



Overview

The **JetAESTM Ultra Fast** encryption and decryption IP cores implement the AES (Rijndael) encryption standard, as described in the NIST Federal Information Processing Standard (FIPS) 197.

The cores are designed to be highly flexible and can be integrated into any AES design with ease. Different options are available for achieving the best speed/area results for specific applications. The cores support both encryption and decryption functionality and can be used with 128, 192, 256-bit key sizes. The cores are available for licensing in both source and netlist form.

Applications

Security in networked environments

- 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 program content

Security in electronic financial transactions

Security in video surveillance systems

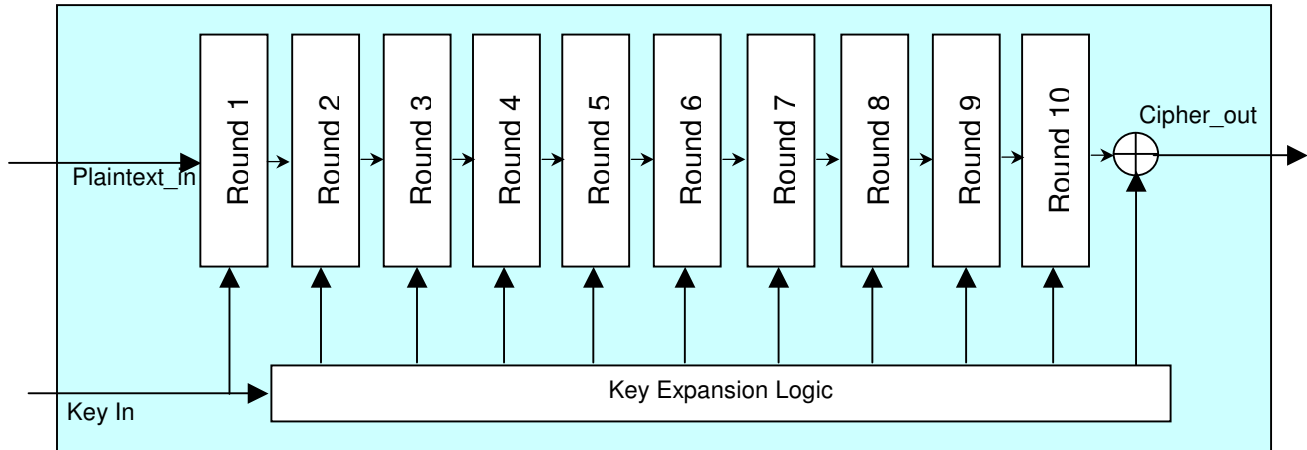
Security in military communications systems

Security in audio communications

Security in data storage

Features

- Fully compliant with AES described in NIST FIPS 197
- High throughput > 50 Gbps
- Simple interface
- Fully synchronous design
- Flow-through design
- 128-bit wide pipelined data path
- Two speed options:
 - version **1C** encrypts / decrypts a 128-bit block in 1 clock cycle
 - version **2C** encrypts / decrypts a 128-bit block in 2 clock cycles
- Support 128, 192 and 256-bit key sizes
- On-the-fly hardware key expansion
- No dead cycle when changing keys
- Key expansion can also be done in software to reduced the gate count
- Separate cores for encryption and decryption
- Combined encryption-decryption core also available with minimum gate count
- Available solutions for more advanced modes of AES, such as AES-GCM, LRW-AES
- Core is available as a synthesizable Verilog source code, or as a netlist
- Self-checking test bench with FIPS test vectors



Block Diagram

Functional Description

The architecture of the **JetAES™ Ultra Fast 1C encryption core** for 128-bit key size is shown in the above figure. The AES algorithm is composed of a sequence of steps that are repeated a particular number of times, or “rounds”, depending upon the input key size.

- 128-bit key → 10 rounds
- 192-bit key → 12 rounds
- 256-bit key → 14 rounds

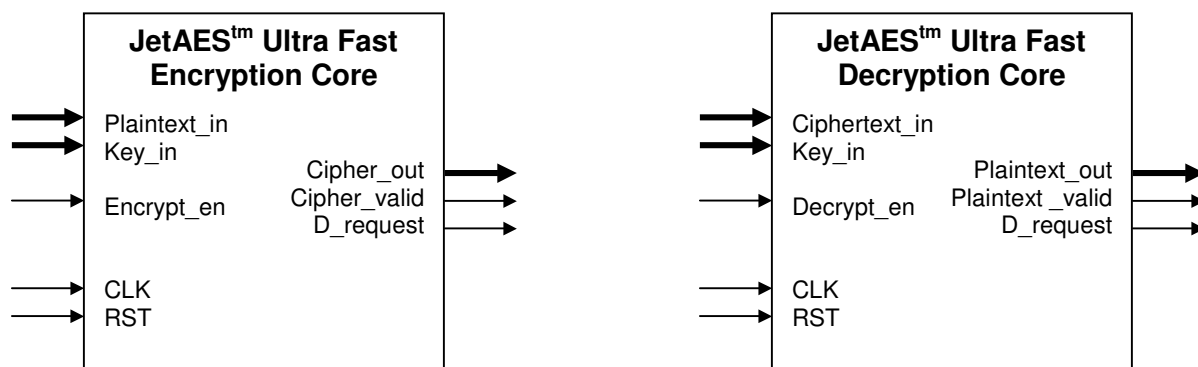
The core implements a 128-bit wide pipelined data path and 128-bit wide data interface. After a latency of 11 cycles (13 cycles for 192-bit keys, 15 cycles for 256-bit keys) the core outputs 128-bit cipher text every clock cycle, thus, achieving ultra high throughput. Similarly, JetAES™ Ultra Fast 2C AES encryption core outputs 128-bit cipher text every 2 clock cycles.

