

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.

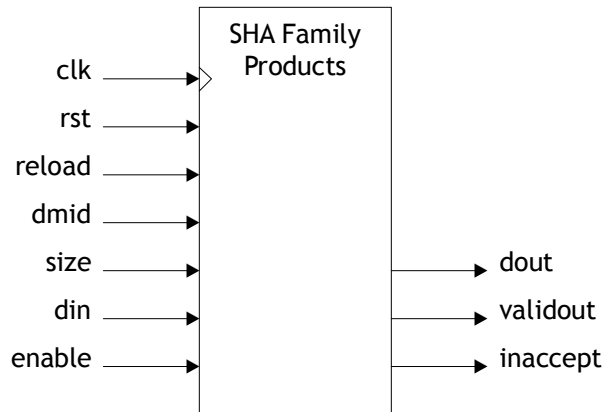


Figure 1: Interface Block Diagram of SHA Family Members

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.