- Combine both AES-GCM/XTS/CCM encryption--authentication and decryption-verification
- Support 128-bit, or 256-bit key sizes
- XTS-AES support CTS (Cipher Text Stealing) for sector size not divisible by 128
- 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.

CCM mode (Counter with CBC-MAC) is a mode of operation for use with block cipher such as AES. CCM mode combines the counter mode of encryption with the CBC-MAC mode of authentication. This mode is used by several wireless security standards, tape storage encryption / authentication, and networking security such as IPsec,

XEX (Xor-Encrypt-Xor), a tweakable encryption mode, was designed to allow very efficient processing of consecutive blocks of data. XTS-AES specified in the IEEE draft P1619 for encryption of sector-based storage applications is a variant of tweakable block cipher. It is defined as XEX-based Tweakable CodeBook mode (TCB) with CipherText Stealing (CTS).

XTS-AES combines AES with the Galois field multiplication. One of its features is the Galois Field Multiplication used can be simplified to shift and exclusive-or to reduce implementation size. Also, its implementation can be pipelined to gain higher throughput than other algorithms that use feedback, such as AES-CBC mode. The CTS supports storage with sector size not divisible by 128. This IEEE draft replaces the previous draft LRW-AES (Lislov, Rivest and Wagner) mode.

JetCombo<sup>TM</sup>-3 core implements AES-GCM and AES-XTS modes as specified in the following applications:

- IEEE P1619 – *disk storage privacy*  
P1619 specifies encryption of data in sector-based storage. The XTS-AES mode of operation utilizes two keys with key sizes equal to 128+128 bits or 256+256 bits. Sector sizes need not be divisible by 128.
- 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*
- IETF RFC-4309 – *CCM 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.

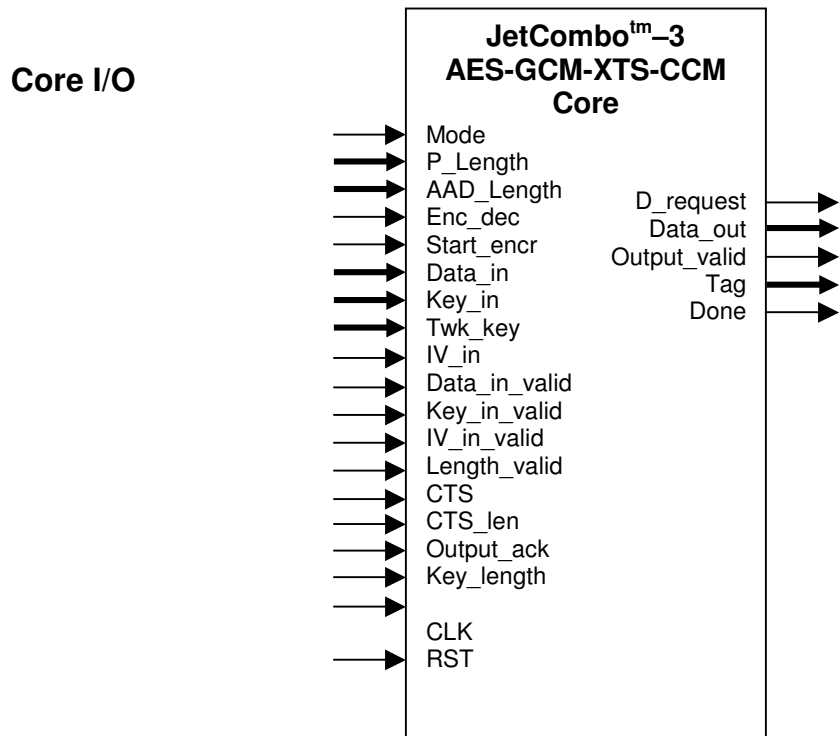
- Fibre Channel Security Protocols – *ANSI (INCITS) draft FC-SP*

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 core integrates 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 core is implemented for flow-through operation. The design is fully synchronous for portability.

JetCombo<sup>TM</sup>-3 Fast core, with throughput up to 3 Gbps, is implemented with a 128-bit wide data path without pipeline and 128-bit wide data interfaces.

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.



The core I/O signals of the JetCombo<sup>tm</sup>-3 core are described in the table below.

Signal	I/O	Width	Description
CLK	Input	1	Master clock
RST	Input	1	Master reset, 1 = reset
Mode	Input	2	0 = GCM mode ; 1 = CCM mode, 2 = XTS mode
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_encr	Input	1	Start process
Data_in	Input	128	Input data (AAD followed by plain or cipher text)
Key_in	Input	256	AES-key in 256-bit (other sizes also supported)
Twk_key	Input	256	Tweak key
IV_in	Input	128	GCM – Initialization vector (96-bit followed by 32 zeros) CCM – Nonce (103-bit followed by 25 zeros) XTS – Logical position
Data_in_valid	Input	1	Input data valid
Key_in_valid	Input	1	Key valid
IV_in_valid	Input	1	IV valid
Length_valid	Input	1	Lengths valid
CTS	Input	1	Cipher text stealing mode. It signals the current block is the last full 128-bit data block of the sector, and the next block is a partial data block.
CTS_len	Input	4	Number of bytes in the partial data block
Output_ack	Input	1	Output acknowledgement
Key_length	Input	1	Select 128-bit or 256-bit key
Data_out	Output	128	Output ciphertext or plaintext
D_request	Output	1	Data request signal
Output_valid	Output	1	Cipher or plaintext output valid
Tag	Output	128	MAC (message authentication code)
Done	Output	1	Process done and Tag output valid

### Support

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

### Verification

The JetCombo<sup>™</sup>-3 core has been thoroughly simulated and verified on Xilinx FPGA hardware using the IEEE and NIST test vectors and additional software-generated test vectors.

### Deliverables

The core is 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)