Each AES round requires a unique 128-bit key. These keys are generated by the **Key Expansion Logic**. The Key expansion logic accepts the input 128, 192 or 256-bit key and outputs a sequence of 128-bit roundkeys. For a 128-bit key size 11 roundkeys are generated; or 192 and 256-bit key sizes, 13 and 15 roundkeys are generated respectively.

The Key Expansion Logic can work as a standalone block which can generate the 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 a processor. These options reduce gate count.

For the AES decryption process, the roundkeys need to be generated in the reverse order. Hence, the key expansion has to start with the last round key of the encryption process.

Core I/O



The core I/O signals of the JetAES™ Ultra Fast 1C & 2C AES encryption core with hardware on-the-fly key expansion are described in the table below.

Signal	I/O	Width	Description
CLK	Input	1	Master clock
RST	Input	1	Master reset; 1 = reset
Plaintext_in	Input	128	Plain text input
Key_in	Input	128, 192 or 256	Key input
Encrypt_en	Input	1	Encryption enable
Cipher_out	Output	128	Cipher text output
Cipher_valid	Output	1	Cipher text output valid
D_request	Output	1	Data input request

The core I/O signals for JetAES™ Ultra Fast 1C & 2C AES decryption core with hardware on-the-fly key expansion are described in the table below.

Signal	I/O	Width	Description
CLK	Input	1	Master Clock
RST	Input	1	Master reset; 1 = reset
Ciphertext_in	Input	128	Cipher text input
Key_in	Input	128, 192 or 256	Inverse key in
Decrypt_en	Input	1	Decryption enable
Plaintext_out	Output	128	Plain text out
Plaintext_valid	Output	1	Plain text valid signal
D_request	Output	1	Data input request

Implementation Results

Example ASIC implementation statistics for the JetAES[™] Ultra Fast 1C AES encryption core (128-bit key) are shown below

Key Size	Technology	Gate Count
128	TSMC 0.18 μm	300,000
256	TSMC 0.18 μm	440,163

Example ASIC implementation statistics for the JetAES[™] Ultra Fast 2C AES encryption core (128-bit key) are shown below

Key Size	Technology	Gate Count
128	TSMC 0.18 μm	150,000
256	TSMC 0.18 μm	220,018

Example implementation statistics for the JetAES[™] Ultra Fast 1C AES encryption for the 128-bit and 256-bit key are shown below.

Key Size	Xilinx Family	Device	Slices	BRAM	CLK	I/O	FMax(MHz)	Throughput
128	Virtex-5 [™]	XC5VLX30	866	100	1	389	341	43 Gbps
	Virtex-4 [™]	XC4VLX30	2184	100	1	389	268	34 Gbps
256	Virtex-5 [™]	XC5VLX30	1108	138	1	389	341	87 Gbps
	Virtex-4 [™]	XC4VLX30	3896	138	1	517	286	54 Gbps

Example implementation statistics for the JetAES[™] Ultra Fast 2C AES encryption for the 128-bit and 256-bit key are shown below.

Key Size	Xilinx Family	Device	Slices	BRAM	CLK	I/O	FMax(MHz)	Throughput
128	Virtex-5 [™]	XC5VLX30	743	50	1	389	277	17 Gbps
	Virtex-4 [™]	XC4VLX100	1595	50	1	389	237	15 Gbps
256	Virtex-5 [™]	XC5VLX30	1265	70	1	389	311	39 Gbps
	Virtex-4 [™]	XC4VLX100	2862	70	1	517	268	21 Gbps

AES Cipher Modes Support

The JetAES[™] Ultra Fast encryption and decryption cores support Electronic Codebook (ECB) mode. Comprehensive solutions are also available for more advanced modes of AES, such as AES-GCM and LRW-AES.

Support

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

Verification

The JetAES[™] Ultra Fast encryption and decryption cores have been thoroughly simulated and verified on Xilinx FPGA hardware using the NIST FIPS test vectors, including full Monte Carlo tests.

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

