ADSP-2141 SafeNet® DSP SECURITY SYSTEM ON A CHIP

High Performance Security System on a Chip

KEY FEATURES:

HIGH THROUGHPUT

- 3-DES at 214 Mbps
- DES at 640 Mbps
- MD-5 at 315 Mbps
- SHA-1 at 253 Mbps

IPSec TRANSFORMS (3-DES, SHA-1) AT OC-3 RATES (155 Mbps)

STRONG SECURITY

- Unencrypted keys never leave the SafeNet DSP nor reside in unprotected memory
- Meets certification requirements for FIPS140-1, level 3
- Security functions isolated by DSP-controlled protection circuitry

FAST DEVELOPMENT TIME

- SafeNet CGX Toolkit and Library of cryptographic functions embedded on-chip
- ADSP-218x DSP core is user programmable

OVERVIEW

The ADSP-2141 SafeNet® DSP is a fully integrated, high-speed Virtual Private Network (VPN) security system on a chip. Jointly developed by Analog Devices, Inc. and IRE, it provides cryptographic acceleration and enhanced security for a wide range of protocols and applications, including:

- IPsec ESP and AH transforms
- IPsec IKE acceleration
- SSL
- Link encryption protocols

Not only are the core algorithms supplied in the ADSP-2141 but it can also perform other elements of the application protocol, such as header addition and stripping. Features are implemented on-chip that are typically delegated to an external host CPU with other chip solutions, such as:

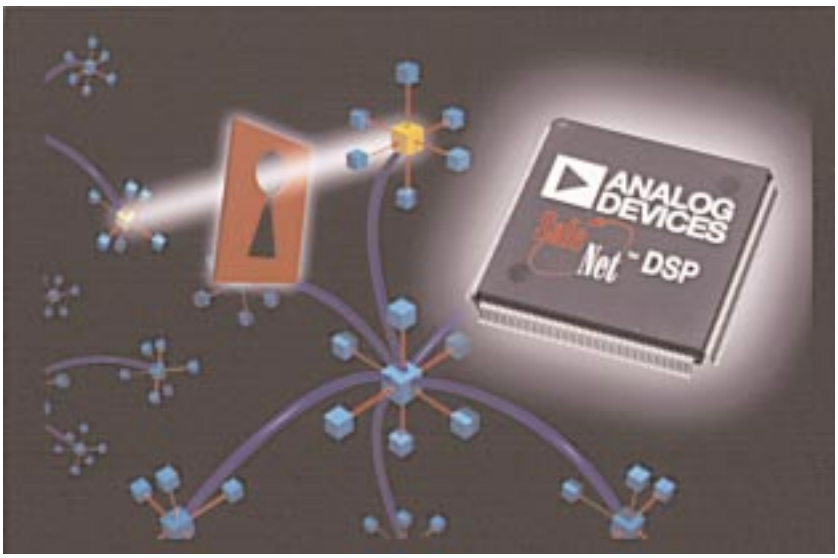
- AH 'mutable bit' processing, including both IPv4 and IPv6 headers
- HMAC ICV validation on inbound packets
- Automatic IV generation
- Automatic pad insertion and removal
- 'Black Key' handling (Keys in off-chip memory are stored encrypted and are decrypted on-the-fly by the ADSP-2141 prior to use.)

FULL SUITE OF ALGORITHMS

The ADSP-2141 SafeNet DSP incorporates all of the necessary algorithms for VPN applications:

- DES and Triple-DES encryption
- MD-5 and SHA-1 hashing with HMAC
- Public key computations:
  - –Diffie-Hellman Key Negotiation
  - –RSA encryption and signatures
  - –DSA signatures

The SafeNet DSP integrates the most advanced cryptography technology available today, a programmable DSP core, and flexible system interfaces to enable high performance, secure data solutions for networking and telecom equipment designers.



SafeNet®

ANALOG DEVICES

- Random number generation
- Full suite of key management functions

With the ADSP-2141 installed, host processors can offload not only VPN packet transforms, but also the cryptographic computations needed for key management handshaking (e.g., IPsec IKE) which can have a serious impact on system performance if solely implemented in software.

WIRE-SPEED PERFORMANCE

The ADSP-2141 combines extremely fast processing engines with a very efficient system architecture to remove performance bottlenecks. By performing most of the security protocol steps on-chip, multiple bus movements are avoided, and operations may be pipelined to minimize latency. When used with IRE's optimized packet driver, a Descriptor Ring located in shared memory efficiently controls packet movements. This allows asynchronous processing between the Host and the ADSP-2141. Since multiple packets may be queued for processing, it avoids 'starving' the ADSP-2141.

When processing IPsec with the worst-case algorithms (3-DES and SHA-1), the ADSP-2141 provides 155 Mbps (OC-3) throughput. Multiple chips may be used to scale throughput as necessary.

