RX Family

M3S-SHA-LIB: SHA-1/SHA-256 Library Introduction Guide

R20AN0157EJ0100
Rev.1.00
Apr 16, 2012

Introduction

This document explains M3S-SHA-LIB: SHA-1/SHA-256 Library for the RX Family (hereafter referred to as "SHA-1/SHA-256 Library") that depends on MCUs.

The SHA-1/SHA-256 Library is the software library incorporated in the RX series. Also it is designed in dedicated algorithm and fully-tuned up by assembly language. Please refer to the User's Manual to know how to use this software library. User's Manual is in installer package.

Target Device

RX Family

Contents

1. Structure of product

SHA-1/SHA-256 Library comprises the following elements.

1. M3S-SHA-LIB: SHA-1/SHA-256 Library for the RX Family V.1.00 Release00E, Installer
2. M3S-SHA-LIB: SHA-1/SHA-256 Library Introduction Guide Rev. 1.00 (r20an0157ej0100_rx_sha.pdf)

part number of this product : R0MRX00QS0010RRC

Table 1 SHA-1/SHA-256 Library product files

name		Description
Installer (setup.exe)		Installer for Windows. Installer will show the Library agreement. If user admits this agreement, installer will copy the file to the path below. [Version for a fee] C:\Renesas\an_r20an0157ej_rx_sha_v100r00p [Evaluation version] C:\Renesas\an_r20an0157ej_rx_sha_v100r00
Library(lib)		
	sha_rx600_big.lib	SHA-1/SHA-256 Library file for the RX600 series (big endian)
	sha_rx600_little.lib	SHA-1/SHA-256 Library file for the RX600 series (little endian)
	sha_rx200_big.lib	SHA-1/SHA-256 Library file for the RX200 series (big endian)
	sha_rx200_little.lib	SHA-1/SHA-256 Library file for the RX200 series (little endian)
	r_sha.h	SHA-1/SHA-256 Library header file
	r_stdint.h	typedef header file
Sample program(sample)		
	sha_rx200_sim_sample	SHA-1/SHA-256 sample program (High-performance Embedded Workshop workspace)
Document(doc)		
	r20uw0101ej0100_sha.pdf	user's manual
	r20an0157ej0100_rx_sha.pdf	Introduction Guide (this document)

Note: When user installs in Windows Vista or Windows 7, Right click the installer (setup.exe) and select the option to "Run as administrator".

2. Specification

2.1 API Function

SHA-1/SHA-256 Library for the RX supports the following functions.

API	Outline
R_Sha1_HashDigest	Generate a SHA-1 hash digest
R_Sha256_HashDigest	Generate a SHA-256 hash digest

2.2 Version information

User can access SHA-1/SHA-256 Library version information with valuable below.

```
extern const char R_sha_version[];

SHA-1/SHA-256 Library file for the RX600 series (big endian)
  "M3S-SHA-LIB version 1.00 for RX600 BIG endian.(Mar 16 2012, 16:56:11)"

SHA-1/SHA-256 Library file for the RX600 series (little endian)
  "M3S-SHA-LIB version 1.00 for RX600 LITTLE endian.(Mar 16 2012, 16:56:17)"

SHA-1/SHA-256 Library file for the RX200 series (big endian)
  "M3S-SHA-LIB version 1.00 for RX200 BIG endian.(Mar 16 2012, 16:55:57)"

SHA-1/SHA-256 Library file for the RX200 series (little endian)
  "M3S-SHA-LIB version 1.00 for RX200 LITTLE endian.(Mar 16 2012, 16:56:06)"
```

2.3 Section

Section Name	Location	Content
P	Program area	Library code
C	Constant area	Constant data
SU	User stack area	Stack
SI	Interrupt stack area	Stack

2.4 SHA-1/SHA-256 Library ROM / RAM / stack size / cycles

2.4.1 ROM/RAM size

library file name	ROM size [byte]	RAM size [byte]
sha_rx600_big.lib	11555	0
sha_rx600_little.lib	11633	0
sha_rx200_big.lib	11555	0
sha_rx200_little.lib	11633	0

2.4.2 stack size

API	stack size [byte]
R_Sha1_HashDigest	168
R_Sha256_HashDigest	180

Note: stack size is same in all library.

2.4.3 cycles

input message length[byte]	SHA-1 [cycles]	SHA-256 [cycles]
0	about 5500	about 5100
64	about 10200	about 9200
128	about 14900	about 13300
192	about 19500	about 17400
256	about 24200	about 21500

Note: Input message is 1 block with padding processing.

