

Features

- SP 800-90 compliant
- Tracks the FIPS 140-3 (draft)
- Silicon proven
- High performance up to 4 Gbps at 500 MHz
- Advanced health monitoring
- Power management
- Prediction and backtracking resistance
- Programmable entropy factor
- Automatic periodic reseeding support
- Personalization string and additional data support
- Microprocessor bus interfaces available
- Portable to any technology library
- Easy integration into any SoC design

Applications

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



Advanced True Random Number Generator

Athena delivers silicon proven semiconductor intellectual property (IP) cores for cryptographic-grade random number generation (RNG). The TeraFire® Advanced RNG core (RNG-A200) complements 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 Advanced RNG core is a fast and reliable way to incorporate cryptographic-grade random numbers into your ASIC or FPGA design. Characterization data are listed in Table 1.

Table 1: RNG-A200 Product Family and Performance Specifications

| Model | Output Rate ^a | Strength ^b | Area |
|---------------|---|-----------------------|------------|
| RNG-A200-AES1 | up to 4 Gbps | 128-256b | 75 K-gates |
| RNG-A200-AES2 | up to 1.2 Gbps | 128-256b | 50 K-gates |
| RNG-A200-AES3 | up to 350 Mbps | 128-256b | 45 K-gates |
| TAI-A100 | AHB bus interface for Athena TeraFire cores | | |
| TXI-A100 | AXI bus interface for Athena TeraFire cores | | |

a. Based on 500 MHz operation.

b. See NIST SP 800-57.

RNG-A200 Description

By combining a proven source of intrinsic non-deterministic entropy with an all-hardware post-processor compliant with NIST SP800-90, the TeraFire Advanced RNG core provides a direct path towards FIPS 140-3 (draft) compliant random number generation.

The non-deterministic entropy is provided by multiple ring oscillators uniquely customized for the customer's needs. The RNG-A200 implements advanced health monitoring of the ring oscillators that provides

Available Deliverables

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

continuous assurance of proper operation with automatic halting on error detection. The health monitoring system is programmable, which allows customers to specify what scenarios result in warnings/errors or to default to Athena's recommended settings. Athena's ring oscillators are designed with built-in support for manufacturing test to simplify system integration. The RNG-A200 can be configured with anywhere from 2 to 32 ring oscillators, allowing a trade-off between area/power and performance. For power-sensitive designs, power management features can disable the ring oscillators when not in use.

The deterministic post-processor is based on AES counter mode as specified in NIST SP800-90. For the AES operations, the RNG-A200 core leverages Athena's proven AES core solutions that provide multiple performance options. In addition to random number generation, the RNG-A200 provides AES cipher functionality when the random number generation is uninstantiated. The core is designed to support user-selectable security strengths of 128-bits or 256-bits for random number generation.

The RNG-A200 provides sophisticated protection of its state variables and output. In accordance with NIST SP800-90, the RNG-A200 provides both prediction resistance and backtracking resistance. In addition, the output is automatically zeroized when it is read, and all unused entropy is discarded. The RNG-A200 supports asynchronous and/or synchronous zeroization of output and state variables to meet FIPS 140-3 (draft) requirements.

The RNG-A200 supports a number of advanced features, such as the programmable entropy factor, and many optional features specified in NIST SP800-90, such as automatic periodic reseeding, personalization strings, and additional data input. The RNG-A200 supports known answer testing of all its subsystems while in test mode, allowing customers to perform operational verification for each chip as required by NIST SP800-90.

Bus Interfaces

Athena's dedicated cryptography solutions are designed for stand-alone operation and provide full-width support to enable maximum performance and flexibility. AHB, AXI, and other bus interfaces are also available.

TeraFire Cryptography Application Library (CAL)

The TeraFire CAL is a portable, ANSI C library of cryptographic software implementations and drivers for TeraFire hardware accelerators. The TeraFire CAL has been implemented and tested on multiple platforms, including leading SoC microprocessors from ARM. Athena's sophisticated configuration management system enables rapid configuration of the TeraFire CAL for your mix of hardware accelerator and software implementation requirements.

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
ipsales@athena-group.com

Copyright The Athena Group, Inc., 2011. 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.