

Features

- 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
- X5200 Library supports multiple public key cryptography algorithms
- Implements Athena's powerful X5200 instruction set architecture
- Scalable for your application's area and performance needs
- Suitable for virtually any implementation technology
- AMBA™ AHB and AXI bus interfaces available
- Simple/differential power analysis (SPA/DPA) resistance available

Benefits

- Family of compatible products optimized for speed and area supports your product succession strategy
- Programmability enables adaptability to future public key standards



E5200 Elliptic Curve Cryptography Microprocessor

From the market leader in public key cryptography cores comes the E5200 series. The E5200 provides leading elliptic curve cryptography performance while maintaining full backwards compatibility with the flagship T5200 public key cryptography microprocessor. Athena's patented arithmetic technology delivers the performance your solution needs - low latency *and* high throughput, in an area efficient package.

Product Description

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.

Table 1: Sample Terafire E5200 Characteristics^a

Operation	E5211 ^b		E5221 ^c	
	op/s	latency	op/s	latency
160-bit EC Point Multiply	2765	362 μ s	2765	362 μ s
192-bit EC Point Multiply	2201	454 μ s	2201	454 μ s
256-bit EC Point Multiply	1727	580 μ s	1727	580 μ s
NIST P-256 EC Point Multiply	2990	334 μ s	2990	334 μ s
384-bit EC Point Multiply	1087	920 μ s	1087	920 μ s
NIST P-384 EC Point Multiply	1513	661 μ s	1513	661 μ s
521-bit EC Point Multiply	648	1.5 ms	648	1.5 ms
RSA-1024 Private Key	4941	202 μ s	4941	202 μ s
RSA-1024 Private Key w/ Paired Cores ^d	9843	102 μ s	9843	102 μ s
1024-bit Expo w/ 1024-bit Exponent	947	1.1 ms	2847	351 μ s

- Autonomous operation minimizes load on host processor

Applications

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

Available Deliverables

- Targeted, timing closed netlist
- Simulation model (Verilog or VHDL)
- Verification suite
- X5200 Library
- TeraFire CAL
- Assembler and Software Simulator
- Documentation
- Support

Table 1: Sample Terafire E5200 Characteristics^a (Continued)

Operation	E5211 ^b		E5221 ^c	
	op/s	latency	op/s	latency
RSA-2048 Private Key	481	2.1 ms	1430	699 μ s
RSA-2048 Private Key w/ Paired Cores ^d	947	1.1 ms	2841	352 μ s
2048-bit Expo w/ 2048-bit Exponent	160	6.2 ms	260	3.8 ms
1024-bit Expo ($e=2^{16}+1$)	78.1K	12.8 μ s	178K	5.6 μ s
Area (K-gates) (not including memory)	194		306	

- Performance characterized at 500 MHz operating frequency.
- Optimized for operations up to 544-bits, including up to RSA-1088 w/ CRT.
- Optimized for operations up to 1024-bits, including up to RSA-2048 w/ CRT.
- RSA with CRT operations using paired cores require two E5200 family core instances operating in parallel.

The E5200 provides up to four times faster elliptic curve cryptography performance than Athena's own T5200. Like the T5200, the E5200 can perform virtually any public key operation and easily accommodate new standards with on-the-fly programmability. Since the maximum operation size for any E5200 implementation is determined solely by the populated memory size, the implementation performance, capabilities, and area can be optimized to meet your requirements.

X5200 Library

The X5200 Library implements high-level algorithms, such as RSA with CRT, and elliptic curve operations, such as point multiply and EC-DSA sign and verify, in native X5200 assembly language. These functions are designed to execute without host processor intervention, thus providing a complete fire-and-forget cryptographic offload solution for your application. The X5200 Library is packaged with the TeraFire CAL when purchased with an X5200 family core product. Optional X5200 development tools are also available.

TeraFire Cryptography Application Library (CAL)

The TeraFire CAL is a portable, ANSI C library of cryptographic software implementations and drivers for TeraFire hardware accelerators, and it includes the X5200 Library assembly code. The TeraFire CAL has been implemented and tested on multiple platforms, including leading SoC microprocessors from ARM. Athena's sophisticated configuration management system enables rapid configuration of the TeraFire CAL for your mix of hardware accelerator and software implementation requirements.

Designed for Easy Integration

Athena has over a decade of experience in delivering first-time physical design success. Athena has become a premier provider of semiconductor IP by always delivering quality. To ensure ease of integration, Athena goes the distance - by synthesizing *our* IP into *your* target library, in *your* process, with *your* constraints, and delivering a completed core, ready for

place and route. Athena standard deliverables include everything you need to integrate our core into your design: netlists, simulation models, test vectors, support, and documentation.

About The Athena Group, Inc.

The Athena Group, Inc. of Gainesville, Florida licenses high performance technology that delivers breakthrough performance, reduced area, and lower power consumption in a broad range of SoC products. Athena's proprietary technology powers leading edge applications such as secure e-commerce, wireless communications, and video compression. In addition to high-value application level solutions, Athena also produces a full line of fundamental DSP functions suitable for SoC integration.

Athena was founded in 1986 and is privately held.



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

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

Copyright The Athena Group, Inc., 2011. All rights reserved. Reproduction in whole or in part is prohibited without the prior written consent of the copyright owner. The information presented in this document does not form part of any quotation or contract, is believed to be accurate and reliable, and may be changed without notice. No liability will be accepted by the publisher for any consequence of its use. Publication thereof does not convey nor imply any license under patent or other industrial or intellectual property rights.