



# *TeraFire Products*

---

*Cryptography and Security IP Products  
for Actel FPGA Devices*



Revision 1.2  
April, 2009

Each copy of this document shall include all copyrights, trademarks, service marks, and proprietary rights notices, if any.

All copies of this document must bear this notice.

This document is Copyright © 2009, The Athena Group, Inc.

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](http://www.athena-group.com)



ATHENA

---

## Table of Contents

Fast AES .....	1
Fast AES-CCM .....	4
Fast AES-GCM .....	7
Standard Performance AES .....	10
Standard Performance AES-CCM .....	13
Standard Performance AES-GCM .....	16
Secure Hash Algorithm SHA-1 .....	19
Secure Hash Algorithm SHA-2 .....	21
True Random Number Generator .....	23
Advanced True Random Number Generator .....	25
TeraFire F5200 Cryptography Microprocessor .....	27



## Features

- FIPS 197 compliant AES cores
- Supports key sizes of 128, 192, and 256-bits
- NIST SP800-38A defined modes *included*
- 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 bus interfaces available

## Benefits

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



## Fast AES

**Athena delivers Advanced Encryption Standard (AES) as a semiconductor intellectual property (IP) core family 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. Fast AES cores are offered as bundles as shown in Table 1, with performance parameters shown in Table 2.

**Table 1: Fast AES Products for Actel FPGAs**

Model	Description
AES-A100-E	Fast AES with ECB encrypt/decrypt
AES-A100-EE	Fast AES with ECB encrypt only
AES-A100-A	Fast AES with encrypt/decrypt ECB/CBC/CFB/OFB/CTR
AES-A100-AE	Fast AES with encrypt-only ECB/CBC/CFB/OFB/CTR <sup>a</sup>

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

**Table 2: Fast AES Performance Parameters for Actel ProASIC3**

Model	Performance	Area
AES-A100-E	702 Mbps/65 MHz	3926 tiles/10 RAMs
AES-A100-EE	962 Mbps/90 MHz	1816 tiles/10 RAMs
AES-A100-A	680 Mbps/64 MHz	6524 tiles/10 RAMs
AES-A100-AE	879 Mbps/82 MHz	4239 tiles/10 RAMs

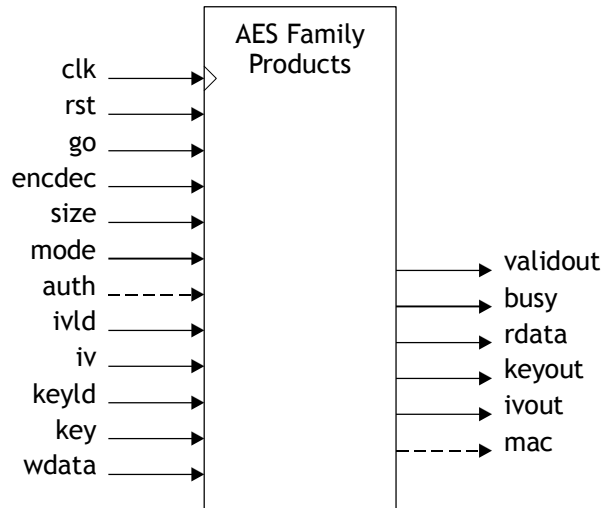
## Applications

- 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

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.



**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 3. 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 3: 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 <sup>a</sup>
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 <sup>a</sup>
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<sup>®</sup> security cores, to Atomic DSP<sup>™</sup> cores, and Atomic SDR<sup>™</sup> software defined radio cores.

Athena was founded in 1986 and is privately held.

## Features

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



## Fast AES-CCM

**Athena delivers Advanced Encryption Standard Counter with Cipher Block Chaining Message Authentication Code mode (AES-CCM) 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 fast AES-CCM encrypt/decrypt only core is shown in Table 1.

**Table 1: Fast AES-CCM Parameters for Actel ProASIC3**

Model	Performance	Area
Fast AES-CCM AES-A100-CO	400 Mbps/75 MHz	4780 tiles/10 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.

