

Features

- FIPS 197 compliant AES cores
- Supports key sizes of 128, 192, and 256-bits
- Supports NIST SP800-38A, B, C, D, and E defined modes
- Three dedicated product series support different performance & area requirements
- Modular architecture
- AES support also available in TeraFire F5200 cryptography microprocessor
- Microprocessor bus interfaces available
- Easy SoC integration
- Simple/differential power analysis (SPA/DPA) resistance available

Benefits

- Modular architecture enables scalable performance and optimal implementation
- Full-width data ports maximize performance, minimize latency
- Fast delivery for accelerated time to profit



Advanced Encryption Standard (AES) Family

Athena delivers the AES as a semiconductor intellectual property (IP) core family. Athena's AES core family complements the market leading TeraFire[®] cryptography microprocessors and standalone TeraFire cryptography accelerators. Whether your application demands high AES performance or the power savings of a dedicated core, Athena's AES core family delivers both performance and power savings.

Athena offers AES both within its cryptography microprocessor family and as dedicated cores. Optional microprocessor bus interfaces are also available for dedicated AES core solutions. The AES product family is summarized in Table 1.

Table 1: AES Product Family Elements

Model Base	Description
AES-A100	Dedicated high-performance AES (5.8 Gbps ^a)
AES-A200	Dedicated standard performance AES (1.4 Gbps ^a)
AES-A300	Dedicated compact AES (360 Mbps ^a)
EXP-F5200B	Full Suite B cryptography microprocessor with AES support (>150 Mbps ^b)
TAI-A100	AHB bus interface for Athena TeraFire cores
TXI-A100	AXI bus interface for Athena TeraFire cores

a. Nominal performance at 500 MHz with 128-bit key.

b. Nominal performance at 500 MHz with 128-bit key.

Dedicated AES core solutions are constructed using a modular architecture, comprising cipher cores, key schedule generators, and modes modules, allowing Athena to configure an AES solution optimized for the performance, area, and power requirements of your application. Common configurations are offered as bundles as listed in Table 2; however, custom configurations using these production proven modules may also

Applications

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

Available Deliverables

- Simulation model (Verilog or VHDL)
- Synthesizable RTL (Verilog or VHDL) and scripts
- Targeted, timing closed netlist
- Verification suite
- Documentation
- Support

be built to meet your unique performance, area, and power requirements.

Table 2: Dedicated AES Product Bundle Selector

Bundle P/N	Performance ^a	ECB/CBC/CFB/ OFB/CTR	CCM	GCM/ GHASH	XTS ^b
AES-A100-A	5.8 Gbps	Y			opt.
AES-A100-C	5.8 Gbps	Y	Y ^c		opt.
AES-A100-G	5.8 Gbps	Y	Y ^c	Y	opt.
AES-A200-A	1.4 Gbps	Y			opt.
AES-A200-C	1.4 Gbps	Y	Y ^c		opt.
AES-A200-G	1.4 Gbps	Y	Y ^c	Y	opt.
AES-A300-A	360 Mbps	Y			opt.
AES-A300-C	360 Mbps	Y	Y ^c		opt.
AES-A300-G	360 Mbps	Y	Y ^c	Y	opt.

a. Nominal performance at 500 MHz with 128-bit key.

b. XTS (SP800-38E) mode may be added to any bundle with -X option.

c. Half speed in this mode also available.

Athena's AES cores are compliant with a range of standards, including:

- FIPS 197,
- NIST SP800-38A (ECB, CBC, CFB, OFB, CTR),
- NIST SP800-38B (CMAC),
- NIST SP800-38C (CCM),
- NIST SP800-38D (GHASH, GCM),
- NIST SP800-38E (XTS),
- Suite B,
- IEEE 802.1ae,
- IEEE 802.11i, and
- IEEE 802.16e.

Bus Interfaces

Athena's dedicated cryptography solutions are designed for stand-alone operation and provide full-width support to enable maximum performance and flexibility. AHB, AXI, and other bus interfaces are also available.

TeraFire Cryptography Application Library (CAL)

The 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.

Designed for Easy Integration

Athena has over a decade of experience in delivering first-time physical design success. Athena has become a premier provider of semiconductor IP by always delivering quality. To ensure ease of integration, Athena goes the distance - by synthesizing *our* IP into *your* target library, in *your* process, with *your* constraints, and delivering a completed core, ready for place and route. Athena standard deliverables include everything you need to integrate our core into your design: netlists, simulation models, test vectors, support, and documentation.

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.



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
ipsales@athena-group.com

Copyright The Athena Group, Inc., 2011. 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.