Freescale Semiconductor
Application Note

Document Number: AN2788
Rev. 1, 05/2008

ColdFire Security

SEC and Hardware Encryption Acceleration Overview

by: Melissa Hunter
MSG Applications

This application note describes the integrated security engine (SEC) available on the ColdFire® MCF547X and MCF548X family microprocessors. It also discusses the encryption hardware accelerator (HA) modules available on the MCF523X and the MCF527X device families, as well as the differences between the hardware accelerators and the full SEC. In addition, it gives information on export controls and import compliance for products that include hardware or software encryption.

Contents

1 Introduction

The MCF547x, MCF548x, MCF523x, and MCF527x families are the first ColdFire microprocessor units (MPUs) with integrated hardware acceleration for common security algorithms. Ethernet connectivity for embedded systems allows additional functionality and flexibility, but security must also be a concern for embedded systems that will be connected to the Internet. Security protocols like IPsec can lessen the threat of

freescale™ semiconductor

hacking or tampering; however, the algorithms used by security protocols require complex math routines that can pose a significant performance drain for a system. Integrated on-chip hardware acceleration for these math routines offloads math-intensive functions from the CPU, leaving more of the CPU bandwidth to remain dedicated to system functions.

2 Supported Security Protocols

The encryption hardware acceleration on the ColdFire family devices supports a number of common security algorithms that are used as building blocks for higher level security protocols. The hardware modules were designed with support for specific security protocols in mind.

Table 1 lists some common security protocols and the supported algorithms that can be used by the protocol for encryption and authentication services. However, the hardware acceleration is flexible and can be used to support any protocol that makes use of one or more of the supported algorithms, including proprietary protocols.

Table 1. Supported Security Protocols and Algorithm Usage

Protocol	Encryption/Decryption	Authentication
IPsec	DES/3DES, AES	HMAC-MD5, HMAC-SHA-1
SSL/TLS	DES/3DES, AES, RC4	HMAC-MD5, HMAC-SHA-1
SSH	DES/3DES	HMAC-MD5, HMAC-SHA-1
SRTP	AES	HMAC-SHA-1
iSCSI	DES/3DES, AES	HMAC-SHA-1

3 MCF547X/8X Integrated Security Engine (SEC)

The SEC is an integrated security coprocessor available on MCF547X/8X family devices designed to offload computationally intensive security algorithms, such as bulk encryption and authentication, from the MCF547X/8X core. The SEC encompasses hardware accelerators for DES/3DES, AES, ARC4, MD5, SHA, and a hardware random number generator (RNG). It is optimized to process all the algorithms associated with IPsec, SSL/TLS, SSH, SRTP, iSCSI, and SSH.

The ColdFire core accesses the SEC primarily through data packet descriptors using system memory for data storage. When an application requires cryptographic functions, it simply creates descriptors that define the cryptographic function to be performed and the location of the data. The SEC's bus-mastering capability permits the host processor to set up a crypto-channel with a few register writes. Afterwards, the SEC can perform reads and writes on system memory to fetch data packet descriptors and complete the specified tasks.

3.1 MCF547X/8X SEC Features

SEC features include:

- DEU—data encryption standard execution unit
  - DES, 3DES

  - Two key (K1, K2, K1) or three key (K1, K2, K3)
  - ECB and CBC modes for both DES and 3DES
- AESU—advanced encryption standard unit
  - Implements the Rijndael symmetric key cipher
  - ECB, CBC, CCM, and counter modes
  - 128-bit, 192-bit, 256-bit key lengths
- AFEU—ARC four execution unit
  - Implements a stream cipher compatible with the RC4 algorithm
  - 40-bit to 128-bit programmable key
- MDEU—message digest execution unit
  - SHA with 160-bit or 256-bit message digest
  - MD5 with 128-bit message digest
  - HMAC with either algorithm
- RNG—one random number generator
- Master/slave logic, with DMA
  - 32-bit address/32-bit data
  - Up to 133 MHz operation
- Two crypto-channels, each supporting multi-command descriptor chains
  - Static and/or dynamic assignment of crypto-execution units via an integrated controller
- Buffer size of 512 bytes for each execution unit, with flow control for large data sizes

3.2 Block Diagram

The ability of the SEC to be a master on the internal bus allows the security core to offload the data-movement bottleneck that is normally associated with slave-only cores.

Figure 1 shows a block diagram of the SEC module. The bus interface module is designed to transfer 32-bit longwords between the internal bus and any register inside the SEC.

