



TeraFire T5200 Public Key Cryptography Microprocessor

From the world leader in high performance public key cryptography cores comes the T5200 series. The T5200 series is a fast, efficient public key cryptography 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 and high throughput, in an area efficient package.

Product Description

The T5200 implements Athena's proprietary public key instruction set architecture, which allows T5200s to perform virtually any public key operation, including the myriad of elliptic curve cryptography algorithms, and easily accommodate new standards with on-the-fly programmability. Multiple models are available, optimized for operations up to 512, 1024, or more bits (see Table 1), with the maximum operation size for any implementation determined by its memory size.

Table 1: Terafire T5200 Characteristics

Operation	T5211 ^a		T5221 ^b	
	op/s	latency	op/s	latency
RSA-1024 Private Key	3947	253 μ s	3947	253 μ s
RSA-1024 Private Key w/ Paired Cores	7893	127 μ s	7893	127 μ s
1024-bit Full Expo	760	1.32 ms	2280	439 μ s
RSA-2048 Private Key	379	2.6 ms	1144	874 μ s
RSA-2048 Private Key w/ Paired Cores	757	1.32 ms	2275	440 μ s
2048-bit Full Expo	128	7.8 ms	207	4.8 ms
1024-bit Expo/s ($e=2^{16}+1$)	61.2K	16 μ s	145	7 μ s
256-bit Elliptic Curve Point Multiply	595	1.7 ms	595	1.7 ms
384-bit Elliptic Curve Point Multiply	373	2.7 ms	373	2.7 ms
521-bit Elliptic Curve Point Multiply	223	4.5 ms	223	4.5 ms
Area (K-gates) ^c	164		276	

a. Optimized for operations up to 512-bits.

b. Optimized for operations up to 1024-bits.

c. Requires memory in addition to listed gate area.

Features

- Thousands of operations per second
- Supports up to 16K-bit public key operations
- Supports elliptic curve cryptography operations
- T5200 Application Library supports multiple public key cryptography algorithms
- Implements Athena's powerful T5200 instruction set architecture
- Customizable for your application's area and performance needs
- Suitable for virtually any implementation technology
- AMBATM AHB bus interface eases SoC integration

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

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.

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.