

Press/Analyst Contact:

Pat Rugg  
VP Sales & Marketing  
The Athena Group, Inc.  
352/371-2567 x307  
Toll-free: 800/741-7440  
pat.rugg@athena-group.com

August 19, 2009

**ELLIPTIC CURVE CRYPTOPROCESSOR CORE FROM ATHENA SETS NEW STANDARD FOR NIST P-CURVE PERFORMANCE**

*Exar Licenses Athena's Elliptic Curve Technology*

Gainesville, FL - August 19, 2009 - The Athena Group, Inc., the leader in high-performance public key cryptography performance, today announced the industry's fastest elliptic curve accelerator core. With an incredibly small area footprint, starting at less than 200K-gates, the E5200 is both the highest performance core available and the highest density in terms of performance per unit area. The E5200 employs Athena's patented arithmetic technology and patented cryptographic algorithms to deliver this extraordinary performance across the entire spectrum of public key operations.

Not only is the TeraFire E5200 the fastest elliptic curve accelerator core, it also delivers the fastest performance for RSA, Diffie-Hellman, EC-DSA, ECMQV, NIST P-curve point multiplication, and other public key cryptography operations. The E5200 implements optimized elliptic curve instructions, P-curve specific hardware acceleration, and is a single-core design rather than an array implementation - so fastest also means lowest latency.

"Elliptic Curve Performance, specifically NIST P-Curve performance for Suite B cryptography, will be essential in the next-generation security products, especially for the government and critical infrastructure markets," said Dr. Doug Whiting, Chief Scientist at Exar. "Our work with Athena is a continuation of Exar's dedication to utilizing world-class technologies to deliver high performing, very efficient, next-generation products."

"Athena is pleased to have Exar as the lead customer for the E5200," said Dr. Jon Mellott, CTO of Athena. "The E5200 combines the performance-density advantages of Athena's patented arithmetic technology with the flexibility of a fully programmable public key cryptography microprocessor to deliver superior performance, area, and system integration attributes in an obsolescence-proof solution. The E5200 is the keystone for the strong security that is essential for connected products."

The E5200 is a member of the TeraFire T5200 family of cryptography microprocessors, the only programmable public key cryptography cores. The E5200 implements Athena's proprietary PK instruction set architecture, enabling the autonomous execution

of any PK operation, including any of the over 50 elliptic curve cryptography algorithms. This powerful, flexible microprocessor can easily accommodate new standards with a simple firmware update, ensuring that your application will always be able to handle new requirements and protocols.

A summary of key performance metrics for the E5200 follows:

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	

The E5200 comes complete with a suite of software that executes high-level algorithms such as RSA and EC-DSA natively on the E5200. The E5200 also includes an assembler and software simulator to enable rapid software development and a host-based library of cryptographic software that includes drivers.

### **Athena's TeraFire Security Accelerator Cores**

With a complete family of security IP cores and software, and multiple levels of performance for every function, Athena supports your product succession strategy. TeraFire cores have been delivered in technologies ranging from FPGAs to structured and standard cell ASICs, ready for integration into your product. Whether your next application is a low speed data terminal or a high performance network security appliance, Athena is ready to help you analyze your security hardware requirements and customize a package of functions for your specific application.

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

Based in Gainesville, Florida, Athena innovates breakthrough technologies that achieve the optimum balance of power, performance, and silicon area in a wide range of applications such as wireless, satellite, and secure communications. Athena provides patented semiconductor intellectual property (IP) solutions, with products ranging from the market-leading TeraFire® security cores, to Atomic DSP™ cores, and Atomic SDR™ software defined radio cores.

---

Athena was founded in 1986 and is privately held.

For more information, please visit: [www.athena-group.com](http://www.athena-group.com).

**Press/Analyst Contact:**

Pat Rugg  
VP Sales & Marketing  
The Athena Group, Inc.  
408 W. University Ave, Suite 306  
Gainesville, FL 32601

Phone: 352/371-2567 x307  
Toll-free: 800/741-7440  
E-mail: [pat.rugg@athena-group.com](mailto:pat.rugg@athena-group.com)



The Athena Group, Inc. / 408 W. University Avenue, 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.