



# ***TeraFire***<sup>®</sup>

---

*Cryptography and Security IP Products  
For Microsemi FPGAs*



Revision 2.7  
February 2017



# **ATHENA**

**T H E A T H E N A G R O U P**

Each copy of this document shall include all copyrights, trademarks, service marks, and proprietary rights notices, if any.

The Athena logo, TeraFire name, and TeraFire logo are trademarks or registered trademarks of The Athena Group, Inc. The Licensed DPA Countermeasures logo is a trademark or registered trademark of Cryptography Research, Inc. in the United States and other countries, used under license. All other trademarks, registered trademarks, and/or service marks are the property of their respective owners. Company, product, and service names used in this document are for identification purposes only.

All copies of this document must bear this notice.

This document is Copyright © 2017, The Athena Group, Inc.

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

[ipsales@athena-group.com](mailto:ipsales@athena-group.com)  
[www.athena-group.com](http://www.athena-group.com)

---

# Table of Contents



TeraFire® Cryptographic Security .....	4
TeraFire® Cryptographic Security with Side Channel Attack (SCA) Countermeasures.....	7
Hardware Root of Trust .....	11
Dragon-QT Embedded Hardware Root of Trust .....	12
Anti-Tamper Technologies .....	16
InCipher™ Inline Memory Encryptor.....	17
Cryptography Microprocessors.....	19
5200 Series 32-bit Cryptography Microprocessors.....	20
F5200 Embedded Cryptography Microprocessor.....	23
EC Ultra Elliptic Curve Cryptography Microprocessor .....	26
True Random Number Generators.....	28
Compact True Random Number Generator.....	29
Advanced True Random Number Generator.....	31
Ciphers and Hashing .....	34
Advanced Encryption Standard (AES) .....	35
Secure Hash Algorithm (SHA).....	37
3GPP Ciphers .....	39
Legacy Cores .....	41
Triple Data Encryption Standard (3DES) .....	42
ARC4 Stream Cipher .....	44
Message Digest 5 (MD5) .....	46
Software, Firmware, and Interface .....	48
TeraFire® Firmware Library .....	49
Cryptographic Application Library .....	52
AHB/AXI Bus Interfaces .....	56

# PRODUCT BRIEF



## Features

- **NEW- DPA/SCA Countermeasures**



- Comprehensive suite of data security and data integrity products
- Optimized for speed, power, and area requirements
- Microprocessor bus interfaces available
- Portable to any technology library
- Easy integration

## Benefits

- Hardware acceleration minimizes load on host processor
- Family of compatible products optimized for speed and area supports your product succession strategy
- Multiple interface choices simplify system integration

## Applications

- Encrypted data storage
- Secure communications
- Secure processing
- SSL and IPsec acceleration
- Mobile Platforms

## TeraFire® Cryptographic Security

**Athena delivers a comprehensive suite of security IP, ready for your Microsemi application.** Cryptographic security is simply required in today's connected world. With a broad selection of IP cores, software, firmware, drivers, and multiple levels of performance for every function, Athena supports your product succession strategy. Athena is ready to help you analyze your security hardware requirements and customize a package of functions for your application.

Athena's TeraFire® family of hardware security IP delivers everything you need to get your Microsemi device built. Athena's market-leading public key cryptography accelerators are complemented by symmetric key cryptography functions for confidentiality, cryptographic hash functions for data integrity, and random number generators for keying. System integration is simplified with optional bus interfaces, host drivers software, and a comprehensive software library. Multiple performance levels are available, enabling optimum area/performance solutions to be realized.

Athena offers solutions for every Microsemi device family, including Igloo, ProASIC3, Fusion, SmartFusion, and SmartFusion2. Each solution is optimized specifically for the resources and architecture of the unique device family, delivering optimum performance and minimum area. ASIC optimized versions are also available.

TeraFire security IP cores are the foundation of any hardware security solution and are summarized in Table 1. C software and drivers for the host processor are summarized in Table 2, and X5200 firmware executables are listed in Table 3.

TeraFire cryptography microprocessors are ideal for applications requiring hardware-accelerated public key cryptography. The TeraFire processors are available in multiple models, optimized for different goals. The E5200 is optimized for high performance RSA and ECC, where the F5200 is compact, sized for embedded applications, and has the flexibility to perform all Suite B operations in a single core. EC Ultra is optimized for ECC operations only, and delivers extreme performance in a small footprint. All TeraFire cryptography microprocessors are firmware compatible, so the same firmware will run on any core. These programmable cores have the flexibility to execute virtually any public key algorithm without burdening your host processor.

## Support

- 12 months maintenance and support included

## Available Deliverables

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

## Standards Compliance

TeraFire products are compliant with the applicable Federal Information Processing Standards (FIPS), National Institute of Standards and Technology (NIST) publications, and Internet Engineering Task Force Request for Comments (IETF RFC).

**Table 1: TeraFire Security IP Cores for Microsemi**

Model	Description
Dragon-QT	Embedded Hardware Root of Trust
InCipher	Inline Memory Encryptor
EXP-F5200	Embedded Cryptography Microprocessor
EXP-F5200B	Embedded Suite B Cryptography Microprocessor
EXP-E5200	32-bit Cryptography Microprocessor
EC Ultra 2000	High Performance Elliptic Curve Accelerator
EC Ultra 4000	Extreme Performance Elliptic Curve Accelerator
EC Ultra 8000	Ultimate Performance Elliptic Curve Accelerator
AES-A500	Ultra Performance AES
AES-A100	High Performance AES
AES-A200	Standard Performance AES
SHA2-A300	SHA-1 plus SHA-2 (224/256/384/512)
SHA2-A400	Double Performance SHA2-A300
RNG-A100	SP800-22 True Random Number Generator
RNG-A200	SP800-90 True Random Number Generator
KAS-A100	Kasumi 3GPP Cipher
SNOW-A100	SNOW 3GPP Cipher
ZUC-A100	ZUC 3GPP Cipher
3DES-A100	Data Encryption Standard (DES/3DES)
ARC4-A100	ARC4 Stream Cipher
MD5-A100	Message Digest 5 (MD5)

**Table 2: TeraFire C Software and Drivers for Host Processors**

Name	Description	For Products
CAL-PK	CAL Host Drivers for 5200/6400 IP Cores	X5200/6400
CAL-SYM	CAL Host Drivers for TAI/TXI Connected IP Cores	AES/SHA/TRNG/3GPP
CAL-SW	C Software Library for Cryptography	Host
CAL-DRBG	C Software for SP800-90 DRBG	Host

**Table 3: TeraFire X5200 Executable Firmware**

Name	Description	For Products
PKX-5200	PK Executables Firmware	X5200/6400
DTX-5200	Direct Transfer I/F Packet Drivers	X5200/6400
AEX-5200	AES Executable Firmware	F5200
SHX-5200	SHA Executable Firmware	F5200
RNX-5200	SP800-90 DRBG Executable Firmware	F5200
SBX-5200	Secure Boot Executables	F5200

## Side Channel Attack Countermeasures

Side channel attacks are a class of attacks discovered by Rambus'



The Athena Group, Inc.  
408 W. University Ave.,  
Suite 306  
Gainesville, FL 32601

---

Cryptography Research division (cryptography.com). SCA attacks are non-invasive, easily automated, and can be mounted without knowing the design of the target device. Unlike invasive tampering, electromagnetic attacks can even be performed at a distance: attacks on cell phones have been demonstrated at a range of 30 feet. SCA countermeasures are needed to protect devices that use cryptographic keys, especially sensitive defense applications that require strong anti-tamper protection to defend advanced electronics from reverse engineering as well as commercial devices that perform content protection or payment processing, including mobile devices and IoT endpoints. The advanced countermeasures of the TeraFire SCA-resistant cores limit biases in both power consumption (protects against SPA/DPA/CPA) and electromagnetic emissions (protects against SEMA/DEMA), providing a safe environment for use of the cryptographic keys.

### **About The Athena Group, Inc.**

Athena is a leading provider of security, cryptography, anti-tamper, and signal processing IP cores to many of the world's largest semiconductor companies, defense contractors, and OEMs, as well as emerging providers. Embedded in millions of ASIC and FPGA devices, Athena technologies enable high-value solutions where security and performance are mission critical – defense and aerospace, vehicle safety (V2V, V2X, telematics), networking and communications, satellites, cellular base stations, handsets, the Internet of Things (IoT), and more.

Athena's innovative and experienced team architects best-in-class products: security microprocessors with unmatched hardware efficiency and programmable flexibility, dedicated accelerators for cryptography and security protocols, a comprehensive set of tamper-resistant security cores with SCA/DPA countermeasures developed under a Developer agreement with Rambus' Cryptography Research division, highly optimized FFTs and signal processing cores for communications applications, and related technologies. For more information, visit [athena-group.com](http://athena-group.com).



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)  
[ipsales@athena-group.com](mailto:ipsales@athena-group.com)


Copyright The Athena Group, Inc., 2017. 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.

The Athena logo, TeraFire name, and TeraFire logo are trademarks or registered trademarks of The Athena Group, Inc. All other trademarks, registered trademarks, and/or service marks are the property of their respective owners. Company, product, and service names used in this document are for identification purposes only.

# PRODUCT BRIEF



## Features

- **NEW- DPA/SCA Countermeasures** 
- Strong SCA countermeasures in a comprehensive suite of data security and data integrity products
- Sophisticated, low-leakage SCA implementations
- Extensively verified
- Best-in-Class SCA protection
- Portable to any Microsemi FPGA

## Benefits

- Protects cryptographic keys from SPA, DPA, SEMA, and DEMA attacks
- Provides anti-tamper, anti-reverse engineering, and anti-cloning protection
- Defense in Depth

## Applications

- Encrypted data storage
- Secure communications
- Secure processing
- IoT
- Mobile platforms
- Defense systems
- Hardware Root of Trust

## **TeraFire<sup>®</sup> Cryptographic Security with Side Channel Attack (SCA) Countermeasures**

**Athena delivers a comprehensive suite of security IP with SCA Protection, ready for your Microsemi FPGA application.** While there are many types of SCA, differential power analysis (DPA) has become synonymous with SCA. Athena SCA countermeasures include protection against DPA, as well as simple power analysis (SPA), simple electromagnetic analysis (SEMA), and differential power analysis (DEMA).

### **SCA Countermeasures Overview**

SCAs are a class of non-invasive attack used to extract keys and other secret information from devices that have cryptographic functions. Unlike invasive tampering, electromagnetic attacks can even be performed at a distance: attacks on cell phones have been demonstrated at a range of 30 feet. SCA countermeasures are needed to protect devices that use cryptographic keys, especially hand-held devices and any device that will not have the physical security of a protected facility. Cell phones, IoT endpoints, any device with access to banking (smart cards, cell phones, etc.), commercial electronics that require anti-cloning protections, and especially defense electronics that require strong anti-tamper protection to defend advanced electronics from reverse engineering.

DPA countermeasures are patented by Cryptography Research, Inc. (CRI), and Athena is a licensed DPA countermeasure developer. Athena is committed to leadership in DPA countermeasures, with offerings across its entire product line, including AES, SHA, elliptic curve cryptography, public key cryptography IP cores, and even the Athena advanced TRNG.

### **AES Countermeasures**

Protecting AES encryption is at the heart of anti-tamper SCA countermeasures, so the protection better be good. And the Athena implementation is not just good - it is superior. Compared to alternative countermeasures, the Athena SCA implementation of AES is smaller, faster, and has less leakage. Using TVLA testing, the Athena AES core surpasses 1 *billion* traces, unprecedented resistance to SCA attacks. And the Athena SCA AES core is available in 4 performance levels, with support for every mode ( ECB, CBC, CFB, OFB, CTR, CMAC, CCM, GCM,



## Support

- 12 months maintenance and support included

## Available Deliverables

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

## Standards Compliance

TeraFire products are compliant with the applicable Federal Information Processing Standards (FIPS), National Institute of Standards and Technology (NIST) publications, and Internet Engineering Task Force Request for Comments (IETF RFC).

GHASH, and XTS), every key size (128, 192, and 256), and even supports context switching.

**Table 1: TeraFire Security IP Cores with SCA Countermeasures**

Model	Description
Dragon-QT-DPA	Embedded Hardware Root of Trust
InCipher-DPA	Inline Memory Encryptor
EXP-F5200-DPA	Embedded Cryptography Microprocessor
EXP-F5200B-DPA	Embedded Suite B Cryptography Microprocessor
EXP-E5200-DPA	32-bit Cryptography Microprocessor
EXP-E6400-DPA	64-bit Cryptography Microprocessor
EC Ultra 2000-DPA	High Performance Elliptic Curve Accelerator
EC Ultra 4000-DPA	Extreme Performance Elliptic Curve Accelerator
EC Ultra 8000-DPA	Ultimate Performance Elliptic Curve Accelerator
AES-A500-DPA	Ultra Performance AES
AES-A100-DPA	High Performance AES
AES-A200-DPA	Standard Performance AES
AES-A300-DPA	Compact AES
SHA2-A300-DPA	SHA-1 plus SHA-2 (224/256/384/512)
SHA2-A400-DPA	Double Performance SHA2-A300
RNG-A200-DPA	SP800-90 True Random Number Generator

**Table 2: TeraFire X5200 Executable Firmware with SCA Countermeasures**

Name	Description
PKX-5200	PK Executables Firmware
DTX-5200	Direct Transfer I/F Packet Drivers
AEX-5200	AES Executable Firmware
SHX-5200	SHA Executable Firmware
RNX-5200	SP800-90 DRBG Executable Firmware
SBX-5200	Secure Boot Executables

## SHA Countermeasures

Protecting SHA hashing is notoriously difficult, but as Athena did with AES, our SHA implementation employs an innovative approach that delivers superior SCA protection while maintaining all the performance and advanced features of the Athena standard cores, which include automatic message padding, context switching, HMAC, and even a double speed version.

