TB3176

What is ICM? How to Use the ICM For Cryptography

Introduction

The Integrity Check Monitor (ICM) is a DMA controller that performs hash calculation on multiple memory regions using the transfer descriptors located in the memory (ICM Descriptor Area) of Cortex™ M7 MCUs. The ICM integrates a Secure Hash Algorithm Engine (SHA) for hashing. The SHA based hashing is suitable for password validation, challenge hash authentication, anti-tamper, and digital signatures.

Secured Image Verification: The hash function produces a message digest for a piece of data. Conversely, this means to an error detection code, every piece of data must have its own unique digest. To verify the integrity of a firmware, the digest is calculated and verified after the programming is complete. This is used in the secured bootloader, which after receiving the firmware and its fingerprint, recomputes the digest, and compares it to the original digest. If both are identical, the firmware has not been altered and is suitable for programming.

Figure 1. Secure Image Verification

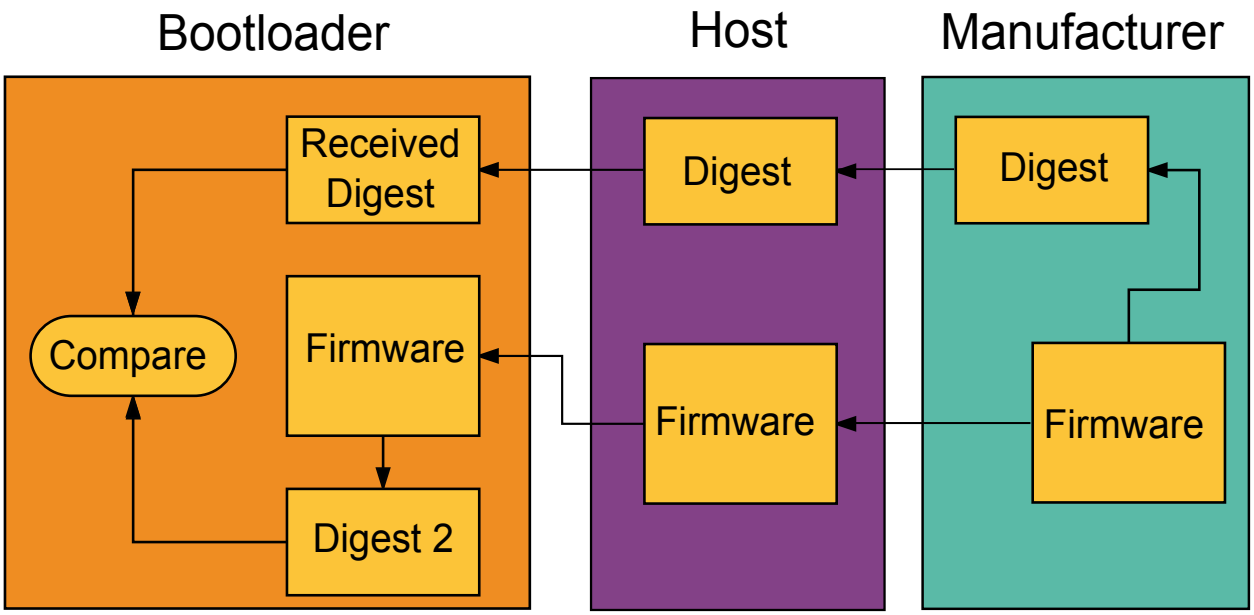


Table of Contents

Introduction....1

1. Concept.... 3

2. Solution/Implementation....4

3. Relevant Resources.... 7

The Microchip Web Site.... 8

Customer Change Notification Service....8

Customer Support.... 8

Microchip Devices Code Protection Feature.... 8

Legal Notice....9

Trademarks.... 9

Quality Management System Certified by DNV....10

Worldwide Sales and Service.... 11

1. Concept

A cryptographic hash function is a special class of hash function that has certain properties, which makes it suitable for use in cryptography. A cryptographic hash function is a mathematical algorithm that maps data of an arbitrary size to a bit string of a fixed size (a hash function). The cryptographic hash is designed to be a one-way function, that is, a function that is impossible to invert and retrieve the original message.