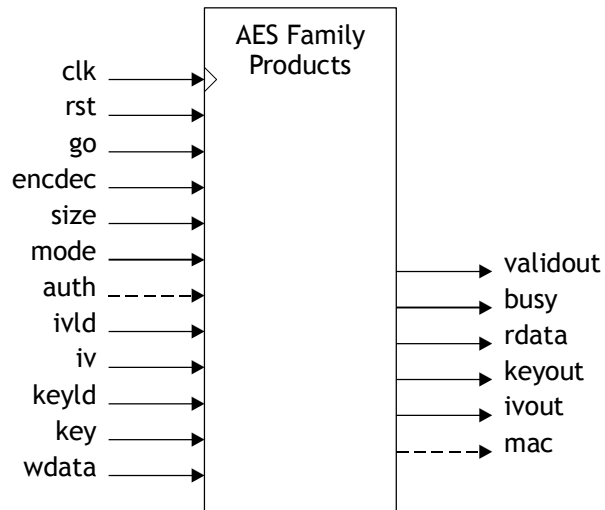


## Applications

- 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 <sup>a</sup>
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 <sup>a</sup>
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<sup>®</sup> security cores, to Atomic DSP<sup>™</sup> cores, and Atomic SDR<sup>™</sup> software defined radio cores.

Athena was founded in 1986 and is privately held.

## 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



## Fast AES-GCM

**Athena delivers Advanced Encryption Standard Galois Counter Mode (AES-GCM) as a semiconductor intellectual property (IP) core family 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 fast AES-GCM encrypt/decrypt only core is shown in Table 1.

**Table 1: Fast AES-GCM Parameters for Actel ProASIC3**

Model	Performance	Area
Fast AES-GCM AES-A100-GO	600 Mbps/75 MHz	5500 tiles/10 RAMs

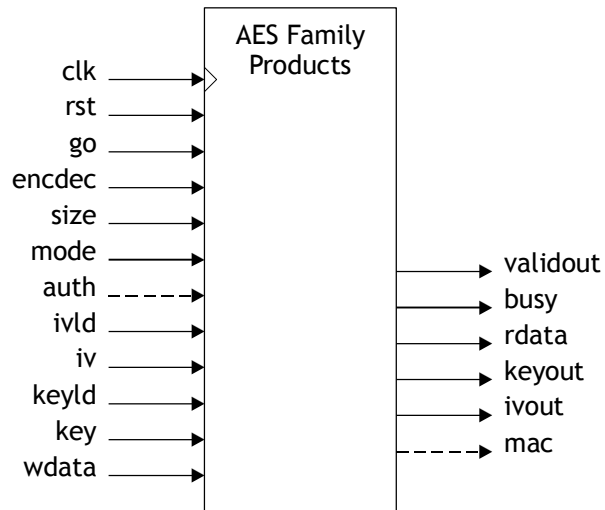
Athena's AES cores are complete, silicon-proven implementations, loaded with features including integrated modes support, key schedule generation, and context switching. These cores can also be provided with optional bus interfaces, such as AHB and AXI, to jumpstart your system integration efforts. The 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 <sup>a</sup>
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 <sup>a</sup>
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<sup>®</sup> security cores, to Atomic DSP<sup>™</sup> cores, and Atomic SDR<sup>™</sup> software defined radio cores.

Athena was founded in 1986 and is privately held.

## Features

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

**Athena delivers Advanced Encryption Standard (AES) as a semiconductor intellectual property (IP) core family 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. Standard performance AES cores are offered as bundles as shown in Table 1, with performance parameters shown in Table 2.

**Table 1: Standard Performance AES Products for Actel FPGAs**

Model	Description
AES-A200-E	Std AES with ECB encrypt/decrypt
AES-A200-EE	Std AES with ECB encrypt only
AES-A200-A	Std AES with full encrypt/decrypt ECB/CBC/CFB/OFB/CTR
AES-A200-AE	Std AES with encrypt-only ECB/CBC/CFB/OFB/CTR <sup>a</sup>

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

**Table 2: Standard AES Performance Parameters for Actel ProASIC3**

Model	Performance	Area
AES-A200-E	177 Mbps/65 MHz	2852 tiles/3 RAMs
AES-A200-EE	256 Mbps/93 MHz	1718 tiles/3 RAMs
AES-A200-A	163 Mbps/60 MHz	5634 tiles/3 RAMs
AES-A200-AE	187 Mbps/69 MHz	4227 tiles/3 RAMs

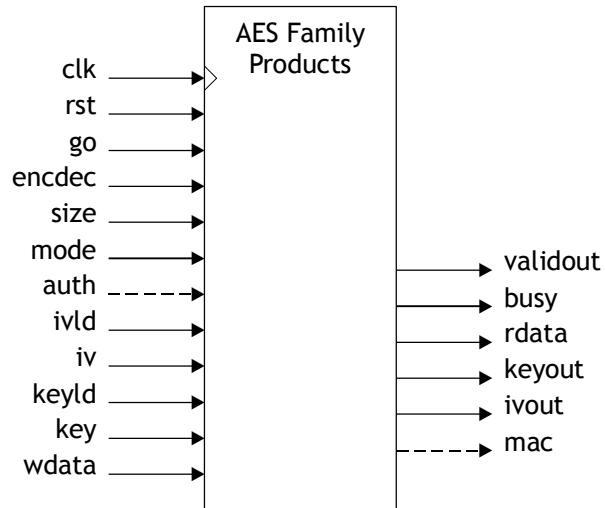
## Applications

- 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

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.



