

Features

- FIPS 197 compliant AES core
- Supports key sizes of 128, 192, and 256-bits
- Performance >1 Gbps
- Higher performance available
- Supports NIST SP800-38A defined operating modes
- 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



AES-A100 **Advanced Encryption Standard**

The Athena Group delivers the Advanced Encryption Standard (AES) as a semiconductor intellectual property (IP) core. Athena's AES-A100 AES core complements Athena's leading-edge TeraFire public key (PK) cryptography accelerators. Whether your application demands AES performance or the power savings of a dedicated core, Athena's AES-A100 core delivers.

The AES-A100 is compliant with FIPS 197 and supports user programmable key sizes of 128, 192, and 256-bits, and NIST SP800-38A defined operating modes: electronic codebook (ECB), cipher block chaining (CBC), cipher feedback (CFB), output feedback (OFB), and counter (CTR). With a 100 MHz clock, the AES-A100 provides greater than 1 Gbps encryption/decryption performance.

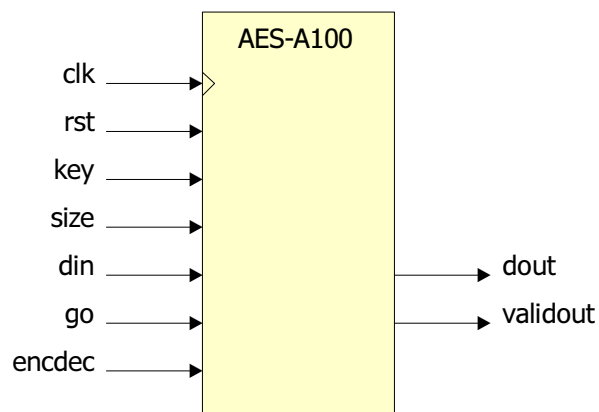


Figure 1: Block Diagram of AES-A100

Product Description

The AES-A100, shown in Figure 1, is a fully synchronous design and features dedicated, full-width data input, output, and key input ports for maximum throughput and minimum latency. A data valid output is provided to simplify retrieval of output data.

Each AES-A100 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.
5522 NW 43rd Street, Suite B
Gainesville, FL 32653

Phone: (352) 371-2567
Toll-free: (800) 741-7440
Fax: (352) 373-5182
www.athena-group.com

Copyright The Athena Group, Inc., 2003. 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.
