TeraFire®

Cryptography and Security IP Products For Altera FPGAs

Revision 2.7
February 2017

ATHENA

THE ATHENA GROUP

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
www.athena-group.com

Table of Contents

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 Altera 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 Altera 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 Altera device family, including Cyclone, Arria, and Stratix. 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).

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

Table 1: TeraFire Security IP Cores for Altera

Model	Description
Dragon-QT	Embedded Hardware Root of Trust
SPaRC	Secure Partial Reconfiguration Controller
InCipher-DPA	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' 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.

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

Phone: (352) 371-2567
Toll-free: (800) 741-7440
Fax: (352) 373-5182
www.athena-group.com
ipsales@athena-group.com

TeraFire® Cryptographic Security with Side Channel Attack (SCA) Countermeasures

Features

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

Athena delivers a comprehensive suite of security IP with SCA Protection, ready for your Altera 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. Vulnerable devices include smart phones, IoT endpoints, any device with access to banking (smart cards, smart 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, GHASH, and

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).

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

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 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-

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

tiple 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 Altera device family, including Cyclone, Stratix and Arria.

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.

ATHENA
THE ATHENA GROUP

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

Phone: (352) 371-2567
Toll-free: (800) 741-7440
Fax: (352) 373-5182
www.athena-group.com
ipsales@athena-group.com

Hardware Root of Trust

PRODUCT BRIEF

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

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 Intrinisic-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 device-dependent unique PUF. Quiddikey-Flex makes use of the unique a 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.

Benefits

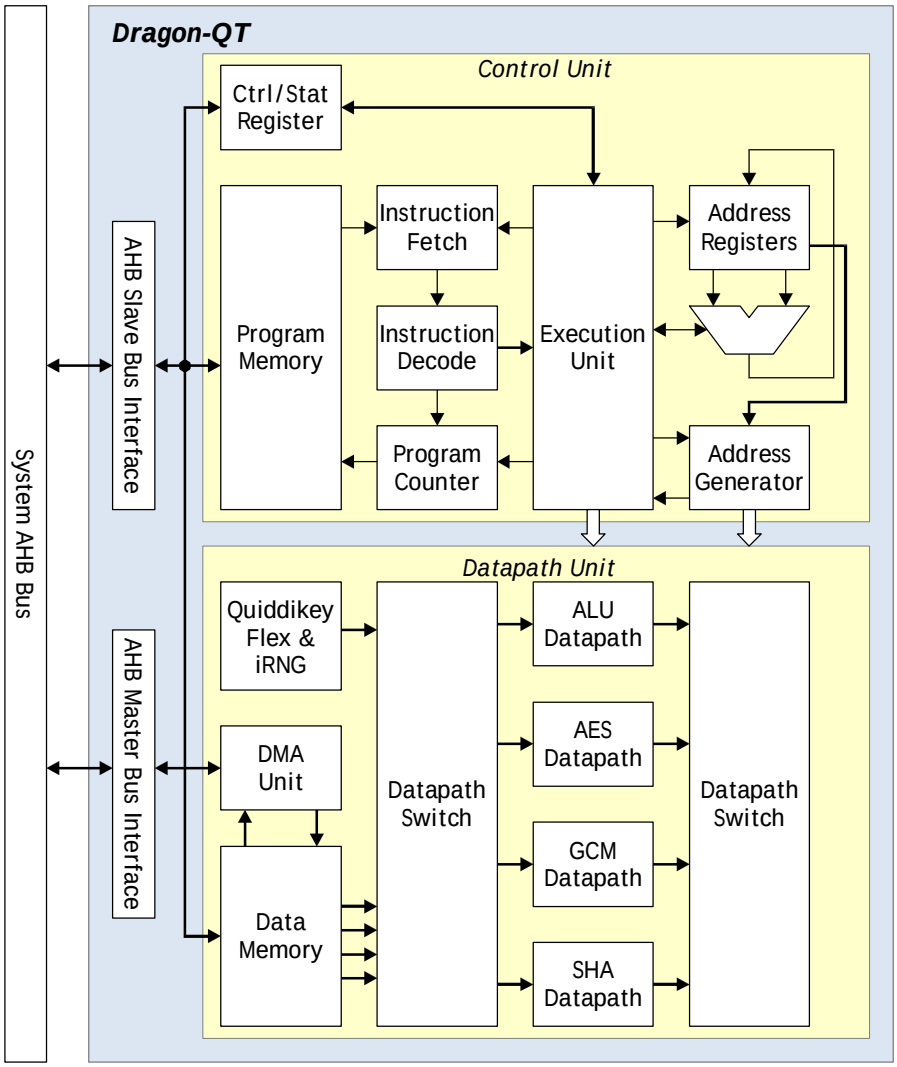
- Superior anti-tamper and anti-cloning protection based on Hardware Intrinsic Security™
- Invasively reading out a memory will not reveal information about the key
- Tampering with the memory will not reveal the key
- No key present at power-off in the system
- SCA/DPA countermeasures protect keys while 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)
- Mobile
- Defense



