

Features

- SP 800-22 compliant
- FIPS 140-1 compliant
- Silicon proven
- High performance starting at 50 Mbps output with 100 MHz input clock
- Internal fault detection for NRNG subsystem
- AHB/AXI microprocessor bus interfaces available

Benefits

- Gold standard NRNG plus DRNG architecture provides cryptographic-grade random data

Available Deliverables

- Netlist
- RTL (VHDL/Verilog)
- Verification suite
- Simulation model
- AHB/AXI bus interfaces
- TeraFire CAL software
- Documentation
- Support



True Random Number Generator

Athena delivers cryptographic-grade true random number generators (RNG) as a silicon proven intellectual property (IP) core for Actel FPGA. The TeraFire RNG core provide essential cryptographic-grade random numbers for use in key generation, key exchange, noise generation in communications applications, and more. The TeraFire RNG core is a fast and reliable way to incorporate cryptographic-grade random numbers into your next FPGA design.

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.

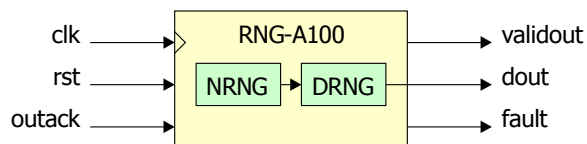


Figure 1: Block Diagrams of RNG-A100 Core

Table 1: RNG Performance Specifications for Actel ProASIC3

Model	Performance	Area
RNG-A100	30 Mbps/60 MHz	2818 tiles

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-

Device Compatibility

Athena RNG 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.

rates the entropy of the NRNG 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.

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.

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.