RX Family

SHA Library Firmware Integration Technology

R20AN0157EJ0106
Rev.1.06
Mar.20.2025

Introduction

This application note explains information for implementing the RX Family SHA library (hereafter referred to as the SHA FIT library) using Firmware Integration Technology (FIT).

SHA FIT library is a software library for realizing SHA-1 / SHA-256 / SHA-384 hash calculation processing with RX microcomputer. The SHA FIT library is designed for efficient processing using an RX microcontroller. Please refer to the user's manual (R20UW0101JJ0200) included in the package for details on how to use the SHA FIT library.

Target Device

RX Family

When applying this application note to other microcontrollers, please modify it according to the specifications of the microcontroller and evaluate it thoroughly.

Target Compiler

Renesas Electronics C/C++ Compiler Package for RX Family

GCC for Renesas RX

IAR Embedded Workbench for Renesas RX

For detailed information on the compiler's system requirements, please refer to Section "4.1 Confirmed Operation Environment".

Related Documents

Firmware Integration Technology User’s Manual (R01AN1833)

Board Support Package Module Using Firmware Integration Technology (R01AN1685)

Adding Firmware Integration Technology Modules to Projects (R01AN1723)

Adding Firmware Integration Technology Modules to CS+ Projects (R01AN1826)

Renesas e2studio Smart Configurator User's Guide (R20AN0451)

Contents

1. Overview

1.1 SHA FIT Library

This library is used as an API to be embedded in a project. See "2.9 Adding the FIT Module to Your Project " for details on how to incorporate this library.

1.2 SHA FIT Library Overview

Please refer to the user's manual (R20UW0101JJ0200) stored in the package.

1.3 API Function

SHA Library for the RX supports the following functions.

For details on each API function, please refer to the user's manual (R20UW0101JJ0200).

Table 1-1 SHA Library API Function

API	Outline
R_Sha1_HashDigest	Generate a SHA-1 hash digest
R_Sha256_HashDigest	Generate a SHA-256 hash digest
R_Sha384_HashDigest	Generate a SHA-384 hash digest

1.4 Version Information

In the SHA-1/SHA-256/SHA-384 Library, the version information is stored as a character string in the R_sha_version variable. This variable can be accessed by the following extern declaration.

```
extern const char R_sha_version[];
```

1.5 The Structure of SHA FIT Library

1.5.1 Application Note Structure

This product includes the files listed in Table 1-2 Structure of Product Files below.

Table 1-2 Structure of Product Files

File / Directory(bold) Names	Description
r20an0157jj0106-rx-sha.pdf	SHA FIT Library Application Note (Japanese)
r20an0157ej0106-rx-sha.pdf	SHA FIT Library Application Note (English)
r20uw0101jj0200-sha.pdf	SHA FIT Library User's manual (Japanese)
r20uw0101ej0200-sha.pdf	SHA FIT Library User's manual (English)
FITDemos	FIT Module Demo Program folder
sha_demo_65n_2m.zip	SHA FIT Module Demo Program
FITModules	FIT Module folder
r_sha_rx_v1.06.zip	SHA FIT Module
r_sha_rx_v1.06.xml	SHA FIT Module XML file
r_sha_rx_v1.06_extend.mdf	SHA FIT Module MDF file

1.5.2 File Structure

The folder to which the content of r_sha_rx_v1.06.zip is extracted will contain the files listed in Table 1-3 File Structure below.

Table 1-3 File Structure

File / Directory(bold) Names	Description
r_sha_rx	FIT Module folder
doc	Document folder
en	Document folder (English)
r20an0157ej0106-rx-sha.pdf	SHA FIT Library Application Note (English)
r20uw0101ej0200-sha.pdf	SHA FIT Library User's manual (English)
ja	Document folder (Japanese)
r20an0157jj0106-rx-sha.pdf	SHA FIT Library Application Note (Japanese)
r20uw0101jj0200-sha.pdf	SHA FIT Library User's manual (Japanese)
ref	Reference folder
r_sha_config_reference.h	Configure reference file
src	Source code folder
sha1if.c	SHA-1 API function definition
sha256if.c	SHA-256 API function definition
sha384if.c	SHA-384 API function definition
shaif.h	Core part of API function
sha1.c	Core part of SHA-1 calculation
sha256.c	Core part of SHA-256 calculation
sha512.c	Core part of SHA-384 / SHA-512 calculation
r_sha_version.c	SHA library Version Information
r_mw_version.h	Version data header file
r_stdint.h	Typedef header file
r_sha_rx_if.h	SHA library header file
readme.txt	Readme file
r_config	Config file folder
r_sha_config.h	Config file (default)

2. API Information

2.1 Hardware Requirements

There are no hardware requirements.

