

## Features

- FIPS 180-2 compliant SHA
- SHA-1/224/256/384/512 support in product family
- Multi-Gbps performance
- Higher performance available
- Full-width message digest output
- Rapid context switching
- Microprocessor bus interfaces available
- SHA support also available in TeraFire F5200 cryptography microprocessor
- Portable to any technology library
- Easy integration into any SoC design

## Benefits

- Full-width data ports maximize performance, minimize latency
- Fast delivery for accelerated time to profit

## Applications

- Encrypted data storage
- Secure communications
- Secure processing
- IPsec acceleration
- E-commerce



## Secure Hash Algorithm (SHA) Family

**Athena delivers the Secure Hash Algorithms as semiconductor intellectual property (IP) cores.** Whether your application demands high-performance cryptographic hashing or the power savings of a dedicated core, Athena's SHA family cores deliver. The SHA family cores are compliant with FIPS 180-2 and can accept data input rates ranging from 2.9 Gbps up to 5.7 Gbps at 500 MHz, with even higher frequencies and corresponding throughputs available. SHA support is also available in Athena's TeraFire® cryptography microprocessor family.

### Product Description

Dedicated SHA family cores feature 32-bit and/or 64-bit data input ports and a full-width message digest output for maximum throughput and minimum latency. Input/output flow control simplifies system integration, and standard bus interfaces are available for applications that require bus connectivity. Context save and reload, automatic message padding, and HMAC features address a range of use cases. The members of the SHA family are summarized in Table 1. SHA support is also available in the EXP-F5200B cryptography microprocessor.

**Table 1: SHA Product Family and Performance Specifications**

Model	SHA-1	SHA-2	Context Change	Auto Padding	HMAC	Throughput <sup>a</sup> (Gbps)
SHA1-A100	◆		◆			2.9
SHA2-A100	◆	◆	◆			2.9 (SHA-1)
SHA2-A200	◆	◆		◆		3.5 (224/256)
SHA2-A300	◆	◆		◆	◆	5.7 (384/512)
EXP-F5200B <sup>b</sup> SHA-1	◆	◆	◆	◆	◆	240 Mbps
SHA-224/256						195 Mbps
SHA-384/512						150 Mbps
TAI-A100	AHB bus interface for Athena TeraFire cores					
TXI-A100	AXI bus interface for Athena TeraFire cores					

- 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  
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.

- Throughput at 500 MHz operation. Maximum clock frequency depends upon process and library. Throughput is specified in Gbps unless otherwise noted.
- The EXP-F5200 is a multi-function cryptography microprocessor. Throughput figures by algorithm at 500 MHz.

### 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.