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

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

Table 1: Dragon-QT Performance[a,b]

Operation	op/s	latency
Key Reconstruction	2000	500 µs
RSA-1024 Private Key	132	7.6 ms
RSA-2048 Private Key	19	52 ms
RSA-3072 Private Key	5.7	174 ms
256-bit ECDSA Sign	102	9.7 ms
256-bit ECDSA Verify	89	11.3 ms
384-bit ECDSA Sign	36	27.3 ms
384-bit ECDSA Verify	31	62.6 ms

a. Performance characterized at 220 MHz operating frequency for Stratix V.
b. Refer to the Athena TeraFire F5200 Product Brief for additional performance data.

Table 2: Dragon-QT Options[a,b]

Operation	Throughput
AES	300 Mbps
SHA	390 Mbps
SP800-90 DRBG	100 Mbps

a. Performance characterized at 220 MHz operating frequency for Stratix V.
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'

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 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.

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

Phone: (352) 371-2567
Toll-free: (800) 741-7440
Fax: (352) 373-5182
www.athena-group.com
ipsales@athena-group.com

Anti-Tamper Technologies

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.

Features

- ***NEW- DPA/SCA Countermeasures***
- Secure external memory random access using encryption and authentication
- Protects virtually any standard external memory: DDR*n*, 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

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-

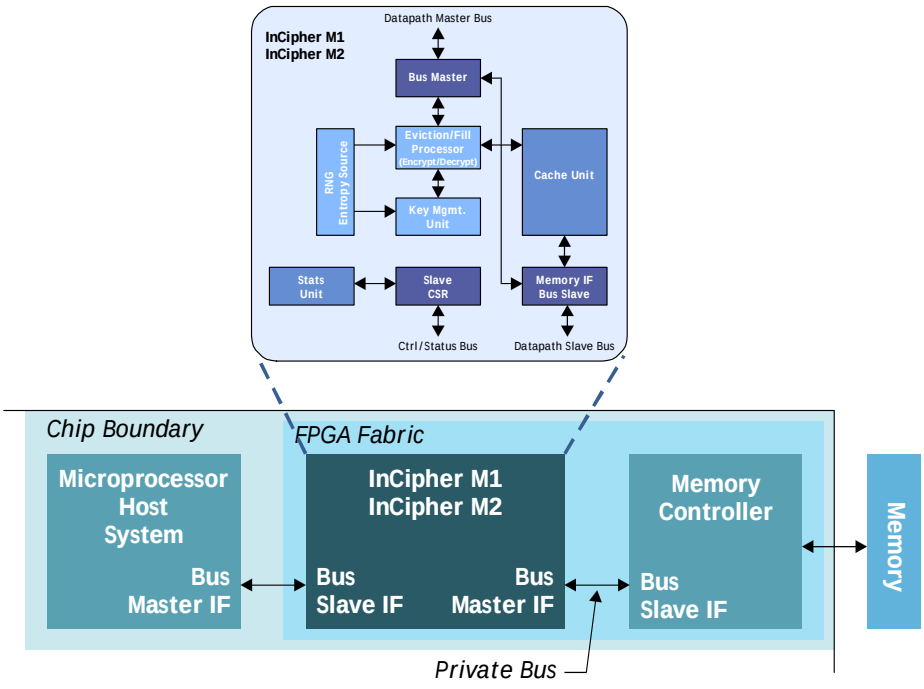


Figure 1: InCipher M1/M2 Inline Memory Encryptor Application

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
ipsales@athena-group.com

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 microcontrollers to the latest full-featured microprocessors running in multicore configurations.

