RL78 Family

SHA Hash Function Library: Introduction Guide

R20AN0211EJ0103
Rev.1.03
Jul 01, 2016

Introduction

This document explains SHA Hash Function Library for the RL78 Family V.1.02 Release 01 (hereafter referred to as "SHA Library") that depends on MCUs.

The SHA Library is the software library that processes HASH calculation for RL78 Family. 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.

Target Device

RL78/G13, RL78/G14

Contents

1. Structure of product

Table 1 SHA Library product files

Name	Description
Document(doc)	
English (en)	
r20uw0101ej0101_sha.pdf.pdf	User's manual
r20an0211jej0103_rl78_sha.pdf	Introduction Guide (this document)
Japanese (ja)	
r20uw0101jj0101_sha.pdf	User's manual
r20an0211jj0103_rl78_sha.pdf	Introduction Guide
for CS+ for CA, CX(CS+ for CA)	
Library(lib)	
sha_rl78_l.lib sha_rl78_m.lib sha_rl78_s.lib	SHA Library - Large model - Medium model - Small model
r_sha.h	SHA Library header file
r_mw_version.h	Version data header file
r_stdint.h	typedef header file
Sample program(sample)	
rl78_sim_sha	Sample program (CS+ for CA, CX Project)
for CS+ for CC(CS+ for CC)	
Library(lib)	
sha_rl78_s2_ccrl_m.lib sha_rl78_s2_ccrl_s.lib sha_rl78_s3_ccrl_m.lib sha_rl78_s3_ccrl_s.lib	SHA Library - RL78 core S2- Medium model - RL78 core S2- Small model - RL78 core S3- Medium model - RL78 core S3- Small model
r_sha.h	SHA Library header file
r_mw_version.h	Version data header file
r_stdint.h	typedef header file
Sample program(sample)	
rl78_sim_sha_ccrl	Sample program (CS+ for CC Project)
for IAR Embedded Workbench (IAR)	
Library(lib)	
sha_rl78_s2_l.a sha_rl78_s2_m.a sha_rl78_s2_s.a sha_rl78_s3_l.a sha_rl78_s3_m.a sha_rl78_s3_s.a	SHA Library(Device / Code model / Data model) - RL78 core S2 - Unspecified / Far / Far - RL78 core S2 - Unspecified / Far / Near - RL78 core S2 - Unspecified / Near / Near - RL78 core S3 - Unspecified / Far / Far - RL78 core S3 - Unspecified / Far / Near - RL78 core S3 - Unspecified / Near / Near
r_sha.h	SHA Library header file
r_mw_version.h	Version data header file
r_stdint.h	typedef header file
Sample program(sample)	
rl78_sim_sha_iar	Sample program (IAR IDE Workspace)

2. API Function

SHA Library for the RL78 supports the following functions.

Table 2 Library Functions (API)

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

3. For CS+ for CA, CX

3.1 Development environment

Please use the same or a later version of the toolchain listed below:

- Integrated Development Environment:
  CS+ V2.02.00
- C compiler:
  CA78K0R V1.70

3.2 Compiler option

Library file is built with the following options.

・sha_rl78_l.lib:
```
-cf1006a -qx2 -common -ml -mi0 –ng –nga
```

・sha_rl78_m.lib:
```
-cf1006a -qx2 -common -mm -mi0 –ng –nga
```

・sha_rl78_s.lib:
```
-cf1006a -qx2 -common -ms -mi0 –ng –nga
```

3.3 ROM / RAM / Stack size

The ROM, RAM, and stack size of SHA Library functions (API) are shown below (Unit = byte):

Table 3 ROM, RAM Size

library file name	ROM size [byte] (Note)	RAM size [byte]
sha_rl78_l.lib	4882	0
sha_rl78_m.lib	4804	0
sha_rl78_s.lib	4796	0

Note SHA Library needs 388 bytes (max) for mirror area.
In case, user does not use version information or, user uses large model, the memory size for mirror area requires 256 bytes.

Table 4 Stack Size

API	stack size [byte] (Note)
R_Sha1_HashDigest	138
R_Sha256_HashDigest	174

Note: stack size is same in all library.

3.4 Section Information

The following table shows program sections (segments) used by SHA Library.

Table 5 Sections

Section name	Contents	Section Attributes
@@CODE / @@CODEL	program code	CSEG
@@CNST / @@CNSTL	constant data	CSEG MIRRORP

3.5 Performance

Library performance between the each library does not almost exist.

The following table values are executing time of "Medium model library" in RL78/G13.

Table 6 SHA Library Performance

system clock = 32MHz

input message length[byte]	SHA-1 [us]	SHA-256 [us]
0	700	1058
64	1326	2030
128	1947	2998
192	2568	3965
256	3189	4932

Note: Input message is 1 block with padding processing.