## Cryptography Microprocessors Countermeasures

TeraFire cryptography microprocessors with SCA countermeasures are ideal for applications requiring strong SCA resistance. The TeraFire processors are available in multiple configurations, optimized for different applications: The F5200 is compact, sized for embedded applications, and has the flexibility to perform all Suite B operations in a single core.



The Athena Group, Inc.  
408 W. University Ave.,  
Suite 306  
Gainesville, FL 32601



---

The E6400 is optimized for RSA-2048 operations, while the E5200 is optimized for RSA-1024 operations. Both E6400 and E5200 are enhanced with additional logic specifically designed to accelerate NIST P-Curve elliptic curve cryptography. All TeraFire cryptography microprocessors are firmware compatible, so the same firmware will run on any core. These programmable cores have the flexibility to execute virtually any public key algorithm without burdening your host processor.

Like AES and SHA cores, the Athena ECC and PK algorithms employ measures to deliver strong SCA protection, while also delivering fire and forget algorithmic support for RSA-CRT, DSA, ECDSA, ECDH, and more.

### **EC Ultra Countermeasures**

EC Ultra employs a breakthrough architecture to deliver unprecedented ECC performance across a range of devices. Coupling Athena's SCA countermeasures with ultra-performance and fire and forget capability makes the EC Ultra the perfect solution for secure, low latency ECDSA and ECDH anti-tamper applications.

### **Dragon QT Cryptographic Microprocessor**

Athena and Intrinsic ID have teamed to create Dragon-QT, an anti-tamper security processor offering flexible, scalable security for IoT and Cloud applications. By integrating Quiddikey-flex secure key management from Intrinsic-ID, the Dragon QT can prevent data theft across an extensive array of devices. Quiddikey's patented PUF technology, Hardware Intrinsic Security™ (HIS), protects the keys from loss during storage while the advanced security architecture and features of the TeraFire security microprocessor protect the keys from loss during use. And of course, Dragon-QT with SCA countermeasures represents the state-of-the-art in anti-tamper secure processing.

The Dragon-QT processor performs all cryptographic operations without ever exposing the keys to the host application processor. With hands-off key management, the Dragon-QT processor prevents loss of keys even if the host application processor is hacked. Using the integrated key wrap and unwrap facility, the Dragon-QT processor can store an essentially unlimited number of application keys without requiring vulnerable key storage memory such as battery-backed RAM.

### **TVLA Testing**

Athena employs the sophisticated test vector leakage assessment (TVLA) testing approach, a fast and reliable testing methodology for side-channel resistance validation that yields statistical confidence scores upon which pass/fail criteria may be established. Different countermeasure implementations, therefore, can yield different SCA resistance levels, resulting in different TVLA "scores". Athena's SCA countermeasures are available in different resistance levels ranging from 10M traces to approaching 1 *Billion* traces (as measured using TVLA) and in four performance levels for AES, two performance levels for SHA, mul-



The Athena Group, Inc.  
408 W. University Ave.,  
Suite 306  
Gainesville, FL 32601

multiple performance levels and configurations for PK and ECC in both the 5200 and 6400 series security microprocessors, three performance levels in the EC Ultra elliptic curve accelerators, and with both protocol and intrinsic SCA countermeasures in the RNG-A200, an SP800-90 true random number generator. Silicon proven, off-the-shelf solutions as well as device-specific solutions are available for every Microsemi device family, including Igloo, ProASIC3, Fusion, SmartFusion, and SmartFusion2.

### **Silicon Proven**

Athena's SCA implementations are silicon tested and silicon proven on multiple FPGA targets, and verification/validation of countermeasure effectiveness is available on your specific device. Contact Athena for more details.

### **About The Athena Group, Inc.**

Athena is a leading provider of security, cryptography, anti-tamper, and signal processing IP cores to many of the world's largest semiconductor companies, defense contractors, and OEMs, as well as emerging providers. Embedded in millions of ASIC and FPGA devices, Athena technologies enable high-value solutions where security and performance are mission critical – defense and aerospace, vehicle safety (V2V, V2X, telematics), networking and communications, satellites, cellular base stations, handsets, the Internet of Things (IoT), and more.

Athena's innovative and experienced team architects best-in-class products: security microprocessors with unmatched hardware efficiency and programmable flexibility, dedicated accelerators for cryptography and security protocols, a comprehensive set of tamper-resistant security cores with SCA/DPA countermeasures developed under a Developer agreement with Rambus' Cryptography Research division, highly optimized FFTs and signal processing cores for communications applications, and related technologies. For more information, visit [athena-group.com](http://athena-group.com).



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)  
[ipsales@athena-group.com](mailto:ipsales@athena-group.com)

Copyright The Athena Group, Inc., 2017. 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.

The Athena logo, TeraFire name, and TeraFire logo are trademarks or registered trademarks of The Athena Group, Inc. All other trademarks, registered trademarks, and/or service marks are the property of their respective owners. Company, product, and service names used in this document are for identification purposes only.


---

## ***Hardware Root of Trust***



## Quiddikey®-Flex

### Features

- **NEW- DPA/SCA Countermeasures** 
- **NEW- AMBA AHB master bus interface with integrated DMA Controller**
- Quiddikey Physically Unclonable Function (PUF) technology from Intrinsic-ID
- Integrated Quiddikey-Flex secure key management
- Flexible and dynamic key programming of multiple, cryptographically separated keys
- Complete Suite B cryptography solution
- Supports RSA, DSA, Diffie-Hellman, and elliptic curve cryptography operations
- Optional integrated AES, GCM, SHA, and SP800-90 true random number generator functions
- Optional iRNG true random number generator
- 100Mbit AES
- Dozens of public key cryptography operations per second

# INTRINSIC ID

## Dragon-QT

### **Embedded Hardware Root of Trust**

**Athena and Intrinsic-ID team to introduce the Dragon-QT embedded cryptography microprocessor core, the ultimate in hardware root of trust.** With state-of-the-art anti-tamper protection for keys at rest and keys in use, the Dragon-QT delivers unprecedented security for applications ranging from IoT to mobile to sensitive government applications. With the flexibility of software and the performance and efficiency of dedicated hardware, the Dragon-QT delivers unbeatable power efficiency with an incredibly small silicon footprint.

### **Product Description**

The Dragon-QT combines Athena's TeraFire F5200 security microprocessor with Intrinsic-ID's Quiddikey-Flex secure key management to deliver the ultimate in embedded hardware root of trust. Intrinsic-ID's patented physically unclonable function (PUF) technology, hardware intrinsic security (HIS®), protects the keys from loss during storage, while the advanced security architecture of Athena's TeraFire F5200 processor protects the keys from loss during use. The fast, efficient, and compact Dragon-QT can be configured for nearly any cryptographic operation, including AES, SHA, elliptic curve cryptography, public key cryptography, advanced true random number generation, SCA/DPA countermeasures, and more. All cryptographic operations are performed without exposing the keys to the host processor. This hands-off key management architecture allows the Dragon-QT processor to prevent loss of keys even when the host application processor is compromised.

Intrinsic-ID's Quiddikey-Flex is a secure key management solution that provides an innovative anti-tamper solution for key protection, by dynamically reconstructing on-chip secret keys without ever storing those keys. This means that the keys are not present on the device when it is powered off, but generated only when needed on-demand using a device-dependent unique PUF. Quiddikey-Flex makes use of the unique device fingerprint originating from deep submicron manufacturing process variations. It defeats the most advanced invasive hardware attacks on the key itself by simply not storing the key. It is also able to extract a unique and unclonable identifier from any device, greatly simplifying key management and distribution.

- Available on SmartFusion2, Igloo2

### Benefits

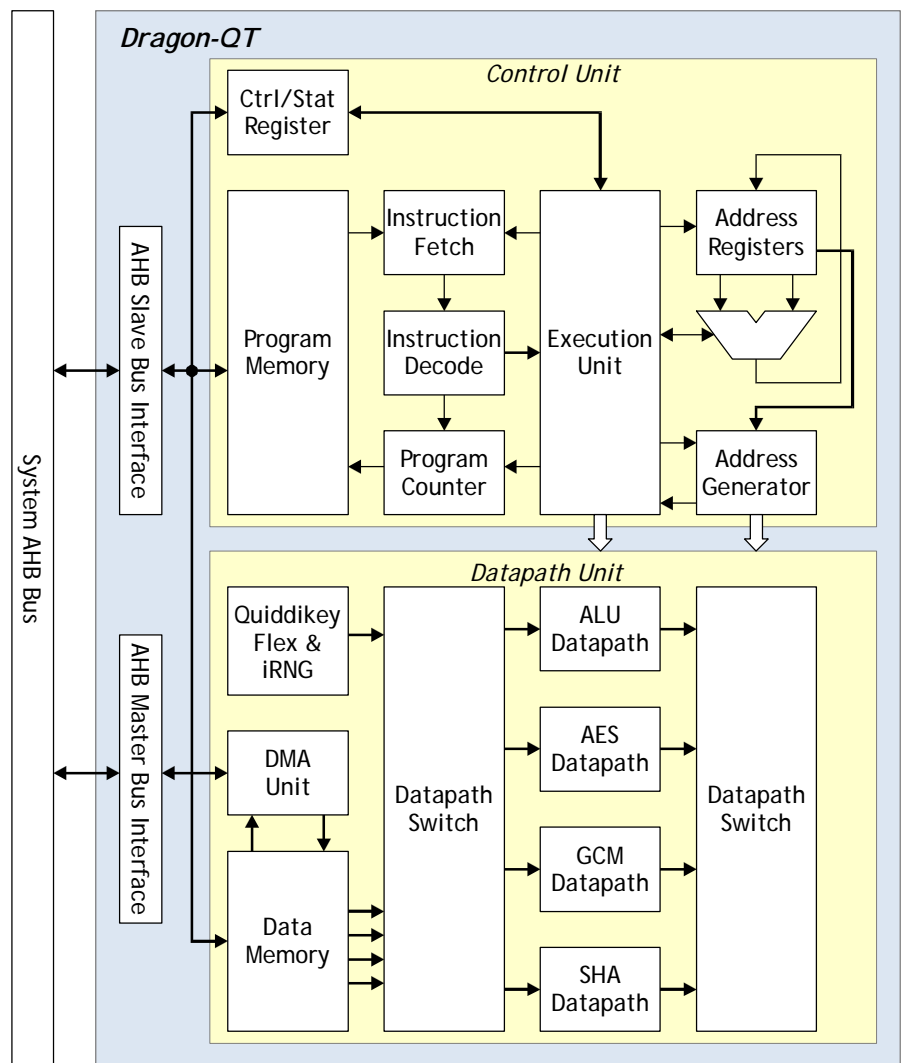
- Superior anti-tamper and anti-cloning protection based on Hardware Intrinsic Security™
- Invasively reading out a memory will not reveal information about the key
- Tampering with the memory will not reveal the key
- No key present at power-off in the system
- SCA/DPA countermeasures protect keys while in use
- Autonomous operation minimizes host processor load
- Programmability enables adaptability to future standards
- Integrated AES, SHA, and TRNG ensure minimum power per operation

### Applications

- Hardware root-of-trust
- Boot memory validation
- Secure element
- Sensitive government applications

### Markets

- Internet of things (IoT)
- Bluetooth low energy (BLE)



The TeraFire F5200 microprocessors are the world's smallest single core solution when configured for Suite B cryptography. The Dragon-QT employs Athena's X5200 instruction set architecture (ISA), making it virtually future-proof through firmware updates instead of costly silicon respins. The X5200 library implements high-level algorithms in firmware, enabling complex algorithms such as RSA with CRT, elliptic curve point multiply, and ECDSA sign and verify to execute without host processor intervention, providing a complete fire-and-forget cryptographic offload solution for your application.

When the AES, GCM, SHA, and random number generator functions of the TeraFire F5200 microprocessor are enabled, the Dragon-QT becomes a highly flexible, single core Suite B security coprocessor. By leveraging the AMBA AHB bus master with integrated DMA controller, the Dragon-QT can enable functions ranging from secure boot memory validation to bump-in-the-wire IPsec coprocessing. The capacity of the Dragon-QT is limited only by memory, and, with support for any Suite B operation, the Dragon-QT is ready to support the greater security requirements of the future, today.



