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 fingerprint, then:

$Y = \text{sha}\_\text{hash}(f(x))$

$f(x) \neq \text{any}\_\text{function}(Y)$
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 $2^{264} - 1$ 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**

<table>
<thead>
<tr>
<th>Block 1</th>
<th>Block 2</th>
<th></th>
<th>Block N</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bit 0</td>
<td>Bit M</td>
<td>1</td>
<td>K bits of zero padding</td>
</tr>
</tbody>
</table>

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.
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:

```
ba7816bf8f01cfe414140de5dae2223b00361a396177a9cb410ff61f20015ad
```

This value should match with the hash value generated using the ICM.
3. Relevant Resources

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.


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**

Information contained in this publication regarding device applications and the like is provided only for your convenience and may be superseded by updates. It is your responsibility to ensure that your application meets with your specifications. MICROCHIP MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WHETHER EXPRESS OR IMPLIED, WRITTEN OR ORAL, STATUTORY OR OTHERWISE, RELATED TO THE INFORMATION, INCLUDING BUT NOT LIMITED TO ITS CONDITION, QUALITY, PERFORMANCE, MERCHANTABILITY OR FITNESS FOR PURPOSE. Microchip disclaims all liability arising from this information and its use. Use of Microchip devices in life support and/or safety applications is entirely at the buyer’s risk, and the buyer agrees to defend, indemnify and hold harmless Microchip from any and all damages, claims, suits, or expenses resulting from such use. No licenses are conveyed, implicitly or otherwise, under any Microchip intellectual property rights unless otherwise stated.

**Trademarks**

The Microchip name and logo, the Microchip logo, AnyRate, AVR, AVR logo, AVR Freaks, BeaconThings, BitCloud, CryptoMemory, CryptoRF, dsPIC, FlashFlex, flexPWR, Heldo, JukeBlox, KeeLoq, KeeLoq logo, Kleer, LANCheck, LINK MD, maXStylus, maXTouch, MediaLB, megaAVR, MOST, MOST logo, MPLAB, OptoLyzer, PIC, picoPower, PICSTART, PIC32 logo, Prochip Designer, QTouch, RightTouch, SAM-BA, SpyNIC, SST, SST Logo, SuperFlash, tinyAVR, UNI/O, and XMEGA are registered trademarks of Microchip Technology Incorporated in the U.S.A. and other countries.

ClockWorks, The Embedded Control Solutions Company, EtherSynch, Hyper Speed Control, HyperLight Load, IntelliMOS, mTouch, Precision Edge, and Quiet-Wire are registered trademarks of Microchip Technology Incorporated in the U.S.A.


SQTP is a service mark of Microchip Technology Incorporated in the U.S.A.

Silicon Storage Technology is a registered trademark of Microchip Technology Inc. in other countries.

GestIC is a registered trademark of Microchip Technology Germany II GmbH & Co. KG, a subsidiary of Microchip Technology Inc., in other countries.

All other trademarks mentioned herein are property of their respective companies.

© 2017, Microchip Technology Incorporated, Printed in the U.S.A., All Rights Reserved.
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\textsuperscript{®} MCUs and dsPIC\textsuperscript{®} DSCs, KEELQ\textsuperscript{®} 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

<table>
<thead>
<tr>
<th>AMERICAS</th>
<th>ASIA/PACIFIC</th>
<th>ASIA/PACIFIC</th>
<th>EUROPE</th>
</tr>
</thead>
</table>
| Corporate Office  
2355 West Chandler Blvd.  
Chandler, AZ 85224-6199  
Tel: 480-792-7200  
Fax: 480-792-7277  
Technical Support:  
http://www.microchip.com/  
Web Address:  
www.microchip.com |
| Asia Pacific Office  
Suites 3707-14, 37th Floor  
Tower 6, The Gateway  
Harbour City, Kowloon |
| 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 |
| 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: 886-2-2508-0102 |
| Thailand - Bangkok  
Tel: 66-2-694-1351  
Fax: 66-2-694-1350 |

© 2017 Microchip Technology Inc.