2.2 Software Requirements

There are no software requirements.

2.3 Limitations

There are no software limitations.

2.4 Supported Toolchain

This driver has been confirmed to work with the toolchain listed in “4.1 Confirmed Operation Environment”.

2.5 Header Files

All API calls and their supporting interface definitions are in r_sha_rx_if.h.

2.6 Integer Type

This project uses ANSI C99. These types are defined in stdint.h.

2.7 Notes on Building

If this FIT Module is used together with any of the following FIT Modules, build errors may occur depending on the project settings.

When using the following FIT Modules together with this FIT module, please adjust the build order so that this FIT Module is built first.

FIT Module	Short Name
JPEG Decoder Module	r_jpegd_rx
JPEG Encoder Module	r_jpege_rx
TCP/IP for Embedded system M3S-T4-Tiny Module	r_t4_rx
Sound Playback/Compression System (Original ADPCM Codec) [M3S-S2-Tiny] Module	r_s2_rx

2.8 How to Use Library Functions

2.8.1 Execution Performance vs. Code Size

The SHA library for RX has two approaches: one is to emphasize execution performance (faster) by optimizing the program code size (hereinafter referred to as "execution performance-oriented"), and the other is to emphasize the program code size (smaller) rather than improving execution performance (hereinafter referred to as "code size-oriented").

The configuration options for this module are set in r_sha_config.h.

The table below describes the option names and setting values.

Configuration option in r_sha_config.h	
Definition	**Description**
#define SHA_CFG_BUILD_OPTION	You can choose to " execution performance-oriented" or "code size-oriented".

※The default value is "0": "execution performance-oriented " will be set.	0 : SPEED (emphasis on execution performance) 1 : SIZE (emphasis on code size)

The following macro definitions are enabled by the above option settings.

Macro	Select Implementation	API
__COMPILE_EMPHASIS_SPEED__	compile with emphasis on execution performance	R_Sha256_HashDigest / R_Sha384_HashDigest
__COMPILE_EMPHASIS_SIZE__	compile with emphasis on code size	R_Sha256_HashDigest / R_Sha384_HashDigest

2.9 SHA Library ROM / RAM / Stack Size / Performance

The various sizes and processing cycles when building with the following optimization options are described for reference.

CCRX : Level2 performs whole module optimization

GCC : -O2

IAR : High (size)

2.9.1 ROM/RAM Size

API	Little/Big Endian	Implementation	ROM size [byte]			RAM size [byte]		
			CCRX	GCC	IAR	CCRX	GCC	IAR
R_Sha1_HashDigest	Little/Big	-	421	576	483	0	0	0
R_Sha256_HashDigest	Little/Big	-	444	592	499	0	0	0
R_Sha384_HashDigest	Little/Big	-	397	552	469	0	0	0

Note: "-" means execution performance-oriented and code size-oriented, and there is no change in the code.

2.9.2 Stack Size

API	Little/Big Endian	Implementation	Stack Size [byte]		
			CCRX	GCC	IAR
R_Sha1_HashDigest	Little/Big	-	32	36	28
R_Sha256_HashDigest	Little/Big	-	32	36	28
R_Sha384_HashDigest	Little/Big	-	32	36	28

Note: "-" means execution performance-oriented and code size-oriented, and there is no change in the code.

2.9.3 Performance

The performance of SHA library.

The measurement condition is CC-RX and optimization level 2.

The implementation is execution performance oriented.