The Athena Group, Inc.  
408 W. University Ave.,  
Suite 306  
Gainesville, FL 32601

- Mobile
- Defense

**Table 1: Dragon-QT Performance<sup>a,b</sup>**

Operation	op/s	latency
Key Reconstruction	454	2.2 ms
RSA-1024 Private Key	30	33 ms
RSA-2048 Private Key	4.3	230 ms
RSA-3072 Private Key	1.3	770 ms
256-bit ECDSA Sign	23	43 ms
256-bit ECDSA Verify	20	50 ms
384-bit ECDSA Sign	8.3	120 ms
384-bit ECDSA Verify	7.1	140 ms

- a. Performance characterized at 50 MHz operating frequency.
- b. Refer to the Athena TeraFire F5200 Product Brief for additional performance data.

**Table 2: Dragon-QT Options<sup>a,b</sup>**

Operation	Throughput
AES	120 Mbps
SHA	40 Mbps
SP800-90 DRBG	30 Mbps

- a. Performance characterized at 50 MHz operating frequency.
- b. Refer to the Athena TeraFire F5200 Product Brief for additional performance data.

### Standards Support

The Dragon-QT supports a broad range of standards, including:

- AES: FIPS 197, SP800-38A/B/C/D/E/F
- SHA/HMAC: FIPS 180-4, FIPS 198
- RNG: SP800-90A
- Elliptic Curve: FIPS 186-4, Suite B
- Public Key: FIPS 186-4, PKCS #1, PKCS #3
- IEEE 1363-2000 ECSVDP

### Hardware Intrinsic Security and PUF Technology

Instead of storing keys in non-volatile memory (typically secure EEPROM or E-fuses), Quiddikey-Flex allows for secure key extraction and programming from unique physical properties of the underlying hardware. This patented approach is called Hardware Intrinsic Security™ (HIS) and makes use of Physical Unclonable Functions (PUFs). The principle can best be described as “biometrics for electronic devices” and uses the device unique start-up values of an uninitialized SRAM block.

### Side Channel Attack Countermeasures

Side channel attacks are a class of attacks discovered by Rambus'



The Athena Group, Inc.  
408 W. University Ave.,  
Suite 306  
Gainesville, FL 32601



## Available Deliverables

- Simulation model (Verilog or VHDL)
- Synthesizable RTL (Verilog or VHDL) and scripts
- Targeted, timing closed netlist
- FPGA netlists
- Verification suite
- C Software for Host Processor (CAL-PK) and X5200 Executable Firmware

## Support

- 12 months maintenance and support included



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)  
[ipsales@athena-group.com](mailto:ipsales@athena-group.com)

Copyright The Athena Group, Inc., 2017. 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.

The Athena logo, TeraFire name, and TeraFire logo are trademarks or registered trademarks of The Athena Group, Inc. All other trademarks, registered trademarks, and/or service marks are the property of their respective owners. Company, product, and service names used in this document are for identification purposes only.

Cryptography Research division ([cryptography.com](http://cryptography.com)). SCA attacks are non-invasive, easily automated, and can be mounted without knowing the design of the target device. Unlike invasive tampering, electromagnetic attacks can even be performed at a distance: attacks on cell phones have been demonstrated at a range of 30 feet. SCA countermeasures are needed to protect devices that use cryptographic keys, especially sensitive defense applications that require strong anti-tamper protection to defend advanced electronics from reverse engineering as well as commercial devices that perform content protection or payment processing, including mobile devices and IoT endpoints. The advanced countermeasures of the TeraFire SCA-resistant cores limit biases in both power consumption (protects against SPA/DPA/CPA) and electromagnetic emissions (protects against SEMA/DEMA), providing a safe environment for use of the cryptographic keys.

## About Intrinsic-ID

Intrinsic-ID is the world-wide leader in security IP cores and applications based on patented Hardware Intrinsic Security™ technology (HIS), also referred to as a "Physical Unclonable Function" or PUF. In HIS, secret keys are extracted from the properties of chips like an 'electronic fingerprint' and used to offer a total protection of sensitive private and corporate data on mobile devices, embedded systems and in the cloud. Intrinsic-ID's wide range of security solutions serves security applications in the following markets: embedded systems, IoT, identification, automotive, communications, content distribution, pay TV, government and defense. Intrinsic-ID is headquartered in Eindhoven, The Netherlands and has sales offices in San Jose, Tokyo and Seoul.

## About The Athena Group, Inc.

Athena is a leading provider of security, cryptography, anti-tamper, and signal processing IP cores to many of the world's largest semiconductor companies, defense contractors, and OEMs, as well as emerging providers. Embedded in millions of ASIC and FPGA devices, Athena technologies enable high-value solutions where security and performance are mission critical – defense and aerospace, vehicle safety (V2V, V2X, telematics), networking and communications, satellites, cellular base stations, handsets, the Internet of Things (IoT), and more.

Athena's innovative and experienced team architects best-in-class products: security microprocessors with unmatched hardware efficiency and programmable flexibility, dedicated accelerators for cryptography and security protocols, a comprehensive set of tamper-resistant security cores with SCA/DPA countermeasures developed under a Developer agreement with Rambus' Cryptography Research division, highly optimized FFTs and signal processing cores for communications applications, and related technologies. For more information, visit [athena-group.com](http://athena-group.com).




---

# ***Anti-Tamper Technologies***

# PRODUCT BRIEF



## Features

- **NEW- DPA/SCA Countermeasures** 
- Secure external memory random access using encryption and authentication
- Protects virtually any standard external memory: DDRn, Flash, QSPI, etc.
- Leverages mature TeraFire AES products
- Supports both 128-bit and 256-bit key strengths
- Available in single and multiple AES core configurations
- Integrated configurable N-way write-back cache
- Portable to any Xilinx device
- AMBA™ AHB and AXI bus interfaces available
- Simple/differential power analysis (SPA/DPA) resistance available

## Benefits

- Eliminates the need for custom complex data/code paging to on-chip memories
- Enables existing applications to run unchanged directly from external memories
- Enhanced tamper resistance

## InCipher™ Inline Memory Encryptor

Athena delivers external memory protection for your Xilinx design with the InCipher inline memory encryptor family of cores. Using Athena's mature portfolio of TeraFire® security solutions, the InCipher M1 provides cryptographic confidentiality for sensitive programs and data, while the InCipher M2 adds authentication for applications requiring greater tamper resistance. The InCipher M1/M2 inline memory encryptor cores provide secure random access to data and programs stored in vulnerable bulk memory devices, whether these devices are RAM or non-volatile memories such as Flash. This enables your application to execute using the protected memories directly – without depending on the application to load sensitive code and data into on-chip memories. Athena's sophisticated SCA/DPA countermeasures, both protocol and leakage reduction, are available as an option.

## Product Description

The InCipher cores are designed to be placed between the host bus interface and the external memory controller, as shown in Figure 1. InCipher works with any memory technology, since the InCipher cores interoperate with external memory controllers at the bus transactional level. The choice of single or multi-core AES solutions allows each InCi-

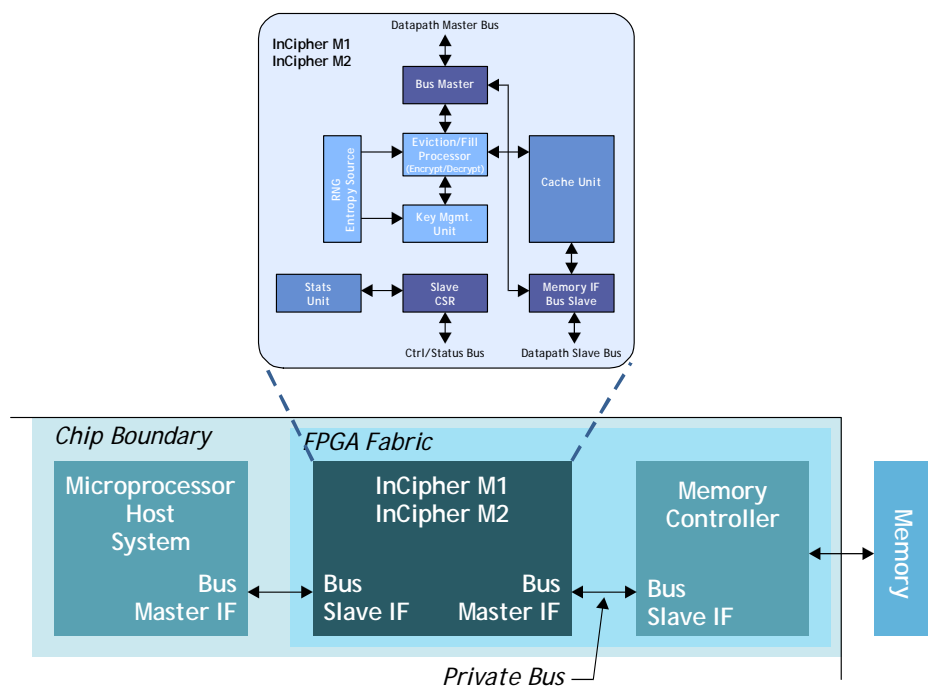


Figure 1: InCipher M1/M2 Inline Memory Encryptor Application

## Support

- 12 months maintenance and support included

## Applications

- Embedded secure processing

## Available Deliverables

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



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)  
[ipsales@athena-group.com](mailto:ipsales@athena-group.com)

Copyright The Athena Group, Inc., 2017. 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.

The Athena logo, TeraFire name, and TeraFire logo are trademarks or registered trademarks of The Athena Group, Inc. All other trademarks, registered trademarks, and/or service marks are the property of their respective owners. Company, product, and service names used in this document are for identification purposes only.

Xilinx, Virtex, Kintex, Artix, and Ultrascale words and logos are trademarks of Xilinx Corporation and registered in the U.S. Patent and Trademark Office and in other countries.

pher implementation to be tuned to the specific requirements of the application. InCipher further increases the performance of your system by implementing a configurable *N*-way, write-back cache. Using standard bus interfaces, integration is a snap, and, since the InCipher acts as a physical cache between the system and the memory controller, there are no cache coherency challenges. The InCipher M1/M2 cores are available with a choice of AHB-32, AHB-64, AXI-32, AXI-64, or AXI-128 buses. and can support integration in a range of applications from small micro-controllers to the latest full-featured microprocessors running in multi-core configurations.

## Side Channel Attack Countermeasures

Side channel attacks are a class of attacks discovered by Rambus' Cryptography Research division ([cryptography.com](http://cryptography.com)). SCA attacks are non-invasive, easily automated, and can be mounted without knowing the design of the target device. Unlike invasive tampering, electromagnetic attacks can even be performed at a distance: attacks on cell phones have been demonstrated at a range of 30 feet. SCA countermeasures are needed to protect devices that use cryptographic keys, especially sensitive defense applications that require strong anti-tamper protection to defend advanced electronics from reverse engineering as well as commercial devices that perform content protection or payment processing, including mobile devices and IoT endpoints. The advanced countermeasures of the TeraFire SCA-resistant cores limit biases in both power consumption (protects against SPA/DPA/CPA) and electromagnetic emissions (protects against SEMA/DEMA), providing a safe environment for use of the cryptographic keys.

## About The Athena Group, Inc.

Athena is a leading provider of security, cryptography, anti-tamper, and signal processing IP cores to many of the world's largest semiconductor companies, defense contractors, and OEMs, as well as emerging providers. Embedded in millions of ASIC and FPGA devices, Athena technologies enable high-value solutions where security and performance are mission critical – defense and aerospace, vehicle safety (V2V, V2X, telematics), networking and communications, satellites, cellular base stations, handsets, the Internet of Things (IoT), and more.

Athena's innovative and experienced team architects best-in-class products: security microprocessors with unmatched hardware efficiency and programmable flexibility, dedicated accelerators for cryptography and security protocols, a comprehensive set of tamper-resistant security cores with SCA/DPA countermeasures developed under a Developer agreement with Rambus' Cryptography Research division, highly optimized FFTs and signal processing cores for communications applications, and related technologies. For more information, visit [athena-group.com](http://athena-group.com).


---

# ***Cryptography Microprocessors***

# PRODUCT BRIEF



## Features

- **NEW- DPA/SCA Countermeasures** 
- Thousands of operations per second
- Supports up to 16K-bit public key operations
- Enhanced performance for elliptic curve operations
- Accelerates Suite B P-curve operations
- Implements Athena's powerful X5200 instruction set architecture
- Scalable for your application's area and performance needs
- Portable to any Microsemi device
- AMBA™ AHB and AXI bus interfaces available
- Simple/differential power analysis (SPA/DPA) resistance available

## Benefits

- Programmability enables adaptability to future public key standards
- Autonomous operation minimizes load on host processor

## 5200 Series 32-bit Cryptography Microprocessors

From the market leader in high performance public key cryptography cores comes the 5200 series, a fast and efficient public key cryptography solution with multiple size and performance options that can be matched to the requirements of your application. Athena's patented arithmetic technology delivers the performance your solution needs – low latency *and* high throughput – in an area-efficient IP Core portable to any Microsemi device.

