RX ファミリ

M3S-SHA-LIB: SHA-1/SHA-256 ライブラリ 導入ガイド

R20AN0157JJ0100
Rev.1.00
2012.04.16

要旨

本資料は、M3S-SHA-LIB: SHA-1/SHA-256 Library for the RX Family (以下SHA-1/SHA-256 ライブラリ)を導入するための情報を記します。

SHA-1/SHA-256 ライブラリは SHA-1/SHA-256 のハッシュ演算処理を RX 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-1/SHA-256 ライブラリは RX 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-1/SHA-256 ライブラリの使用方法については、インストーラパッケージに格納されている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

RX ファミリ

目次

1. 製品構成

本製品は、以下のものから構成されています。

1. M3S-SHA-LIB: SHA-1/SHA-256 Library for the RX Family V.1.00 Release00 インストーラ
2. M3S-SHA-LIB: SHA-1/SHA-256 ライブラリ 導入ガイド Rev. 1.00（r20an0157jj0100_rx_sha.pdf）

本製品の型名：R0MRX00QS0010RRC

表 1　SHA-1/SHA-256 ライブラリの製品構成

		内容
インストーラ (setup.exe)		Windows 用のインストーラです。 インストール時に表示されるライブラリの使用許諾契約書に同意いただいた場合、以下フォルダにデータがコピーされます。 【有償版】 C:¥Renesas¥an_r20an0157jj_rx_sha_v100r00p 【無償評価版】 C:¥Renesas¥an_r20an0157jj_rx_sha_v100r00
ライブラリ(lib)		
	sha_rx600_big.lib	RX600 用SHA-1/SHA-256 ライブラリファイル(big endian)
	sha_rx600_little.lib	RX600 用SHA-1/SHA-256 ライブラリファイル(little endian)
	sha_rx200_big.lib	RX200 用SHA-1/SHA-256 ライブラリファイル(big endian)
	sha_rx200_little.lib	RX200 用SHA-1/SHA-256 ライブラリファイル(little endian)
	r_sha.h	SHA-1/SHA-256 ライブラリヘッダファイル
	r_stdint.h	型定義ヘッダファイル
サンプルプログラム(sample)		
	sha_rx200_sim_sample	SHA-1/SHA-256 サンプルプログラム (High-performance Embedded Workshop のワークスペース)
ドキュメント(doc)		
	r20uw0101jj0100_sha.pdf	ユーザーズマニュアル
	r20an0157jj0100_rx_sha.pdf	導入ガイド(本書)

【注】 Windows Vista、Windows 7 にインストールする場合、インストーラ(setup.exe)の右クリックメニューから「管理者として実行」を選択してください。

2. 製品仕様

2.1 API関数

SHA-1/SHA-256 ライブラリは以下の関数をサポートしています。

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

2.2 バージョン情報

SHA-1/SHA-256 ライブラリでは、R_sha_version 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。

```
extern const char R_sha_version[];

RX600 用SHA-1/SHA-256 ライブラリファイル(big endian)
  "M3S-SHA-LIB version 1.00 for RX600 BIG endian.(Mar 16 2012, 16:56:11)"

RX600 用SHA-1/SHA-256 ライブラリファイル(little endian)
  "M3S-SHA-LIB version 1.00 for RX600 LITTLE endian.(Mar 16 2012, 16:56:17)"

RX200 用SHA-1/SHA-256 ライブラリファイル(big endian)
  "M3S-SHA-LIB version 1.00 for RX200 BIG endian.(Mar 16 2012, 16:55:57)"

RX200 用SHA-1/SHA-256 ライブラリファイル(little endian)
  "M3S-SHA-LIB version 1.00 for RX200 LITTLE endian.(Mar 16 2012, 16:56:06)"
```

2.3 セクション

セクション名	配置場所	内容
P	プログラム領域	ライブラリプログラムデータ
C	定数データ領域	定数データ
SU	ユーザスタック領域	スタック
SI	割り込みスタック領域	スタック

2.4　SHA-1/SHA-256 ライブラリROM / RAM / stack size / 処理サイクル数

2.4.1　ROM/RAMサイズ

ライブラリファイル名	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　スタックサイズ

API	stack size [byte]
R_Sha1_HashDigest	168
R_Sha256_HashDigest	180

【注】 全ライブラリで共通

2.4.3　処理サイクル数

入力メッセージ長[byte]	SHA-1 [cycles]	SHA-256 [cycles]
0	約 5500	約 5100
64	約 10200	約 9200
128	約 14900	約 13300
192	約 19500	約 17400
256	約 24200	約 21500

【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。

2.5　開発環境

[開発ホスト]

Windows XP SP3

[ソフトウェアツール]

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

High Performance Embedded Workshop Version 4.09.00.007

-C コンパイラ

RX ファミリ用 C/C++コンパイラパッケージ V.1.01 Release 00

-デバッガ

(RX600 シリーズの場合)

RX Family Simulator/Debugger V.1.02.00.005

RX600 Simulator Target Platform V.1.02.00.005

(RX200 シリーズの場合)

RX Family Simulator/Debugger V.1.02.00.005

RX200 Simulator Target Platform V.1.00.00.001

2.6　ライブラリ生成時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。

— RX600 用SHA-1/SHA-256 ライブラリファイル(big endian)

- コンパイラオプション

  -cpu=rx600 -endian=big -include="$(WORKSPDIR)¥..¥src¥library_header"
  -output=obj="$(CONFIGDIR)¥$(FILELEAF).obj" -nologo