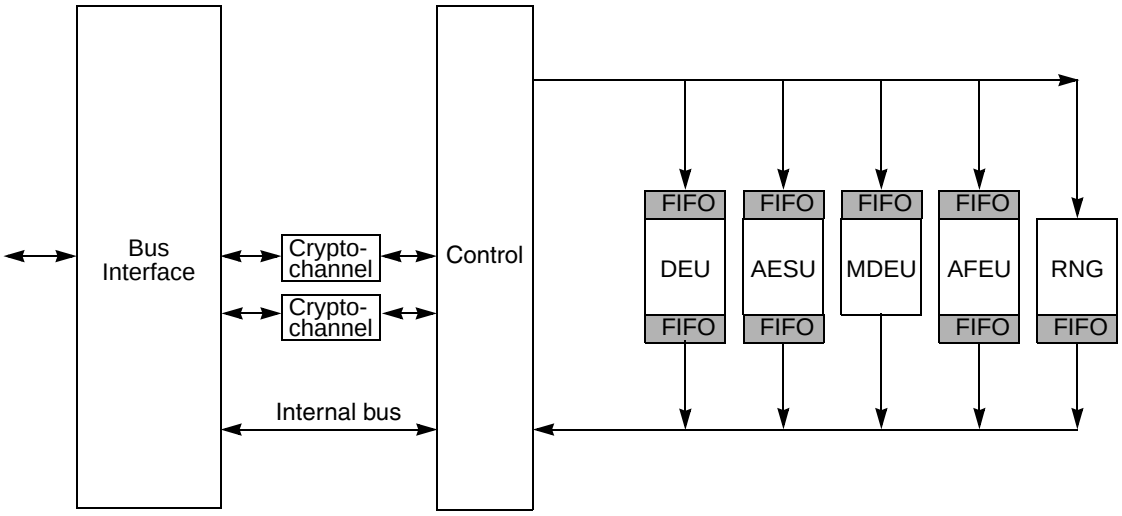

Figure 1. SEC Block Diagram

A typical operation consists of these steps:

1. An operation begins with the write of a pointer to a crypto-channel fetch register that points to a data packet descriptor.
2. The channel requests the descriptor and decodes the operation to be performed.
3. The channel requests the controller to assign crypto execution units, then fetch the keys, context, initialization vectors (IVs), and data needed to perform the given operation.
4. The controller satisfies the requests by assigning execution units to the channel and making requests to the master interface per the programmable priority scheme.
5. As data is processed, it is written to the individual execution unit's output FIFO (or in the case of the MDEU, an output register) and back to system memory via the bus interface.

3.2.1 Bus Interface

The bus interface manages communication between the SEC internal execution units and the internal bus. The interface uses the bus master/slave protocols. All on-chip resources are memory-mapped, and the target accesses and initiator writes from the SEC must be addressed on longword boundaries. The SEC will perform initiator reads on byte boundaries and adjust the data (realign the data) to place on longword boundaries as appropriate. Access to system memory is a critical factor in co-processor performance, and the bus interface of the SEC core allows it to achieve performance unattainable on secondary busses.

3.2.2 SEC Controller Unit

The SEC controller unit manages on-chip resources, including the individual execution units (EUs), FIFOs, the bus interface, and the internal buses that connect all the various modules. The controller receives service requests from the bus interface and various crypto-channels, and schedules the required activities.

3.2.3 Crypto-Channels

The SEC includes two crypto-channels that manage data and EU function. Each crypto-channel consists of:

- Control registers containing information about the transaction in process
- A status register containing an indication of the last unfulfilled bus request
- A pointer register indicating the location of a new descriptor to fetch
- Buffer memory used to store the active data packet descriptor

Crypto-channels analyze the data packet descriptor header and request the first required cryptographic service from the controller. After the controller grants access to the required EU, the crypto-channel and the controller perform these steps:

1. Set the appropriate mode bits available in the EU for the required service.
2. Fetch context and other parameters as indicated in the data packet descriptor buffer and use these to program the EU.
3. Fetch data as indicated and place in either the EU input FIFO or the EU itself (as appropriate).
4. Wait for the EU to complete processing.
5. Upon completion, unload results and context and write them to external memory, as indicated by the data packet descriptor.
6. If multiple services are requested, go back to step 2.
7. Reset the appropriate EU if it is dynamically assigned. Note that if it is statically assigned, an EU is reset only upon a direct command being written to the SEC.
8. Perform descriptor completion notification as appropriate. This notification comes in one of two forms—interrupt or header writeback modification—and can occur at the end of every descriptor, at the end of a descriptor chain, or at the end of specially designated descriptors within a chain.