2.5 Development environment

[Host OS]

Windows XP SP3

[Software]

When user develops, choose newer version than below.

-Integrated Development Environment

High Performance Embedded Workshop Version 4.09.00.007

-C compiler

C/C++ Compiler Package for RX Family V.1.01 Release 00

-Debugger

(RX600 series)

RX Family Simulator/Debugger V.1.02.00.005

RX600 Simulator Target Platform V.1.02.00.005

(RX200 series)

RX Family Simulator/Debugger V.1.02.00.005

RX200 Simulator Target Platform V.1.00.00.001

2.6 Compiler option for generating library

Libraryfile is built with the following options.

— SHA-1/SHA-256 Library file for the RX600 series (big endian)

- Compiler Options
  -cpu=rx600 -endian=big -include="$(WORKSPDIR)\..\src\library_header" -output=obj="$(CONFIGDIR)\$(FILELEAF).obj" -nologo
- Assembler Options
  -cpu=rx600 -endian=big -output="$(CONFIGDIR)\$(FILELEAF).obj" -nologo
- Optimizing Linkage Editor Options
  -noprelink -form=library -nomessage -list="$(CONFIGDIR)\$(PROJECTNAME).lbp" -nologo -output="$(CONFIGDIR)\$(PROJECTNAME).lib" -exit

— SHA-1/SHA-256 Library file for the RX600 series (little endian)

- Compiler Options
  -cpu=rx600 -include="$(WORKSPDIR)\..\src\library_header" -output=obj="$(CONFIGDIR)\$(FILELEAF).obj" -nologo
- Assembler Options
  -cpu=rx600 -output="$(CONFIGDIR)\$(FILELEAF).obj" -nologo
- Optimizing Linkage Editor Options
  -noprelink -form=library -nomessage -list="$(CONFIGDIR)\$(PROJECTNAME).lbp" -nologo -output="$(CONFIGDIR)\$(PROJECTNAME).lib" -exit

— SHA-1/SHA-256 Library file for the RX200 series (big endian)

- Compiler Options
  -cpu=rx200 -endian=big -include="$(WORKSPDIR)\..\src\library_header" -output=obj="$(CONFIGDIR)\$(FILELEAF).obj" -nologo
- Assembler Options
  -cpu=rx200 -endian=big -output="$(CONFIGDIR)\$(FILELEAF).obj" -nologo
- Optimizing Linkage Editor Options
  -noprelink -form=library -nomessage -list="$(CONFIGDIR)\$(PROJECTNAME).lbp" -nologo -output="$(CONFIGDIR)\$(PROJECTNAME).lib" -exit

— SHA-1/SHA-256 Library file for the RX200 series (little endian)

- Compiler Options
  -cpu=rx200 -include="$(WORKSPDIR)\..\src\library_header" -output=obj="$(CONFIGDIR)\$(FILELEAF).obj" -nologo
- Assembler Options
  -cpu=rx200 -output="$(CONFIGDIR)\$(FILELEAF).obj" -nologo
- Optimizing Linkage Editor Options
  -noprelink -form=library -nomessage -list="$(CONFIGDIR)\$(PROJECTNAME).lbp" -nologo -output="$(CONFIGDIR)\$(PROJECTNAME).lib" -exit

3. Limitations

- This library cannot be used except Microcontroller Options fint_register=0 (Fast interrupt vectorregister [None]). The default for this option is fint_register=0.

Website and Support

Renesas Electronics Website
http://www.renesas.com/

Inquiries
http://www.renesas.com/contact/

Revision Record

		Description	
Rev.	**Date**	**Page**	**Summary**
1.00	Apr.16.12	—	First edition issued

General Precautions in the Handling of MPU/MCU Products

The following usage notes are applicable to all MPU/MCU products from Renesas. For detailed usage notes on the products covered by this manual, refer to the relevant sections of the manual. If the descriptions under General Precautions in the Handling of MPU/MCU Products and in the body of the manual differ from each other, the description in the body of the manual takes precedence.