If *f(x)* represents the data set to be hashed, and *Y* is the *SHA* hashed finger print, then:

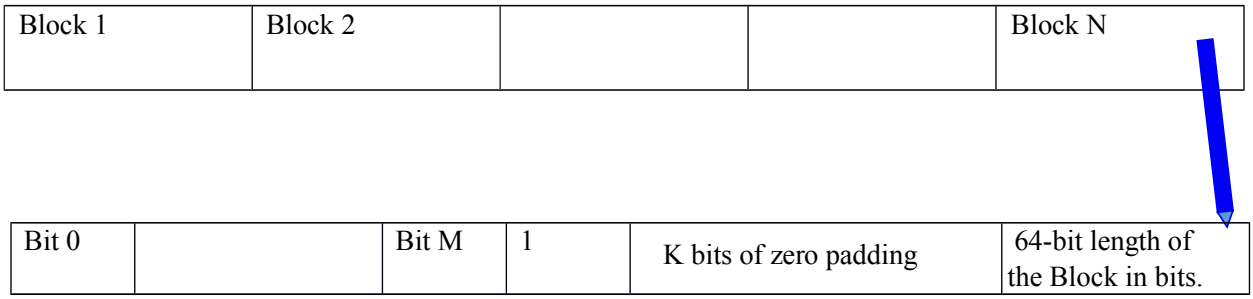
$Y = sha\_hash(f(x))$

$f(x) \neq any\_function(Y)$

2. Solution/Implementation

The ICM requires a message to be updated in the FIPS 180-2 standard. As per the FIPS 180-2 standard, for SHA-256, the message to be hashed needs to be of a maximum size 264 – 1 bits. The SHA-256 crypto engine requires the message to be divided into multiple blocks, where each block is 512 bits in size.

Figure 2-1. FIPS180-2 Message Format



Each Block has a 512 bit width, the last block format is shown above, where K= 448-X-1.

For a message less than 512 bits, one block is sufficient.

For the message: “abc” => {0x61, 0x62 and 0x63}.

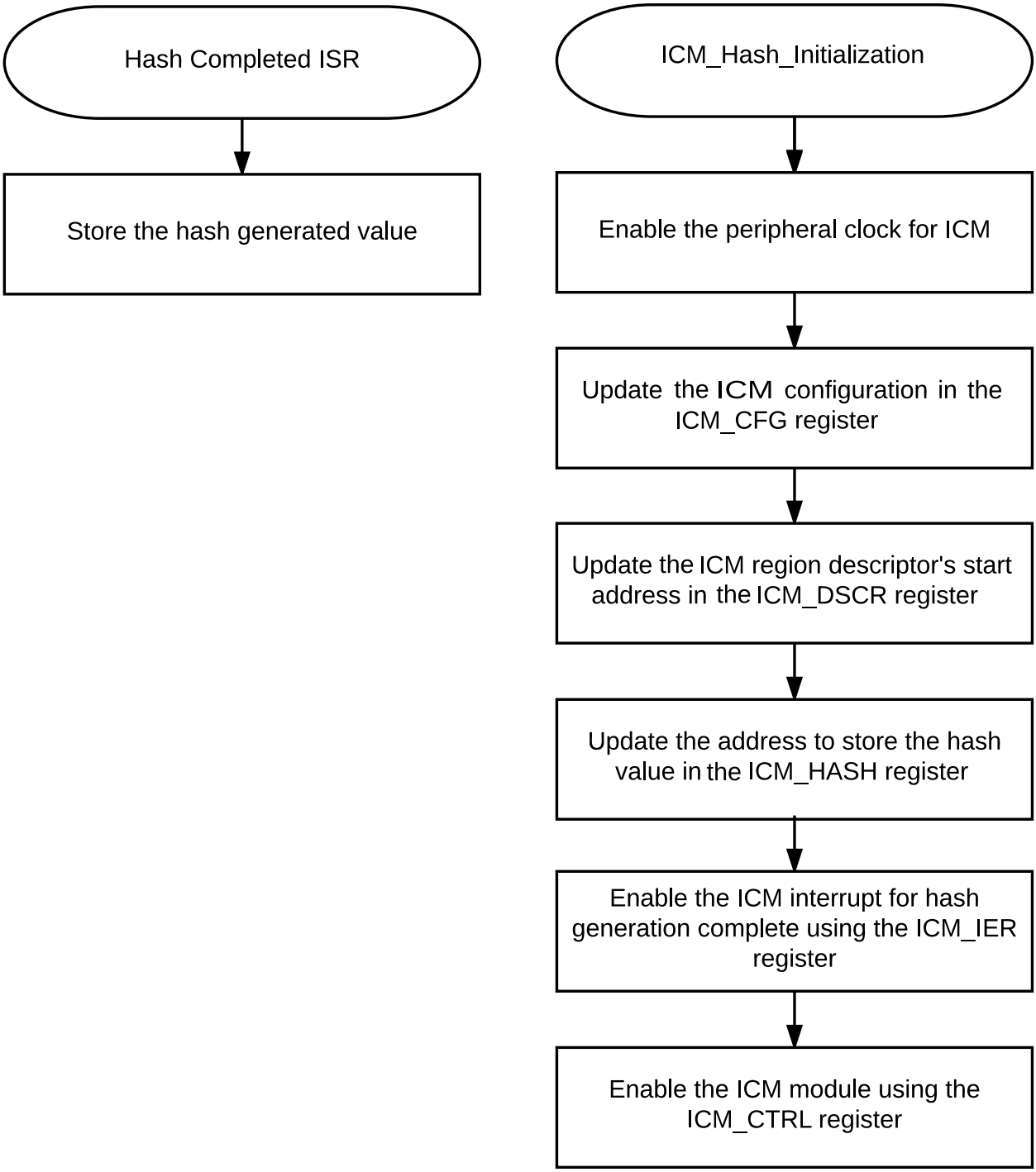
Bit 0 – Bit 23 filled with the previous message, Bit 24 = 1 (as per FIPS 180-2) Bit 25-447 = 0 (K zero bits).