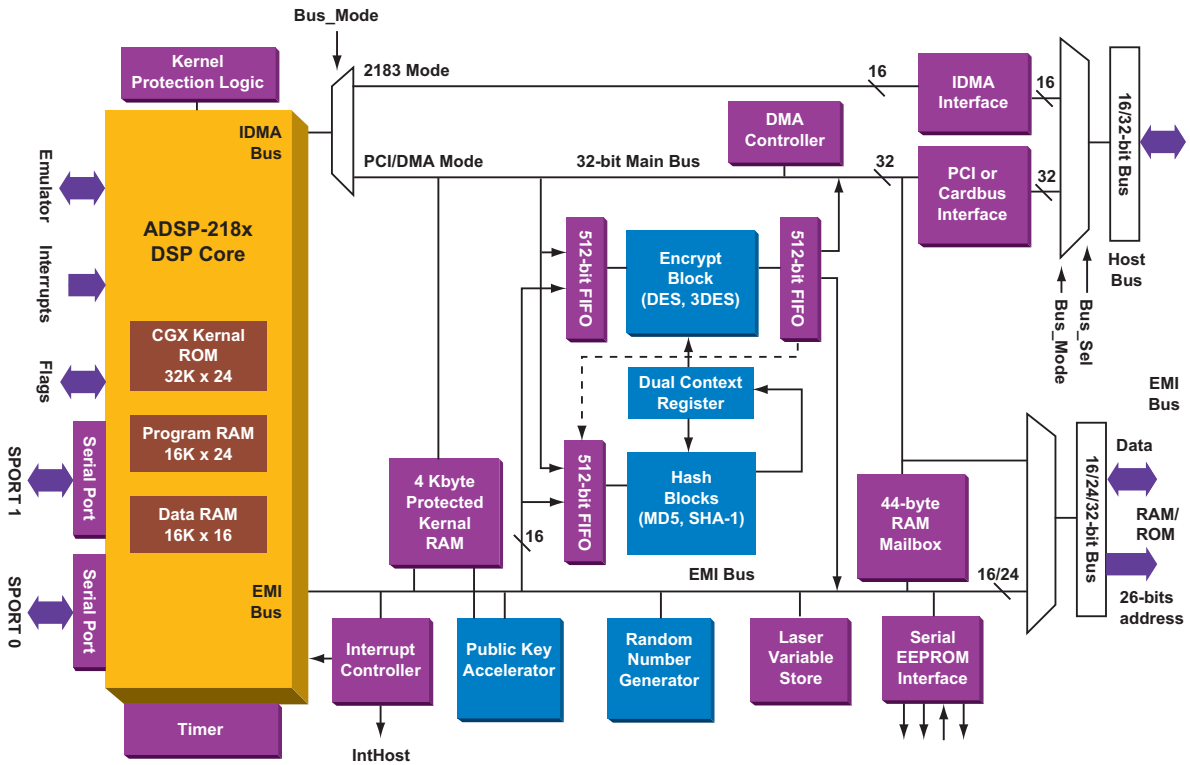
HARDWARE-BASED SECURITY

The SafeNet DSP was designed from the ground up with security in mind. It provides uncompromising protection for its algorithms, key material, and key generation processes. Unencrypted (red) key material is never permitted to leave the ADSP-2141.

A sophisticated Key Management system is contained within the CGX library on the ADSP-2141. The Key Management is carefully designed to enforce hacker-resistant security while at the same time providing a flexible set of key-handling scenarios.

The ADSP-2141 even protects against poor application programming techniques that could otherwise compromise system security. The

ADSP 2141 SafeNet DSP Functional Diagram



Application Programming Interface (API) in the ADSP-2141 is designed to disallow requests that violate good security practice.

The ADSP-2141 is being certified for FIPS 140-1, level 3 security. The ADSP-2141 is the only single-chip FIPS 140-1 solution that provides full IPsec support.

POWERFUL CGX CRYPTOGRAPHIC LIBRARY

The ADSP-2141 is unique in its class by providing an entire cryptographic library right on the chip. This library, designated **C**rypto**G**raphic e**X**tensions (CGX), includes functions such as:

- Generate a random Triple-DES key
- Encrypt and hash data
- Negotiate a Diffie-Hellman key
- Verify DSA digital signature

With the CGX interface, the programmer is spared the significant work required to write a proprietary library, or link-in a costly purchased one. The CGX library incorporates drivers for the on-chip hardware engines, abstracting the programmer from the hardware details.

In addition to a full suite of basic CGX library functions, new commands have been added to the ADSP-2141 to optimize IKE performance. These new commands compress up to 10 primitive cryptographic functions into a single call, streamlining the IKE process. For each IKE packet transaction, only one or two calls to CGX are required.

DEVELOPMENT SUPPORT

IRE offers a Developer's Toolkit to assist the OEM with the system integration process. It includes drivers for various platforms such as Windows® NT and Linux®, source and object code for the "Packet Engine Firmware" (described in the next section), sample applications, BIST test code, and reference schematics. Also available is a CryptPCI development board which includes the ADSP-2141, memory, a serial port and a PCI interface. For those implementing custom applications, a full suite of DSP development tools, including an in-circuit emulator, is available from Analog Devices.