3.6 Version information

Version information is stored in this library. Version information can be accessed if the header of this library is included. The data stored in this library is as follows.

```
#include "r_sha.h"
```

Table 7 Version information

Library	R_sha_version.library[]	R_sha_version.compiler
sha_rl78_l.lib	SHA Hash Function Library version 1.01 for RL78 (S2, LARGE).(Jun 20 2014, 10:45:16)	0xFFFFFFFF (n/a)
sha_rl78_m.lib	SHA Hash Function Library version 1.01 for RL78 (S2, MEDIUM).(Jun 20 2014, 10:45:15)	
sha_rl78_s.lib	SHA Hash Function Library version 1.01 for RL78 (S2, SMALL).(Jun 20 2014, 10:45:15)	

3.7 Notes

- Modules for which a different memory model is specified cannot be linked.
- The pointer of a variable with a __far instruction modifier cannot be specified as an argument.

4. For CS+ for CC

4.1 Development environment

Please use the same or a later version of the toolchain listed below:

- Integrated Development Environment:
  CS+ V4.00.00
- C compiler:
  CC-RL V1.02

4.2 Compiler option

Library file is built with the following options.

・sha_rl78_s2_ccrl_m.lib:
-cpu=S2 -memory_model=medium -asmopt=-mirror_source=common –NOLOgo

・sha_rl78_s2_ccrl_s.lib:
-cpu=S2 -memory_model=small -asmopt=-mirror_source=common –NOLOgo

・sha_rl78_s3_ccrl_m.lib:
-cpu=S3 -memory_model=medium -asmopt=-mirror_source=common –NOLOgo

・SHA_rl78_s3_ccrl_s.lib:
-cpu=S3 -memory_model=small -asmopt=-mirror_source=common -NOLOgo

4.3 ROM / RAM / Stack size

The ROM, RAM, and stack size of SHA Library functions (API) are shown below (Unit = byte):

Table 8 ROM, RAM Size

library file name	ROM size [byte] (Note)	RAM size [byte]
sha_rl78_s2_ccrl_m.lib	4362	0
sha_rl78_s2_ccrl_s.lib	4354	0
sha_rl78_s3_ccrl_m.lib	4362	0
sha_rl78_s3_ccrl_s.lib	4354	0

Note SHA Library needs 388 bytes (max) for mirror area.
In case, user does not use version information or, user uses large model, the memory size for mirror area requires 256 bytes.

Table 9 Stack Size

API	stack size [byte] (Note)
R_Sha1_HashDigest	136
R_Sha256_HashDigest	172

Note: stack size is same in all library.

4.4 Section Information

The following table shows program sections (segments) used by SHA Library.

Table 10 Sections

Section name	Contents	Section Attributes
.textf .text(*1)	プログラム	.CSEG
.const	定数データ	.CSEG CONST

(*1) For Code model=near.

4.5 Performance

Library performance between the each library does not almost exist.

The following table values are executing time of "Medium model library" in RL78/G13.

Table 11 SHA Library Performance

system clock = 32MHz

input message length[byte]	SHA-1 [us]	SHA-256 [us]
0	661	1016
64	1280	1983
128	1895	2944
192	2510	3906
256	3126	4867

Note: Input message is 1 block with padding processing.

4.6 Version information

Version information is stored in this library. Version information can be accessed if the header of this library is included. The data stored in this library is as follows.

```
#include "r_sha.h"
```

Table 12 Version information

Library	R_sha_version.library[]	R_sha_version.compiler
sha_rl78_s2_ccrl_m.lib	SHA Hash Function Library version 1.02 for RL78 (CCRL, S2, MEDIUM).(Jun 30 2016, 09:37:53)	0x01020000
sha_rl78_s2_ccrl_s.lib	SHA Hash Function Library version 1.02 for RL78 (CCRL, S2, SMALL).(Jun 30 2016, 09:37:51)	
sha_rl78_s3_ccrl_m.lib	SHA Hash Function Library version 1.02 for RL78 (CCRL, S3, MEDIUM).(Jun 30 2016, 09:36:46)	
sha_rl78_s3_ccrl_s.lib	SHA Hash Function Library version 1.02 for RL78 (CCRL, S3, SMALL).(Jun 30 2016, 09:36:34)	

4.7 Notes

- Modules for which a different memory model is specified cannot be linked.
- The pointer of a variable with a __far instruction modifier cannot be specified as an argument.

