RL78 ファミリ
SHA ハッシュ関数ライブラリ: 導入ガイド

R20AN0211JJ0103
Rev.1.03
2016.07.01

要旨

本資料は、RL78 ファミリ用 SHA ハッシュ関数ライブラリ V.1.02 Release 01 (以下 SHA ライブラリ)を導入するための情報を記します。

SHA ライブラリは SHA-1/SHA-256 のハッシュ演算処理を RL78 マイコンで実現するためのソフトウェアライブラリです。SHA ライブラリは RL78 マイコン専用にアセンブラ言語を用いて効率よく処理が出来るように設計されています。SHA ライブラリの使用方法については、ユーザーズマニュアルを参照してください。

動作確認デバイス

RL78/G13, RL78/G14

目次

1. 製品構成

表 1　SHA ライブラリの製品構成

構成	内容
ドキュメント(doc)	
英語版(en)	
r20uw0101ej0101_sha.pdf.pdf	ユーザーズマニュアル
r20an0211jej0103_rl78_sha.pdf	導入ガイド
日本語版(ja)	
r20uw0101jj0101_sha.pdf	ユーザーズマニュアル
r20an0211jj0103_rl78_sha.pdf	導入ガイド(本書)
CS+ for CA, CX 用(CS+ for CA)	
ライブラリ(lib)	
sha_rl78_l.lib sha_rl78_m.lib sha_rl78_s.lib	SHA ライブラリ - ラージ・モデル用 - ミディアム・モデル用 - スモール・モデル用
r_sha.h	SHA ライブラリヘッダファイル
r_mw_version.h	バージョン情報ヘッダファイル
r_stdint.h	型定義ヘッダファイル
サンプルプログラム(sample)	
rl78_sim_sha	サンプルプログラム(CS+ for CA, CX プロジェクト)
CS+ for CC 用(CS+ for CC)	
ライブラリ(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 ライブラリ - RL78 core S2- ミディアム・モデル用 - RL78 core S2- スモール・モデル用 - RL78 core S3- ミディアム・モデル用 - RL78 core S3- スモール・モデル用
r_sha.h	SHA ライブラリヘッダファイル
r_mw_version.h	バージョン情報ヘッダファイル
r_stdint.h	型定義ヘッダファイル
サンプルプログラム(sample)	
rl78_sim_sha_ccrl	サンプルプログラム(CS+ for CC プロジェクト)
IAR Embedded Workbench 用(IAR)	
ライブラリ(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 ライブラリ(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 ライブラリヘッダファイル
r_mw_version.h	バージョン情報ヘッダファイル
r_stdint.h	型定義ヘッダファイル
サンプルプログラム(sample)	
rl78_sim_sha_iar	サンプルプログラム(IAR IDE Workspace)

2. ライブラリ関数

SHA ライブラリは以下の関数をサポートしています。

表 2 SHA ライブラリの API 関数

API	Outline
R_Sha1_HashDigest	SHA-1 ハッシュ値の演算
R_Sha256_HashDigest	SHA-256 ハッシュ値の演算

3. CS+ for CA, CX 用

3.1 開発環境

ユーザアプリケーション開発時は以下のバージョンより新しいものをご使用下さい。

-統合開発環境

CS+ V2.02.00

-C コンパイラ

CA78K0R V1.70

3.2 コンパイラオプション

以下のオプションにてライブラリを生成しています。

・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

SHA ライブラリの ROM / RAM /スタックのサイズは次のとおりです（単位はバイト）。

表 3　ROM / RAM サイズ

ライブラリファイル名	ROM size [byte] 【注】	RAM size [byte]
sha_rl78_l.lib	4882	0
sha_rl78_m.lib	4804	0
sha_rl78_s.lib	4796	0

【注】 ミラー領域を最大 388 バイト使用します。
バージョン情報を使用しない場合またはラージ・モデルの場合、ミラー領域は 256 バイトになります。

表 4　スタックサイズ

API	stack size [byte] 【注】
R_Sha1_HashDigest	138
R_Sha256_HashDigest	174

【注】 全ライブラリで共通

3.4 セクション

表 5　使用するセクション

セクション名	内容	セクション属性
@@CODE / @@CODEL	プログラム	CSEG
@@CNST / @@CNSTL	定数データ	CSEG MIRRORP

3.5 ライブラリ性能

ライブラリ性能は、メモリ・モデルの違いによる差はほとんどありません。

以下は代表例として、ミディアム・モデルのライブラリを RL78/G13 で実行したときの値です。

表 6　ライブラリ性能

system clock = 32MHz

入力メッセージ長[byte]	SHA-1 [us]	SHA-256 [us]
0	700	1058
64	1326	2030
128	1947	2998
192	2568	3965
256	3189	4932

