

Features

- FIPS 197 compliant AES cores
- Supports key sizes of 128, 192, and 256-bits
- Supports NIST SP800-38D defined GCM mode
- Key schedule generator *included*
- Standard and fast product series support different performance & area requirements
- AES support also available in TeraFire F5200 cryptography microprocessor
- AHB and AXI microprocessor bus interfaces available

Benefits

- Modular architecture enables scalable performance and optimal implementation
- Full 128-bit data ports maximize performance, minimize latency



Standard Performance AES-GCM

Athena delivers Advanced Encryption Standard Galois Counter Mode (AES-GCM) as a semiconductor intellectual property (IP) core for Actel FPGA. Athena has been a leader in cryptography for a decade with the TeraFire line of products that includes solutions for AES, SHA, 3DES, MD5, public key cryptography, including RSA, DSA, and ECC, and more. Whatever your application, Athena has the functionality and an area/performance option that is right for you — and with discounted pricing for multiple cores, TeraFire products are sure to save both development time and money.

Product Description

TeraFire AES core solutions are constructed using a modular architecture that optimizes AES solutions specifically for Actel FPGAs. The performance parameters for the standard performance AES-GCM encrypt/decrypt only core are shown in Table 1.

Table 1: Standard Performance AES-GCM Parameters for Actel ProASIC3

Model	Performance	Area
Std AES-GCM AES-A200-GO	190 Mbps/70 MHz	4650 tiles/3 RAMs

Athena's AES cores are complete, silicon-proven implementations, loaded with features including integrated modes support, key schedule generation, and context switching. These cores can also be provided with optional bus interfaces, such as AHB and AXI, to jumpstart your system integration efforts. The interface block diagram for the AES core is shown in Figure 1.

Applications

- Encrypted data storage
- Secure communications
- Secure processing
- IPsec acceleration
- E-commerce
- VPN
- Financial transactions

Available Deliverables

- Netlist
- RTL (VHDL/Verilog)
- Verification suite
- Simulation model
- AHB/AXI bus interfaces
- TeraFire CAL software
- Documentation
- Support

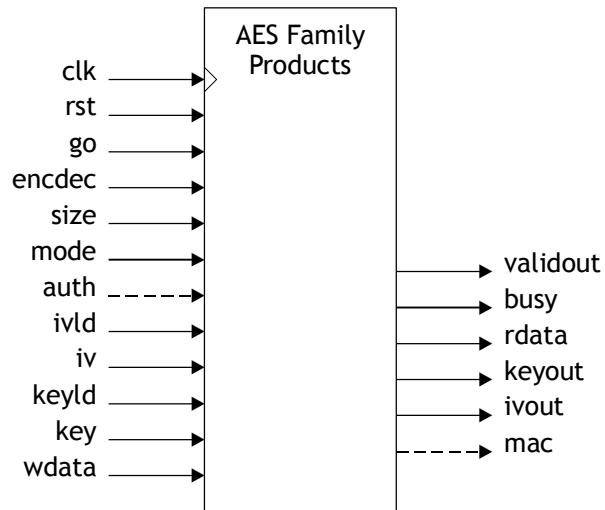


Figure 1: Interface Block Diagram of AES Family Members

AES for Actel Product Selector

Athena's family of AES cores are compliant with FIPS 197 and NIST SP800-38A, C, and D defined operating modes: ECB, CBC, CFB, OFB, CTR, CCM, and GCM. AES cores are offered at two performance tiers, and as an option in Athena's F5200 cryptography microprocessor. Athena's family of AES products for Actel is summarized in Table 2. Contact Athena if you don't see the performance or functionality that you need – we can produce a custom solution just right for your application.

Licensing and Deliverables

Athena offers a number of licensing alternatives, including single design, multiple design, and site licenses. License upgrades are also available. Athena also offers several deliverables options, including RTL and netlist. Contact Athena for additional information.