5. For IAR Embedded Workbench

5.1 Development environment

Please use the same or a later version of the toolchain listed below:

- Integrated Development Environment:
  IAR Embedded Workbench for Renesas RL78 version 2.21.1
- C compiler:
  IAR C/C++ Compiler for Renesas RL78 : 2.21.1.1833 (2.21.1.1833)

5.2 Compiler option

Library file is built with the following options.

- sha_rl78_s2_l.a

  --core=s2, --code_model=far, --data_model=far,

  --near_const_location=rom0, -e, -Oh, ---calling_convention=v2

- sha_rl78_s2_m.a

  --core=s2, --code_model=far, --data_model=near,

  --near_const_location=rom0, -e, -Oh, ---calling_convention=v2

- sha_rl78_s2_s.a

  --core=s2, --code_model=near, --data_model=near,

  --near_const_location=rom0, -e, -Oh, ---calling_convention=v2

- sha_rl78_s3_l.a

  --core=s3, --code_model=far, --data_model=far,

  --near_const_location=rom0, -e, -Oh, ---calling_convention=v2

- sha_rl78_s3_m.a

  --core=s3, --code_model=far, --data_model=near,

  --near_const_location=rom0, -e, -Oh, ---calling_convention=v2

- sha_rl78_s3_s.a

  --core=s3, --code_model=near, --data_model=near,

  --near_const_location=rom0, -e, -Oh, ---calling_convention=v2

5.3 ROM / RAM / Stack size

The ROM, RAM, and stack size of SHA Library functions (API) are shown below (Unit = byte):

Table 13 ROM, RAM Size

library file name	ROM size [byte] (Note)	RAM size [byte]
sha_rl78_s2_l.a	4445	0
sha_rl78_s2_m.a	4445	0
sha_rl78_s2_s.a	4423	0
sha_rl78_s3_l.a	4445	0
sha_rl78_s3_m.a	4445	0
sha_rl78_s3_s.a	4423	0

Note SHA Library needs 388 bytes (max) for mirror area.

In case, user does not use version information or, user uses large model, the memory size for mirror area requires 256 bytes.

Table 14 Stack Size

API	stack size [byte] (Note)
R_Sha1_HashDigest	138
R_Sha256_HashDigest	174

Note: stack size is same in all library.

5.4 Section Information

The following table shows program sections (segments) used by SHA Library.

Table 15 Segments

Segments	Contents
.text .textf(*1)	program code
.const .constf(*2)	constant data

(*1) For Code model=far.

(*2) For Data model=far.

5.5 Performance

There is no difference between the each library.

This table value is executing sha_rl78_s2_m.a(RL78 core S2 - Unspecified / Far / Near) “” in Renesas Starter Kit for RL78/G13.(Using the Function Profiler)

Table 16 SHA Library Performance

system clock = 32MHz

input message length[byte]	SHA-1 [us]	SHA-256 [us]
0	594	931
64	1162	1831
128	1726	2727
192	2291	3622
256	2856	4517

Note: Input message is 1 block with padding processing.

5.6 Version information

Version information is stored in this library. Version information can be accessed if the header of this library is included. The data stored in this library is as follows.

#include "r_sha.h"

Table 17 Version information

Library	R_sha_version.library[]	R_sha_version.compiler
sha_rl78_s2_l.lib	SHA Hash Function Library version 1.02 for RL78 (IAR, S2, code_model=far, data_model=far).(Jun 16 2016, 14:01:50)	0x000000DD (221)
sha_rl78_s2_m.lib	SHA Hash Function Library version 1.02 for RL78 (IAR, S2, code_model=far, data_model=near).(Jun 16 2016, 14:02:37)	
sha_rl78_s2_s.lib	SHA Hash Function Library version 1.02 for RL78 (IAR, S2, code_model=near, data_model=near).(Jun 16 2016, 14:03:28)	
sha_rl78_s3_l.lib	SHA Hash Function Library version 1.02 for RL78 (IAR, S3, code_model=far, data_model=far).(Jun 16 2016, 14:05:28)	
sha_rl78_s3_m.lib	SHA Hash Function Library version 1.02 for RL78 (IAR, S3, code_model=far, data_model=near).(Jun 16 2016, 14:06:13)	
sha_rl78_s3_s.lib	SHA Hash Function Library version 1.02 for RL78 (IAR, S3, code_model=near, data_model=near).(Jun 16 2016, 14:06:58)	

5.7 Notes

- Modules for which a different memory model is specified cannot be linked.
- The pointer of a variable with a __far instruction modifier cannot be specified as an argument.

