

Features

- FIPS 197 compliant AES cores
- Supports key sizes of 128, 192, and 256-bits
- Supports NIST SP800-38A, C, and D defined modes
- Two 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

Benefits

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

Applications

- Encrypted data storage
- Secure communications
- Secure processing



Advanced Encryption Standard Family

The Athena Group delivers the Advanced Encryption Standard (AES) as a semiconductor intellectual property (IP) core family. Athena's AES core family complements the leading-edge TeraFire® public key (PK) cryptography accelerators and other cryptography accelerators. Whether your application demands AES performance or the power savings of a dedicated core, Athena's AES core family delivers.

Athena's dedicated AES core solutions are constructed using a modular architecture that allows Athena to configure an AES solution optimized for your application. These are offered as bundles as shown in Table 1.

Table 1: Dedicated AES Product Bundle Selector

Bundle P/N	Performance ^a	ECB/CBC/CFB/OFB/CTR	CCM	GCM
AES-A100-A	1.2-3.2 Gbps	Y		
AES-A100-C1	1.2-3.2 Gbps	Y	Y ^b	
AES-A100-C2	1.2-3.2 Gbps	Y	Y	
AES-A100-G1	1.2-3.2 Gbps	Y	Y ^b	Y
AES-A100-G2	1.2-3.2 Gbps	Y	Y	Y
AES-A200-A	256-640 Mbps	Y		
AES-A200-C1	256-640 Mbps	Y	Y ^b	
AES-A200-C2	256-640 Mbps	Y	Y	
AES-A200-G1	256-640 Mbps	Y	Y ^b	Y
AES-A200-G2	256-640 Mbps	Y	Y	Y

a. Nominal performance at 100 to 250 MHz with 128-bit key.

b. Performance in this mode is at half of the listed speed.

Athena's AES cores are compliant with FIPS 197 and NIST SP800-38A defined operating modes: ECB, CBC, CFB, OFB, and CTR. Support for CCM and GCM is also available. Dedicated AES cores are offered at two performance tiers and can be provided with optional bus interfaces. Athena also offers AES as an option in its EXP-F5200 cryptography microproces-

- 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



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., 2008. 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.

sor. The bundles listed in Table 1 are constructed using AES product family elements from Table 2. Custom configurations are also available.

Table 2: AES Product Family Elements

Model	Description
AES-A100	High-performance AES (1.2-3.2 Gbps ^a)
AES-A101	High-performance AES key schedule generator for AES-A100
AES-A102	NIST SP800-38A operating modes package for AES-A100
AES-A112	NIST SP800-38A modes plus GCM mode for AES-A100
AES-A200	Standard performance AES (256-640 Mbps ^a)
AES-A201	AES key schedule generator for AES-A200
AES-A202	NIST SP800-38A operating modes package for AES-A200
AES-A212	NIST SP800-38A modes plus GCM mode for AES-A200
EXP-F5200	Cryptography microprocessor with optional AES support
TAI-A100	AHB bus interface for Athena TeraFire cores
TXI-A100	AXI bus interface for Athena TeraFire cores

a. Nominal performance at 100 to 250 MHz with 128-bit key.

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.