**Table 1: 5200 Igloo2/SmartFusion2 Specifications<sup>a</sup>**

Operation	Op/s	Latency
RSA-1024 Private Key	468	2.1 ms
RSA-1024 Private Key (Paired Cores)	936	1.1 ms
1024-bit Expo w/ 1024-bit Expo.	92.5	10.8 ms
1024-bit DSA Sign	531.9	1.9 ms
1024-bit DSA Verify	269.9	3.7 ms
RSA-2048 Private Key	47	21.3 ms
RSA-2048 Private Key (Paired Cores)	94	10.6 ms
2048-bit Expo w/ 2048-bit Exponent	15.8	63.3 ms
2048-bit DSA Sign	133.9	7.5 ms
2048-bit DSA Verify	70.6	14.2 ms
RSA-3072 Private Key	16.8	59.5 ms
RSA-3072 Private Key (Paired Cores)	33.6	29.8 ms
NIST P-256 EC Point Multiply	207.3	4.8 ms
NIST P-256 ECDSA Sign	188.3	5.3 ms
NIST P-256 ECDSA Verify	162.7	6.1 ms
NIST P-384 EC Point Multiply	103.7	9.6 ms
NIST P-384 ECDSA Sign	96	10.4 ms
NIST P-384 ECDSA Verify	81.4	12.3 ms
Area	18,700 LEs	
Frequency	50 MHz	

a. Other Microsemi device families supported.

## Support

- 12 months maintenance and support included

## Applications

- Embedded secure processing
- SSL and IPsec acceleration
- E-commerce
- SSL VPN
- Security appliances

## Available Deliverables

- Simulation model (Verilog or VHDL)
- Synthesizable RTL (Verilog or VHDL) and scripts
- Targeted, timing closed netlist
- Verification suite
- C Software for Host Processor (CAL-PK) and X5200 Executable Firmware
- Assembler and Software Simulator
- Documentation

**Table 2: TeraFire E5200 Non-NIST P-Curve ECC Performance<sup>a</sup>**

Operation	E5200 <sup>b</sup>	
	Op/s	Latency
256-bit EC Point Multiply	133	7.5 ms
256-bit ECDSA Sign	126	7.9 ms
256-bit ECDSA Verify	107	9.3 ms
384-bit EC Point Multiply	81	12.2 ms
384-bit ECDSA Sign	77	12.9 ms
384-bit ECDSA Verify	65	15.4 ms
521-bit EC Point Multiply	49	20.4 ms

a. Igloo2/SmartFusion2. Other Microsemi device families supported.

b. Performance, characterized at 50 MHz, applies for all E5200 series processors.

## Product Description

The TeraFire® 5200 series implements Athena's proprietary public key instruction set architecture, which allows the 5200 series to perform virtually any public key operation, including the myriad elliptic curve cryptography algorithms. New standards and algorithms can be quickly accommodated with on-the-fly programmability. The TeraFire E5200 augments Athena's proprietary public key instruction set architecture with enhanced performance elliptic curve instructions that accelerate all odd characteristic operations and further accelerate Suite B P-curve operations. Multiple models are available (see Table 1), optimized for operations up to 256-bits (E5209), 512-bits (E5211), 1024-bits (E5221), or more.

The TeraFire family of PK processors can perform virtually any public key operation and easily accommodates new standards with on-the-fly programmability. The performance, capabilities, and area can be optimized to meet your requirements since the maximum operation size for any TeraFire processor is determined solely by the populated memory size.

## X5200 Executable Firmware

The X5200 library implements high-level algorithms in assembly language. Complex algorithms such as RSA with CRT, elliptic curve point multiply, and ECDSA sign and verify can all execute without host processor intervention, providing a complete fire-and-forget cryptographic offload solution for your application. Optional X5200 development tools, including an assembler and software simulator, are also available (sold separately).



The Athena Group, Inc.  
408 W. University Ave.,  
Suite 306  
Gainesville, FL 32601



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)  
[ipsales@athena-group.com](mailto:ipsales@athena-group.com)

Copyright The Athena Group, Inc., 2017. 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.

The Athena logo, TeraFire name, and TeraFire logo are trademarks or registered trademarks of The Athena Group, Inc. All other trademarks, registered trademarks, and/or service marks are the property of their respective owners. Company, product, and service names used in this document are for identification purposes only.

## **C Software for Host Processor**

The TeraFire CAL-PK is a portable, ANSI C library of drivers for TeraFire public key processors. CAL-PK has been implemented and tested on multiple platforms, including leading SoC microprocessors from ARM.

## **Side Channel Attack Countermeasures**

Side channel attacks are a class of attacks discovered by Rambus' Cryptography Research division ([cryptography.com](http://cryptography.com)). SCA attacks are non-invasive, easily automated, and can be mounted without knowing the design of the target device. Unlike invasive tampering, electromagnetic attacks can even be performed at a distance: attacks on cell phones have been demonstrated at a range of 30 feet. SCA countermeasures are needed to protect devices that use cryptographic keys, especially sensitive defense applications that require strong anti-tamper protection to defend advanced electronics from reverse engineering as well as commercial devices that perform content protection or payment processing, including mobile devices and IoT endpoints. The advanced countermeasures of the TeraFire SCA-resistant cores limit biases in both power consumption (protects against SPA/DPA/CPA) and electromagnetic emissions (protects against SEMA/DEMA), providing a safe environment for use of the cryptographic keys.

## **About The Athena Group, Inc.**

Athena is a leading provider of security, cryptography, anti-tamper, and signal processing IP cores to many of the world's largest semiconductor companies, defense contractors, and OEMs, as well as emerging providers. Embedded in millions of ASIC and FPGA devices, Athena technologies enable high-value solutions where security and performance are mission critical – defense and aerospace, vehicle safety (V2V, V2X, telematics), networking and communications, satellites, cellular base stations, handsets, the Internet of Things (IoT), and more.


Athena's innovative and experienced team architects best-in-class products: security microprocessors with unmatched hardware efficiency and programmable flexibility, dedicated accelerators for cryptography and security protocols, a comprehensive set of tamper-resistant security cores with SCA/DPA countermeasures developed under a Developer agreement with Rambus' Cryptography Research division, highly optimized FFTs and signal processing cores for communications applications, and related technologies. For more information, visit [athena-group.com](http://athena-group.com).



# PRODUCT BRIEF



## Features

- **NEW- DPA/SCA Countermeasures** 
- Supports RSA, DSA, Diffie-Hellman, and Suite B elliptic curve cryptography operations
- Optional integrated AES, GCM, SHA, and random number generator functions
- Implements Athena's powerful X5200 instruction set architecture
- Hundreds of public key cryptography operations per second
- Portable to any Microsemi device
- AMBA™ AHB bus interface eases integration
- Simple/differential power analysis (SPA/DPA) resistance available

## Benefits

- Programmability enables adaptability to future standards
- Autonomous operation minimizes host processor load
- Integrated AES and SHA enables single core Suite B solution

## F5200 Embedded Cryptography Microprocessor

Athena introduces the TeraFire® F5200 embedded cryptography microprocessor core, a fast, efficient microprocessor designed for public key and secret key cryptography applications. With an area footprint starting at 25K-gates and over 45 RSA-1024 private key operations per second, the F5200 provides more than 10× greater performance than competitive solutions with similar area. With AES, SHA, and random number generator options, the F5200 is a single core solution for Suite B cryptography.

**Table 1: F5200 Igloo2/SmartFusion2 Specifications<sup>a</sup>**

Operation	F5200		F5210	
	Op/s	Latency	Op/s	Latency
RSA-1024 Private Key	30	33 ms	45	22 ms
RSA-1024 Private Key (Paired Cores)	60	16 ms	90	16 ms
1024-bit Expo w/ 1024-bit Exponent	8.4	118 ms	12	79 ms
1024-bit DSA Sign	55	18 ms	83	12 ms
1024-bit DSA Verify	26	38 ms	39	25 ms
RSA-2048 Private Key	4.3	230 ms	6.4	150 ms
RSA-2048 Private Key (Paired Cores)	8.6	115 ms	13	77 ms
2048-bit Expo w/ 2048-bit Exponent	1.1	890 ms	1.6	600 ms
2048-bit DSA Sign	9.8	100 ms	1.3	740 ms
2048-bit DSA Verify	5.1	200 ms	7.6	130 ms
RSA-3072 Private Key	1.3	770 ms	1.9	510 ms
RSA-3072 Private Key w/ Paired Cores	2.6	390 ms	3.9	250 ms
256-bit EC Point Multiply	25	40 ms	37	26 ms
256-bit ECDSA Sign	23	43 ms	35	28 ms
256-bit ECDSA Verify	20	50 ms	30	33 ms
384-bit EC Point Multiply	9.0	110 ms	13	74 ms
384-bit ECDSA Sign	8.3	120 ms	12	80 ms
384-bit ECDSA Verify	7.1	140 ms	10	94 ms
521-bit EC Point Multiply	3.6	280 ms	5.4	180 ms
Area	7,200 LEs		8,100 LEs	
Frequency	50 MHz		50 MHz	

a. Other Microsemi device families supported.

## Support

- 12 months maintenance and support included

## Applications

- FPGA bitstream validation
- Secure boot memory validation
- Embedded secure processing
- SSL and IPsec acceleration
- E-commerce
- SSL VPN
- Mobile Platforms

## Available Deliverables

- Simulation model (Verilog or VHDL)
- Synthesizable RTL (Verilog or VHDL) and scripts
- Targeted, timing closed netlist
- Verification suite
- C Software for Host Processor (CAL-PK) and X5200 Executable Firmware
- Assembler and Software Simulator
- Documentation

## Product Description

The F5200 implements Athena's X5200 instruction set architecture (ISA), making it firmware compatible with the high-performance TeraFire T5200 and E5200 cryptography microprocessors and the X5200 Library. The fully programmable X5200 ISA enables the F5200 to execute virtually any public key cryptography algorithm today, and the algorithms of tomorrow can be supported with a simple firmware update.

When the optional AES, GCM, SHA, and random number generator functions are enabled, the F5200 becomes a highly flexible, single core security application coprocessor. By leveraging the direct transfer interface, the F5200 can enable functions ranging from secure boot memory validation to 'bump-in-the-wire' IPsec coprocessing. The direct transfer interface can also be used to pair two F5200 cores, enabling twice the throughput and half the latency for RSA private key operations with CRT. The capacity of the F5200 is limited only by memory, and with support for virtually any length operation, the F5200 is ready to support the greater security requirements of the future, today.

**Table 2: TeraFire F5200 Options<sup>a</sup>**

Operation	Performance	Area
AES-128	120 Mbps	1,300 LEs <sup>b</sup>
AES-192	100 Mbps	
AES-256	92.5 Mbps	
SHA-1	24 Mbps	3,200 LEs
SHA-224/256	19.5 Mbps	
SHA-384/512	15.0 Mbps	
SP800-90 DRBG	30 Mbps	400 LEs

a. Performance characterized at 50 MHz operating frequency.

b. Add 1,000 LEs for GCM Mode.

## X5200 Executable Firmware

The X5200 library implements high-level algorithms in assembly language. Complex algorithms such as RSA with CRT, elliptic curve point multiply, and ECDSA sign and verify can all execute without host processor intervention, providing a complete fire-and-forget cryptographic offload solution for your application. Optional X5200 development tools, including an assembler and software simulator, are also available (sold separately).

## Standards Support

The F5200 has been designed with broad standards support, including:

- AES: FIPS 197, SP800-38A/B/C/D/E/F
- SHA/HMAC: FIPS 180-4, FIPS 198
- RNG: SP800-90
- Elliptic Curve: FIPS 186-4, Suite B



The Athena Group, Inc.  
408 W. University Ave.,  
Suite 306  
Gainesville, FL 32601

- Public Key: FIPS 186-4, PKCS #1, PKCS #3
- IEEE 1363-2000 ECSVDP

### **C Software for Host Processor**

The TeraFire CAL-PK is a portable, ANSI C library of drivers for TeraFire public key processors. CAL-PK has been implemented and tested on multiple platforms, including leading SoC microprocessors from ARM.

### **Side Channel Attack Countermeasures**

Side channel attacks are a class of attacks discovered by Rambus' Cryptography Research division (cryptography.com). SCA attacks are non-invasive, easily automated, and can be mounted without knowing the design of the target device. Unlike invasive tampering, electromagnetic attacks can even be performed at a distance: attacks on cell phones have been demonstrated at a range of 30 feet. SCA countermeasures are needed to protect devices that use cryptographic keys, especially sensitive defense applications that require strong anti-tamper protection to defend advanced electronics from reverse engineering as well as commercial devices that perform content protection or payment processing, including mobile devices and IoT endpoints. The advanced countermeasures of the TeraFire SCA-resistant cores limit biases in both power consumption (protects against SPA/DPA/CPA) and electromagnetic emissions (protects against SEMA/DEMA), providing a safe environment for use of the cryptographic keys.

