

Features

- FIPS 140-1 compliant
- 50+ Mbps output with 100 MHz input clock
- Higher performance available
- Upgradable to FIPS 140-2 annex C “approved” configuration
- Internal fault detection for non-deterministic RNG subsystem
- Portable to any technology library
- Easy integration into any SoC design

Benefits

- Gold standard non-deterministic plus non-linear deterministic RNG architecture provides cryptographic-grade random data
- Fast delivery for accelerated time to profit

Applications

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



RNG-A100

True Random Number Generator

The Athena Group delivers a true random number generator (RNG) as a semiconductor intellectual property (IP) core. Athena’s RNG-A100 RNG core complements Athena’s leading-edge TeraFire public key (PK) cryptography accelerators by providing a cryptographic-grade source for random data.

The RNG-A100 couples a non-deterministic RNG with a non-linear deterministic RNG to provide a solid cryptographic-grade random number source. When operating at 100 MHz in the recommended configuration, the deterministic RNG part of the RNG-A100 has a period of >5800 years. The RNG-A100 is compliant with FIPS 140-1 randomness tests, and can be upgraded to a FIPS 140-2 annex C “approved” configuration with the addition of an Athena SHA1-A100 core.

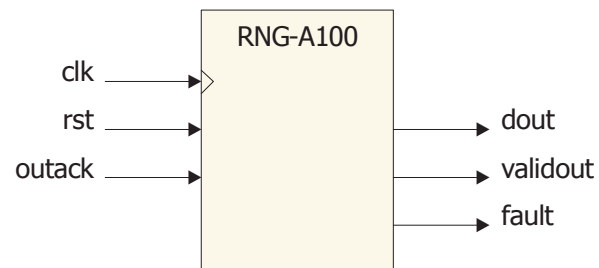


Figure 1: Block Diagram of RNG-A100

Product Description

The RNG-A100, shown in Figure 1, is a fully synchronous design and features a dedicated, 32-bit random data output. A validout/outack handshake prevents re-reading of random data. A fault output indi-

cates if there is a fault in the non-deterministic RNG portion of the RNG-A100, helping to ensure system-level integrity.

Each RNG-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.