3.2.4 Execution Units (EUs)

Execution unit is the generic term for a functional block that performs the mathematical permutations required by protocols used in cryptographic processing. The EUs are compatible with IPsec, SSL/TLS, iSCSI, and SRTP processing, and can work together to perform high level cryptographic tasks. The SEC execution units are:

- DEU (data encryption standard execution unit) for performing block cipher, symmetric key cryptography using DES and 3DES
- AFEU for performing RC-4 compatible stream cipher symmetric key cryptography
- AESU for performing the advanced encryption standard algorithm
- MDEU for performing security hashing using MD-5, SHA-1, or SHA-256
- RNG for random number generation

4 MCF523X and MCF527X Family Encryption Hardware Accelerators (HAs)

Like the SEC, the encryption hardware accelerators available on the MCF523X and MCF527X family processors are designed to offload computationally intensive security algorithms such as bulk encryption and authentication from the CPU core. However, the hardware accelerators are a scaled-down implementation that is designed to offer the same type of functionality available when using the full SEC. The HAs encompass hardware accelerators for DES/3DES, AES, MD5, SHA, and a hardware random number generator (RNG).

The HAs are programmed directly by the user instead of being programmed indirectly via data packet descriptors. The HAs do not have bus-mastering capability, so CPU intervention is required to load and unload data from the HA FIFOs.

4.1 MCF523X and MCF527X HA Features

The Symmetric Key Hardware Accelerator (SKHA) supports these block ciphers:

- AES
  - 128-bit key
  - Electronic Code Book (ECB), Cipher Block Chaining (CBC), and Counter (CTR) cipher modes
- DES
  - 64-bit key (with parity)
  - ECB, CBC, and CTR modes
- Triple-DES
  - 2 key & 3 key (128-bit and 192-bit with parity)
  - Key parity check
  - ECB, CBC, and CTR modes

The Message Digest Hardware Accelerator (MDHA) computes a single message digest (or hash or integrity check) value of all the data presented on the input bus, using either the MD5 or SHA-1 algorithms for bulk data hashing. The MDHA includes these distinctive features:

- MD5 one-way 128-bit hash function as specified in RFC 1321
- SHA-1 one-way 160-bit hash function specified by the ANSI X9.30-2 and FIPS 180-1 standards
- HMAC support for all algorithms as specified in RFC 2104
- EHMAC support for the SHA-1 algorithm
- EHMAC key support up to 160 bits
- Processes 512-bit blocks organized as 16 × 32 bit longwords
- Automatic message and key padding
- Internal 16 × 32 bit FIFO for temporary storage of hashing data

The random number generator (RNG) module is capable of generating 32-bit random numbers. It is designed to comply with FIPS-140 standards for randomness and non-determinism.

4.2 Block Diagrams

The HAs are more or less the execution units (EUs) from the SEC. The block diagrams are similar, but the HAs do not include the bus interface, crypto-channels, or the control block.

Figure 2 shows the block diagrams of the HA modules. Although the module block diagrams are shown together, in this implementation the modules are stand-alone and do not interact with each other.

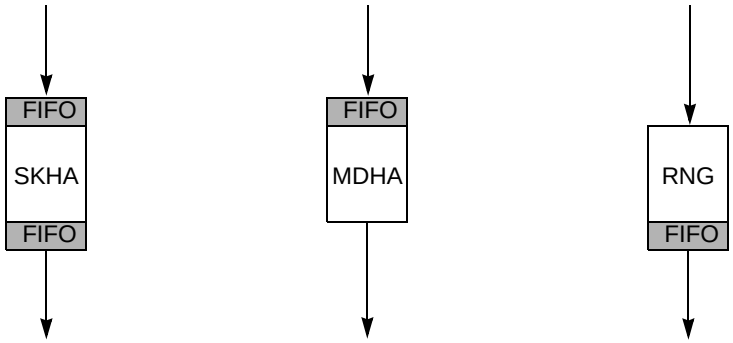

Figure 2. HA Block Diagrams

5 Integrated Security Engine (SEC) vs. Encryption Hardware Accelerators (HAs) Comparison

Table 2 lists differences in algorithm coverage between the SEC and HAs based on the functionality that is directly supported by hardware.

