Freescale Semiconductor
Application Note

Document Number: AN4307
Rev. Rev.0, 5/ 2011

Using the CAU and mmCAU in ColdFire, ColdFire+ and Kinetis

by: Paolo Alcantara
RTAC Americas
Mexico

Contents

1 Introduction

This document describes how to use the CAU and mmCAU present in the ColdFire, ColdFire+, and Kinetis MCU and MPUs.

The following document is a guide on how to use the crypto algorithms and hashing function as the lowest blocks of a communication security application like: the SSL, SSH, IPsec, and so on.

1.1 Audience description

This document is intended to be used by all software development engineers, test engineers, and anyone else who wants to integrate the CAU and mmCAU software library on an application focused on communication security to increase performance, or reduce memory footprint.

2 Overview of the Crypto and Hashing Application

The following application uses all the functions included in the CAU and mmCAU software library. For more details about the functions, consult the Crypto Acceleration Software Library V1.0 User Guide document. The example software includes examples for the following targets and compilers:

- MCF51JF + CW10.1 (ColdFire+) using TWR-MCF51JF board
- MCF5441x + CW10.1 (ColdFire) using TWR-MCF5441x board
- K60 + CW10.1 (Kinetis) using TWR-K60 board
- K60 + IAR 6.20 (Kinetis) using TWR-K60 board

The example software is the same showing how endianes are handled internally by the CAU and mmCAU software libraries. Both libraries share the same C-language header file.

2.1 ColdFire+ considerations

The new ColdFire+ family is enabled by a 90 nm thin film storage (TFS) flash process technology with Flexmemory that contains the cryptographic acceleration unit (CAU) version 2 that adds support to SHA256 hashing function.

2.2 Microcontroller and microprocessor units with CAU and mmCAU

- The CAU is only present in ColdFire and ColdFire+ devices.
- The mmCAU is only present in Kinetis devices (ARM Cortex-M4).

The following table shows which MCUs and MPUs contain a cryptographic acceleration unit. The CAU and the mmCAU main difference is that the CAU is accessible through CPU registers and the mmCAU is accessible as an external peripheral to a CPU connected to the processor private peripheral bus (PPB). Then, during the rest of the document, CAU refers to CAU and mmCAU unless explicitly noted.

Table 1. CAU availability

	CAU v1	CAU v2
ColdFire+		
MCF51JF	—	x
MCF51JU	—	x
MCF51QM	—	x
MCF51QF	—	x
ColdFire		
MCF51JM	x	—
MCF5223x	x	—
MCF5225x	x	—
MCF5301x	x	—
MCF5441x	—	x

Table continues on the next page...

Table 1. CAU availability (continued)

	CAU v1	CAU v2
MCF5445x	x	—
Kinetis		
K50	—	x
K60	—	x

NOTE

Go to www.freescale.com to check for CAU and mmCAU coprocessor availability per package.

2.3 Details about the Crypto algorithms

The following crypto algorithms are used in the example software:

- AES128
- AES192
- AES256
- DES
- 3DES

All the crypto algorithms are executed in Cipher-block chaining (CBC) block cipher mode to increase block encryption and decryption security. For more details about CBC, go to the application note titled *Using the Cryptographic Service Engine (CSE)* (document AN4234) in the section called " Cipher Modes Overview " .

The key handling, encryption and decryption basic functions are executed by the CAU software library.

Encryption and decryption are symmetric-key operations, this means the operation of encrypting and decrypting a message results in the original message, if using the same key. This symmetric feature is used to test functionality.

2.4 Details about the hashing functions

The following hashing functions are used:

- MD5
- SHA1
- SHA256

The examples show how to use the padding requirement for hashing. Encryption padding refers to extending the payload to a size that fits the encryption cipher block size. For MD5, SHA1, and SHA256, the cipher block size is fixed to 64 bytes (512 bits).

2.5 Padding explanation

The following steps describe how padding is added to a message:

1. Message is extended so that its length is 448 modulo 512. This operation is always performed even if the message is already 448 modulo 512. The extension is added to the end of the message by adding one bit set (0b1) and the rest as zeros (0b0)
2. The length of the original message is appended as 64-bit data. Endianes must be considered when adding the length message. MD5 uses little endian and SHA1 and SHA256 use big endian.

After all these steps, the message will be in multiples of 512 bits or 64 bytes.

2.6 Hashing output considerations

MD5 output is represented in little endian representation as stated in standard RFC1321. Then the output is represented as a pointer to a character (8-bit) for little endian architectures, like Kinetis devices.

SHA1 and SHA256 output is represented in big endian representation as stated in the standard FIPS 180-2. Then the output is represented as a pointer to an integer (32-bit) for a little endian architecture, like Kinetis devices.

NOTE

Only ColdFire devices with CAU v2 are able to handle SHA256 in hardware. Refer to table 1 for details.

3 Conclusion

This document described how to use the CAU software library, using the crypto algorithms and hashing functions present in the hardware. By using the CAU software library, the performance of crypto algorithms AES, DES, 3DES, and hashing functions MD5, SHA1, and SHA256 is increased rather than using only a software implementation.

3.1 Problem reporting instructions

Issues and suggestions about this document and drivers must be provided through the support web page at www.freescale.com/support.

3.2 Considerations and references

Find the newest software updates and information about this document on the Freescale Semiconductor home page: www.freescale.com

- Details about the CAU and mmCAU software library can be found in the document *Crypto Acceleration Software Library V1.0 User Guide*
- For details about CBC go to the application note titled *Using the Cryptographic Service Engine (CSE)* (document AN4234) in the section titled “ Cipher Modes Overview ” .
- AN4307SW includes all the tests mentioned in this document.
- Download the software for AN4307 (AN4307SW.zip) from www.freescale.com.

How to Reach Us:

Home Page:
www.freescale.com

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

USA/Europe or Locations Not Listed:
Freescale Semiconductor
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 China Ltd.
Exchange Building 23F
No. 118 Jianguo Road
Chaoyang District
Beijing 100022
China
+86 10 5879 8000
support.asia@freescale.com

For Literature Requests Only:
Freescale Semiconductor Literature Distribution Center
1-800-441-2447 or +1-303-675-2140
Fax: +1-303-675-2150
LDCForFreescaleSemiconductor@hibbertgroup.com

Document Number: AN4307
Rev. Rev.0, 5/ 2011