

## Features

- FIPS 180-2 compliant SHA
- SHA-224/256/384/512 support in product family
- >500 Mbps performance
- Higher performance available
- Full width message digest output
- 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

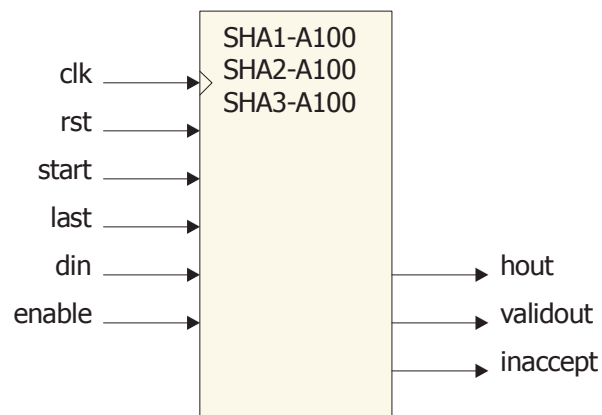
## Applications

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



## *Secure Hash Algorithm Family*

**The Athena Group delivers the Secure Hash Algorithms as semiconductor intellectual property (IP) cores.** Athena's SHA family cores complement Athena's leading-edge TeraFire public key (PK) cryptography accelerators. 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 greater than 500 Mbps.



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

## Product Description

The SHA family cores, shown in Figure 1, are fully synchronous and feature 32-bit or 64-bit data input ports, and a full width message digest output for maximum throughput and minimum latency. An inaccept output indicates when the processor is able to accept data, and a data valid output is provided to simplify retrieval of the message digest.

The three members of the SHA family are summarized in Table 1. Each successive member of the SHA family can perform the operations of the prior member with an order-time option.

**Table 1: SHA Product Family**

Model	SHA <sup>a</sup> 1	SHA 224	SHA 256	SHA 384	SHA 512	Interface Width	Throughput <sup>b</sup> (Mbps)
SHA1-A100	•					32b	640
SHA2-A100	◆	•	•			32b	800
SHA3-A100	◆	◆	◆	•	•	64b	1280

a. Optional algorithm support indicated by ◆.

b. Nominal maximum throughput at 100 MHz operation. Maximum clock frequency depends upon process and library.

Each SHA core is delivered as a firm core optimized to any customer-specified library. The package includes the core, verification suites, timing and simulation models, and documentation.

Athena's IP cores are designed for efficient implementation and rapid delivery. The company's proprietary, wholly automated implementation and verification methodology produces synchronous, testable IP cores of the highest quality. All Athena IP cores achieve a score of 95% or better on the OpenMore scale of IP reusability.

#### **About The Athena Group, Inc.**

The Athena Group, Inc. of Gainesville, Florida licenses high-performance DSP technology that delivers breakthrough performance, reduced area, and lower power consumption in a broad range of SoC products. Athena's proprietary technology powers leading edge applications such as secure e-commerce, wireless communications, and video compression. In addition to their high-value application level solutions, Athena also produces a full line of fundamental DSP functions suitable for SoC integration.

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

Copyright The Athena Group, Inc., 2005. 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.