Bit 448-Bit 511 = 0x0000000000000018 (64-bit length of message).

Configuration of ICM in Cortex-M7 MCUs:

To generate the SHA-256 hash value in ICM, follow the configuration sequence shown in the following figure.

Figure 2-2. ICM Configuration Sequence



Tip: For ICM Configuration:

1. The hash value address needs to be stored in the ICM_HASH register. The address must be a multiple of 128 bytes.
2. The region descriptor content needs to be filled based on FIPS180-2 as explained previously, and the start address needs to be assigned to the ICM_DSCR register.

Tip: For ICM Hashing: When using ICM in the digital signature, the hash value needs to be generated first, then verified by the MCU using ICM's hashing feature. To generate the SHA-256 hash value for a given string in Linux, use the below command.

- `echo -n <String> | sha256sum` should give you the SHA-256 hash value of the string.
- For the message example used above ("abc"), the command is: `echo -n abc | sha256sum`

Tip: Output Hash Value:
`ba7816bf8f01cfea414140de5dae2223b00361a396177a9cb410ff61f20015ad`

This value should match with the hash value generated using the ICM.

3. Relevant Resources

- AT12869: ICM Usage on SAM S/E/V70/71 Microcontrollers http://www.atmel.com/Images/Atmel-42703-ICM-Usage-on-SAM-S7-E7-V7-Microcontrollers_ApplicationNote_AT12869.pdf
- http://www.atmel.com/Images/Atmel-42782-SAM-V70-E70-Ethernet-Bootloader_ApplicationNote_AT17629.pdf
- http://asf.atmel.com/docs/latest/same70/html/sam_drivers_icm_quick_start.html
- http://asf.atmel.com/docs/latest/sam.drivers.icm.example.same70_xplained/html/index.html
- http://csrc.nist.gov/publications/fips/fips180-2/fips180-2withchangenotice.pdf

The Microchip Web Site

Microchip provides online support via our web site at http://www.microchip.com/. This web site is used as a means to make files and information easily available to customers. Accessible by using your favorite Internet browser, the web site contains the following information:

- **Product Support** – Data sheets and errata, application notes and sample programs, design resources, user's guides and hardware support documents, latest software releases and archived software
- **General Technical Support** – Frequently Asked Questions (FAQ), technical support requests, online discussion groups, Microchip consultant program member listing
- **Business of Microchip** – Product selector and ordering guides, latest Microchip press releases, listing of seminars and events, listings of Microchip sales offices, distributors and factory representatives

Customer Change Notification Service

Microchip's customer notification service helps keep customers current on Microchip products. Subscribers will receive e-mail notification whenever there are changes, updates, revisions or errata related to a specified product family or development tool of interest.

