

Features

- RFC 1321 compliant MD5
- Performance >7.5 Gbps at 500 MHz
- Higher performance available
- 32-bit data input port
- Microprocessor bus interfaces available
- 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
- SSL acceleration
- E-commerce
- VPN
- Financial Transactions



Message Digest 5 (MD5)

Athena delivers the Message Digest 5 (MD5) as a semiconductor intellectual property (IP) core. Athena's MD5-A100 MD5 core complements Athena's leading-edge TeraFire[®] public key cryptography accelerators. Whether your application demands MD5 performance or the power savings of a dedicated core, Athena's MD5-A100 core delivers. The MD5-A100 is compliant with RFC 1321 and can accept data input rates greater than 1.3 Gbps.

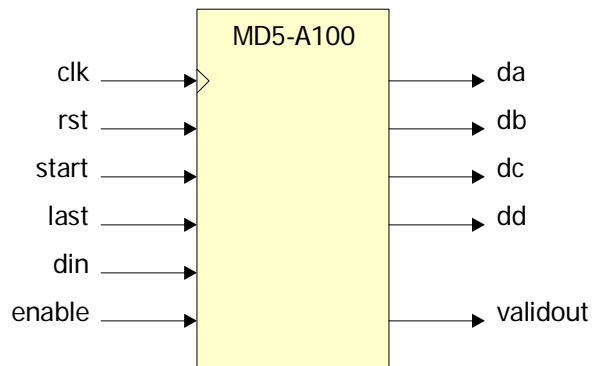


Figure 1: Block Diagram of MD5-A100

Product Description

The MD5-A100, shown in Figure 1, is a fully synchronous design and features a 32-bit data input port, and full width message digest output for maximum throughput and minimum latency. A data valid output is provided to simplify retrieval of the message digest.

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., 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.

The MD5-A100 area starts at 12 K-gates in a typical 130 nm process, and can readily scale beyond 500 MHz. The MD5-A100 may be delivered with an optional microprocessor bus interface to simplify SoC integration.

Table 1: MD5 Family and Performance Specifications

Model	Performance ^a	Area
MD5-A100	7.5 Gbps	12 K-gates
TAI-A100	AHB bus interface for Athena TeraFire cores	
TXI-A100	AXI bus interface for Athena TeraFire cores	

a. Performance 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.