**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 3. 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 3: 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 <sup>a</sup>
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 <sup>a</sup>
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<sup>®</sup> security cores, to Atomic DSP<sup>™</sup> cores, and Atomic SDR<sup>™</sup> software defined radio cores.

Athena was founded in 1986 and is privately held.

## Features

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

**Athena delivers Advanced Encryption Standard Counter with Cipher Block Chaining Message Authentication Code mode (AES-CCM) 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-CCM encrypt/decrypt only core is shown in Table 1.

**Table 1: Standard Performance AES-CCM Parameters for Actel ProASIC3**

Model	Performance	Area
Std AES-CCM AES-A200-CO	89 Mbps/65 MHz	4680 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.

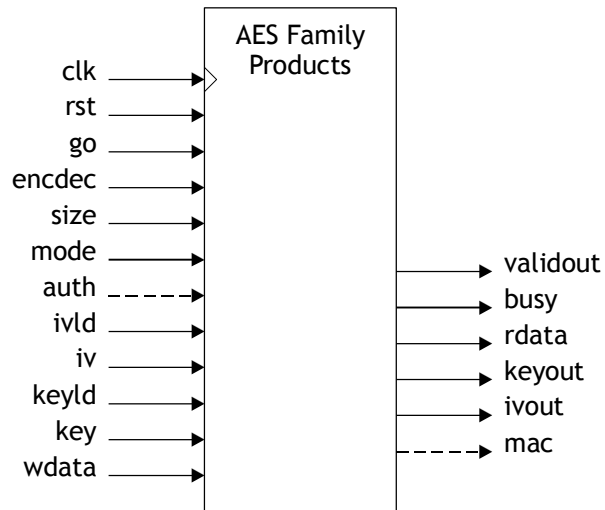


## Applications

- 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 <sup>a</sup>
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 <sup>a</sup>
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<sup>®</sup> security cores, to Atomic DSP<sup>™</sup> cores, and Atomic SDR<sup>™</sup> software defined radio cores.

Athena was founded in 1986 and is privately held.

## 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

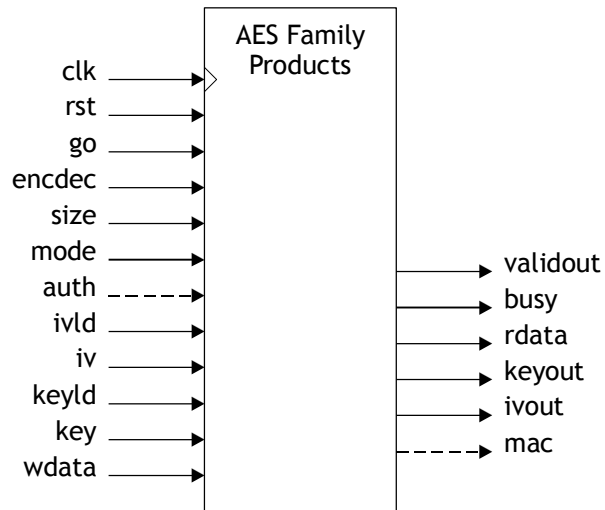
Athena's AES cores are complete, silicon-proven implementations, loaded with features including integrated modes support, key schedule generation, and context switching. These cores can also be provided with optional bus interfaces, such as AHB and AXI, to jumpstart your system integration efforts. The 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 <sup>a</sup>
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 <sup>a</sup>
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<sup>®</sup> security cores, to Atomic DSP<sup>™</sup> cores, and Atomic SDR<sup>™</sup> software defined radio cores.

Athena was founded in 1986 and is privately held.