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.

Cryptography Microprocessors

PRODUCT BRIEF

TERAFIRE®

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 Altera 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

Support

- 12 months maintenance and support included

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 Altera device.

Table 1: TeraFire® 5200 Series Performance[a]

Operation	Cyclone V		Stratix V	
	Op/s	Latency	Op/s	Latency
RSA-1024 Private Key	758	1.3 ms	1,788	559 µs
RSA-1024 Private Key (Paired Cores)	1516	650 µs	3,576	279 µs
1024-bit Expo w/ 1024-bit Expo.	150	6.7 ms	353	2.83 ms
1024-bit DSA Sign	861	1.2 ms	2,032	492 µs
1024-bit DSA Verify	437	2.3 ms	1,031	970 µs
RSA-2048 Private Key	76	13.1 ms	180	5.56 ms
RSA-2048 Private Key (Paired Cores)	152	6.5 ms	360	2.78 ms
2048-bit Expo w/ 2048-bit Expo.	25.7	39 ms	60.5	16.5 ms
2048-bit DSA Sign	217	4.6 ms	511	1.95 ms
2048-bit DSA Verify	114	8.7 ms	269	3.70 ms
RSA-3072 Private Key	27.3	36.6 ms	64.4	15.5 ms
RSA-3072 Private Key (Paired Cores)	54.6	18.3 ms	128	7.75 ms
NIST P-256 EC Point Multiply	335	2.98 ms	792	1.26 ms
NIST P-256 ECDSA Sign	305	3.28 ms	719	1.39 ms
NIST P-256 ECDSA Verify	263	3.79 ms	621	1.61 ms
NIST P-384 EC Point Multiply	168	5.95 ms	312	3.20 ms
NIST P-384 ECDSA Sign	155	6.43 ms	366	2.73 ms
NIST P-384 ECDSA Verify	131	7.59 ms	310	3.22 ms
521-bit EC Point Multiply	34.2	29.3 ms	80.6	12.4 ms
Area (ALUTs)	10,696		11,767	
Frequency	81 MHz		191 MHz	

a. Other Altera device families supported. Contact Athena for more information.

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

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

Table 2: TeraFire E5200 Non-NIST P-Curve ECC Performance[a]

Operation	Cyclone V		Stratix V	
	Op/s	Latency	Op/s	Latency
256-bit EC Point Multiply	100	9.9 ms	237	4.2 ms
256-bit ECDSA Sign	97.7	10.2 ms	230	4.3 ms
256-bit ECDSA Verify	83.3	12.0 ms	196	5.1 ms
384-bit EC Point Multiply	56.7	17.6 ms	133	7.5 ms
384-bit ECDSA Sign	55.1	18.1 ms	130	7.7 ms
384-bit ECDSA Verify	46.2	21.6 ms	109	9.2 ms
Frequency	81 MHz		191 MHz	

a. Other Altera device families supported. Contact Athena for more information.

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).

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.

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

Phone: (352) 371-2567
Toll-free: (800) 741-7440
Fax: (352) 373-5182
www.athena-group.com
ipsales@athena-group.com

PRODUCT BRIEF

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 ~2,700 ALUT's and over 100 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.

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 Altera 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

Table 1: TeraFire F5200 Performance[a]