To register, access the Microchip web site at http://www.microchip.com/. Under "Support", click on "Customer Change Notification" and follow the registration instructions.

Customer Support

Users of Microchip products can receive assistance through several channels:

- Distributor or Representative
- Local Sales Office
- Field Application Engineer (FAE)
- Technical Support

Customers should contact their distributor, representative or Field Application Engineer (FAE) for support. Local sales offices are also available to help customers. A listing of sales offices and locations is included in the back of this document.

Technical support is available through the web site at: http://www.microchip.com/support

Microchip Devices Code Protection Feature

Note the following details of the code protection feature on Microchip devices:

- Microchip products meet the specification contained in their particular Microchip Data Sheet.
- Microchip believes that its family of products is one of the most secure families of its kind on the market today, when used in the intended manner and under normal conditions.
- There are dishonest and possibly illegal methods used to breach the code protection feature. All of these methods, to our knowledge, require using the Microchip products in a manner outside the operating specifications contained in Microchip's Data Sheets. Most likely, the person doing so is engaged in theft of intellectual property.
- Microchip is willing to work with the customer who is concerned about the integrity of their code.

- Neither Microchip nor any other semiconductor manufacturer can guarantee the security of their code. Code protection does not mean that we are guaranteeing the product as “unbreakable.”

Code protection is constantly evolving. We at Microchip are committed to continuously improving the code protection features of our products. Attempts to break Microchip’s code protection feature may be a violation of the Digital Millennium Copyright Act. If such acts allow unauthorized access to your software or other copyrighted work, you may have a right to sue for relief under that Act.

Legal Notice

Trademarks

ISBN: 978-1-5224-2346-1

Quality Management System Certified by DNV

ISO/TS 16949

Microchip received ISO/TS-16949:2009 certification for its worldwide headquarters, design and wafer fabrication facilities in Chandler and Tempe, Arizona; Gresham, Oregon and design centers in California and India. The Company's quality system processes and procedures are for its PIC® MCUs and dsPIC® DSCs, KEELOQ® code hopping devices, Serial EEPROMs, microperipherals, nonvolatile memory and analog products. In addition, Microchip's quality system for the design and manufacture of development systems is ISO 9001:2000 certified.