【注】 メッセージは 1 回で入力し、内部のパディング処理を含む処理時間です。

3.6 バージョン情報

本ライブラリは、変数に文字列でバージョン情報を格納しています。以下の extern 宣言により、この変数にアクセスすることが出来ます。また、本製品のライブラリに格納されているデータは以下の通りです。

表 7 バージョン情報

ライブラリ	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 (バージョン情報なし)
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 注意事項

- 異なるメモリ・モデルを指定したモジュール同士は、リンクすることはできません。
- __far 修飾子のある変数のポインタは引数に指定できません。

4. CS+ for CC 用

4.1 開発環境

ユーザアプリケーション開発時は以下のバージョンより新しいものをご使用下さい。

-統合開発環境

CS+ V4.00.00

-C コンパイラ

CC-RL V1.02

4.2 コンパイラオプション

以下のオプションにてライブラリを生成しています。

・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

SHA ライブラリの ROM / RAM /スタックのサイズは次のとおりです（単位はバイト）。

表 8 ROM / RAM サイズ

ライブラリファイル名	ROM size [byte] 【注】	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

【注】 ミラー領域を最大 388 バイト使用します。
バージョン情報を使用しない場合またはラージ・モデルの場合、ミラー領域は 256 バイトになります。

表 9 スタックサイズ

API	stack size [byte] 【注】
R_Sha1_HashDigest	136
R_Sha256_HashDigest	172

【注】 全ライブラリで共通

4.4 セクション

表 10 使用するセクション

セクション名	内容	セクション属性
.textf .text(*1)	プログラム	.CSEG
.const	定数データ	.CSEG CONST

(*1) code model=near の場合に使用します。

4.5 ライブラリ性能

ライブラリ性能は、メモリ・モデルの違いによる差はほとんどありません。

以下は代表例として、ミディアム・モデルのライブラリを RL78/G13 で実行したときの値です。

表 11 ライブラリ性能

system clock = 32MHz

入力メッセージ長[byte]	SHA-1 [us]	SHA-256 [us]
0	661	1016
64	1280	1983
128	1895	2944
192	2510	3906
256	3126	4867

【注】 メッセージは 1 回で入力し、内部のパディング処理を含む処理時間です。

4.6 バージョン情報

本ライブラリは、変数に文字列でバージョン情報を格納しています。以下の extern 宣言により、この変数にアクセスすることが出来ます。また、本製品のライブラリに格納されているデータは以下の通りです。

表 12 バージョン情報

ライブラリ	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 注意事項

- 異なるメモリ・モデルを指定したモジュール同士は、リンクすることはできません。
- __far 修飾子のある変数のポインタは引数に指定できません。

5. IAR Embedded Workbench 用

5.1 開発環境

ユーザアプリケーション開発時は以下のバージョンより新しいものをご使用下さい。

-統合開発環境

IAR Embedded Workbench for Renesas RL78 version 2.21.1

-C コンパイラ

IAR C/C++ Compiler for Renesas RL78 : 2.21.1.1833 (2.21.1.1833)

5.2 コンパイラオプション

以下のオプションにてライブラリを生成しています。

・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

SHA ライブラリの ROM / RAM /スタックのサイズは次のとおりです（単位はバイト）。

表 13 ROM / RAM サイズ

ライブラリファイル名	ROM size [byte] 【注】	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

【注】 ミラー領域を最大 388 バイト使用します。
バージョン情報を使用しない場合またはラージ・モデルの場合、ミラー領域は 256 バイトになります。

表 14 スタックサイズ

API	stack size [byte] 【注】
R_Sha1_HashDigest	138
R_Sha256_HashDigest	174

【注】 全ライブラリで共通

5.4 セクション

表 15 使用するセグメント

セグメント名	内容
.text .textf(*1)	プログラム
.const .constf(*2)	定数データ

(*1) code model=far の場合に使用します。
(*2) data model=far の場合に使用します。

5.5 ライブラリ性能

ライブラリ性能は、メモリ・モデルの違いによる差はほとんどありません。

以下は代表例として、sha_rl78_s2_m.a(RL78 core S2 - Unspecified / Far / Near)のライブラリを RL78/G13 で実行したときの値です。(関数プロファイラ機能使用)

表 16 ライブラリ性能

system clock = 32MHz

入力メッセージ長[byte]	SHA-1 [us]	SHA-256 [us]
0	594	931
64	1162	1831
128	1726	2727
192	2291	3622
256	2856	4517