Input message length [byte]	Little/Big Endian	SHA-1 [cycles]	SHA-256 [cycles]	SHA-384 [cycles]
0	Little	4938	4628	16544
	Big	4954	4456	16512
64	Little	9358	8668	15824
	Big	9382	8316	15802
128	Little	13636	12556	30624
	Big	13666	12182	30576
192	Little	17768	16256	30456
	Big	17950	15902	30414
256	Little	21902	19970	44588
	Big	21934	19616	44526

Note: The message is entered once and is the processing time including the internal padding process.

2.10 Adding the FIT Module to Your Project

This module must be added to each project in which it is used. Renesas recommends the method using the Smart Configurator described in (1) or (3) below. However, the Smart Configurator only supports some RX devices. Please use the methods of (2) or (4) for RX devices that are not supported by the Smart Configurator.

(1) Adding the FIT module to your project using the Smart Configurator in e2 studio

By using the Smart Configurator in e2 studio, the FIT module is automatically added to your project.

Refer to “Renesas e2 studio Smart Configurator User Guide (R20AN0451)” for details.

(2) Adding the FIT module to your project using the FIT Configurator in e2 studio

By using the FIT Configurator in e2 studio, the FIT module is automatically added to your project.

Refer to “Adding Firmware Integration Technology Modules to Projects (R01AN1723)” for details.

(3) Adding the FIT module to your project using the Smart Configurator in CS+

By using the Smart Configurator Standalone version in CS+, the FIT module is automatically added to your project. Refer to “Renesas e2 studio Smart Configurator User Guide (R20AN0451)” for details.

(4) Adding the FIT module to your project in CS+

In CS+, please manually add the FIT module to your project. Refer to “Adding Firmware Integration Technology Modules to CS+ Projects (R01AN1826)” for details.

3. Demo project

The demo project is a stand-alone program. The demo projects include function main() that utilizes the FIT module and its dependent modules (e.g. r_bsp). This FIT module includes the following demo projects.

3.1 sha_demo_65n_2m

sha_demo_65n_2m shows how to use the SHA library API. This demo project will perform using the SHA-1, SHA-256, and SHA-384 algorithms.

3.2 Add the Demo to Workspace

The demo projects are found in the FITDemos subdirectory of the distribution file for this application note. To add a demo project to a workspace,

- Select "File" -> "Import".
- In the "Import" dialog, select "Existing Project to Workspace" under "General" and click the "Next" button.
- In the "Import" dialog, select the "Select archive file" radio button.
- Click the "Browse" button to open the FITDemos subdirectory.
- Select the desired demo zip file, then click “Finish”.

The above process will add the demo project to the workspace.

4. Appendix

4.1 Confirmed Operation Environment

This section describes confirmed operation environment for the SHA FIT Library.

Table 4-1 Confirmed Operation Environment (Rev. 1.06)

Item	Contents
Integrated Development Environment	Renesas Electronics e2 studio Version 2025-01 IAR Embedded Workbench for Renesas RX 5.10.1
C compiler	Renesas Electronics C/C++ Compiler Package for RX Family V3.07.00 Compiler option: The following option is added to the default settings of the integrated development environment. -lang = c99
	GCC for Renesas RX 8.3.0.202411 Compiler option: The following option is added to the default settings of the integrated development environment. -std=gnu99 Linker option: The following user defined option should be added to the default settings of the integrated development environment, if “Optimize size (-Os)” is used: -Wl,--no-gc-sections This is to work around a GCC linker issue whereby the linker erroneously discards interrupt functions declared in FIT peripheral module
	IAR C/C++ Compiler for Renesas RX version 5.10.1 Compiler option: The default settings of the integrated development environment
Endian	Big endian/little endian
Revision of the module	Rev.1.06
Board used	Target Board for RX65N Target Board for RX130 Renesas Envision Kit for RX72N

5. Reference Documents

Related Technical Updates

This module reflects the content of the following technical updates.