Operation	Cyclone V		Stratix V	
	Op/s	Latency	Op/s	Latency
RSA-1024 Private Key	66	15.2 ms	132	7.6 ms
RSA-1024 Private Key (Paired Cores)	132	7.6 ms	264	3.8 ms
1024-bit Expo w/ 1024-bit Exponent	18.6	53.7 ms	37.2	26.9 ms
1024-bit DSA Sign	122	8.1 ms	245	4.1 ms
1024-bit DSA Verify	57.9	17.3 ms	115	8.6 ms
RSA-2048 Private Key	9.5	105 ms	19.1	52.4 ms
RSA-2048 Private Key (Paired Cores)	19	52.4 ms	38.2	26.2 ms
2048-bit Expo w/ 2048-bit Exponent	2.5	404 ms	5.0	201 ms
2048-bit DSA Sign	21.8	45.9 ms	43.5	23 ms
2048-bit DSA Verify	11.2	89 ms	22.5	44.5 ms
RSA-3072 Private Key	2.9	348 ms	5.7	174 ms
RSA-3072 Private Key w/ Paired Cores	5.8	174 ms	11.4	87 ms
256-bit EC Point Multiply	55.4	18.1 ms	110	9.0ms
256-bit ECDSA Sign	51.4	19.5 ms	102	9.7 ms
256-bit ECDSA Verify	44.4	22.5 ms	88.8	11.3 ms
384-bit EC Point Multiply	19.9	50.3 ms	39.7	25.2 ms
384-bit ECDSA Sign	18.3	54.6 ms	36.7	27.3 ms
384-bit ECDSA Verify	15.7	63.8 ms	31.3	31.9 ms
521-bit EC Point Multiply	8.0	125 ms	16	62.6 ms
Area (ALUTs)	2831		2742	
Frequency	110 MHz		220 MHz	

a. Other Altera device families supported. Contact Athena for more information.

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

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

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[a]

Operation	Cyclone V		Stratix V	
	Perf.	Area	Perf.	Area
AES	150 Mbps	889	300 Mbps	860
GCM	150 Mbps	476	300 Mbps	503
SHA	195 Mbps	1238	390 Mbps	1239
SP800-90 DRBG	50 Mbps	688	100 Mbps	688

a. Area (ALUTs) in addition to base F5200 core, for each feature. Other Altera device families supported. Contact Athena for more information.

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

- 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.

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

Phone: (352) 371-2567
Toll-free: (800) 741-7440
Fax: (352) 373-5182
www.athena-group.com
ipsales@athena-group.com

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 5× over Athena's E5200.

Features

- ***NEW- DPA/SCA Countermeasures***
- NIST P-Curve Support
- Brainpool Curve Support with the -P (programmable) option
- Portable to any Altera 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

Support

- 12 months maintenance and support included

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-singlular 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 Stratix V Specifications[a]

Operation	EC Ultra 2K	EC Ultra 8K
NIST P-256 EC Point Multiply	1,300 ops/s	5,500 ops/s
NIST P-256 ECDSA Sign	1,200 ops/s	5,000 ops/s
NIST P-256 ECDSA Verify	1,000 ops/s	4,100 ops/s
NIST P-384 EC Point Multiply	850 ops/s	3,600 ops/s
NIST P-384 ECDSA Sign	800 ops/s	3,300 ops/s
NIST P-384 ECDSA Verify	700 ops/s	2,700 ops/s
Area (P-256 curve only)	4,100 ALUTs 10 DSPs	11,500 ALUTs 30 DSPs
Area (Both P-256 and P-384 Curves)	5,900 ALUTs 15 DSPs	13,600 ALUTs 45 DSPs
Frequency	270 MHz	270 MHz

a. Other Altera device families supported.

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

Table 2: TeraFire® EC Ultra Cyclone V Specifications[a]

Operation	EC Ultra 2K	EC Ultra 8K
NIST P-256 EC Point Multiply	800 ops/s	3,300 ops/s
NIST P-256 ECDSA Sign	700 ops/s	3,000 ops/s
NIST P-256 ECDSA Verify	600 ops/s	2,400 ops/s
NIST P-384 EC Point Multiply	500 ops/s	2,300 ops/s
NIST P-384 ECDSA Sign	450 ops/s	2,200 ops/s
NIST P-384 ECDSA Verify	400 ops/s	1,700 ops/s
Area (P-256 curve only)	3,500 ALUTs 10 DSPs	9,100 ALUTs 30 DSPs
Area (Both P-256 and P-384 Curves)	4,800 ALUTs 15 DSPs	10,800 ALUTs 45 DSPs
Frequency	160 MHz	160 MHz

a. Other Altera 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 Athena 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). 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.

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

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.

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

Phone: (352) 371-2567
Toll-free: (800) 741-7440
Fax: (352) 373-5182
www.athena-group.com
ipsales@athena-group.com

True Random Number Generators

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 Performance[a]

RNG-A100	Cyclone V	Stratix V
Area (ALUTs)	5859	5861
Output Rate	115 Mbps	180 Mbps
Frequency	231 MHz	361 MHz

a. Other Altera device families supported. Contact Athena for more information.

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.