Website and Support

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

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

Revision History

		Description	
Rev.	**Date**	**Page**	**Summary**
1.03	Jul 01, 2016	—	Supported CC-RL. Supported IAR Embedded Workbench 7.4(v2.21.1).
1.02	Apr 01, 2015	—	Supported IAR Embedded Workbench.
1.01	Sep 30, 2014		Improved document. Changed for V.1.01 Release 00. - Fixed problem when input pointer is an odd address.
		—	Added support for the small model and the large model.
1.00	Oct 16, 2012	—	First edition issued

General Precautions in the Handling of Microprocessing Unit and Microcontroller Unit Products

The following usage notes are applicable to all Microprocessing unit and Microcontroller unit products from Renesas. For detailed usage notes on the products covered by this document, refer to the relevant sections of the document as well as any technical updates that have been issued for the products.

1. Handling of Unused Pins

   Handle unused pins in accordance 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 a product with a different part number, confirm that the change will not lead to problems.

   — The characteristics of Microprocessing unit or Microcontroller unit products in the same group but having a different part number may differ in terms of the internal memory capacity, layout pattern, and other factors, which can affect the ranges of electrical characteristics, such as characteristic values, operating margins, immunity to noise, and amount of radiated noise. When changing to a product with a different part number, implement a system-evaluation test for the given product.

Notice

1. 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.
2. 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.
3. 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.
4. You should not alter, modify, copy, or otherwise misappropriate any Renesas Electronics product, whether in whole or in part. Renesas Electronics assumes no responsibility for any losses incurred by you or third parties arising from such alteration, modification, copy or otherwise misappropriation of Renesas Electronics product.
5. Renesas Electronics products are classified according to the following two quality grades: "Standard" and "High Quality". The recommended applications for each Renesas Electronics product depends on the product's quality grade, as indicated below.
   "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 etc.
   "High Quality": Transportation equipment (automobiles, trains, ships, etc.); traffic control systems; anti-disaster systems; anti-crime systems; and safety equipment etc.
   Renesas Electronics products are neither intended nor authorized for use in products or systems that may pose a direct threat to human life or bodily injury (artificial life support devices or systems, surgical implantations etc.), or may cause serious property damages (nuclear reactor control systems, military equipment etc.). 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 for which it is not intended. 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 which the product is not intended by Renesas Electronics.
6. 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.
7. 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 systems manufactured by you.
8. 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.
9. 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. You should not use Renesas Electronics products or 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. When exporting the Renesas Electronics 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.
10. It is the responsibility of the buyer or distributor of Renesas Electronics products, who distributes, disposes of, or otherwise places the product with a third party, to notify such third party in advance of the contents and conditions set forth in this document, Renesas Electronics assumes no responsibility for any losses incurred by you or third parties as a result of unauthorized use of Renesas Electronics products.
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.
2801 Scott Boulevard Santa Clara, CA 95050-2549, U.S.A.
Tel: +1-408-588-6000, Fax: +1-408-588-6130

Renesas Electronics Canada Limited
9251 Yonge Street, Suite 8309 Richmond Hill, Ontario Canada L4C 9T3
Tel: +1-905-237-2004

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: +49-211-6503-0, Fax: +49-211-6503-1327

Renesas Electronics (China) Co., Ltd.
Room 1709, Quantum Plaza, No.27 ZhiChunLu Haidian District, Beijing 100191, P.R.China
Tel: +86-10-8235-1155, Fax: +86-10-8235-7679

Renesas Electronics (Shanghai) Co., Ltd.
Unit 301, Tower A, Central Towers, 555 Langao Road, Putuo District, Shanghai, P. R. China 200333
Tel: +86-21-2226-0888, Fax: +86-21-2226-0999

Renesas Electronics Hong Kong Limited
Unit 1601-1611, 16/F., Tower 2, Grand Century Place, 193 Prince Edward Road West, Mongkok, Kowloon, Hong Kong
Tel: +852-2265-6688, Fax: +852 2886-9022

Renesas Electronics Taiwan Co., Ltd.
13F, No. 363, Fu Shing North Road, Taipei 10543, Taiwan
Tel: +886-2-8175-9600, Fax: +886 2-8175-9670

Renesas Electronics Singapore Pte. Ltd.
80 Bendemeer Road, Unit #06-02 Hyflux Innovation Centre, Singapore 339949
Tel: +65-6213-0200, Fax: +65-6213-0300

Renesas Electronics Malaysia Sdn.Bhd.
Unit 1207, 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 India Pvt. Ltd.
No.777C, 100 Feet Road, HALII Stage, Indiranagar, Bangalore, India
Tel: +91-80-67208700, Fax: +91-80-67208777

Renesas Electronics Korea Co., Ltd.
12F., 234 Teheran-ro, Gangnam-Gu, Seoul, 135-080, Korea
Tel: +82-2-558-3737, Fax: +82-2-558-5141

Colophon 5.0