

Features

- SP 800-22 and SP 800-90 compliant
- FIPS 140-1 compliant
- Tracks the FIPS 140-3 draft
- Silicon proven
- High performance starting at 50 Mbps output with 100 MHz input clock
- Internal fault detection for NRNG subsystem
- Microprocessor bus interfaces available
- Portable to any technology library
- Easy integration into any SoC design

Benefits

- Gold standard NRNG plus DRNG architecture provides cryptographic-grade random data
- Fast delivery for accelerated time to profit

Applications

- Encrypted data storage
- Secure communications
- E-commerce
- Financial transactions
- Noise generation



True Random Number Generators

The Athena Group delivers silicon proven intellectual property (IP) cores for cryptographic-grade random number generation (RNG). The TeraFire RNG cores complement Athena's comprehensive suite of cryptographic IP cores, providing the essential cryptographic-grade random numbers for use in key generation, key exchange, noise generation in communications applications, and more. Portable to any semiconductor process, the TeraFire RNG cores are a fast and reliable way to incorporate cryptographic-grade random numbers into your SoC design. Athena offers the two RNG solutions shown in Figure 1: a minimum area solution (RNG-A100), and a high-performance integrated Approved configuration (RNG-A200). Characterization data are listed in Table 1.

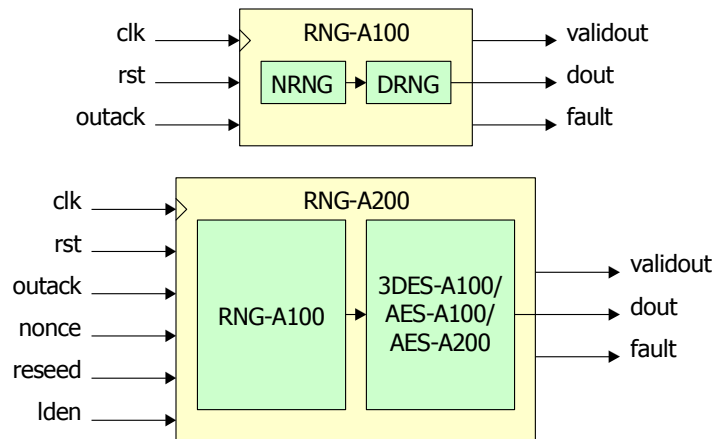


Figure 1: Block Diagrams of RNG-A100 and RNG-A200 Cores

RNG-A100 Description

The RNG-A100 is a minimum area solution that couples a non-deterministic entropy source (NRNG), containing multiple random oscillators, with a non-linear deterministic RNG (DRNG) to produce the highest quality RNG available today. Athena's innovative architecture uses non-deterministic data as an initialization vector, and also continuously incorpo-

Available Deliverables

- Simulation model (Verilog or VHDL)
- Synthesizable RTL (Verilog or VHDL) and scripts
- Targeted, timing closed netlist
- Verification suite
- Documentation
- Support

rates the entropy of the NTRNG with that of the DRNG. The RNG-A100 has been proven compliant with NIST SP800-22 and FIPS 140-1 randomness tests in commercial customer silicon.

The RNG-A100 continuously monitors its operation to detect potential fault conditions. On top of that, the RNG-A100 is built to *survive* faults while continuing to provide cryptographic-grade random numbers. It has also been designed to mitigate attacks on RNGs, and exploit application-level sources of non-deterministic randomness.

RNG-A200 Description

The RNG-A200 is an all-hardware configuration that meets the demanding requirements of NIST SP 800-90 and tracks the new FIPS 140-3 draft standard, including treatment of the internal state of the RNG as a critical security parameter. The RNG-A200 is available in three variants to provide a range of speed, area, and cryptographic strength options.

Table 1: RNG Performance Specifications^a

Model	Output Rate	Strength ^b	Area
RNG-A100	50 Mbps	N/A	5 K-gates
RNG-A200-3DES	266 Mbps	112b	10 K-gates
RNG-A200-AES1	914-1280 Mbps	128-256b	50 K-gates
RNG-A200-AES2	228-320 Mbps	128-256b	35 K-gates

a. Based on 100 MHz operation in 130nm process.

b. See NIST SP 800-57.

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.



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., 2008. 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.