

Features

- Supports RSA, DSA, Diffie-Hellman, and Suite B elliptic curve cryptography operations
- Optional integrated AES, GCM, SHA, and random number generator functions
- Implements Athena's powerful X5200 instruction set architecture
- Hundreds of public key cryptography operations per second
- X5200 Library implements algorithms such as RSA and EC-DSA
- Suitable for virtually any implementation technology
- AMBA™ AHB bus interface eases SoC integration
- Simple/differential power analysis (SPA/DPA) resistance available

Benefits

- TeraFire X5200 family compatibility enables your product succession strategy
- Programmability enables adaptability to future standards
- Autonomous operation minimizes host processor load



F5200 Embedded Cryptography Microprocessor

The Athena Group introduces the TeraFire® F5200 embedded cryptography microprocessor core. From the market leader in high performance public key cryptography cores comes the F5200, a fast, efficient microprocessor designed for public key and secret key cryptography applications. With an area footprint starting at 25K-gates and nearly 300 RSA-1024 private key operations per second, the F5200 provides more than 50x greater performance than competitive solutions with similar area. With AES, SHA, and random number generator options, the F5200 is a single core solution for Suite B cryptography.

The F5200 implements Athena's X5200 instruction set architecture (ISA), making it firmware compatible with the high-performance TeraFire T5200 and E5200 cryptography microprocessors and the X5200 Library. The fully programmable X5200 ISA enables the F5200 to execute virtually any public key cryptography algorithm today, and the algorithms of tomorrow can be supported with a simple firmware update.

When the optional AES, GCM, SHA, and random number generator functions are enabled, the F5200 becomes a highly flexible single core security application coprocessor. By leveraging the 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. The capacity of the F5200 is limited only by memory, and with support for virtually any length operation, the F5200 is ready to support the greater security requirements of the future, today.

- Integrated AES and SHA enables single core Suite B solution

Applications

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

Available Deliverables

- Targeted, timing closed netlist
- Simulation model (Verilog or VHDL)
- Verification suite
- Cryptographic Application Library (CAL) and X5200 Library
- Assembler and Software Simulator
- Documentation
- Support

Table 1: Terafire F5200 Performance^a

Operation	op/s	latency
RSA-1024 Private Key	294	3.4 ms
1024-bit Exponentiation w/ 1024-bit Exponent	85	11.8 ms
RSA-2048 Private Key	54	18.5 ms
2048-bit Exponentiation w/ 2048-bit Exponent	11	88.6 ms
1024-bit Exponentiation ($e=2^{16}+1$)	4.2K	233 μ s
EC Point Multiply, P256	254	3.9 ms
EC Point Multiply, P384	91	11 ms
EC-DSA Verify, P256	203	4.9 ms
EC-DSA Verify, P384	32	31.7 ms
EC-DSA Sign, P256	236	4.2 ms
EC-DSA Sign, P384	84	11.9 ms
AES-128/192/256	150-210 Mbps	
SHA-1	240 Mbps	
SHA-224/256	195 Mbps	
SHA-384/512	150 Mbps	
Area (K-gates)	25-60	

a. Throughput characterized at 500 MHz with X5200 Library.

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.

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.

Standards Support

The F5200 has been designed with broad standards support, including:

- AES: FIPS 197, SP800-38A/B/C/D/E
- SHA/HMAC: FIPS 180-3, FIPS 198
- RNG: SP800-90
- Elliptic Curve: FIPS 186-3, Suite B
- Public Key: FIPS 186-3, PKCS #1, PKCS #3

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
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.