### **About The Athena Group, Inc.**

Athena is a leading provider of security, cryptography, anti-tamper, and signal processing IP cores to many of the world's largest semiconductor companies, defense contractors, and OEMs, as well as emerging providers. Embedded in millions of ASIC and FPGA devices, Athena technologies enable high-value solutions where security and performance are mission critical – defense and aerospace, vehicle safety (V2V, V2X, telematics), networking and communications, satellites, cellular base stations, handsets, the Internet of Things (IoT), and more.

Athena's innovative and experienced team architects best-in-class products: security microprocessors with unmatched hardware efficiency and programmable flexibility, dedicated accelerators for cryptography and security protocols, a comprehensive set of tamper-resistant security cores with SCA/DPA countermeasures developed under a Developer agreement with Rambus' Cryptography Research division, highly optimized FFTs and signal processing cores for communications applications, and related technologies. For more information, visit [athena-group.com](http://athena-group.com).



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)  
[ipsales@athena-group.com](mailto:ipsales@athena-group.com)


Copyright The Athena Group, Inc., 2017. 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.

The Athena logo, TeraFire name, and TeraFire logo are trademarks or registered trademarks of The Athena Group, Inc. All other trademarks, registered trademarks, and/or service marks are the property of their respective owners. Company, product, and service names used in this document are for identification purposes only.

# PRODUCT BRIEF



## Features

- **NEW- DPA/SCA Countermeasures** 
- Over 760 ECDSA P-256 verify operations per second
- Over 430 ECDSA P-384 verify operations per second
- Portable to any Microsemi device
- AMBA™ AHB and AXI bus interfaces available
- Simple/differential power analysis (SPA/DPA) resistance available

## Benefits

- Autonomous operation minimizes load on host processor
- Complete Suite B solution with ultra ECC performance when integrated with the F5200B

## Applications

- Embedded secure processing
- Vehicle to Vehicle Communications (V2V)
- SSL and IKE acceleration
- E-commerce
- Security appliances

## EC Ultra Elliptic Curve Cryptography Microprocessor

**From the leader in elliptic curve cryptography (ECC) cores comes the fastest ECC accelerator yet.** The TeraFire® EC Ultra family of semiconductor IP cores unleashes a new class of ECC performance, based on a breakthrough architecture for ECC acceleration. Athena has achieved extraordinary performance density with EC Ultra, yielding an impressive increase of almost 5x over Athena's E5200.

### Product Description

TeraFire® EC Ultra IP cores accelerate EC point multiplies and ECDSA signs and verifies over NIST P-curves. Configurations can include as many P-curves as needed or can eliminate unnecessary curves to save system resources. Any curve may be supported, including Brainpool curves and non-singular Weierstrass curves with the optional Programmable Curves feature.

EC Ultra 8K is the fastest core in the EC Ultra family and is capable of performing an ECDSA P-256 verify in less than 1.1 ms at 60MHz. EC Ultra 4K and 2K offer the same outstanding performance density as EC Ultra 8K in more compact forms.

**Table 1: TeraFire® EC Ultra Igloo2/SmartFusion2 Specifications<sup>a</sup>**

Operation	EC Ultra 2K	EC Ultra 4K	EC Ultra 8K
NIST P-256 EC Point Multiply (op/s)	318	612	1,224
NIST P-256 ECDSA Sign (op/s)	282	552	1,116
NIST P-256 ECDSA Verify (op/s)	234	456	912
NIST P-384 EC Point Multiply (op/s)	174	360	732
NIST P-384 ECDSA Sign (op/s)	156	318	624
NIST P-384 ECDSA Verify (op/s)	126	264	516
Area (P-256 curve only)	9,900 LEs	14,100 LEs	18,400 LEs
Area (P-384 curve only)	14,700 LEs	20,900 LEs	27,600 LEs
Area (Both P-256 and P-384 Curves)	16,600 LEs	24,000 LEs	30,900 LEs
Frequency	60 MHz	60 MHz	60 MHz

a. Other Microsemi device families supported.

### Interface

TeraFire® EC Ultra cores are designed for stand-alone operation to enable maximum flexibility. Any EC Ultra core can be integrated with the Ath-

## Support

- 12 months maintenance and support included

## Available Deliverables

- Simulation model (Verilog or VHDL)
- Synthesizable RTL (Verilog or VHDL) and scripts
- Targeted, timing closed netlist
- Verification suite
- C Software for Host Processor (CAL-PK)
- Documentation



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)  
[ipsales@athena-group.com](mailto:ipsales@athena-group.com)

Copyright The Athena Group, Inc., 2017. 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.

The Athena logo, TeraFire name, and TeraFire logo are trademarks or registered trademarks of The Athena Group, Inc. All other trademarks, registered trademarks, and/or service marks are the property of their respective owners. Company, product, and service names used in this document are for identification purposes only.

ena F5200B, creating a complete, single interface Suite B solution with ultra fast elliptic curve performance. AHB and AXI, and other bus interfaces are also available for EC Ultra cores.

## C Software for Host Processor

The TeraFire CAL-PK is a portable, ANSI C library of drivers for TeraFire public key processors. CAL-PK has been implemented and tested on multiple platforms, including leading SoC microprocessors from ARM.

## Side Channel Attack Countermeasures

Side channel attacks are a class of attacks discovered by Rambus' Cryptography Research division ([cryptography.com](http://cryptography.com)). SCA attacks are non-invasive, easily automated, and can be mounted without knowing the design of the target device. Unlike invasive tampering, electromagnetic attacks can even be performed at a distance: attacks on cell phones have been demonstrated at a range of 30 feet. SCA countermeasures are needed to protect devices that use cryptographic keys, especially sensitive defense applications that require strong anti-tamper protection to defend advanced electronics from reverse engineering as well as commercial devices that perform content protection or payment processing, including mobile devices and IoT endpoints. The advanced countermeasures of the TeraFire SCA-resistant cores limit biases in both power consumption (protects against SPA/DPA/CPA) and electromagnetic emissions (protects against SEMA/DEMA), providing a safe environment for use of the cryptographic keys.

## About The Athena Group, Inc.

Athena is a leading provider of security, cryptography, anti-tamper, and signal processing IP cores to many of the world's largest semiconductor companies, defense contractors, and OEMs, as well as emerging providers. Embedded in millions of ASIC and FPGA devices, Athena technologies enable high-value solutions where security and performance are mission critical – defense and aerospace, vehicle safety (V2V, V2X, telematics), networking and communications, satellites, cellular base stations, handsets, the Internet of Things (IoT), and more.

Athena's innovative and experienced team architects best-in-class products: security microprocessors with unmatched hardware efficiency and programmable flexibility, dedicated accelerators for cryptography and security protocols, a comprehensive set of tamper-resistant security cores with SCA/DPA countermeasures developed under a Developer agreement with Rambus' Cryptography Research division, highly optimized FFTs and signal processing cores for communications applications, and related technologies. For more information, visit [athena-group.com](http://athena-group.com).

---

# ***True Random Number Generators***





## Features

- SP800-22 compliant
- FIPS 140-1 compliant
- Silicon proven
- Fast delivery
- Internal fault detection for NRNG subsystem
- Microprocessor bus interfaces available
- Portable to any Microsemi device
- Easy integration

## Benefits

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

## Applications

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

## Support

- 12 months maintenance and support included

## Available Deliverables

- Simulation model (Verilog or VHDL)

## Compact True Random Number Generator

**Athena delivers silicon-proven semiconductor intellectual property (IP) cores for cryptographic-grade random number generation (RNG).** The TeraFire® Compact TRNG core (RNG-A100) 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 RNG core is a fast and reliable way to incorporate cryptographic-grade random numbers into your ASIC or FPGA design.

**Table 1: RNG-A100 Igloo2/SmartFusion2 Specifications<sup>a</sup>**

	RNG-A100
Output Rate	72.5 Mbps
Area	1,400 LEs
Frequency	145 MHz

a. Other Microsemi device families supported.

## 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 incorporates 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.

## 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.



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

## C Software for Host Processor

The TeraFire CAL-SYM is a portable, ANSI C library of drivers for TeraFire hardware accelerators. The TeraFire CAL-SYM has been implemented and tested on multiple platforms, including leading SoC microprocessors from ARM.

## About The Athena Group, Inc.

Athena is a leading provider of security, cryptography, anti-tamper, and signal processing IP cores to many of the world's largest semiconductor companies, defense contractors, and OEMs, as well as emerging providers. Embedded in millions of ASIC and FPGA devices, Athena technologies enable high-value solutions where security and performance are mission critical – defense and aerospace, vehicle safety (V2V, V2X, telematics), networking and communications, satellites, cellular base stations, handsets, the Internet of Things (IoT), and more.

Athena's innovative and experienced team architects best-in-class products: security microprocessors with unmatched hardware efficiency and programmable flexibility, dedicated accelerators for cryptography and security protocols, a comprehensive set of tamper-resistant security cores with SCA/DPA countermeasures developed under a Developer agreement with Rambus' Cryptography Research division, highly optimized FFTs and signal processing cores for communications applications, and related technologies. For more information, visit [athena-group.com](http://athena-group.com).



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)  
[ipsales@athena-group.com](mailto:ipsales@athena-group.com)

Copyright The Athena Group, Inc., 2017. 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.

The Athena logo, TeraFire name, and TeraFire logo are trademarks or registered trademarks of The Athena Group, Inc. All other trademarks, registered trademarks, and/or service marks are the property of their respective owners. Company, product, and service names used in this document are for identification purposes only.



## Features

- **NEW- DPA/SCA Countermeasures** 
- SP800-90 compliant
- Tracks the FIPS 140-3 (draft)
- Silicon proven
- Fast delivery
- 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 Microsemi device
- Simple/differential power analysis (SPA/DPA) resistance available

## Applications

- Encrypted data storage
- Secure communications
- 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 TRNG 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.

**Table 1: RNG-A200 Igloo2/SmartFusion2 Specifications<sup>a</sup>**

	RNG-A200-AES1	RNG-A200-AES2	NRBG-A100
Output Rate	520 Mbps	144 Mbps	Custom
Area	15,000 LEs	10,200 LEs	500 LEs
Frequency	65 MHz	60 MHz	200 MHz
Strength	128-256b	128-256b	128-256b

a. Other Microsemi device families supported.

### RNG-A200 Description

By combining the Athena NRBG-A200 composite ring oscillator module, a proven source of intrinsic non-deterministic entropy, with an all-hardware post-processor compliant with NIST SP800-90, the TeraFire Advanced TRNG core provides a direct path to FIPS 140-3 (draft) compliant random number generation.

The NRBG-A200 module in the RNG-A200 generates non-deterministic entropy using a proprietary topology of ring oscillators, uniquely customized based on library and target operating frequency. The RNG-A200 implements advanced health monitoring of the ring oscillator module that provides 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 and/or errors. Athena’s NRBG-A200 is designed with built-in support for manufacturing test to simplify system integration and may 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.

---

## Support

- 12 months maintenance and support included

## Available Deliverables

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

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 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 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.

## C Software for Host Processor

The TeraFire CAL-SYM is a portable, ANSI C library of drivers for TeraFire hardware accelerators. The TeraFire CAL-SYM has been implemented and tested on multiple platforms, including leading SoC microprocessors from ARM.

## Side Channel Attack Countermeasures

Side channel attacks are a class of attacks discovered by Rambus' Cryptography Research division ([cryptography.com](http://cryptography.com)). SCA attacks are non-invasive, easily automated, and can be mounted without knowing the design of the target device. Unlike invasive tampering, electromagnetic attacks can even be performed at a distance: attacks on cell phones have been demonstrated at a range of 30 feet. SCA countermeasures are needed to protect devices that use cryptographic keys, especially sensitive defense applications that require strong anti-tamper protection to defend advanced electronics from reverse engineering as well as commercial devices that perform content protection or payment processing, including mobile devices and IoT endpoints. The advanced countermeasures of the TeraFire SCA-resistant



The Athena Group, Inc.  
408 W. University Ave.,  
Suite 306  
Gainesville, FL 32601

cores limit biases in both power consumption (protects against SPA/DPA/CPA) and electromagnetic emissions (protects against SEMA/DEMA), providing a safe environment for use of the cryptographic keys.

### **About The Athena Group, Inc.**

Athena is a leading provider of security, cryptography, anti-tamper, and signal processing IP cores to many of the world's largest semiconductor companies, defense contractors, and OEMs, as well as emerging providers. Embedded in millions of ASIC and FPGA devices, Athena technologies enable high-value solutions where security and performance are mission critical – defense and aerospace, vehicle safety (V2V, V2X, telematics), networking and communications, satellites, cellular base stations, handsets, the Internet of Things (IoT), and more.

Athena's innovative and experienced team architects best-in-class products: security microprocessors with unmatched hardware efficiency and programmable flexibility, dedicated accelerators for cryptography and security protocols, a comprehensive set of tamper-resistant security cores with SCA/DPA countermeasures developed under a Developer agreement with Rambus' Cryptography Research division, highly optimized FFTs and signal processing cores for communications applications, and related technologies. For more information, visit [athena-group.com](http://athena-group.com).