## Features

- FIPS 180-2 compliant SHA
- SHA-1/224/256/384/512 support in product family
- Full width message digest output
- Rapid context switching
- AHB/AXI microprocessor bus interfaces available
- SHA support also available in TeraFire F5200 cryptography microprocessor

## Benefits

- Full-width data ports maximize performance, minimize latency

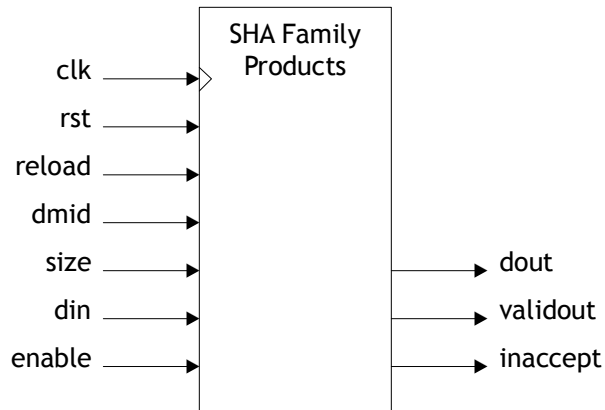
## Available Deliverables

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



## Secure Hash Algorithm SHA-1

**Athena delivers the Secure Hash Algorithms 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.



**Figure 1: Interface Block Diagram of SHA Family Members**

## Product Description

The SHA family cores, shown in Figure 1, are fully synchronous and have full width input and message digest output for maximum throughput and minimum latency. Configurations are available with single algorithm (e.g., SHA-1, SHA-256) and multiple algorithm support. Input and output flow control simplifies system integration, and standard bus interfaces (e.g., AHB, AXI) are available for applications that require bus connectivity. The SHA family cores also feature rapid context save and reload features to enable timesharing of the SHA cores for large messages. The

## Device Compatibility

Athena SHA family products are compatible with all Actel devices with sufficient logic 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.

performance characteristics of this core, and other members of the SHA family, are summarized in Table 1. Additionally, SHA support is available in the EXP-F5200 cryptography microprocessor.

**Table 1: SHA Family Performance Parameters for Actel ProASIC3**

Model	Area	Performance
SHA1-A100	2455 tiles	275 Mbps/44 MHz
SHA224-A100	4607 tiles	336 Mbps/43 MHz
SHA256-A100	4607 tiles	336 Mbps/43 MHz
SHA384-A100	15563 tiles	611 Mbps/40 MHz
SHA512-A100	15563 tiles	611 Mbps/40 MHz

Support for two or more algorithms can also be built into a single core, contact Athena for more information.

### 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.

### 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.

## Features

- FIPS 180-2 compliant SHA
- SHA-1/224/256/384/512 support in product family
- Full width message digest output
- Rapid context switching
- AHB/AXI microprocessor bus interfaces available
- SHA support also available in TeraFire F5200 cryptography microprocessor

## Benefits

- Full-width data ports maximize performance, minimize latency

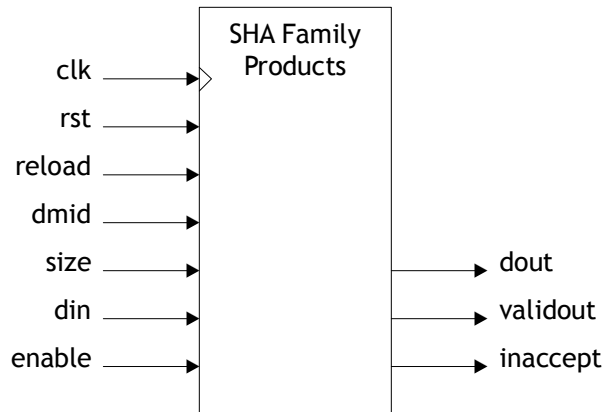
## Available Deliverables

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



## Secure Hash Algorithm SHA-2

**Athena delivers the Secure Hash Algorithms 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.



**Figure 1: Interface Block Diagram of SHA Family Members**

## Product Description

The SHA family cores, shown in Figure 1, are fully synchronous and have full width input and message digest output for maximum throughput and minimum latency. Configurations are available with single algorithm (e.g., SHA-1, SHA-256) and multiple algorithm support. Input and output flow control simplifies system integration, and standard bus interfaces (e.g., AHB, AXI) are available for applications that require bus connectivity. The SHA family cores also feature rapid context save and reload features to enable timesharing of the SHA cores for large messages. The

## Device Compatibility

Athena SHA family products are compatible with all Actel devices with sufficient logic 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.

performance characteristics of this core, and other members of the SHA family, are summarized in Table 1. Additionally, SHA support is available in the EXP-F5200 cryptography microprocessor.