1. Handling of Unused Pins
   Handle unused pins in accord with the directions given under Handling of Unused Pins in the manual.
   — The input pins of CMOS products are generally in the high-impedance state. In operation with an unused pin in the open-circuit state, extra electromagnetic noise is induced in the vicinity of LSI, an associated shoot-through current flows internally, and malfunctions occur due to the false recognition of the pin state as an input signal become possible. Unused pins should be handled as described under Handling of Unused Pins in the manual.
2. Processing at Power-on
   The state of the product is undefined at the moment when power is supplied.
   — The states of internal circuits in the LSI are indeterminate and the states of register settings and pins are undefined at the moment when power is supplied.
   In a finished product where the reset signal is applied to the external reset pin, the states of pins are not guaranteed from the moment when power is supplied until the reset process is completed.
   In a similar way, the states of pins in a product that is reset by an on-chip power-on reset function are not guaranteed from the moment when power is supplied until the power reaches the level at which resetting has been specified.
3. Prohibition of Access to Reserved Addresses
   Access to reserved addresses is prohibited.
   — The reserved addresses are provided for the possible future expansion of functions. Do not access these addresses; the correct operation of LSI is not guaranteed if they are accessed.
4. Clock Signals
   After applying a reset, only release the reset line after the operating clock signal has become stable. When switching the clock signal during program execution, wait until the target clock signal has stabilized.
   — When the clock signal is generated with an external resonator (or from an external oscillator) during a reset, ensure that the reset line is only released after full stabilization of the clock signal. Moreover, when switching to a clock signal produced with an external resonator (or by an external oscillator) while program execution is in progress, wait until the target clock signal is stable.
5. Differences between Products
   Before changing from one product to another, i.e. to one with a different type number, confirm that the change will not lead to problems.
   — The characteristics of MPU/MCU in the same group but having different type numbers may differ because of the differences in internal memory capacity and layout pattern. When changing to products of different type numbers, implement a system-evaluation test for each of the products.

Notice

1. All information included in this document is current as of the date this document is issued. Such information, however, is subject to change without any prior notice. Before purchasing or using any Renesas Electronics products listed herein, please confirm the latest product information with a Renesas Electronics sales office. Also, please pay regular and careful attention to additional and different information to be disclosed by Renesas Electronics such as that disclosed through our website.
2. Renesas Electronics does not assume any liability for infringement of patents, copyrights, or other intellectual property rights of third parties by or arising from the use of Renesas Electronics products or technical information described in this document. No license, express, implied or otherwise, is granted hereby under any patents, copyrights or other intellectual property rights of Renesas Electronics or others.
3. You should not alter, modify, copy, or otherwise misappropriate any Renesas Electronics product, whether in whole or in part.
4. Descriptions of circuits, software and other related information in this document are provided only to illustrate the operation of semiconductor products and application examples. You are fully responsible for the incorporation of these circuits, software, and information in the design of your equipment. Renesas Electronics assumes no responsibility for any losses incurred by you or third parties arising from the use of these circuits, software, or information.
5. When exporting the products or technology described in this document, you should comply with the applicable export control laws and regulations and follow the procedures required by such laws and regulations. You should not use Renesas Electronics products or the technology described in this document for any purpose relating to military applications or use by the military, including but not limited to the development of weapons of mass destruction. Renesas Electronics products and technology may not be used for or incorporated into any products or systems whose manufacture, use, or sale is prohibited under any applicable domestic or foreign laws or regulations.
6. Renesas Electronics has used reasonable care in preparing the information included in this document, but Renesas Electronics does not warrant that such information is error free. Renesas Electronics assumes no liability whatsoever for any damages incurred by you resulting from errors in or omissions from the information included herein.
7. Renesas Electronics products are classified according to the following three quality grades: "Standard", "High Quality", and "Specific". The recommended applications for each Renesas Electronics product depends on the product's quality grade, as indicated below. You must check the quality grade of each Renesas Electronics product before using it in a particular application. You may not use any Renesas Electronics product for any application categorized as "Specific" without the prior written consent of Renesas Electronics. Further, you may not use any Renesas Electronics product for any application for which it is not intended without the prior written consent of Renesas Electronics. Renesas Electronics shall not be in any way liable for any damages or losses incurred by you or third parties arising from the use of any Renesas Electronics product for an application categorized as "Specific" or for which the product is not intended where you have failed to obtain the prior written consent of Renesas Electronics. The quality grade of each Renesas Electronics product is "Standard" unless otherwise expressly specified in a Renesas Electronics data sheets or data books, etc.
   - "Standard": Computers; office equipment; communications equipment; test and measurement equipment; audio and visual equipment; home electronic appliances; machine tools; personal electronic equipment; and industrial robots.
   - "High Quality": Transportation equipment (automobiles, trains, ships, etc.); traffic control systems; anti-disaster systems; anti-crime systems; safety equipment; and medical equipment not specifically designed for life support.
   - "Specific": Aircraft; aerospace equipment; submersible repeaters; nuclear reactor control systems; medical equipment or systems for life support (e.g. artificial life support devices or systems), surgical implantations, or healthcare intervention (e.g. excision, etc.), and any other applications or purposes that pose a direct threat to human life.
8. You should use the Renesas Electronics products described in this document within the range specified by Renesas Electronics, especially with respect to the maximum rating, operating supply voltage range, movement power voltage range, heat radiation characteristics, installation and other product characteristics. Renesas Electronics shall have no liability for malfunctions or damages arising out of the use of Renesas Electronics products beyond such specified ranges.
9. Although Renesas Electronics endeavors to improve the quality and reliability of its products, semiconductor products have specific characteristics such as the occurrence of failure at a certain rate and malfunctions under certain use conditions. Further, Renesas Electronics products are not subject to radiation resistance design. Please be sure to implement safety measures to guard them against the possibility of physical injury, and injury or damage caused by fire in the event of the failure of a Renesas Electronics product, such as safety design for hardware and software including but not limited to redundancy, fire control and malfunction prevention, appropriate treatment for aging degradation or any other appropriate measures. Because the evaluation of microcomputer software alone is very difficult, please evaluate the safety of the final products or system manufactured by you.
10. Please contact a Renesas Electronics sales office for details as to environmental matters such as the environmental compatibility of each Renesas Electronics product. Please use Renesas Electronics products in compliance with all applicable laws and regulations that regulate the inclusion or use of controlled substances, including without limitation, the EU RoHS Directive. Renesas Electronics assumes no liability for damages or losses occurring as a result of your noncompliance with applicable laws and regulations.
11. This document may not be reproduced or duplicated, in any form, in whole or in part, without prior written consent of Renesas Electronics.
12. Please contact a Renesas Electronics sales office if you have any questions regarding the information contained in this document or Renesas Electronics products, or if you have any other inquiries.

