



## TeraFire E5200 Elliptic Curve Cryptography Microprocessor

**From the 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 E5200 augments Athena's proprietary public key instruction set architecture with enhanced performance elliptic curve instructions that accelerate all odd characteristic operations, and provide additional performance for Suite B P-curve operations. Multiple models are available, optimized for operations from 512-bits (E5211), 1024-bits (E5221), or more (see Table 1).

**Table 1: Sample Terafire E5200 Characteristics**

Operation	E5211		E5221	
	op/s	latency	op/s	latency
160-bit EC Point Multiply	2211	452 $\mu$ s	2211	452 $\mu$ s
192-bit EC Point Multiply	1761	568 $\mu$ s	1761	568 $\mu$ s
256-bit EC Point Multiply	1381	724 $\mu$ s	1381	724 $\mu$ s
NIST P-256 EC Point Multiply	2393	418 $\mu$ s	2393	418 $\mu$ s
384-bit EC Point Multiply	868	1.15 ms	868	1.15 ms
NIST P-384 EC Point Multiply	1211	826 $\mu$ s	1211	826 $\mu$ s
521-bit EC Point Multiply	519	1.93 ms	519	1.93 ms
RSA-1024 Private Key	3947	253 $\mu$ s	3947	253 $\mu$ s
RSA-1024 Private Key w/ Paired Cores	7893	127 $\mu$ s	7893	127 $\mu$ s
1024-bit Full Expo	760	1.32 ms	2280	439 $\mu$ s
RSA-2048 Private Key	379	2.6 ms	1144	874 $\mu$ s
RSA-2048 Private Key w/ Paired Cores	757	1.32 ms	2275	440 $\mu$ s
2048-bit Full Expo	128	7.8 ms	207	4.8 ms
1024-bit Expo/s ( $e=2^{16}+1$ )	61.2K	16 $\mu$ s	145K	7 $\mu$ s
Area (K-gates) (not including memory)	194		306	

### 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
- T5200 Application Library supports multiple public key cryptography algorithms
- Implements Athena's powerful T5200 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

### Benefits

- Family of compatible products optimized for speed and area supports your product succession strategy
- Programmability enables adaptability to future public key standards
- Autonomous operation minimizes load on host processor

---

## Applications

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

## Available Deliverables

- Targeted, timing closed netlist
- Simulation model (Verilog or VHDL)
- Verification suite
- T5200 Application Library
- Assembler and Software Simulator
- Documentation
- Support



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

Phone: (352) 371-2567  
Toll-free: (800) 741-7440  
Fax: (352) 373-5182  
[www.athena-group.com](http://www.athena-group.com)

Copyright The Athena Group, Inc., 2009. All rights reserved. Reproduction in whole or in part is prohibited without the prior written consent of the copyright owner. The information presented in this document does not form part of any quotation or contract, is believed to be accurate and reliable, and may be changed without notice. No liability will be accepted by the publisher for any consequence of its use. Publication thereof does not convey nor imply any license under patent or other industrial or intellectual property rights.

The E5200 provides up to four times the elliptic curve cryptography performance as Athena's own T5200, and 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.

## T5200 Application Library

T5200 family products include the T5200 Application Library, which implements high-level algorithms such as RSA with CRT and elliptic curve operations in native T5200 assembly language, providing a complete solution for your application.

## TeraFire Cryptography Application Library (CAL)

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

## Designed for Easy Integration

Athena has over a decade of experience in delivering first-time physical design success. Athena has become a premier provider of semiconductor IP by always delivering quality. To ensure ease of integration, Athena goes the distance - by synthesizing *our* IP into *your* target library, in *your* process, with *your* constraints, and delivering a completed core, ready for place and route. Athena standard deliverables include everything you need to integrate our core into your design: netlists, simulation models, test vectors, support, and documentation.

## About The Athena Group, Inc.

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.