

Features

- Implements Athena's powerful T5200 instruction set architecture
- Supports up to 16K-bit public key operations
- Supports elliptic curve cryptography operations
- Optional integrated AES and SHA functions
- T5200 Application Library provides offload of algorithms such as RSA and ECDSA
- AMBA™ AHB bus interface

Benefits

- TeraFire T5200 family compatibility enables your product succession strategy
- Programmability enables adaptability to future standards
- Autonomous operation minimizes load on host processor
- Integrated AES and SHA enables single core Suite B solution



TeraFire F5200 Cryptography Microprocessor

Athena introduces the TeraFire F5200 public key cryptography core. From the world leader in high performance public key cryptography cores comes the F5200, a fast, efficient microprocessor designed for public and secret key cryptography applications that is ideal for area sensitive FPGA designs.

Athena has been a leader in cryptography for a decade with the TeraFire line of products that includes solutions for AES, SHA, 3DES, MD5, public key cryptography, including RSA, DSA, and ECC, and more. Whatever your application, Athena has the functionality and an area/performance option that is right for you — and with discounted pricing for multiple cores, TeraFire products are sure to save both development time and money.

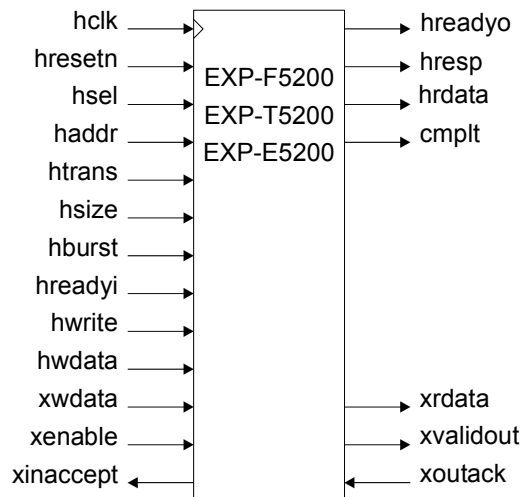


Figure 1: Interface Block Diagram of EXP-F5200 Family

Applications

- Secure boot memory validation
- Embedded secure processing
- SSL and IPsec acceleration
- E-commerce
- SSL VPN
- Mobile Platforms

Device Compatibility

The TeraFire F5200 is compatible with all Actel devices with sufficient logic and memory capacity, including:



Product Description

The F5200 implements Athena's T5200 instruction set architecture (ISA), making it firmware compatible with the high-performance TeraFire T5200 cryptography microprocessor and T5200 Application Library. With the programmable T5200 ISA, the F5200 can execute virtually any public key cryptography algorithm today, and can execute the algorithms of tomorrow with a simple firmware update. The F5200 is ready for system integration with both an AHB interface and direct transfer interface, and has been optimized specifically for Actel FPGA. Characterization data is shown in Table 1.

Table 1: Terafire F5200 Performance, Actel ProASIC3 @ 36 MHz

Operation	op/s	latency
RSA-1024 Private Key	20	50 ms
RSA-1024 Private Key w/ Paired F5200s	40	35 ms
1024-bit Full Expo	5	200 ms
RSA-2048 Private Key	2.5	400 ms
RSA-2048 Private Key w/ Paired F5200s	5	200 ms
2048-bit Full Expo	0.6	1.7 s
1024-bit Expo/s ($e=2^{16}+1$)	500	2 ms
optional AES-128/192/256	>10 Mbps	
optional SHA-1/224/256/384/512	>10 Mbps	
Area	10764 tiles/5 RAMs	

With AES and SHA functions (optional) enabled, the F5200 becomes a highly flexible security application coprocessor in your SoC. By leveraging the T5200 ISA direct transfer interface, the F5200 can enable functions ranging from secure boot memory validation to 'bump-in-the-wire' IPsec coprocessing. The direct transfer interface can also be used to pair two F5200 cores, enabling twice the throughput and half the latency for RSA private key operations with CRT.

Base configurations of the F5200 support 1,024-bit operations. The F5200 may be configured for larger operations with additional memory. With support for virtually any length operation, the F5200 is ready to support even greater security requirements in the future.

Licensing and Deliverables

Athena offers a number of licensing alternatives, including single design, multiple design, and site licenses. License upgrades are also available. Athena also offers several deliverables options, including RTL and netlist. Contact Athena for additional information.

TeraFire Cryptography Application Library (CAL)

The optional 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 design success. Athena has become a premier provider of semiconductor IP by always delivering quality. Athena standard deliverables include everything you need to integrate our core into your design.

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.



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.