

Features

- High performance public key cryptography processors available as IP cores
- Selectable clock frequency
- Choose the right area and performance for your application
- Unparalleled "performance density"
- Portable to any technology library
- Easy integration into any SoC design
- Direct support for up to 4,096-bit Diffie-Hellman
- Direct support for up to 8,192-bit RSA
- FPGA implementations available

Benefits

- Select from a family of compatible products optimized for throughput, latency, or area
- Fast delivery for accelerated time to profit

Applications

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



TeraFire® T5000

Big chip performance from a small IP core

The Athena Group introduces the T5000 series modular exponentiation cores. From the leader in high performance public key cryptography/modular exponentiation cores comes the T5000 series, small but fast exponentiation solutions in a variety of size/performance options that are just right for your application. Athena's patent pending multiplication technology delivers the performance your solution needs - low latency, or high throughput - with the 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, delivering performance comparable to the fastest standalone chips in less than one square millimeter. This unparalleled "performance density" is characteristic of Athena's proprietary technology.

The T5000 family of public key cryptography accelerators complement the rest of the TeraFire family, which includes ultra-high-performance public key cryptography accelerators, secure hash accelerators, and symmetric key encryption accelerators. The TeraFire family joins Athena's complete signal processing IP library designed for power-sensitive applications that require competitive performance.

Product Description

T5000 cores can do the work that previously demanded an array, and do it in a fraction of the area and power. T5000 security accelerators are available in configurations optimized for native key lengths from 512-bits to 4096-bits, and performance levels ranging from 100 to 10,000 RSA private key operations per second. Table 1 summarizes the

single core performance of several members of the T5000 family of public key cryptography accelerators.

Table 1: Terafire T5000 Product Family

Model	T5004	T5008	T5011	T5021
RSA-1024 Private Key/s	350	475	750	750
1024-bit Full Expo/s	120	180	310	410
RSA-3072 Private Key/s	20	30	55	65
2048-bit Full Expo/s	15	30	55	80
1024-bit Expo/s (Exponent= $2^{16}+1$)	10,000	16,000	26,000	35,000
Area ^a (K-gates)	75	95	135	215

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

Base configurations of the T5000 family members can support up to 4,096-bit exponentiation and 8,192-bit RSA operations. The T5000 family can also be extended for operations beyond these lengths with additional memory. With support for any length of operation, the T5000 family is ready to support ever 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.
5522 NW 43rd Street, Suite B
Gainesville, FL 32653

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

Copyright The Athena Group, Inc., 2004. 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.