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)  
[ipsales@athena-group.com](mailto:ipsales@athena-group.com)

Copyright The Athena Group, Inc., 2017. 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.


The Athena logo, TeraFire name, and TeraFire logo are trademarks or registered trademarks of The Athena Group, Inc. All other trademarks, registered trademarks, and/or service marks are the property of their respective owners. Company, product, and service names used in this document are for identification purposes only.

---

## ***Ciphers and Hashing***



## Features

- **NEW- DPA/SCA Countermeasures** 
- FIPS 197 compliant AES cores
- Supports key sizes of 128, 192, and 256-bits
- Supports NIST SP800-38A, B, C, D, and E defined modes
- Three dedicated product series support different performance and area requirements
- Modular architecture
- AES support also available in TeraFire F5200 cryptography microprocessor
- Microprocessor bus interfaces available
- Portable to any Microsemi device
- Simple/differential power analysis (SPA/DPA) resistance available

## Benefits

- Modular architecture enables scalable performance and optimal implementation
- Full-width data ports maximize performance, minimize latency

## Advanced Encryption Standard (AES)

**Athena delivers the Advanced Encryption Standard (AES) ciphers as semiconductor intellectual property (IP) cores.** Athena's AES cores complement the market-leading TeraFire<sup>®</sup> cryptography microprocessors and standalone TeraFire cryptography accelerators. Whether your application demands high AES performance or the power savings of a dedicated core, Athena's AES cores deliver both performance and power savings.

Athena offers AES both within its cryptography microprocessor family and as dedicated cores. Optional microprocessor bus interfaces are also available for dedicated AES core solutions.

**Table 1: AES Igloo2/SmartFusion2 Specifications<sup>a</sup>**

	AES-A500	AES-A100	AES-A200
Performance	2.8 Gbps	1.6 Gbps	350 Mbps
Area	4,500 LEs	3,100 LEs	2,800 LEs
Frequency	120 MHz	135 MHz	125 MHz

a. Other Microsemi device families supported.

Dedicated AES core solutions are constructed using a modular architecture, comprising cipher cores, key schedule generators, and modes modules, allowing Athena to configure an AES solution optimized for the functional, performance, area, and power requirements of your application.

Athena supports all AES modes, including ECB, CBC, CFB, OFB, CTR, CMAC, CCM, GCM, and GHASH, and even XTS mode (SP800-38E). Any modes and/or key sizes not required can be omitted to reduce area.

### AES Standards Compliance

- FIPS 197
- NIST SP800-38A (ECB, CBC, CFB, OFB, CTR)
- NIST SP800-38B (CMAC)
- NIST SP800-38C (CCM)
- NIST SP800-38D (GHASH, GCM)
- NIST SP800-38E (XTS)
- NIST SP8700-38F (Key Rolling)
- Suite B
- IEEE 802.1ae
- IEEE 802.11i



## Support

- 12 months maintenance and support included

## Applications

- Encrypted data storage
- Secure communications
- Secure processing
- IPsec acceleration
- E-commerce
- VPN
- Financial Transactions

## Available Deliverables

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



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)  
[ipsales@athena-group.com](mailto:ipsales@athena-group.com)

Copyright The Athena Group, Inc., 2017. 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.

The Athena logo, TeraFire name, and TeraFire logo are trademarks or registered trademarks of The Athena Group, Inc. All other trademarks, registered trademarks, and/or service marks are the property of their respective owners. Company, product, and service names used in this document are for identification purposes only.

- IEEE 802.16e

## 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.

## C Software for Host Processor

The TeraFire CAL-SYM is a portable, ANSI C library of drivers for TeraFire hardware accelerators. The TeraFire CAL-SYM has been implemented and tested on multiple platforms, including leading SoC microprocessors from ARM.

## Side Channel Attack Countermeasures

Side channel attacks are a class of attacks discovered by Rambus' Cryptography Research division ([cryptography.com](http://cryptography.com)). SCA attacks are non-invasive, easily automated, and can be mounted without knowing the design of the target device. Unlike invasive tampering, electromagnetic attacks can even be performed at a distance: attacks on cell phones have been demonstrated at a range of 30 feet. SCA countermeasures are needed to protect devices that use cryptographic keys, especially sensitive defense applications that require strong anti-tamper protection to defend advanced electronics from reverse engineering as well as commercial devices that perform content protection or payment processing, including mobile devices and IoT endpoints. The advanced countermeasures of the TeraFire SCA-resistant cores limit biases in both power consumption (protects against SPA/DPA/CPA) and electromagnetic emissions (protects against SEMA/DEMA), providing a safe environment for use of the cryptographic keys.

## About The Athena Group, Inc.

Athena is a leading provider of security, cryptography, anti-tamper, and signal processing IP cores to many of the world's largest semiconductor companies, defense contractors, and OEMs, as well as emerging providers. Embedded in millions of ASIC and FPGA devices, Athena technologies enable high-value solutions where security and performance are mission critical – defense and aerospace, vehicle safety (V2V, V2X, telematics), networking and communications, satellites, cellular base stations, handsets, the Internet of Things (IoT), and more.

Athena's innovative and experienced team architects best-in-class products: security microprocessors with unmatched hardware efficiency and programmable flexibility, dedicated accelerators for cryptography and security protocols, a comprehensive set of tamper-resistant security cores with SCA/DPA countermeasures developed under license from Rambus' Cryptography Research division, highly optimized FFTs and signal processing cores for communications applications, and related technologies. For more information, visit [athena-group.com](http://athena-group.com).





## Features

- **NEW- DPA/SCA Countermeasures**



- FIPS 180-2 compliant SHA
- SHA-1 and SHA2-224/256/384/512 support in product family
- Multi-Gbps performance
- Higher performance available
- Full-width message digest output
- Rapid context switching
- Microprocessor bus interfaces available
- SHA support also available in TeraFire F5200 cryptography microprocessor
- Portable to any Microsemi device
- Silicon proven
- Fast delivery
- Easy integration

## Benefits

- Full-width data ports maximize performance, minimize latency

## Support

- 12 months maintenance and support included

## Secure Hash Algorithm (SHA)

Athena delivers Secure Hash Algorithms (SHA) as semiconductor intellectual property (IP) cores. Whether your application demands high-performance cryptographic hashing or the power savings of a dedicated core, Athena's SHA cores deliver. Athena SHA cores are compliant with FIPS 180-4.

**Table 1: SHA Igloo2/SmartFusion2 Specifications<sup>a</sup>**

	SHA2-A300	SHA2-A400
SHA1	435 Mbps	915 Mbps
SHA2-224/256	525 Mbps	1,125 Mbps
SHA2-384/512	855 Mbps	930 Mbps
Area	7,300 LEs	9,100 LEs
Frequency	75 MHz	75 MHz

a. Other Microsemi device families supported.

## Product Description

Dedicated SHA family cores feature 32-bit and/or 64-bit data input ports and a full-width message digest output for maximum throughput and minimum latency. Input/output flow control simplifies system integration, and standard bus interfaces are available for applications that require bus connectivity. Context save and reload, automatic message padding, and HMAC features address a range of use cases. The members of the SHA family are summarized in Table 1. SHA support is also available in the EXP-F5200B cryptography microprocessor.

## 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.

## C Software for Host Processor

The TeraFire CAL-SYM is a portable, ANSI C library of drivers for TeraFire hardware accelerators. The TeraFire CAL-SYM has been implemented and tested on multiple platforms, including leading SoC microprocessors from ARM.

## Side Channel Attack Countermeasures

Side channel attacks are a class of attacks discovered by Rambus' Cryptography Research division (cryptography.com). SCA attacks are

## Applications

- Encrypted data storage
- Secure communications
- Secure processing
- IPsec acceleration
- E-commerce
- VPN
- Financial Transactions

## Available Deliverables

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



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)  
[ipsales@athena-group.com](mailto:ipsales@athena-group.com)

Copyright The Athena Group, Inc., 2017. 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.

The Athena logo, TeraFire name, and TeraFire logo are trademarks or registered trademarks of The Athena Group, Inc. All other trademarks, registered trademarks, and/or service marks are the property of their respective owners. Company, product, and service names used in this document are for identification purposes only.

non-invasive, easily automated, and can be mounted without knowing the design of the target device. Unlike invasive tampering, electromagnetic attacks can even be performed at a distance: attacks on cell phones have been demonstrated at a range of 30 feet. SCA countermeasures are needed to protect devices that use cryptographic keys, especially sensitive defense applications that require strong anti-tamper protection to defend advanced electronics from reverse engineering as well as commercial devices that perform content protection or payment processing, including mobile devices and IoT endpoints. The advanced countermeasures of the TeraFire SCA-resistant cores limit biases in both power consumption (protects against SPA/DPA/CPA) and electromagnetic emissions (protects against SEMA/DEMA), providing a safe environment for use of the cryptographic keys.

## About The Athena Group, Inc.

Athena is a leading provider of security, cryptography, anti-tamper, and signal processing IP cores to many of the world's largest semiconductor companies, defense contractors, and OEMs, as well as emerging providers. Embedded in millions of ASIC and FPGA devices, Athena technologies enable high-value solutions where security and performance are mission critical – defense and aerospace, vehicle safety (V2V, V2X, telematics), networking and communications, satellites, cellular base stations, handsets, the Internet of Things (IoT), and more.

Athena's innovative and experienced team architects best-in-class products: security microprocessors with unmatched hardware efficiency and programmable flexibility, dedicated accelerators for cryptography and security protocols, a comprehensive set of tamper-resistant security cores with SCA/DPA countermeasures developed under a Developer agreement with Rambus' Cryptography Research division, highly optimized FFTs and signal processing cores for communications applications, and related technologies. For more information, visit [athena-group.com](http://athena-group.com).



## Features

- ETSI compliant Kasumi, SNOW 3G, and ZUC cores
- High performance and low area
- Portable to any Microsemi device
- Easy integration into any design
- Silicon proven
- Fast delivery
- Microprocessor bus interfaces available

## Benefits

- Full-width data ports maximize performance, minimize latency

## Support

- 12 months maintenance and support included

## Applications

- 3G Telephony

## 3GPP Ciphers

### *Kasumi, SNOW, and ZUC 3G Ciphers for Telephony Applications*

**Athena delivers the 3GPP ciphers Kasumi, SNOW 3G, and ZUC as semiconductor intellectual property (IP) cores.** Athena's Kasumi, SNOW 3G, and ZUC cores for 3G telephony complement Athena's leading-edge TeraFire® public key (PK) cryptography accelerators. Whether your application demands 3GPP cipher performance or the power savings of a dedicated core, Athena's 3GPP cores are the ideal solution.

### Product Description

Athena's 3GPP cores all feature dedicated, full-width data input, output, and key input ports for maximum throughput and minimum latency. Standardized input and output handshaking simplifies system integration. All Athena 3GPP cores may be delivered with an optional microprocessor bus interface to simplify integration..

**Table 1: 3GPP Igloo2/SmartFusion2 Specifications<sup>a</sup>**

	KAS-A100	SNOW-A100	ZUC-A100
Performance	315 Mbps	3.2 Gbps	1.6 Gbps
Area	1,600 LEs	4,700 LEs	4,900 LEs
Frequency	45 MHz	100 MHz	55 MHz

a. Other Microsemi device families supported.

### 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.

### C Software for Host Processor

The TeraFire CAL-SYM is a portable, ANSI C library of drivers for TeraFire hardware accelerators. The TeraFire CAL-SYM has been implemented and tested on multiple platforms, including leading SoC microprocessors from ARM.

### About The Athena Group, Inc.

Athena is a leading provider of security, cryptography, anti-tamper, and signal processing IP cores to many of the world's largest semiconductor companies, defense contractors, and OEMs, as well as emerging provid-

---

## Available Deliverables

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

ers. Embedded in millions of ASIC and FPGA devices, Athena technologies enable high-value solutions where security and performance are mission critical – defense and aerospace, vehicle safety (V2V, V2X, telematics), networking and communications, satellites, cellular base stations, handsets, the Internet of Things (IoT), and more.

Athena's innovative and experienced team architects best-in-class products: security microprocessors with unmatched hardware efficiency and programmable flexibility, dedicated accelerators for cryptography and security protocols, a comprehensive set of tamper-resistant security cores with SCA/DPA countermeasures developed under a Developer agreement with Rambus' Cryptography Research division, highly optimized FFTs and signal processing cores for communications applications, and related technologies. For more information, visit [athena-group.com](http://athena-group.com).



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)  
[ipsales@athena-group.com](mailto:ipsales@athena-group.com)

Copyright The Athena Group, Inc., 2017. 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.

The Athena logo, TeraFire name, and TeraFire logo are trademarks or registered trademarks of The Athena Group, Inc. All other trademarks, registered trademarks, and/or service marks are the property of their respective owners. Company, product, and service names used in this document are for identification purposes only.

