

## Features

- High performance public key cryptography microprocessor available as an IP core
- Implements Athena's powerful public key instruction set architecture
- Thousands of RSA-1024 operations per second
- Supports up to 16K-bit public key operations
- Portable to any technology library
- Customizable for your application's area and performance needs
- Unparalleled "performance density"
- AMBA™ AHB bus interface eases SoC integration
- User defined maximum operation size
- FPGA implementations 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
- Fast delivery for accelerated time to profit



## *TeraFire® T5200*

### *The First Public Key Microprocessor*

**The Athena Group introduces the T5200 series public key cryptography cores.** From the world leader in high performance public key cryptography/modular exponentiation cores comes the T5200 series - a fast, efficient exponentiation solution with several size and performance options that are just right for your application. Athena's patented arithmetic technology delivers the performance your solution needs - low latency or high throughput - with the area efficiency to make your silicon small and inexpensive. For any performance requirement, Athena has a solution for you.

Athena technology delivers impressive performance while actually reducing silicon area and clock frequency - performance comparable to the fastest standalone chips. This unparalleled "performance density" is characteristic of Athena's proprietary technology.

The T5200 series of public key cryptography accelerators is the most efficient member of the Athena TeraFire® Public Key family. This family also includes the smaller T5100 processor, as well as the ultra-high performance T5400 processor, which can reach latencies of as low as 100 microseconds per RSA-1024 operation.

### **Product Description**

The T5200 implements Athena's proprietary public key instruction set architecture. This flexible instruction set-based implementation allows TeraFire® Public Key accelerators to perform any public key operation, including the myriad of Elliptic Curve Cryptography algorithms. This powerful, flexible instruction set can easily accommodate new stan-

## Applications

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

dards with on-the-fly programmability, ensuring that your application will always be able to handle new requirements.

**Table 1: Terafire T5200 Product Family**

Model	T5211	T5221
RSA-1024 Private Key/s	2960	2960
1024-bit Full Expo/s	570	1710
RSA-2048 Private Key/s	284	858
2048-bit Full Expo/s	63	103
1024-bit Expo/s (Exponent= $2^{16}+1$ )	45.9K	109K
Area <sup>a</sup> (K-gates)	220	370

a. Requires memory in addition to listed gate area. Memory size varies in proportion to desired maximum operation length.

Base configurations of the T5200 series members can support up to 4,096-bit exponentiation and 8,192-bit RSA operations. The T5200 series can also be extended for operations beyond these lengths with additional memory. With support for any length operation, the T5200 series is ready to support even greater security requirements in the future.

Athena cores are delivered as a firm or hard core optimized to any customer-specified library. The package includes the core, verification suites, timing and simulation models, and documentation. Physical design services are also available.

Athena's IP cores are designed for efficient implementation and rapid delivery. The company's proprietary, wholly automated implementation and verification methodology produces synchronous, testable IP cores of the highest quality. All Athena IP cores achieve a score of 95% or better on the OpenMore scale of IP reusability.

### 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

Copyright The Athena Group, Inc., 2007. 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.