【注】 メッセージは 1 回で入力し、内部のパディング処理を含む処理時間です。

5.6 バージョン情報

本ライブラリは、変数に文字列でバージョン情報を格納しています。以下の extern 宣言により、この変数にアクセスすることが出来ます。また、本製品のライブラリに格納されているデータは以下の通りです。

表 17 バージョン情報

ライブラリ	R_sha_version.library[]	R_sha_version.compiler
sha_rl78_s2_l.a	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.a	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.a	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.a	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.a	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.a	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 注意事項

- アプリケーションとライブラリは同じ設定(Device, Code model, Data model)を使用してください。
- 本ライブラリのポインタ型の引数で扱うデータは、near 領域に用意してください。

ホームページとサポート窓口

ルネサス エレクトロニクスホームページ
http://japan.renesas.com/

お問合せ先
http://japan.renesas.com/contact/

改訂記録

Rev.	発行日	改訂内容	
		ページ	ポイント
1.03	2016.07.01	—	CC-RL に対応しました。 IAR Embedded Workbench 7.4(v2.21.1)に対応しました。
1.02	2015.04.01	—	IAR Embedded Workbench に対応しました。
1.01	2014.09.30	—	章の構成を見直しました。 V.1.01 Release 00 の変更点 ・ 入力ポインタに奇数アドレスを指定した場合に不正動作する問題を修正しました。 ・ 各メモリ・モデルに対応しました。
1.00	2012.10.16	—	初版発行

製品ご使用上の注意事項

ここでは、マイコン製品全体に適用する「使用上の注意事項」について説明します。個別の使用上の注意事項については、本ドキュメントおよびテクニカルアップデートを参照してください。

1. 未使用端子の処理
   【注意】未使用端子は、本文の「未使用端子の処理」に従って処理してください。
   CMOS製品の入力端子のインピーダンスは、一般に、ハイインピーダンスとなっています。未使用端子を開放状態で動作させると、誘導現象により、LSI周辺のノイズが印加され、LSI内部で貫通電流が流れたり、入力信号と認識されて誤動作を起こす恐れがあります。未使用端子は、本文「未使用端子の処理」で説明する指示に従い処理してください。
2. 電源投入時の処置
   【注意】電源投入時は，製品の状態は不定です。
   電源投入時には、LSIの内部回路の状態は不確定であり、レジスタの設定や各端子の状態は不定です。
   外部リセット端子でリセットする製品の場合、電源投入からリセットが有効になるまでの期間、端子の状態は保証できません。
   同様に、内蔵パワーオンリセット機能を使用してリセットする製品の場合、電源投入からリセットのかかる一定電圧に達するまでの期間、端子の状態は保証できません。
3. リザーブアドレス（予約領域）のアクセス禁止
   【注意】リザーブアドレス（予約領域）のアクセスを禁止します。
   アドレス領域には、将来の機能拡張用に割り付けられているリザーブアドレス（予約領域）があります。これらのアドレスをアクセスしたときの動作については、保証できませんので、アクセスしないようにしてください。
4. クロックについて
   【注意】リセット時は、クロックが安定した後、リセットを解除してください。
   プログラム実行中のクロック切り替え時は、切り替え先クロックが安定した後に切り替えてください。
   リセット時、外部発振子（または外部発振回路）を用いたクロックで動作を開始するシステムでは、クロックが十分安定した後、リセットを解除してください。また、プログラムの途中で外部発振子
   （または外部発振回路）を用いたクロックに切り替える場合は、切り替え先のクロックが十分安定してから切り替えてください。
5. 製品間の相違について
   【注意】型名の異なる製品に変更する場合は、製品型名ごとにシステム評価試験を実施してください。
   同じグループのマイコンでも型名が違うと、内部ROM、レイアウトパターンの相違などにより、電気的特性の範囲で、特性値、動作マージン、ノイズ耐量、ノイズ輻射量などが異なる場合があります。型名が違う製品に変更する場合は、個々の製品ごとにシステム評価試験を実施してください。