---

## ***Legacy Cores***



## Features

- FIPS 46-3/ANSI X9.52 compliant triple DES core
- Optional SP800-38A modes support (ECB, CBC, CFB, OFB, CTR)
- Supports key sizes of 56, 112, and 168-bits
- Portable to any Microsemi device
- Silicon proven
- Fast delivery
- Easy integration into any design
- Microprocessor bus interfaces available

## Benefits

- Full-width data ports maximize performance, minimize latency

## Applications

- Secure communications
- IPsec acceleration
- E-commerce
- VPN

## Support

- 12 months maintenance and support included

## Triple Data Encryption Standard (3DES)

Athena delivers the Triple Data Encryption Standard (3DES) as a semiconductor intellectual property (IP) core. Athena's 3DES-A100 3DES/DES core complements Athena's leading-edge TeraFire® public key (PK) cryptography accelerators. This dedicated 3DES solution provides both performance and power savings.

The 3DES-A100 is compliant with FIPS 46-3 and ANSI X9.52 and supports user programmable key sizes of 56, 112, and 168-bits.

### Product Description

The 3DES-A100 is a fully synchronous design and features dedicated, full-width data input, output, and key input ports for maximum throughput and minimum latency. A data valid output is provided to simplify retrieval of output data. The 3DES-A100 area starts at 6K LEs, and is available with an optional bus interface to simplify integration.

**Table 1: DES/3DES Igloo2/SmartFusion2 Specifications<sup>a</sup>**

	3DES-A100
Performance	117/360 Mbps
Area	6,500 LEs
Frequency	45 MHz

a. Other Microsemi device families supported.

### 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.

### C Software for Host Processor

The TeraFire CAL-SYM is a portable, ANSI C library of drivers for TeraFire hardware accelerators. The TeraFire CAL-SYM has been implemented and tested on multiple platforms, including leading SoC microprocessors from ARM.

### About The Athena Group, Inc.

Athena is a leading provider of security, cryptography, anti-tamper, and signal processing IP cores to many of the world's largest semiconductor companies, defense contractors, and OEMs, as well as emerging provid-



---

## Available Deliverables

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

ers. Embedded in millions of ASIC and FPGA devices, Athena technologies enable high-value solutions where security and performance are mission critical – defense and aerospace, vehicle safety (V2V, V2X, telematics), networking and communications, satellites, cellular base stations, handsets, the Internet of Things (IoT), and more.

Athena's innovative and experienced team architects best-in-class products: security microprocessors with unmatched hardware efficiency and programmable flexibility, dedicated accelerators for cryptography and security protocols, a comprehensive set of tamper-resistant security cores with SCA/DPA countermeasures developed under a Developer agreement with Rambus' Cryptography Research division, highly optimized FFTs and signal processing cores for communications applications, and related technologies. For more information, visit [athena-group.com](http://athena-group.com).



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)  
[ipsales@athena-group.com](mailto:ipsales@athena-group.com)

Copyright The Athena Group, Inc., 2017. 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.

The Athena logo, TeraFire name, and TeraFire logo are trademarks or registered trademarks of The Athena Group, Inc. All other trademarks, registered trademarks, and/or service marks are the property of their respective owners. Company, product, and service names used in this document are for identification purposes only.



## Features

- Implements ARC4 stream cipher
- Supports key sizes up to 256-bytes (2K-bits)
- Portable to any Microsemi device
- Easy integration into any design
- Silicon proven
- Fast delivery
- Microprocessor bus interfaces available

## Benefits

- Full-width data ports maximize performance, minimize latency

## Applications

- Encrypted data storage
- Secure communications

## Support

- 12 months maintenance and support included

## ARC4 Stream Cipher

**Athena delivers the ARC4 stream cipher as a semiconductor intellectual property (IP) core.** Athena's ARC4-A100 ARC4 core complements Athena's leading-edge TeraFire® public key cryptography accelerators. This dedicated ARC4 solution provides both high performance and power savings.

The ARC4-A100 core implements the ARC4 stream cipher and supports user definable maximum key sizes of up to 2K-bits.

### Product Description

The ARC4-A100 is a fully synchronous design and features dedicated, full-width data input, output, and key input ports for maximum throughput and minimum latency. A data valid output is provided to simplify retrieval of output data. The ARC4-A100 area starts at 1,500 LEs plus state and key memory and is available with an optional bus interface to simplify integration.

**Table 1: ARC4 Igloo2/SmartFusion2 Specifications<sup>a</sup>**

	ARC4-A100
Performance	312 Mbps
Area	1,500 LEs
Frequency	120 MHz

a. Other Microsemi device families supported.

### 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.

### C Software for Host Processor

The TeraFire CAL-SYM is a portable, ANSI C library of drivers for TeraFire hardware accelerators. The TeraFire CAL-SYM has been implemented and tested on multiple platforms, including leading SoC microprocessors from ARM.

### About The Athena Group, Inc.

Athena is a leading provider of security, cryptography, anti-tamper, and signal processing IP cores to many of the world's largest semiconductor

---

## Available Deliverables

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

companies, defense contractors, and OEMs, as well as emerging providers. Embedded in millions of ASIC and FPGA devices, Athena technologies enable high-value solutions where security and performance are mission critical – defense and aerospace, vehicle safety (V2V, V2X, telematics), networking and communications, satellites, cellular base stations, handsets, the Internet of Things (IoT), and more.

Athena's innovative and experienced team architects best-in-class products: security microprocessors with unmatched hardware efficiency and programmable flexibility, dedicated accelerators for cryptography and security protocols, a comprehensive set of tamper-resistant security cores with SCA/DPA countermeasures developed under a Developer agreement with Rambus' Cryptography Research division, highly optimized FFTs and signal processing cores for communications applications, and related technologies. For more information, visit [athena-group.com](http://athena-group.com).



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)  
[ipsales@athena-group.com](mailto:ipsales@athena-group.com)

Copyright The Athena Group, Inc., 2017. 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.

The Athena logo, TeraFire name, and TeraFire logo are trademarks or registered trademarks of The Athena Group, Inc. All other trademarks, registered trademarks, and/or service marks are the property of their respective owners. Company, product, and service names used in this document are for identification purposes only.



## Features

- RFC 1321 compliant MD5
- Performance >1 Gbps at 70 MHz
- Higher performance available
- 32-bit data input port
- Microprocessor bus interfaces available
- Portable to any Microsemi device
- Silicon proven
- Fast delivery
- Easy integration into any design

## Benefits

- Full-width data ports maximize performance, minimize latency

## Applications

- Encrypted data storage
- Secure processing
- E-commerce
- VPN
- Financial Transactions

## Support

- 12 months maintenance and support included

## Message Digest 5 (MD5)

**Athena delivers the Message Digest 5 (MD5) as a semiconductor intellectual property (IP) core.** Athena's MD5-A100 MD5 core complements Athena's leading-edge TeraFire® public key cryptography accelerators. Whether your application demands MD5 performance or the power savings of a dedicated core, Athena's MD5-A100 core delivers. The MD5-A100 is compliant with RFC 1321.

### Product Description

The MD5-A100 is a fully synchronous design that features a 32-bit data input port and full-width message digest output for maximum throughput and minimum latency. A data valid output is provided to simplify retrieval of the message digest.

The MD5-A100 may be delivered with an optional microprocessor bus interface to simplify integration.

**Table 1: MD5 Igloo2/SmartFusion2 Specifications<sup>a</sup>**

	MD5-A100
Performance	1.0 Gbps
Area	1,100 LEs
Frequency	70 MHz

a. Other Microsemi device families supported.

### 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.

### C Software for Host Processor

The TeraFire CAL-SYM is a portable, ANSI C library of drivers for TeraFire hardware accelerators. The TeraFire CAL-SYM has been implemented and tested on multiple platforms, including leading SoC microprocessors from ARM.

### About The Athena Group, Inc.

Athena is a leading provider of security, cryptography, anti-tamper, and signal processing IP cores to many of the world's largest semiconductor companies, defense contractors, and OEMs, as well as emerging provid-

---

## Available Deliverables

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

ers. Embedded in millions of ASIC and FPGA devices, Athena technologies enable high-value solutions where security and performance are mission critical – defense and aerospace, vehicle safety (V2V, V2X, telematics), networking and communications, satellites, cellular base stations, handsets, the Internet of Things (IoT), and more.

Athena's innovative and experienced team architects best-in-class products: security microprocessors with unmatched hardware efficiency and programmable flexibility, dedicated accelerators for cryptography and security protocols, a comprehensive set of tamper-resistant security cores with SCA/DPA countermeasures developed under a Developer agreement with Rambus' Cryptography Research division, highly optimized FFTs and signal processing cores for communications applications, and related technologies. For more information, visit [athena-group.com](http://athena-group.com).



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)  
[ipsales@athena-group.com](mailto:ipsales@athena-group.com)

Copyright The Athena Group, Inc., 2017. 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.

The Athena logo, TeraFire name, and TeraFire logo are trademarks or registered trademarks of The Athena Group, Inc. All other trademarks, registered trademarks, and/or service marks are the property of their respective owners. Company, product, and service names used in this document are for identification purposes only.

---

# ***Software, Firmware, and Interface***





## Features

- Software cryptography algorithm implementations
- Integrates with TeraFire CAL-PK and CAL-SYM drivers
- Sophisticated configuration management
- Simple/differential power analysis (SPA/DPA) resistance available

## Benefits

- Comprehensive algorithm support
- Integrates with C software drivers

## Applications

- Encrypted data storage
- Secure communications
- Secure processing
- SSL and IPsec acceleration
- E-commerce
- VPN
- Mobile platforms

## Support

- 12 months maintenance and support included

## TeraFire® Firmware Library

**Athena delivers a robust suite of firmware for TeraFire® 5200/6400 series processors.** The TeraFire Firmware Library is a set of cryptographic firmware, compiled for the Athena 5200/6400 instruction set, for use on Athena public key cryptography microprocessors. With support for every popular public key algorithm, the TeraFire Firmware Library provides a comprehensive solution for public key cryptography and Suite B cryptography, including TRNG when using the EXP-F5200 Embedded Cryptography Microprocessor. These functions are designed to execute without host processor intervention, thus providing a complete fire-and-forget cryptographic offload solution. The TeraFire Firmware Library integrates directly with the C Software Drivers (CAL-PK) running on a host processor.

**Table 1: TeraFire Firmware Library Members**

Name	Description	For Products
PKX-5200	Public Key Firmware	X5200/6400
DTX-5200	Direct Transfer I/F Packet Drivers Firmware	X5200/6400
AEX-5200	AES Firmware	F5200
SHX-5200	SHA Firmware	F5200
RNX-5200	SP800-90 DRBG Firmware	F5200
SBX-5200	Secure Boot Firmware	F5200
DEV-5200	X5200/6400 Firmware Development Tools	X5200/6400

### Public Key and Elliptic Curve Firmware

The PKX-5200 firmware implements the most requested public key and elliptic curve cryptography algorithms, including:

- Diffie-Hellman
- RSA encrypt
- RSA-CRT decrypt
- DSA sign and verify
- Modular exponentiation
- ECDSA sign and verify
- EC Diffie-Hellman with cofactor
- EC point multiplication
- EC point multiply and add

---

## Available Deliverables

- Compiled binaries
- Documentation

- EC point decompression
- EC point validation

### Direct Transfer Interface Packet Drivers Firmware

The DTX-5200 firmware enables operation of the X5200/6400 family of processors using packet-based protocol on the direct transfer interface, instead of a bus connection to an AHB or AXI bus.

### AES Firmware

The AEX-5200 firmware provides access to the following AES-based capabilities:

- AES encrypt and decrypt with ECB, CBC, CFB, OFB, and CTR modes
- AES authenticated encryption and decryption with AES-GCM
- GHASH
- AES key wrap and unwrap (KW)
- AES key wrap and unwrap with padding (KWP)

These AES-based capabilities support key sizes of 128-bits, 192-bits, and 256-bits.

### SHA Firmware

The SHX-5200 firmware provides access to the following capabilities:

- SHA computation
- HMAC-SHA computation

Both SHA and HMAC-SHA support partial message processing with context output and reload capabilities. Comprehensive support for SHA-1 and SHA-2 includes:

- SHA-1, SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, and SHA-512/256

### Random Number Generator Firmware

The RNX-5200 firmware implements a TRNG that conforms to the NIST SP800-90A DRBG standard. Functions include:

- RNG instantiate
- RNG reseed
- RNG generate
- RNG uninstantiate
- NRBG entropy output

The RNX-5200 functions include support for the following:



The Athena Group, Inc.  
408 W. University Ave.,  
Suite 306  
Gainesville, FL 32601

- SP800-90A CTR\_DRBG using AES
- security strengths of 128-bits and 256-bits
- personalization string input for instantiation
- prediction resistance option for instantiated DRBGs
- additional input for reseed and generation operations

### **Secure Boot Firmware**

The SBX-5200 enables secure boot memory validation using the EXP-F5200 with SHA option.

### **X5200/6400 Firmware Development Services and Tools**

For applications that require custom firmware for the X5200/6400 cryptography microprocessors, firmware development services, as well as tools, including an assembler and software simulator, are available.