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 Altera 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)

- 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.

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

Phone: (352) 371-2567
Toll-free: (800) 741-7440
Fax: (352) 373-5182
www.athena-group.com
ipsales@athena-group.com

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.

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 Altera device
- Simple/differential power analysis (SPA/DPA) resistance available

Applications

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

Table 1: RNG-A200 Cyclone V Specifications[a]

	RNG-A200-AES1	RNG-A200-AES2	NRBG-A100
Output Rate	1.15 Gbps	350 Mbps	Custom
Area	11,000 ALUTs	10,100 ALUTs	500 ALUTs
Frequency	150 MHz	150 MHz	200 MHz
Strength	128-256b	128-256b	128-256b

a. Other Altera device families supported.

Table 2: RNG-A200 Stratix V Specifications[a]

	RNG-A200-AES1	RNG-A200-AES2	NRBG-A100
Output Rate	1.9 Gbps	580 Mbps	Custom
Area	11,000 ALUTs	10,100 ALUTs	500 ALUTs
Frequency	250 MHz	250 MHz	200 MHz
Strength	128-256b	128-256b	128-256b

a. Other Altera 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

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

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.

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'

ATHENA
THE ATHENA GROUP
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.

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

Phone: (352) 371-2567
Toll-free: (800) 741-7440
Fax: (352) 373-5182
www.athena-group.com
ipsales@athena-group.com

Ciphers and Hashing

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® 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.

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 Altera 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

Table 1: AES Cyclone V Specifications[a]

	AES-A500	AES-A100	AES-A200
Throughput	3.2 Gbps	1.7 Gbps	400 Mbps
Area	1,300 ALUTs	640 ALUTs	550 ALUTs
Frequency	150 MHz	150 MHz	145 MHz

a. Other Altera device families supported. Contact Athena for more information.

Table 2: AES Stratix V Specifications[a]

	AES-A500	AES-A100	AES-A200
Throughput	6.4 Gbps	3.2 Gbps	800 Mbps
Area	1,300 ALUTs	640 ALUTs	550 ALUTs
Frequency	270 MHz	270 MHz	300 MHz

a. Other Altera device families supported. Contact Athena for more information.

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.

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

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 SP800-38F (Key Wrapping)
- Suite B
- IEEE 802.1ae
- IEEE 802.11i
- 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). 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.

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

Phone: (352) 371-2567
Toll-free: (800) 741-7440
Fax: (352) 373-5182
www.athena-group.com
ipsales@athena-group.com

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 Cyclone V Specifications[a]

	SHA2-A300	SHA2-A400
SHA1	700 Mbps	1.4 Gbps
SHA2-224/256	840 Mbps	1.8 Gbps
SHA2-384/512	1.3 Gbps	1.5 Gbps
Area	1,050 ALUTs	TBD
Frequency	120 MHz	120 MHz

a. Other Altera device families supported.

Table 2: SHA Stratix V Specifications[a]

	SHA2-A300	SHA2-A400
SHA1	1.1 Gbps	2.4 Gbps
SHA2-224/256	1.4 Gbps	3.0 Gbps
SHA2-384/512	2.3 Gbps	2.5 Gbps
Area	1,050 ALUTs	TBD
Frequency	200 MHz	200 MHz

a. Other Altera 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 perfor-

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 Altera device
- Silicon proven
- Fast delivery
- Easy integration

Benefits

- Full-width data ports 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

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
ipsales@athena-group.com

mance 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 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.

Software, Firmware, and Interface

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

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

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:

ATHENA THE ATHENA GROUP
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). 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-

ATHENA
THE ATHENA GROUP
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.

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

Phone: (352) 371-2567
Toll-free: (800) 741-7440
Fax: (352) 373-5182
www.athena-group.com
ipsales@athena-group.com

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.

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

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/*f*9 (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

ATHENA THE ATHENA GROUP
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). 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-

ATHENA
THE ATHENA GROUP
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.

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

Phone: (352) 371-2567
Toll-free: (800) 741-7440
Fax: (352) 373-5182
www.athena-group.com
ipsales@athena-group.com

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.

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

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.

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

Phone: (352) 371-2567
Toll-free: (800) 741-7440
Fax: (352) 373-5182
www.athena-group.com
ipsales@athena-group.com