

## Features

- Tracks the FIPS 140-3 draft
- SP 800-22 and SP 800-90 compliant
- FIPS 140-1 compliant
- Silicon proven
- High performance starting at 550 Mbps output
- 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

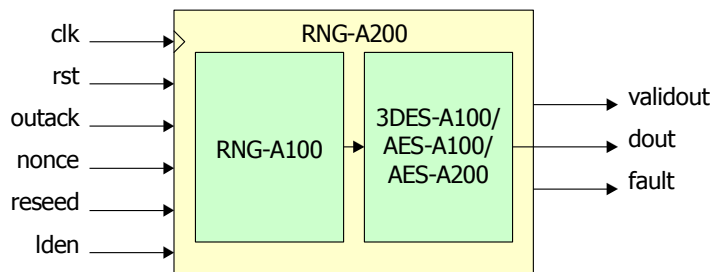
- Netlist
- RTL (VHDL/Verilog)
- Verification suite
- Simulation model
- AHB/AXI bus interfaces
- TeraFire CAL software
- Documentation
- Support



## Advanced 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 time and money.



**Figure 1: Interface Block Diagram of RNG-A200 Core**

**Table 1: RNG Performance Specifications<sup>a</sup>**

Model	Strength <sup>b</sup>	Performance	Area
RNG-A200-AES1	128-256b	550-768 Mbps/60 MHz	3736 tiles/3 RAMs

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

b. See NIST SP 800-57.

## 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](http://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.

## 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.

## 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.