- アセンブラオプション

  -cpu=rx600 -endian=big -output="$(CONFIGDIR)¥$(FILELEAF).obj" -nologo

- 最適化リンカオプション

  -noprelink -form=library -nomessage -list="$(CONFIGDIR)¥$(PROJECTNAME).lbp" -nologo
  -output="$(CONFIGDIR)¥$(PROJECTNAME).lib" -exit

— RX600 用SHA-1/SHA-256 ライブラリファイル(little endian)

- コンパイラオプション

  -cpu=rx600 -include="$(WORKSPDIR)¥..¥src¥library_header"
  -output=obj="$(CONFIGDIR)¥$(FILELEAF).obj" -nologo

- アセンブラオプション

  -cpu=rx600 -output="$(CONFIGDIR)¥$(FILELEAF).obj" -nologo

- 最適化リンカオプション

  -noprelink -form=library -nomessage -list="$(CONFIGDIR)¥$(PROJECTNAME).lbp" -nologo
  -output="$(CONFIGDIR)¥$(PROJECTNAME).lib" -exit

— RX200 用SHA-1/SHA-256 ライブラリファイル(big endian)

- コンパイラオプション

  -cpu=rx200 -endian=big -include="$(WORKSPDIR)¥..¥src¥library_header"
  -output=obj="$(CONFIGDIR)¥$(FILELEAF).obj" -nologo

- アセンブラオプション

  -cpu=rx200 -endian=big -output="$(CONFIGDIR)¥$(FILELEAF).obj" -nologo

- 最適化リンカオプション

  -noprelink -form=library -nomessage -list="$(CONFIGDIR)¥$(PROJECTNAME).lbp" -nologo
  -output="$(CONFIGDIR)¥$(PROJECTNAME).lib" -exit

— RX200 用SHA-1/SHA-256 ライブラリファイル(little endian)

- コンパイラオプション

  -cpu=rx200 -include="$(WORKSPDIR)¥..¥src¥library_header"
  -output=obj="$(CONFIGDIR)¥$(FILELEAF).obj" -nologo

- アセンブラオプション

  -cpu=rx200 -output="$(CONFIGDIR)¥$(FILELEAF).obj" -nologo

- 最適化リンカオプション

  -noprelink -form=library -nomessage -list="$(CONFIGDIR)¥$(PROJECTNAME).lbp" -nologo
  -output="$(CONFIGDIR)¥$(PROJECTNAME).lib" –exit

3. 制限事項

- 本ライブラリは、マイコンオプション fint_register=0 (高速割り込み専用レジスタ [なし]) 以外では使用できません。本オプションの省略時解釈は、fint_register=0 です。

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
1.00	2012.04.16	—	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、本文を参照してください。なお、本マニュアルの本文と異なる記載がある場合は、本文の記載が優先するものとします。

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. リザーブアドレスのアクセス禁止

   【注意】リザーブアドレス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、事前に問題ないことをご確認下さい。

   同じグループのマイコンでも型名が違うと、内部メモリ、レイアウトパターンの相違などにより、特性が異なる場合があります。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。

ご注意書き

1. 本資料に記載されている内容は本資料発行時点のものであり、予告なく変更することがあります。当社製品のご購入およびご使用にあたりましては、事前に当社営業窓口で最新の情報をご確認いただきますとともに、当社ホームページなどを通じて公開される情報に常にご注意ください。
2. 本資料に記載された当社製品および技術情報の使用に関連し発生した第三者の特許権、著作権その他の知的財産権の侵害等に関し、当社は、一切その責任を負いません。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。
3. 当社製品を改造、改変、複製等しないでください。
4. 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。
5. 輸出に際しては、「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。本資料に記載されている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の目的で使用しないでください。また、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に使用することができません。
6. 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。
7. 当社は、当社製品の品質水準を「標準水準」、「高品質水準」および「特定水準」に分類しております。また、各品質水準は、以下に示す用途に製品が使われることを意図しておりますので、当社製品の品質水準をご確認ください。お客様は、当社の文書による事前の承諾を得ることなく、「特定水準」に分類された用途に当社製品を使用することができません。また、お客様は、当社の文書による事前の承諾を得ることなく、意図されていない用途に当社製品を使用することができません。当社の文書による事前の承諾を得ることなく、「特定水準」に分類された用途または意図されてい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生じた損害等に関し、当社は、一切その責任を負いません。なお、当社製品のデータ・シート、データ・ブック等の資料で特に品質水準の表示がない場合は、標準水準製品であることを表します。

   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

   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、生命維持を目的として設計されていない医療機器（厚生労働省定義の管理医療機器に相当）

   特定水準： 航空機器、航空宇宙機器、海底中継機器、原子力制御システム、生命維持のための医療機器（生命維持装置、人体に埋め込み使用するもの、治療行為（患部切り出し等）を行うもの、その他直接人命に影響を与えるもの）（厚生労働省定義の高度管理医療機器に相当）またはシステム等
8. 本資料に記載された当社製品のご使用につき、特に、最大定格、動作電源電圧範囲、放熱特性、実装条件その他諸条件につきましては、当社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。
9. 当社は、当社製品の品質および信頼性の向上に努めておりますが、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、社会的損害など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、機器またはシステムとしての出荷保証をお願いいたします。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、お客様が製造された最終の機器・システムとしての安全検証をお願いいたします。
10. 当社製品の環境適合性等、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。
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固くお断りいたします。
12. 本資料に関する詳細についてのお問い合わせその他お気付きの点等がございましたら当社営業窓口までご照会ください。

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・電話番号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 エレクトロニクス販売株式会社　〒100-0004　千代田区大手町2-6-2（日本ビル） (03)5201-5307

■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/

Colophon 1.1