Table 2. SEC vs. HAs Algorithm Support Comparison

	Feature	SEC	HAs
Data Encryption Standard	Types	DES and 3DES	DES and 3DES
	Modes	ECB and CBC	ECB, CBC, and CTR
	Key Sizes	64-bit, 128-bit, 192-bit	64-bit, 128-bit, 192-bit
Advanced Encryption Standard	Modes	ECB, CBC, and CTR	ECB, CBC, and CTR
	Key Sizes	128-bit, 192-bit, 256-bit	128-bit

Table 2. SEC vs. HAs Algorithm Support Comparison (continued)

	Feature	SEC	HAs
ARC Four	Key Sizes	40–128 bit	No support
Message Digests	Algorithms	MD-5, SHA-1, and SHA-2	MD5 and SHA-1
	Modes	HMAC	HMAC and EHMAC
Random Number Generator	Hardware random number generator	FIPS 140 compliant	FIPS 140 compliant

Because all of the cipher algorithms supported by either the SEC or HAs can be implemented in software, differences in algorithm coverage do not necessarily impact the functionality of a system. However, if software is used instead of hardware there will be a performance impact.

There are many other differences between the two implementations that will affect the performance of the solution besides the functionality provided. The primary difference is that the SEC is a full coprocessor with bus mastering capability, but the HAs require CPU intervention to read and write to FIFOs. The additional work required by the CPU will decrease the overall throughput as compared to the SEC; however, the HAs nevertheless provide much better performance than software encryption routines.

6 Export Controls and Import Compliance

Export controls on commercial products incorporating strong encryption (implemented in hardware or software) are administered by the Bureau of Industry and Security (BIS) in the U.S. Department of Commerce. If your company intends to export or re-export these devices, your company as exporter is responsible for the proper classification of any item when it is exported. For more information please refer to the Bureau of Industry and Security's website (www.bis.doc.gov).

In addition to satisfying U.S. Government export controls, strong encryption products may require an import certificate from the country in which the customer accepts delivery.

7 Federal Information Protection Standard (FIPS)

The US Government publishes a Federal Information Protection Standard (FIPS) that describes how governmental agencies should protect sensitive data. FIPS 140-2 describes a series of conformance tests which data storage and networking equipment must meet to achieve various levels of FIPS certification, with particular focus on cryptography and assurance.

To achieve various FIPS levels, a product must pass certification at an authorized testing lab.

Freescale has certified the MPC190 to FIPS 140-2, Level 1. To achieve this level of certification the equipment must demonstrate that all encryption algorithms return the expected results, and that the random number generator is non-deterministic. This certification provides no pass-through benefit to our customers, but was an important demonstration of the correctness of our cryptographic implementation.

8 References

Table 3 provides a list of Freescale references used throughout this application note.

Table 3. References

Freescale Document Number	Title	Revision
MCF5475RM	MCF547x Reference Manual	4
MCF5485RM	MCF548x Reference Manual	4
MCF5235RM	MCF5235 Reference Manual	2
MCF5271RM	MCF5271 Reference Manual	2
MCF5275RM	MCF5275 Reference Manual	2

9 Document Revision History

Table 4 provides a document revision history for this application note.

Table 4. Document Revision History

Rev. No.	Substantive Change(s)	Date of Release
0	Initial Release	August 2004
0.1	Minor edits for clarification	November 2004
1	Updated Section 6, “Export Controls and Import Compliance”	May 2008

How to Reach Us:

Home Page:
www.freescale.com

Web Support:
http://www.freescale.com/support

USA/Europe or Locations Not Listed:
Freescale Semiconductor, Inc.
Technical Information Center, EL516
2100 East Elliot Road
Tempe, Arizona 85284
+1-800-521-6274 or +1-480-768-2130
www.freescale.com/support

Europe, Middle East, and Africa:
Freescale Halbleiter Deutschland GmbH
Technical Information Center
Schatzbogen 7
81829 Muenchen, Germany
+44 1296 380 456 (English)
+46 8 52200080 (English)
+49 89 92103 559 (German)
+33 1 69 35 48 48 (French)
www.freescale.com/support

Japan:
Freescale Semiconductor Japan Ltd.
Headquarters
ARCO Tower 15F
1-8-1, Shimo-Meguro, Meguro-ku,
Tokyo 153-0064
Japan
0120 191014 or +81 3 5437 9125
support.japan@freescale.com

Asia/Pacific:
Freescale Semiconductor Hong Kong Ltd.
Technical Information Center
2 Dai King Street
Tai Po Industrial Estate
Tai Po, N.T., Hong Kong
+800 2666 8080
support.asia@freescale.com

For Literature Requests Only:
Freescale Semiconductor Literature Distribution Center
P.O. Box 5405
Denver, Colorado 80217
1-800-441-2447 or 303-675-2140
Fax: 303-675-2150
LDCForFreescaleSemiconductor@hibbertgroup.com

Document Number: AN2788
Rev. 1
05/2008

freescale™
semiconductor