(Note 1) "Renesas Electronics" as used in this document means Renesas Electronics Corporation and also includes its majority-owned subsidiaries.

(Note 2) "Renesas Electronics product(s)" means any product developed or manufactured by or for Renesas Electronics.

RENESAS

SALES OFFICES Renesas Electronics Corporation http://www.renesas.com

Refer to "http://www.renesas.com/" for the latest and detailed information.

Renesas Electronics America Inc.
2880 Scott Boulevard Santa Clara, CA 95050-2554, U.S.A.
Tel: +1-408-588-6000, Fax: +1-408-588-6130

Renesas Electronics Canada Limited
1101 Nicholson Road, Newmarket, Ontario L3Y 9C3, Canada
Tel: +1-905-898-5441, Fax: +1-905-898-3220

Renesas Electronics Europe Limited
Dukes Meadow, Millboard Road, Bourne End, Buckinghamshire, SL8 5FH, U.K
Tel: +44-1628-585-100, Fax: +44-1628-585-900

Renesas Electronics Europe GmbH
Arcadiastrasse 10, 40472 Düsseldorf, Germany
Tel: +49-211-65030, Fax: +49-211-6503-1327

Renesas Electronics (China) Co., Ltd.
7th Floor, Quantum Plaza, No.27 ZhiChunLu Haidian District, Beijing 100083, P.R.China
Tel: +86-10-8235-1155, Fax: +86-10-8235-7679

Renesas Electronics (Shanghai) Co., Ltd.
Unit 204, 205, AZIA Center, No.1233 Lujiazui Ring Rd., Pudong District, Shanghai 200120, China
Tel: +86-21-5877-1818, Fax: +86-21-6887-7858 / -7898

Renesas Electronics Hong Kong Limited
Unit 1601-1613, 16/F., Tower 2, Grand Century Place, 193 Prince Edward Road West, Mongkok, Kowloon, Hong Kong
Tel: +852-2886-9318, Fax: +852 2886-9022/9044

Renesas Electronics Taiwan Co., Ltd.
13F, No. 363, Fu Shing North Road, Taipei, Taiwan
Tel: +886-2-8175-9600, Fax: +886 2-8175-9670

Renesas Electronics Singapore Pte. Ltd.
1 harbourFront Avenue, #06-10, keppel Bay Tower, Singapore 098632
Tel: +65-6213-0200, Fax: +65-6278-8001

Renesas Electronics Malaysia Sdn.Bhd.
Unit 906, Block B, Menara Amcorp, Amcorp Trade Centre, No. 18, Jln Persiaran Barat, 46050 Petaling Jaya, Selangor Darul Ehsan, Malaysia
Tel: +60-3-7955-9390, Fax: +60-3-7955-9510

Renesas Electronics Korea Co., Ltd.
11F., Samik Lavied' or Bldg., 720-2 Yeoksam-Dong, Kangnam-Ku, Seoul 135-080, Korea
Tel: +82-2-558-3737, Fax: +82-2-558-5141

Colophon 1.1