HIGH-PERFORMANCE PACKET ENGINE FIRMWARE

Included in the Developer's Toolkit is a firmware image for the ADSP-2141, which provides a flexible and high-throughput packet engine application. It implements all of the standard IPsec transforms (ESP, AH) as well as basic cryptographic operations such as simple encrypt or hash-and-encrypt. It supports multitasking between high-throughput packet transforms and background Key Management operations.

APPLICATIONS

- Cryptographic engine for high-end internetworking devices (routers, switches, etc.)
- Firewall accelerator
- Server VPN accelerator
- Workstation security module

About IRE...

IRE delivers cost-effective Virtual Private Network (VPN) solutions that enable organizations to use the Internet and other shared networks for private communications. IRE's SafeNet family of VPN products provides a broad range of complete VPN solutions for intranet, extranet, and remote access applications. The SafeNet DSP, with over 10 patents pending, is a breakthrough addition, not only to IRE's family of SafeNet products, but for all network and telecommunications equipment manufacturers who have been searching for a way to increase the throughput and decrease the cost of implementing a VPN solution.

IRE also has extensive experience in security system design and implementation, and provides consulting services to companies implementing designs with the SafeNet DSP.

IRE maintains a website on the ADSP-2141 located at ***www.ire.com/oem/dsp.htm*** *containing documentation such as user's manuals and application notes.*

Security and experience go hand in hand. IRE provided the first commercial VPN solution in 1989 and the first Internet VPN in 1995. Founded in 1983 by a group of data security professionals, IRE has offices in Baltimore, Maryland, and Danvers, Massachusetts.

SPECIFICATIONS

IPsec Performance
155 Mbps sustained ESP
(3-DES, SHA-1, 1500 byte packets)

Crypto Block
640 Mbps Single-DES
214 Mbps Triple-DES
Supports all DES modes: ECB, CBC, 64-bit OFB, and 1, 8, 64-bit CFB
Multimode padding support
Automatic IV updating

Hash Block
Hardware-based MD-5 and SHA-1
315 Mbps MD-5
253 Mbps SHA-1
Implements IPsec AH and HMAC
Intelligent mutable bit handler for AH

Public Key Accelerator
Accelerator for math-intensive public key operations
Supports up to 2048-bit modulus size
Diffie-Hellman negotiate: 29ms
(1024-bit modulus, 180 exponent)
RSA 1024-bit sign: 29ms
RSA 1024-bit verify: 6ms
DSA Sign: 39ms
DSA Verify: 66ms

DSP Co-processor
ADSP-218x compatible DSP
40 MIPS sustained performance
Single-cycle instruction execution
Zero-overhead looping
16K words on-chip Program RAM
32K words on-chip CGX library ROM
16K words on-chip Data RAM
Programmable interval timer

PCI Interface
32-bit 3.3V bus interface
40 MHz max bus speed
Up to 1.3 Gbps burst throughput
PCI v2.1-compliant
Bus master and target capability

External Memory Interface
32-bit 3.3V bus interface
128 Mbyte address space
Asyncronous SRAM and Dual Port SRAM supported
Programmable SRAM wait states

DMA Block
2-Channel, 32-bit DMA controller
Can DMA between PCI, local memory bus and any internal engine
1.2 Gbps burst transfers

Key Management Block
Support for storage of both public and symmetric keys
Trust-model rules enforcement
Only encrypted keys allowed off chip
Unique laser-encoded master key
Internal key-cache for 15 keys – (can be expanded to 731 keys internal or unlimited in local SRAM or PCI memory)

Random Number Generator
Hardware-based nondeterministic random number generator
Can internally generate session keys, IV's, nonces, cookies, public and private keys, etc...
Up to 1 Mbit of random data per second

Electrical
Core and I/O Power: 3.3V ±10%
PCI Voltage: 3.3V ±10%
Core Clock Speed: 40 MHz
Power Consumption: 1W typical

Package
208-pin plastic MQFP

DSP SUPPORT:

Email:
In the U.S.A.: dsp.support@analog.com
In Europe: dsp.europe@analog.com

Fax: In the U.S.A.: 1 781 461-3010
In Europe: +49-89-76903-307

Web Address: http://www.analog.com/dsp

WORLDWIDE HEADQUARTERS
One Technology Way P.O. Box 9106
Norwood, MA 02062-9106, U.S.A.
Tel: 1 781 329 4700
(1 800 262 5643 U.S.A. only)
Fax: 1 781 326 8703
World Wide Web Site: http://www.analog.com

EUROPE HEADQUARTERS
Am Westpark 1-3
81373 München, Germany
Tel: +879 76903-0; Fax +89 76903-157

JAPAN HEADQUARTERS
New Pier Takeshiba, South Tower Building
1-16-1 Kaigan, Minato-ku, Tokyo 105, Japan
Tel: +3 5402 8210; Fax: +3 5402 1063

SOUTHEAST ASIA HEADQUARTERS
2102 Nat West Tower, Times Square
One Matheson Street
Causeway Bay, Hong Kong, PRC
Tel: +2 506 9336; Fax: +2 506 4755

Printed in the U.S.A H3886-5-6/00 (rev. 0)