None

Website and Support

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

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

Revision History

Rev.	Date	Description	
		Page	Summary
1.06	2025.3.20	-	Updated the confirmed operation environment
		-	Changed the disclaimer in program sources
		-	Added the 2.7 Notes on building
1.05	2022.10.31	-	Updated the confirmed operation environment
1.04	2022.07.16	-	With the fixed of FIT, the title was corrected, and FIT-related information was added. The library format has been changed from Lib. format to C source. Support SHA-384.
1.00	2012.04.16	-	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. Precaution against Electrostatic Discharge (ESD)

   A strong electrical field, when exposed to a CMOS device, can cause destruction of the gate oxide and ultimately degrade the device operation. Steps must be taken to stop the generation of static electricity as much as possible, and quickly dissipate it when it occurs. Environmental control must be adequate. When it is dry, a humidifier should be used. This is recommended to avoid using insulators that can easily build up static electricity. Semiconductor devices must be stored and transported in an anti-static container, static shielding bag or conductive material. All test and measurement tools including work benches and floors must be grounded. The operator must also be grounded using a wrist strap. Semiconductor devices must not be touched with bare hands. Similar precautions must be taken for printed circuit boards with mounted semiconductor devices.
2. Processing at power-on

   The state of the product is undefined at the time 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 time 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 time 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 time when power is supplied until the power reaches the level at which resetting is specified.
3. Input of signal during power-off state

   Do not input signals or an I/O pull-up power supply while the device is powered off. The current injection that results from input of such a signal or I/O pull-up power supply may cause malfunction and the abnormal current that passes in the device at this time may cause degradation of internal elements. Follow the guideline for input signal during power-off state as described in your product documentation.
4. 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 the 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.
5. Clock signals

   After applying a reset, only release the reset line after the operating clock signal becomes stable. When switching the clock signal during program execution, wait until the target clock signal is 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. Additionally, 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.
6. Voltage application waveform at input pin

   Waveform distortion due to input noise or a reflected wave may cause malfunction. If the input of the CMOS device stays in the area between V_{IL} (Max.) and V_{IH} (Min.) due to noise, for example, the device may malfunction. Take care to prevent chattering noise from entering the device when the input level is fixed, and also in the transition period when the input level passes through the area between V_{IL} (Max.) and V_{IH} (Min.).
7. Prohibition of access to reserved addresses

   Access to reserved addresses is prohibited. The reserved addresses are provided for possible future expansion of functions. Do not access these addresses as the correct operation of the LSI is not guaranteed.
8. Differences between products

   Before changing from one product to another, for example to a product with a different part number, confirm that the change will not lead to problems. The characteristics of a microprocessing unit or microcontroller unit products in the same group but having a different part number might differ in terms of 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 or any other use of the circuits, software, and information in the design of your product or system. Renesas Electronics disclaims any and all liability for any losses and damages incurred by you or third parties arising from the use of these circuits, software, or information.
2. Renesas Electronics hereby expressly disclaims any warranties against and liability for infringement or any other claims involving 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, including but not limited to, the product data, drawings, charts, programs, algorithms, and application examples.
3. 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 shall be responsible for determining what licenses are required from any third parties, and obtaining such licenses for the lawful import, export, manufacture, sales, utilization, distribution or other disposal of any products incorporating Renesas Electronics products, if required.
5. You shall not alter, modify, copy, or reverse engineer any Renesas Electronics product, whether in whole or in part. Renesas Electronics disclaims any and all liability for any losses or damages incurred by you or third parties arising from such alteration, modification, copying or reverse engineering.
6. Renesas Electronics products are classified according to the following two quality grades: “Standard” and “High Quality”. The intended 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; industrial robots; etc.
   "High Quality": Transportation equipment (automobiles, trains, ships, etc.); traffic control (traffic lights); large-scale communication equipment; key financial terminal systems; safety control equipment; etc.

