



Overview

The **JetAES™ 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 area / performance tradeoff for your requirement including a double speed version. The cores support both encryption and decryption functionality and can be used with all or any of the three AES key sizes (128, 192, 256-bit). 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

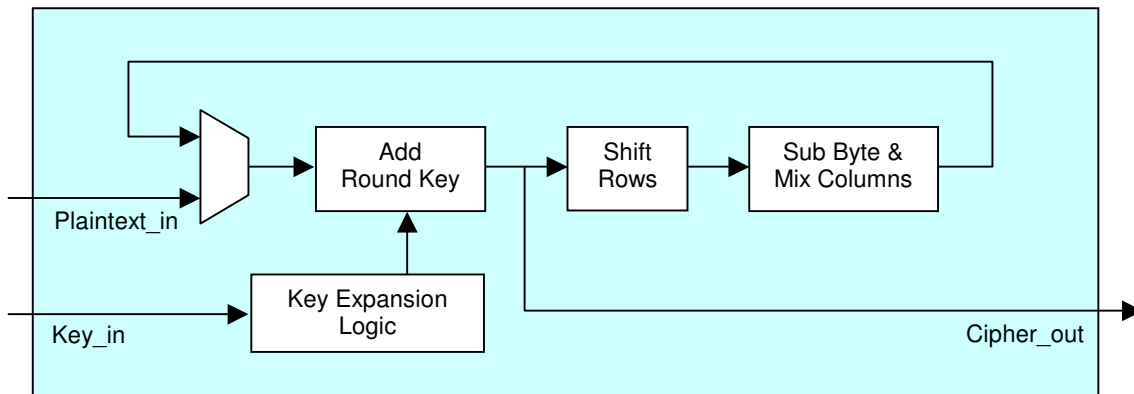
Security in military communications systems

Security in audio communications

Security in data storage

Features

- Fully compliant with AES described in NIST FIPS 197
- Simple interface
- Fully synchronous design
- Flow-through design
- **Fast version**
 - 128-bit wide data path
 - Throughput up to 3 Gbps
- **Fast – Double Speed version**
 - Pipelined 128-bit wide data path
 - Throughput up to 6 Gbps
- User programmable key size of 128, 192 or 256-bit change dynamically
- Cores with lower gate count are also available for specific key size
- Building block for ultra-high throughput solution
- On-the-fly hardware key expansion
- No dead cycle when changing keys
- Key expansion can also be performed in software to reduced the gate count
- Separate cores for encryption and decryption
- Combined encryption-decryption core also available with minimum gate count
- Supports ECB mode. Optional wrapper is included to support all AES classic block cipher modes like CBC, CFB, OFB or CTR
- Available solutions for more advanced “modes” of AES, such as AES-CCM, 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 **JetAESTM** Fast encryption core 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 incoming plain text data is added to the expanded key generated by the key expansion module in the Add Round Key step. The Shift Rows, Sub Byte, Mix Columns and Add Round Key operations are performed iteratively for the specific number of rounds based on the input key size. In the final round the Mix Columns step is ignored.

The core implements 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 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

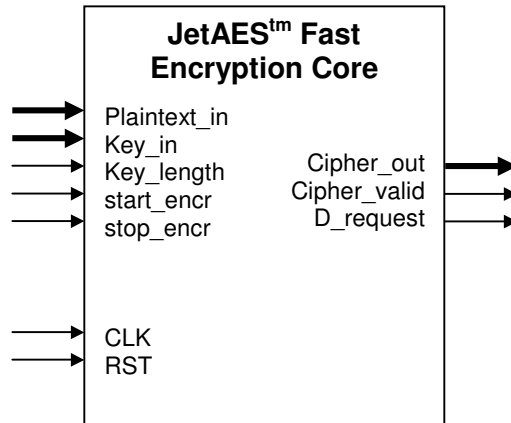
The double speed version is implemented with a pipelined datapath to achieve twice the throughput.

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; for 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 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. These options can further 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™ Fast encryption core with hardware on-the-fly key expansion for all AES key sizes 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	256	Key input
Key_length	Input	2	Key size selection: "00" = 128-bit, "01" = 192-bit, "1x" = 256-bit
Start_encr	Input	1	Start encrypting sequence of blocks
Stop_encr	Input	1	Stop encryption
Cipher_out	Output	128	Cipher text output
Cipher_valid	Output	1	Cipher text output valid
D_request	Output	1	Data input request

Implementation Results

Example ASIC implementation statistics for the JetAES™ Fast encryption core (128-bit key) are shown below

Technology	Gate Count
TSMC 0.18 μm	31,328

Example ASIC implementation statistics for the JetAES™ Fast encryption core (256-bit key) are shown below

Technology	Gate Count
TSMC 0.18 μm	33,095

Example ASIC implementation statistics for the JetAES™ Fast encryption core (128,192 or 256-bit keys) are shown below

Technology	Gate Count
TSMC 0.18 μm	33,346

Example implementation statistics for the JetAES™ Fast 128-bit key encryption core with on-the-fly key expansion are shown below.

Xilinx Family	Device	Slices	BRAM	CLK	I/O	FMax(MHz)	Throughput
Virtex-5™	XC5VLX30	114	10	1	390	289	3.3 Gbps
Virtex-4™	XC4VLX25-11	366	10	1	390	257	3.0 Gbps
Virtex-II Pro™	XC2VP20-7	361	10	1	390	249	2.8 Gbps
Spartan-3™	XC3S1500-5	365	10	1	390	119	1.3 Gbps
Spartan-3E™	XC3S1600E-4	358	10	1	390	113	1.3 Gbps

Example implementation statistics for the JetAES™ Fast 256-bit key encryption core with on-the-fly key expansion are shown below.

Xilinx Family	Device	Slices	BRAM	CLK	I/O	FMax(MHz)	Throughput
Virtex-5™	XC5VLX30	184	10	1	390	310	3.6 Gbps
Virtex-4™	XC4VLX25-11	456	10	1	518	216	2.1 Gbps
Virtex-II Pro™	XC2VP20-7	535	10	1	518	217	2.1 Gbps
Spartan-3™	XC3S1500-5	471	10	1	518	132	1.0 Gbps
Spartan-3E™	XC3S1600E-4	451	10	1	518	97	900 Mbps

Example implementation statistics for the JetAES™ Fast (128,192 or 256-bit keys) encryption core with hardware on-the-fly key expansion are shown below. The throughput is calculated for the 128-bit key only.

Xilinx Family	Device	Slices	BRAM	CLK	I/O	FMax(MHz)	Throughput
Virtex-5™	XC5VLX30	331	10	1	390	256	2.9 Gbps
Virtex-4™	XC4VLX25-11	827	10	1	520	163	1.8 Gbps
Virtex-II Pro™	XC2VP20-7	797	10	1	520	163	1.8 Gbps
Spartan-3™	XC3S1500-5	792	10	1	520	94	1.0 Gbps
Spartan-3E™	XC3S1600E-4	801	10	1	520	78	907 Mbps

AES Cipher Modes Support

The JetAES™ Fast encryption and decryption cores support Electronic Codebook (ECB) mode. A group of wrapper designs are available to support all AES classic block cipher modes like: Cipher Block Chaining (CBC), Cipher Feedback (CFB), Output Feedback (OFB), and Counter (CTR).

Comprehensive solutions are also available for more advanced “modes” of AES, such as AES-CCM, AES-GCM, LRW-AES.

Support

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

Verification

The JetAES™ 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