

Features

- FIPS 197 compliant AES cores
- Supports key sizes of 128 and 256-bits
- NIST SP800-38D defined modes *included*
- Standard and fast product series support different performance & area requirements
- AES support also available in TeraFire F5200 cryptography microprocessor

Benefits

- Pre-configured bundles address a range of requirements
- Bundles may be customized to provide an optimized solution for each application

Applications

- Encrypted data storage
- Secure communications
- Secure processing
- IPsec acceleration
- VPN
- Financial transactions



TeraFire Suite B Bundles for Altera FPGAs

With its market-leading TeraFire family of cryptography cores, Athena has successfully delivered solutions to industry for over a decade. Now, Athena delivers Suite B Cryptography as a family of semiconductor intellectual property (IP) cores family for Altera FPGAs. The TeraFire family includes solutions for random number generators, AES, SHA, and public key cryptography. Athena Suite B platforms for Altera include everything required to satisfy the requirements for Suite B cryptography – with configurations ranging from ultra compact to ultra high performance.

Product Description

Suite B TeraFire bundles include everything you need for a complete Suite B implementation: AES Galois counter mode (GCM) with 128-bit and 256-bit key support, SHA-256 and SHA-384, cryptographic true random number generator, and Athena’s advanced cryptography microprocessor with elliptic curve digital signature algorithm (EC-DSA) and elliptic curve Diffie-Hellman (EC-DH) support.

Athena offers three Suite B bundled solutions: compact, standard, and high performance. Bundle descriptions are provided in Table 1, and performance is characterized in Table 2. Custom bundles using any of Athena’s TeraFire products are also available.

Table 1: Suite B Bundles for Altera FPGA

Model	Description
SUITEB-C	Compact: F5200 cryptography microprocessor with integrated EC-DH, EC-DSA, AES-GCM, SHA-256/384, and RNG
SUITEB-S	Standard performance: F5200 cryptography microprocessor (EC-DH, EC-DSA), standalone AES-GCM, SHA-256/384, and RNG
SUITEB-H	Ultra high-performance: E5200 cryptography microprocessor (EC-DH, EC-DSA), standalone AES-GCM, SHA-256/384, and RNG

Available Deliverables

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

Device Compatibility

Athena AES family products are compatible with all Altera devices with sufficient logic and memory capacity



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., 2010. 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.

Table 2: Suite B Bundle Characterization for Cyclone III LS

Model	AES-GCM	SHA-256	EC-DH 256	EC-DSA 256 Verify	RNG	Area (LEs) ^a
SUITEB-C	35 Mbps	27 Mbps	33 ms	41 ms	35 Mbps	6.7K
SUITEB-S	274 Mbps	434 Mbps	31 ms	38 ms	72 Mbps	12K
SUITEB-H	915 Mbps	476 Mbps	6.7 ms	8.6 ms	72 Mbps	29K

a. Cryptography microprocessor configurations require memories in addition to LEs.

Athena's Suite B core bundles are complete, silicon-proven implementations, loaded with features including integrated modes support, key schedule generation, and context switching. Optional bus interfaces, such as AHB and AXI, accelerate your system integration efforts. Athena's cryptography microprocessors can execute virtually any public key cryptography algorithm, including EC-DH and EC-DSA, as well as conventional algorithms such as RSA, DSA, and Diffie-Hellman.

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.

TeraFire Cryptography Application Library (CAL)

Jumpstart your system development with the optional TeraFire CAL, 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 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.