**Table 1: SHA Family Performance Parameters for Actel ProASIC3**

Model	Area	Performance
SHA1-A100	2455 tiles	275 Mbps/44 MHz
SHA224-A100	4607 tiles	336 Mbps/43 MHz
SHA256-A100	4607 tiles	336 Mbps/43 MHz
SHA384-A100	15563 tiles	611 Mbps/40 MHz
SHA512-A100	15563 tiles	611 Mbps/40 MHz

Support for two or more algorithms can also be built into a single core, contact Athena for more information.

### 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.

### 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.

## Features

- SP 800-22 compliant
- FIPS 140-1 compliant
- Silicon proven
- High performance starting at 50 Mbps output with 100 MHz input clock
- Internal fault detection for NRNG subsystem
- AHB/AXI microprocessor bus interfaces available

## Benefits

- Gold standard NRNG plus DRNG architecture provides cryptographic-grade random data

## Available Deliverables

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



## True Random Number Generator

Athena delivers cryptographic-grade true random number generators (RNG) as a silicon proven intellectual property (IP) core for Actel FPGA. The TeraFire RNG core provide essential cryptographic-grade random numbers for use in key generation, key exchange, noise generation in communications applications, and more. The TeraFire RNG core is a fast and reliable way to incorporate cryptographic-grade random numbers into your next FPGA design.

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.

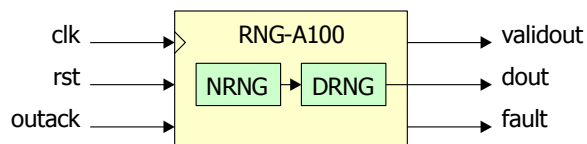


Figure 1: Block Diagrams of RNG-A100 Core

Table 1: RNG Performance Specifications for Actel ProASIC3

Model	Performance	Area
RNG-A100	30 Mbps/60 MHz	2818 tiles

## RNG-A100 Description

The RNG-A100 is a minimum area solution that couples a non-deterministic entropy source (NRNG), containing multiple random oscillators, with a non-linear deterministic RNG (DRNG) to produce the highest quality RNG available today. Athena’s innovative architecture uses non-deterministic data as an initialization vector, and also continuously incorpo-

## Device Compatibility

Athena RNG family products are compatible with all Actel devices with sufficient logic 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](http://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.

rates the entropy of the NRNG with that of the DRNG. The RNG-A100 has been proven compliant with NIST SP800-22 and FIPS 140-1 randomness tests in commercial customer silicon.

The RNG-A100 continuously monitors its operation to detect potential fault conditions. On top of that, the RNG-A100 is built to *survive* faults while continuing to provide cryptographic-grade random numbers. It has also been designed to mitigate attacks on RNGs, and exploit application-level sources of non-deterministic randomness.

## 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.

## 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.

## Features

- Tracks the FIPS 140-3 draft
- SP 800-22 and SP 800-90 compliant
- FIPS 140-1 compliant
- Silicon proven
- High performance starting at 550 Mbps output
- Internal fault detection for NRNG subsystem
- AHB/AXI microprocessor bus interfaces available

## Benefits

- Gold standard NRNG plus DRNG architecture provides cryptographic-grade random data

## Available Deliverables

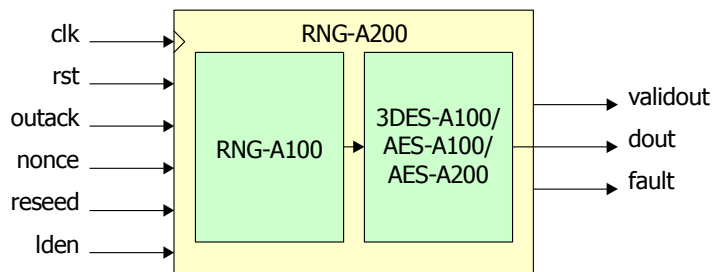
- Netlist
- RTL (VHDL/Verilog)
- Verification suite
- Simulation model
- AHB/AXI bus interfaces
- TeraFire CAL software
- Documentation
- Support



## Advanced True Random Number Generator

**Athena delivers cryptographic-grade true random number generators (RNG) as a silicon proven intellectual property (IP) core for Actel FPGA.** The TeraFire RNG core provide essential cryptographic-grade random numbers for use in key generation, key exchange, noise generation in communications applications, and more. The TeraFire RNG core is a fast and reliable way to incorporate cryptographic-grade random numbers into your next FPGA design.

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 time and money.