ご注意書き

1. 本資料に記載された回路、ソフトウェアおよびこれらに関連する情報は、半導体製品の動作例、応用例を説明するものです。お客様の機器・システムの設計において、回路、ソフトウェアおよびこれらに関連する情報を使用する場合には、お客様の責任において行ってください。これらの使用に起因して、お客様または第三者に生じた損害に関し、当社は、一切その責任を負いません。
2. 本資料に記載されている情報は、正確を期すため慎重に作成したものですが、誤りがないことを保証するものではありません。万一、本資料に記載されている情報の誤りに起因する損害がお客様に生じた場合においても、当社は、一切その責任を負いません。
3. 本資料に記載された製品データ、図、表、プログラム、アルゴリズム、応用回路例等の情報の使用に起因して発生した第三者の特許権、著作権その他の知的財産権に対する侵害に関し、当社は、何らの責任を負うものではありません。当社は、本資料に基づき当社または第三者の特許権、著作権その他の知的財産権を何ら許諾するものではありません。
4. 当社製品を改造、改変、複製等しないでください。かかる改造、改変、複製等により生じた損害に関し、当社は、一切その責任を負いません。
5. 当社は、当社製品の品質水準を「標準水準」および「高品質水準」に分類しており、
   各品質水準は、以下に示す用途に製品が使用されることを意図しております。
   標準水準： コンピュータ、OA機器、通信機器、計測機器、AV機器、
   家電、工作機械、パーソナル機器、産業用ロボット等
   高品質水準：輸送機器（自動車、電車、船舶等）、交通用信号機器、
   防災・防犯装置、各種安全装置等
   当社製品は、直接生命・身体に危害を及ぼす可能性のある機器・システム（生命維持装置、人体に埋め込み使用するもの等）、もしくは多大な物的損害を発生させるおそれのある機器・システム（原子力制御システム、軍事機器等）に使用されることを意図しておらず、使用することはできません。たとえ、意図しない用途に当社製品を使用したことによりお客様または第三者に損害が生じても、当社は一切その責任を負いません。なお、ご不明点がある場合は、当社営業にお問い合わせください。
6. 当社製品をご使用の際は、当社が指定する最大定格、動作電源電圧範囲、放熱特性、実装条件その他の保証範囲内でご使用ください。当社保証範囲を超えて当社製品をご使用された場合の故障および事故につきましては、当社は、一切その責任を負いません。
7. 当社は、当社製品の品質および信頼性の向上に努めていますが、半導体製品はある確率で故障が発生したり、使用条件によっては誤動作したりする場合があります。また、当社製品は耐放射線設計については行っておりません。当社製品の故障または誤動作が生じた場合も、人身事故、火災事故、社会的損害等を生じさせないよう、お客様の責任において、冗長設計、延焼対策設計、誤動作防止設計等の安全設計およびエージング処理等、お客様の機器・システムとしての出荷保証を行ってください。特に、マイコンソフトウェアは、単独での検証は困難なため、お客様の機器・システムとしての安全検証をお客様の責任で行ってください。
8. 当社製品の環境適合性等の詳細につきましては、製品個別に必ず当社営業窓口までお問合せください。ご使用に際しては、特定の物質の含有・使用を規制するRoHS指令等、適用される環境関連法令を十分調査のうえ、かかる法令に適合するようご使用ください。お客様がかかる法令を遵守しないことにより生じた損害に関して、当社は、一切その責任を負いません。
9. 本資料に記載されている当社製品および技術を国内外の法令および規則により製造・使用・販売を禁止されている機器・システムに使用することはできません。また、当社製品および技術を大量破壊兵器の開発等の目的、軍事利用の目的その他軍事用途に使用しないでください。当社製品または技術を輸出する場合は、「外国為替及び外国貿易法」その他輸出関連法令を遵守し、かかる法令の定めるところにより必要な手続を行ってください。
10. お客様の転売等により、本ご注意書き記載の諸条件に抵触して当社製品が使用され、その使用から損害が生じた場合、当社は何らの責任も負わず、お客様にてご負担して頂きますのでご了承ください。
11. 本資料の全部または一部を当社の文書による事前の承諾を得ることなく転載または複製することを禁じます。

注1. 本資料において使用されている「当社」とは、ルネサス エレクトロニクス株式会社およびルネサス エレクトロニクス株式会社がその総株主の議決権の過半数を直接または間接に保有する会社をいいます。
注2. 本資料において使用されている「当社製品」とは、注１において定義された当社の開発、製造製品をいいます。

ルネサス エレクトロニクス株式会社

■営業お問合せ窓口 http://www.renesas.com

※営業お問合せ窓口の住所は変更になることがあります。最新情報につきましては、弊社ホームページをご覧ください。

ルネサス エレクトロニクス株式会社　〒135-0061　東京都江東区豊洲3-2-24（豊洲フォレシア）

■技術的なお問合せおよび資料のご請求は下記へどうぞ。
総合お問合せ窓口：http://japan.renesas.com/contact/