



Overview

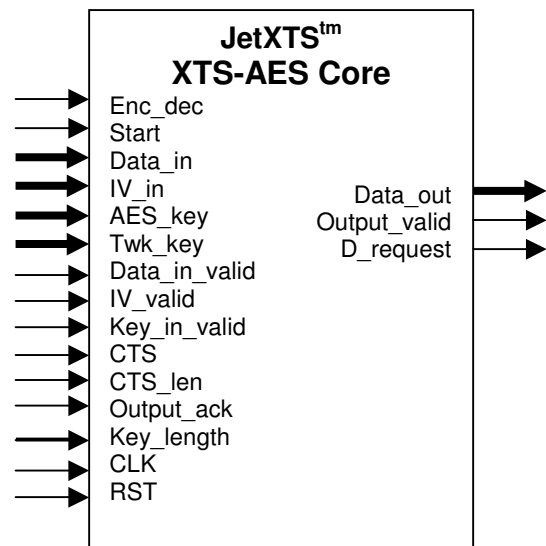
The IEEE draft P1619 specifies the XTS-AES mode (XEX-based Tweaked codebook mode with ciphertext Stealing) of AES operation to provide encryption of storage at the sector level. The AES disk encryption algorithm utilizes a Galois field multiplication, and a pair of keys – an AES key and a tweak key. This recent IEEE draft replaces the previous draft LRW-AES (Lislov, Rivest and Wagner) mode.

JetXTS™ Fast and Ultra Fast cores are optimized for IEEE P1619 applications. They integrate an optimized Galois Field Multiplier with a high performance fully verified JetAES™ cryptographic core. They supports cipher text stealing for any disk with sector size not divisible by 128. The cores perform both encryption and decryption using 128+128 and 256+256 bit key sizes according to the P1619 draft. Their design is fully synchronous for portability. The cores are available for licensing in both source and netlist form.

Application

IEEE P1619 disk encryption applications

Features	
➤	Fully compliant with XTS-AES mode as specified in IEEE draft P1619
➤	Simple interface
➤	Fully synchronous design
➤	Flow-through design
➤	Two cores <ul style="list-style-type: none"> • JetXTS™ Fast Throughput up to 3 Gbps • JetXTS™ Ultra Fast Throughput up to 50 Gbps
➤	Support 128-bit or 256-bit AES key size and 128-bit or 256-bit tweak key size as defined in P1619
➤	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



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.

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 feature 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.

JetXTSTM-Fast and Ultra Fast cores implement XTS-AES mode as specified in the IEEE drift P1619. It integrates an optimized binary Galois Field Multiplier and a fully verified JetAESTM Fast and Ultra Fast cryptographic modules and supports both encryption and decryption functionalities. Both JetXTSTM- Fast and JetXTSTM- Ultra Fast cores take 128-bit and 256-bit AES key and 128-bit and 256-bit tweak key as defined in P1619. The cores are implemented for flow-through operation. Their design is fully synchronous for portability.

JetXTSTM-Ultra Fast core is implemented with a 128-bit wide pipelined data path and 128-bit wide data interface. After an initial latency of a few cycles, the core outputs 128-bit cipher text every clock cycle thus achieving ultra high throughput.

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 JetXTSTM core are described in the table below.

Signal	I/O	Width	Description
CLK	Input	1	Master clock
RST	Input	1	Master reset, 1 = reset
Enc_dec	Input	1	Encrypt when low; Decrypt when high
Start_encr	Input	1	Start Process

Data_in	Input	128	Input plain text or cipher text
IV_in	Input	128	Logical position (initialization vector)
AES_Key	Input	256	AES key
Tweak_key	Input	256	Tweak key
Data_in_valid	Input	1	Data in valid
IV_valid	Input	1	Initialization vector valid
Key_in_valid	Input	1	AES key 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	128+128 bit key or 256+256 bit key
Data_out	Output	128	Output cipher text or plain text
D_request	Output	1	Data input request
Output_valid	Output	1	Output valid

Support

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

Verification

The JetXTS™ cores have been thoroughly simulated and verified on Xilinx FPGA hardware using IEEE 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). 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

or

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