**Figure 1: Interface Block Diagram of RNG-A200 Core**

**Table 1: RNG Performance Specifications**

Model	Strength <sup>a</sup>	Performance	Area
RNG-A200-AES1	128-256b	550-768 Mbps/60 MHz	3736 tiles/3 RAMs

a. See NIST SP 800-57.

## Device Compatibility

Athena RNG family products are compatible with all Actel devices with sufficient logic 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](http://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.

## RNG-A200 Description

The RNG-A200 is an all-hardware configuration that meets the demanding requirements of NIST SP 800-90 and tracks the new FIPS 140-3 draft standard, including treatment of the internal state of the RNG as a critical security parameter.

## 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.

## 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.

## Features

- Implements Athena's powerful T5200 instruction set architecture
- Supports up to 16K-bit public key operations
- Supports elliptic curve cryptography operations
- Optional integrated AES and SHA functions
- T5200 Application Library provides offload of algorithms such as RSA and ECDSA
- AMBA™ AHB bus interface

## Benefits

- TeraFire T5200 family compatibility enables your product succession strategy
- Programmability enables adaptability to future standards
- Autonomous operation minimizes load on host processor
- Integrated AES and SHA enables single core Suite B solution



## TeraFire F5200 Cryptography Microprocessor

**Athena introduces the TeraFire F5200 public key cryptography core.** From the world leader in high performance public key cryptography cores comes the F5200, a fast, efficient microprocessor designed for public and secret key cryptography applications that is ideal for area sensitive FPGA designs.

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.

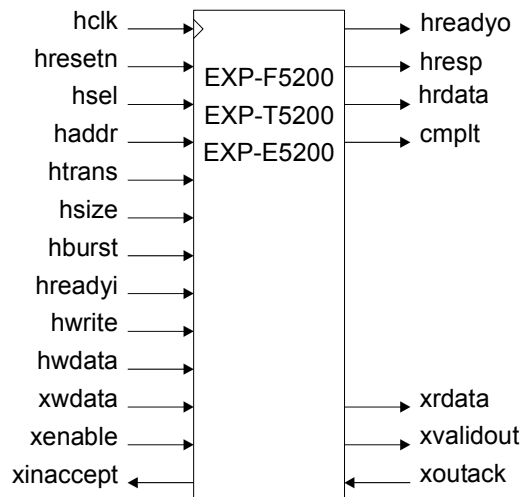


Figure 1: Interface Block Diagram of EXP-F5200 Family

## Applications

- Secure boot memory validation
- Embedded secure processing
- SSL and IPsec acceleration
- E-commerce
- SSL VPN
- Mobile Platforms

## Device Compatibility

The TeraFire F5200 is compatible with all Actel devices with sufficient logic and memory capacity, including:



## Product Description

The F5200 implements Athena's T5200 instruction set architecture (ISA), making it firmware compatible with the high-performance TeraFire T5200 cryptography microprocessor and T5200 Application Library. With the programmable T5200 ISA, the F5200 can execute virtually any public key cryptography algorithm today, and can execute the algorithms of tomorrow with a simple firmware update. The F5200 is ready for system integration with both an AHB interface and direct transfer interface, and has been optimized specifically for Actel FPGA. Characterization data is shown in Table 1.

**Table 1: Terafire F5200 Performance, Actel ProASIC3 @ 36 MHz**

Operation	op/s	latency
RSA-1024 Private Key	20	50 ms
RSA-1024 Private Key w/ Paired F5200s	40	35 ms
1024-bit Full Expo	5	200 ms
RSA-2048 Private Key	2.5	400 ms
RSA-2048 Private Key w/ Paired F5200s	5	200 ms
2048-bit Full Expo	0.6	1.7 s
1024-bit Expo/s ( $e=2^{16}+1$ )	500	2 ms
optional AES-128/192/256	>10 Mbps	
optional SHA-1/224/256/384/512	>10 Mbps	
Area	10764 tiles/5 RAMs	

With AES and SHA functions (optional) enabled, the F5200 becomes a highly flexible security application coprocessor in your SoC. By leveraging the T5200 ISA direct transfer interface, the F5200 can enable functions ranging from secure boot memory validation to 'bump-in-the-wire' IPsec coprocessing. The direct transfer interface can also be used to pair two F5200 cores, enabling twice the throughput and half the latency for RSA private key operations with CRT.

Base configurations of the F5200 support 1,024-bit operations. The F5200 may be configured for larger operations with additional memory. With support for virtually any length operation, the F5200 is ready to support even greater security requirements in the future.

## 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.

### **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.



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](http://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.