### **C Software for Host Processor**

The TeraFire Cryptographic Application Libraries complement Athena's extensive family of cryptographic hardware accelerators by providing both a comprehensive library of software implementations of cryptographic algorithms and the drivers for TeraFire hardware accelerators.

### **Side Channel Attack Countermeasures**

Side channel attacks are a class of attacks discovered by Rambus' Cryptography Research division ([cryptography.com](http://cryptography.com)). SCA attacks are non-invasive, easily automated, and can be mounted without knowing the design of the target device. Unlike invasive tampering, electromagnetic attacks can even be performed at a distance: attacks on cell phones have been demonstrated at a range of 30 feet. SCA countermeasures are needed to protect devices that use cryptographic keys, especially sensitive defense applications that require strong anti-tamper protection to defend advanced electronics from reverse engineering as well as commercial devices that perform content protection or payment processing, including mobile devices and IoT endpoints. The advanced countermeasures of the TeraFire SCA-resistant cores limit biases in both power consumption (protects against SPA/DPA/CPA) and electromagnetic emissions (protects against SEMA/DEMA), providing a safe environment for use of the cryptographic keys.

### **About The Athena Group, Inc.**

Athena is a leading provider of security, cryptography, anti-tamper, and signal processing IP cores to many of the world's largest semiconductor companies, defense contractors, and OEMs, as well as emerging providers. Embedded in millions of ASIC and FPGA devices, Athena technologies enable high-value solutions where security and performance are mission critical – defense and aerospace, vehicle safety (V2V, V2X, telem-



The Athena Group, Inc.  
408 W. University Ave.,  
Suite 306  
Gainesville, FL 32601

---

atics), networking and communications, satellites, cellular base stations, handsets, the Internet of Things (IoT), and more.

Athena's innovative and experienced team architects best-in-class products: security microprocessors with unmatched hardware efficiency and programmable flexibility, dedicated accelerators for cryptography and security protocols, a comprehensive set of tamper-resistant security cores with SCA/DPA countermeasures developed under a Developer agreement with Rambus' Cryptography Research division, highly optimized FFTs and signal processing cores for communications applications, and related technologies. For more information, visit [athena-group.com](http://athena-group.com).



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)  
[ipsales@athena-group.com](mailto:ipsales@athena-group.com)

Copyright The Athena Group, Inc., 2017. 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.

The Athena logo, TeraFire name, and TeraFire logo are trademarks or registered trademarks of The Athena Group, Inc. All other trademarks, registered trademarks, and/or service marks are the property of their respective owners. Company, product, and service names used in this document are for identification purposes only.



## Features

- Portable ANSI C implementation
- Software cryptography algorithm implementations
- Drivers for TeraFire hardware accelerators
- Sophisticated configuration management

## Benefits

- Processor and operating system portable
- Same code base for target hardware and software development systems

## Applications

- Encrypted data storage
- Secure communications
- Secure processing
- SSL and IPsec acceleration
- E-commerce
- VPN
- Mobile platforms

## Support

- 12 months maintenance and support included

## Cryptographic Application Library

**Athena delivers a comprehensive suite of software to jump-start your development efforts.** The TeraFire® Cryptographic Application Library complements Athena's extensive family of cryptographic hardware accelerators by providing both a comprehensive library of software implementations of cryptographic algorithms and the drivers for TeraFire hardware accelerators. This allows you to choose the best combination of software and hardware implementations for your current product and protects your investment for your next application.

### Product Description

The TeraFire CAL-PK and CAL-SYM are portable libraries that provide a standard API to integrate and use TeraFire cryptographic hardware IP cores. The TeraFire CAL-SW provides software implementations of the same cryptographic algorithms and ciphers. Each CAL is implemented in ANSI C, is portable to virtually any application environment, and may even be used for host-based development to jump-start your software development efforts.

### CAL-PK

The TeraFire CAL-PK provides the API to the TeraFire family of public key microprocessors, executing the TeraFire Firmware Library to perform the most requested public key algorithms, including:

- RSA
- DSA
- Suite B Elliptic Curve, including ECDSA Sign and Verify
- Diffie-Hellman
- IEEE 1363-2000 ECSVDP

The EXP-F5200 with optional AES, SHA, and RNG capabilities, and TeraFire Firmware Library executables, is also operated using the CAL-PK API.

### CAL-SYM

The TeraFire CAL-SYM provides the API to the TeraFire family of symmetric key ciphers, accessed via an Athena Bus Interface Module (TAI-A100 or TXI-A100) to perform the following ciphers:

- AES with ECB, CBC, CFB, OFB, CTR, CCM, GCM, and XTS
- 3DES/DES with ECB, CBC, CFB, OFB, and CTR
- Kasumi with UEA1/f8
- SNOW 3G with UEA2

---

## Available Deliverables

- ANSI C Source
- Verification suite
- Documentation

- ZUC with 128-EEA3
- IEEE 1363a-2004 DL/ECIES

CAL-SYM also includes the API to access the following data integrity hashes and message authentication codes via the TAI-A100:

- AES with CMAC, CCM, GHASH, GMAC, and GCM
- SHA-1/224/256/384/512
- MD5
- HMAC
- XCBC MAC
- UIA1/f9 (Kasumi)
- UIA2 (SNOW 3G)
- (128-EIA3)(ZUC)

### **CAL-DRBG**

The TeraFire CAL-DRBG is a software implementation of the NIST SP800-90 AES-CTR DRBG function. Coupled with a hardware entropy source, such as an Athena NRBG composite ring oscillator module or some other source of entropy, the CAL-DRBG is a high quality true random number generator.

### **CAL-SW**

The TeraFire CAL-SW is a library of ANSI-C software implementations of the same algorithms supported in hardware via CAL-PK and CAL-SYM, namely:

#### ***Public Key***

- RSA
- DSA
- Suite B Elliptic Curve, including ECDSA Sign and Verify
- Diffie-Hellman
- IEEE 1363-2000 ECSVDP

#### ***Ciphers***

- AES with ECB, CBC, CFB, OFB, CTR, CCM, GCM, and XTS
- 3DES/DES with ECB, CBC, CFB, OFB, and CTR
- Kasumi with UEA1/f8
- SNOW 3G with UEA2
- ZUC with 128-EEA3
- IEEE 1363a-2004 DL/ECIES

#### ***Data Integrity Hashes and Message Authentication Codes***

- AES with CMAC, CCM, GHASH, and GCM
- SHA-1/224/256/384/512
- MD5
- HMAC



The Athena Group, Inc.  
408 W. University Ave.,  
Suite 306  
Gainesville, FL 32601



- XCBC MAC
- UIA1/f9 (Kasumi)
- UIA2 (SNOW 3G)
- 128-EIA3 (ZUC)

### **Implementation**

The TeraFire CAL-PK, CAL-SYM, CAL-DRBG, and CAL-SW have been implemented and tested on multiple platforms, including leading microprocessors from ARM.

### **TeraFire Firmware Library**

The TeraFire Firmware Library is a set of cryptographic algorithms and embedded firmware, compiled for the Athena 5200/6400 instruction set, for use on Athena public key cryptography microprocessors. With support for every popular public key algorithm, the TeraFire Firmware Library provides a comprehensive solution for public key cryptography and Suite B cryptography including TRNG when using the EXP-F5200 Embedded Cryptography Microprocessor. These functions are designed to execute without host processor intervention, thus providing a complete fire-and-forget cryptographic offload solution. The TeraFire firmware Library integrates directly with the C Software Drivers (CAL-PK) running on a host processor.

### **Side Channel Attack Countermeasures**

Side channel attacks are a class of attacks discovered by Rambus' Cryptography Research division ([cryptography.com](http://cryptography.com)). SCA attacks are non-invasive, easily automated, and can be mounted without knowing the design of the target device. Unlike invasive tampering, electromagnetic attacks can even be performed at a distance: attacks on cell phones have been demonstrated at a range of 30 feet. SCA countermeasures are needed to protect devices that use cryptographic keys, especially sensitive defense applications that require strong anti-tamper protection to defend advanced electronics from reverse engineering as well as commercial devices that perform content protection or payment processing, including mobile devices and IoT endpoints. The advanced countermeasures of the TeraFire SCA-resistant cores limit biases in both power consumption (protects against SPA/DPA/CPA) and electromagnetic emissions (protects against SEMA/DEMA), providing a safe environment for use of the cryptographic keys.

### **About The Athena Group, Inc.**

Athena is a leading provider of security, cryptography, anti-tamper, and signal processing IP cores to many of the world's largest semiconductor companies, defense contractors, and OEMs, as well as emerging providers. Embedded in millions of ASIC and FPGA devices, Athena technologies enable high-value solutions where security and performance are mission critical – defense and aerospace, vehicle safety (V2V, V2X, telem-



The Athena Group, Inc.  
408 W. University Ave.,  
Suite 306  
Gainesville, FL 32601

---

atics), networking and communications, satellites, cellular base stations, handsets, the Internet of Things (IoT), and more.

Athena's innovative and experienced team architects best-in-class products: security microprocessors with unmatched hardware efficiency and programmable flexibility, dedicated accelerators for cryptography and security protocols, a comprehensive set of tamper-resistant security cores with SCA/DPA countermeasures developed under a Developer agreement with Rambus' Cryptography Research division, highly optimized FFTs and signal processing cores for communications applications, and related technologies. For more information, visit [athena-group.com](http://athena-group.com).



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)  
[ipsales@athena-group.com](mailto:ipsales@athena-group.com)

Copyright The Athena Group, Inc., 2017. 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.

The Athena logo, TeraFire name, and TeraFire logo are trademarks or registered trademarks of The Athena Group, Inc. All other trademarks, registered trademarks, and/or service marks are the property of their respective owners. Company, product, and service names used in this document are for identification purposes only.



## Features

- Plug and play integration
- Supports all Athena TeraFire cores
- Designed for TeraFire CAL-SYM drivers
- Modular architecture
- Other microprocessor bus interfaces available
- Easy integration

## Benefits

- Modular architecture enables scalable performance and optimal implementation
- Full-width data ports to hosted TeraFire cores maximize performance, minimize latency

## Support

- 12 months maintenance and support included

## Applications

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

## AHB/AXI Bus Interfaces

**Athena delivers the AHB and AXI bus interface modules for Athena TeraFire cores.** Athena's AHB and AXI bus interfaces have a modular, socketized architecture that supports all Athena cipher and hashing cores, including AES, SHA, 3GPP, 3DES, MD5, ARC4, and TRNGs. With optional C-software drivers for your host processor, integration of Athena TeraFire cores is as simple as plug and play.

**Table 1: Bus Interface Product Family Elements**

Model Base	Description	Supported Cores
TAI-A100	AHB Bus Interface	AES-A100/A200/A300 SHA2-A100/A200/A300/A400 Kasumi, SNOW, ZUC RNG-A100/A200 3DES-A100 MD5-A00, ARC4-A100
TXI-A100	AXI Bus Interface	AES-A100/A200/A300 SHA2-A100/A200/A300/A400 Kasumi, SNOW, ZUC RNG-A100/A200 3DES-A100 MD5-A00, ARC4-A100

Each bus interface module connects directly to its respective system bus, while the Athena TeraFire cores connect to device-specific sockets on the bus interface module. A single AHB/AXI bus interface core can simultaneously host the entire suite of Athena TeraFire cores as memory-mapped slaves. FIFO interfaces to each of the TeraFire cores allow data buffering and can be configured to any depth.

### C Software for Host Processor

The TeraFire CAL-SYM is a portable, ANSI C library of drivers for TeraFire hardware accelerators. The TeraFire CAL-SYM has been implemented and tested on multiple platforms, including leading SoC microprocessors from ARM.

### Designed for Easy Integration

Athena has over a decade of experience in achieving first-time physical design success by always delivering a complete core – synthesized into your target library, in your process, with your constraints, ready for place and route.

---

## Available Deliverables

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

## About The Athena Group, Inc.

Athena is a leading provider of security, cryptography, anti-tamper, and signal processing IP cores to many of the world's largest semiconductor companies, defense contractors, and OEMs, as well as emerging providers. Embedded in millions of ASIC and FPGA devices, Athena technologies enable high-value solutions where security and performance are mission critical – defense and aerospace, vehicle safety (V2V, V2X, telematics), networking and communications, satellites, cellular base stations, handsets, the Internet of Things (IoT), and more.

Athena's innovative and experienced team architects best-in-class products: security microprocessors with unmatched hardware efficiency and programmable flexibility, dedicated accelerators for cryptography and security protocols, a comprehensive set of tamper-resistant security cores with SCA/DPA countermeasures developed under a Developer agreement with Rambus' Cryptography Research division, highly optimized FFTs and signal processing cores for communications applications, and related technologies. For more information, visit [athena-group.com](http://athena-group.com).



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)  
[ipsales@athena-group.com](mailto:ipsales@athena-group.com)

Copyright The Athena Group, Inc., 2017. 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.

The Athena logo, TeraFire name, and TeraFire logo are trademarks or registered trademarks of The Athena Group, Inc. All other trademarks, registered trademarks, and/or service marks are the property of their respective owners. Company, product, and service names used in this document are for identification purposes only.