TeraFire Cryptography Application Library (CAL)

The optional TeraFire CAL is a portable, ANSI C library of cryptographic software implementations and drivers for TeraFire hardware accelerators. The TeraFire CAL has been implemented and tested on multiple platforms, including leading SoC microprocessors from ARM. Athena's sophisticated configuration management system enables rapid configuration of the TeraFire CAL for your mix of hardware accelerator and software implementation requirements.

Device Compatibility

Athena AES family products are compatible with all Actel devices with sufficient logic and memory capacity, including:



The Athena Group, Inc.
408 W. University Ave., Suite 306
Gainesville, FL 32601

Phone: (352) 371-2567
Toll-free: (800) 741-7440
Fax: (352) 373-5182
www.athena-group.com

Copyright The Athena Group, Inc., 2009. All rights reserved. Reproduction in whole or in part is prohibited without the prior written consent of the copyright owner. The information presented in this document does not form part of any quotation or contract, is believed to be accurate and reliable, and may be changed without notice. No liability will be accepted by the publisher for any consequence of its use. Publication thereof does not convey nor imply any license under patent or other industrial or intellectual property rights.

Table 2: AES for Actel Product Selector

Model	Performance	Area	Modes
Fast ECB enc/dec AES-A100-E	702 Mbps/ 65 MHz	3926 tiles/ 10 RAMs	Encrypt/decrypt ECB
Fast ECB enc-only AES-A100-EE	962 Mbps/ 90 MHz	1816 tiles/ 10 RAMs	ECB encrypt only
Fast enc/dec AES- A100-A	680 Mbps/ 64 MHz	6524 tiles/ 10 RAMs	Full encrypt/decrypt ECB/CBC/CFB/OFB/CTR
Fast enc-only AES-A100-AE	879 Mbps/ 82 MHz	4239 tiles/ 10 RAMs	Encrypt only ECB/CBC/CFB/OFB/CTR ^a
Fast CCM AES- A100-CO	400 Mbps/ 75 MHz	4780 tiles/ 10 RAMs	CCM authenticated encrypt/decrypt
Fast GCM AES- A100-GO	600 Mbps/ 75 MHz	5500 tiles/ 10 RAMs	GCM authenticated encrypt/decrypt
Std ECB enc/dec AES-A200-E	177 Mbps/ 65 MHz	2852 tiles/ 3 RAMs	Encrypt/decrypt ECB
Std ECB enc-only AES-A100-EE	256 Mbps/ 93 MHz	1718 tiles/ 3 RAMs	ECB encrypt only
Std enc/dec AES- A200-A	163 Mbps/ 60 MHz	5634 tiles/ 3 RAMs	Full encrypt/decrypt ECB/CBC/CFB/OFB/CTR
Std enc-only AES- A200-AE	187 Mbps/ 69 MHz	4227 tiles/ 3 RAMs	Encrypt only ECB/CBC/CFB/OFB/CTR ^a
Std CCM AES-A200-CO	89 Mbps/65 MHz	4680 tiles/ 3 RAMs	CCM authenticated encrypt/decrypt
Std GCM AES-A200-GO	190 Mbps/ 70 MHz	4650 tiles/ 3 RAMs	GCM authenticated encrypt/decrypt

a. Includes CFB/OFB/CTR decrypt at no area penalty.

Designed for Easy Integration

Athena has over a decade of experience in delivering first-time design success. Athena has become a premier provider of semiconductor IP by always delivering quality. Athena standard deliverables include everything you need to integrate our core into your design.

About The Athena Group, Inc.

Based in Gainesville, Florida, Athena innovates breakthrough technologies that achieve the optimum balance of power, performance, and silicon area in a wide range of applications such as wireless, satellite, and secure communications. Athena provides patented semiconductor intellectual property (IP) solutions, with products ranging from the market-leading TeraFire[®] security cores, to Atomic DSP[™] cores, and Atomic SDR[™] software defined radio cores.

Athena was founded in 1986 and is privately held.