Worldwide Sales and Service

AMERICAS	ASIA/PACIFIC	ASIA/PACIFIC	EUROPE
Corporate Office 2355 West Chandler Blvd. Chandler, AZ 85224-6199 Tel: 480-792-7200 Fax: 480-792-7277 Technical Support: http://www.microchip.com/support Web Address: www.microchip.com **Atlanta** Duluth, GA Tel: 678-957-9614 Fax: 678-957-1455 **Austin, TX** Tel: 512-257-3370 **Boston** Westborough, MA Tel: 774-760-0087 Fax: 774-760-0088 **Chicago** Itasca, IL Tel: 630-285-0071 Fax: 630-285-0075 **Dallas** Addison, TX Tel: 972-818-7423 Fax: 972-818-2924 **Detroit** Novi, MI Tel: 248-848-4000 **Houston, TX** Tel: 281-894-5983 **Indianapolis** Noblesville, IN Tel: 317-773-8323 Fax: 317-773-5453 Tel: 317-536-2380 **Los Angeles** Mission Viejo, CA Tel: 949-462-9523 Fax: 949-462-9608 Tel: 951-273-7800 **Raleigh, NC** Tel: 919-844-7510 **New York, NY** Tel: 631-435-6000 **San Jose, CA** Tel: 408-735-9110 Tel: 408-436-4270 **Canada - Toronto** Tel: 905-695-1980 Fax: 905-695-2078	**Asia Pacific Office** Suites 3707-14, 37th Floor Tower 6, The Gateway Harbour City, Kowloon **Hong Kong** Tel: 852-2943-5100 Fax: 852-2401-3431 **Australia - Sydney** Tel: 61-2-9868-6733 Fax: 61-2-9868-6755 **China - Beijing** Tel: 86-10-8569-7000 Fax: 86-10-8528-2104 **China - Chengdu** Tel: 86-28-8665-5511 Fax: 86-28-8665-7889 **China - Chongqing** Tel: 86-23-8980-9588 Fax: 86-23-8980-9500 **China - Dongguan** Tel: 86-769-8702-9880 **China - Guangzhou** Tel: 86-20-8755-8029 **China - Hangzhou** Tel: 86-571-8792-8115 Fax: 86-571-8792-8116 **China - Hong Kong SAR** Tel: 852-2943-5100 Fax: 852-2401-3431 **China - Nanjing** Tel: 86-25-8473-2460 Fax: 86-25-8473-2470 **China - Qingdao** Tel: 86-532-8502-7355 Fax: 86-532-8502-7205 **China - Shanghai** Tel: 86-21-3326-8000 Fax: 86-21-3326-8021 **China - Shenyang** Tel: 86-24-2334-2829 Fax: 86-24-2334-2393 **China - Shenzhen** Tel: 86-755-8864-2200 Fax: 86-755-8203-1760 **China - Wuhan** Tel: 86-27-5980-5300 Fax: 86-27-5980-5118 **China - Xian** Tel: 86-29-8833-7252 Fax: 86-29-8833-7256	**China - Xiamen** Tel: 86-592-2388138 Fax: 86-592-2388130 **China - Zhuhai** Tel: 86-756-3210040 Fax: 86-756-3210049 **India - Bangalore** Tel: 91-80-3090-4444 Fax: 91-80-3090-4123 **India - New Delhi** Tel: 91-11-4160-8631 Fax: 91-11-4160-8632 **India - Pune** Tel: 91-20-3019-1500 **Japan - Osaka** Tel: 81-6-6152-7160 Fax: 81-6-6152-9310 **Japan - Tokyo** Tel: 81-3-6880- 3770 Fax: 81-3-6880-3771 **Korea - Daegu** Tel: 82-53-744-4301 Fax: 82-53-744-4302 **Korea - Seoul** Tel: 82-2-554-7200 Fax: 82-2-558-5932 or 82-2-558-5934 **Malaysia - Kuala Lumpur** Tel: 60-3-6201-9857 Fax: 60-3-6201-9859 **Malaysia - Penang** Tel: 60-4-227-8870 Fax: 60-4-227-4068 **Philippines - Manila** Tel: 63-2-634-9065 Fax: 63-2-634-9069 **Singapore** Tel: 65-6334-8870 Fax: 65-6334-8850 **Taiwan - Hsin Chu** Tel: 886-3-5778-366 Fax: 886-3-5770-955 **Taiwan - Kaohsiung** Tel: 886-7-213-7830 **Taiwan - Taipei** Tel: 886-2-2508-8600 Fax: 886-2-2508-0102 **Thailand - Bangkok** Tel: 66-2-694-1351 Fax: 66-2-694-1350	**Austria - Wels** Tel: 43-7242-2244-39 Fax: 43-7242-2244-393 **Denmark - Copenhagen** Tel: 45-4450-2828 Fax: 45-4485-2829 **Finland - Espoo** Tel: 358-9-4520-820 **France - Paris** Tel: 33-1-69-53-63-20 Fax: 33-1-69-30-90-79 **France - Saint Cloud** Tel: 33-1-30-60-70-00 **Germany - Garching** Tel: 49-8931-9700 **Germany - Haan** Tel: 49-2129-3766400 **Germany - Heilbronn** Tel: 49-7131-67-3636 **Germany - Karlsruhe** Tel: 49-721-625370 **Germany - Munich** Tel: 49-89-627-144-0 Fax: 49-89-627-144-44 **Germany - Rosenheim** Tel: 49-8031-354-560 **Israel - Ra'anana** Tel: 972-9-744-7705 **Italy - Milan** Tel: 39-0331-742611 Fax: 39-0331-466781 **Italy - Padova** Tel: 39-049-7625286 **Netherlands - Drunen** Tel: 31-416-690399 Fax: 31-416-690340 **Norway - Trondheim** Tel: 47-7289-7561 **Poland - Warsaw** Tel: 48-22-3325737 **Romania - Bucharest** Tel: 40-21-407-87-50 **Spain - Madrid** Tel: 34-91-708-08-90 Fax: 34-91-708-08-91 **Sweden - Gothenberg** Tel: 46-31-704-60-40 **Sweden - Stockholm** Tel: 46-8-5090-4654 **UK - Wokingham** Tel: 44-118-921-5800 Fax: 44-118-921-5820