

Features

- Thousands of operations per second
- Supports up to 16K-bit public key operations
- Supports elliptic curve cryptography operations
- X5200 Library provides offload of algorithms such as RSA and EC-DSA
- Implements Athena's powerful X5200 instruction set architecture
- Customizable for your application's area and performance needs
- Suitable for virtually any implementation technology
- AMBA™ AHB bus interface eases SoC integration
- Simple/differential power analysis (SPA/DPA) resistance 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



T5200 Public Key Cryptography Microprocessor

From the market leader in high performance public key cryptography cores comes the T5200 series. The T5200 is a fast, efficient public key cryptography solution with multiple size and performance options that can be matched to the requirements of 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 TeraFire® 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 (see Table 1), optimized for operations up to 512, 1024, 2048, or more bits, with the maximum operation size for any implementation determined by its memory size.

Table 1: Terafire T5200 Characteristics^a

Operation	T5211 ^b		T5221 ^c	
	op/s	latency	op/s	latency
RSA-1024 Private Key	4941	202 μs	4941	202 μs
RSA-1024 Private Key w/ Paired Cores ^d	9843	102 μs	9843	102 μs
1024-bit Expo w/ 1024-bit Exponent	947	1.1 ms	2847	351 μs
RSA-2048 Private Key	481	2.1 ms	1430	699 μs
RSA-2048 Private Key w/ Paired Cores ^d	947	1.1 ms	2841	352 μs
2048-bit Expo w/ 2048-bit Exponent	160	6.2 ms	260	3.84 ms
1024-bit Expo ($e=2^{16}+1$)	78.1K	12.8 μs	178K	5.6 μs
256-bit Elliptic Curve Point Multiply	735	1.4 ms	735	1.4 ms
384-bit Elliptic Curve Point Multiply	463	2.2 ms	463	2.2 ms
521-bit Elliptic Curve Point Multiply	278	3.6 ms	278	3.6 ms
Area (K-gates) ^e	164		276	

Applications

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

Available Deliverables

- Targeted, timing closed netlist
- Simulation model (Verilog or VHDL)
- Verification suite
- TeraFire CAL
- X5200 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
ipsales@athena-group.com

Copyright The Athena Group, Inc., 2011. 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.

- a. Performance characterized at 500 MHz operating frequency.
- b. Optimized for operations up to 512-bits, including up to RSA-1024 w/ CRT.
- c. Optimized for operations up to 1024-bits, including up to RSA-2048 w/ CRT.
- d. RSA with paired cores requires two parallel T5200 core instances.
- e. Requires memory in addition to listed gate area.

X5200 Library

The X5200 Library implements high-level algorithms, such as RSA with CRT, and elliptic curve operations, such as point multiply and EC-DSA sign and verify, in native X5200 assembly language. These functions are designed to execute without host processor intervention, thus providing a complete fire-and-forget cryptographic offload solution for your application. The X5200 Library is packaged with the TeraFire CAL when purchased with an X5200 family core product. Optional X5200 development tools are also available (sold separately).

TeraFire Cryptography Application Library (CAL)

The TeraFire CAL is a portable, ANSI C library of cryptographic software implementations and drivers for TeraFire hardware accelerators, and it includes the X5200 Library assembly code. 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.