   Unless expressly designated as a high reliability product or a product for harsh environments in a Renesas Electronics data sheet or other Renesas Electronics document, Renesas Electronics products are not intended or 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 damage (space system; undersea repeaters; nuclear power control systems; aircraft control systems; key plant systems; military equipment; etc.). Renesas Electronics disclaims any and all liability for any damages or losses incurred by you or any third parties arising from the use of any Renesas Electronics product that is inconsistent with any Renesas Electronics data sheet, user’s manual or other Renesas Electronics document.
7. No semiconductor product is absolutely secure. Notwithstanding any security measures or features that may be implemented in Renesas Electronics hardware or software products, Renesas Electronics shall have absolutely no liability arising out of any vulnerability or security breach, including but not limited to any unauthorized access to or use of a Renesas Electronics product or a system that uses a Renesas Electronics product. RENESAS ELECTRONICS DOES NOT WARRANT OR GUARANTEE THAT RENESAS ELECTRONICS PRODUCTS, OR ANY SYSTEMS CREATED USING RENESAS ELECTRONICS PRODUCTS WILL BE INVULNERABLE OR FREE FROM CORRUPTION, ATTACK, VIRUSES, INTERFERENCE, HACKING, DATA LOSS OR THEFT, OR OTHER SECURITY INTRUSION (“Vulnerability Issues”). RENESAS ELECTRONICS DISCLAIMS ANY AND ALL RESPONSIBILITY OR LIABILITY ARISING FROM OR RELATED TO ANY VULNERABILITY ISSUES. FURTHERMORE, TO THE EXTENT PERMITTED BY APPLICABLE LAW, RENESAS ELECTRONICS DISCLAIMS ANY AND ALL WARRANTIES, EXPRESS OR IMPLIED, WITH RESPECT TO THIS DOCUMENT AND ANY RELATED OR ACCOMPANYING SOFTWARE OR HARDWARE, INCLUDING BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY, OR FITNESS FOR A PARTICULAR PURPOSE.
8. When using Renesas Electronics products, refer to the latest product information (data sheets, user’s manuals, application notes, “General Notes for Handling and Using Semiconductor Devices” in the reliability handbook, etc.), and ensure that usage conditions are within the ranges specified by Renesas Electronics with respect to maximum ratings, operating power supply voltage range, heat dissipation characteristics, installation, etc. Renesas Electronics disclaims any and all liability for any malfunctions, failure or accident arising out of the use of Renesas Electronics products outside of such specified ranges.
9. Although Renesas Electronics endeavors to improve the quality and reliability of Renesas Electronics products, semiconductor products have specific characteristics, such as the occurrence of failure at a certain rate and malfunctions under certain use conditions. Unless designated as a high reliability product or a product for harsh environments in a Renesas Electronics data sheet or other Renesas Electronics document, Renesas Electronics products are not subject to radiation resistance design. You are responsible for implementing safety measures to guard against the possibility of bodily injury, injury or damage caused by fire, and/or danger to the public in the event of a failure or malfunction of Renesas Electronics products, 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 and impractical, you are responsible for evaluating the safety of the final products or systems 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. You are responsible for carefully and sufficiently investigating applicable laws and regulations that regulate the inclusion or use of controlled substances, including without limitation, the EU RoHS Directive, and using Renesas Electronics products in compliance with all these applicable laws and regulations. Renesas Electronics disclaims any and all liability for damages or losses occurring as a result of your noncompliance with applicable laws and regulations.
11. Renesas Electronics products and technologies shall 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 shall comply with any applicable export control laws and regulations promulgated and administered by the governments of any countries asserting jurisdiction over the parties or transactions.
12. It is the responsibility of the buyer or distributor of Renesas Electronics products, or any other party who distributes, disposes of, or otherwise sells or transfers the product to a third party, to notify such third party in advance of the contents and conditions set forth in this document.
13. This document shall not be reprinted, reproduced or duplicated in any form, in whole or in part, without prior written consent of Renesas Electronics.
14. Please contact a Renesas Electronics sales office if you have any questions regarding the information contained in this document or Renesas Electronics products.

(Note1) “Renesas Electronics” as used in this document means Renesas Electronics Corporation and also includes its directly or indirectly controlled subsidiaries.

(Note2) “Renesas Electronics product(s)” means any product developed or manufactured by or for Renesas Electronics.

(Rev.5.0-1 October 2020)

Corporate Headquarters

TOYOSU FORESIA, 3-2-24 Toyosu,
Koto-ku, Tokyo 135-0061, Japan
www.renesas.com

Trademarks

Renesas and the Renesas logo are trademarks of Renesas Electronics Corporation. All trademarks and registered trademarks are the property of their respective owners.

Contact information

For further information on a product, technology, the most up-to-date version of a document, or your nearest sales office, please visit:
www.renesas.com/contact/.