RL78 ファミリ

タイマーによる乱数の取得

KR01AN0002JJ0001
Rev. 0.01
2018.2.12

要旨

本アプリケーションでは、タイマーよる乱数の取得方法を説明します。

乱数はハードウェアに起因したノイズにより生成しているため、ソフトウェアによる疑似乱数のような再現性がありません。特に周囲温度や動作電圧に依存しないので耐タンパ性に優れ暗号用途にも使用することができます。

本方式による乱数精度は同ビット数の真性乱数よりもやや劣っていますが、1 ビットあたり 130usec 程度(32MHz 動作時)と比較的高速に乱数を生成することができます。(タイマーによる 24 ビットの乱数は、真性乱数 21 ビット程度に相当)。

動作確認デバイス

RL78/G14

本アプリケーションノートを他のマイコンへ適用する場合、そのマイコンの仕様にあわせて変更し、十分に評価してください。(マイコンによっては RTCEN レジスタを TMKAEN に、ITIF レジスタを TMKAIF に読み替える必要がある場合があります。)

目次

1. 仕様 3

2. 動作確認条件 4

3. ハードウェア説明 5
3.1 ハードウェア構成例 5
3.2 使用端子一覧 5

4. ソフトウェア説明 5
4.1 動作概要 5
4.2 オプション・バイトの設定一覧 6
4.3 定数一覧 6
4.4 変数一覧 6
4.5 関数（サブルーチン）一覧 7
4.6 関数（サブルーチン）仕様 7

1.　仕様

本アプリケーションノートでは、インターバル・タイマを低速オンチップ・オシレータで動作させ、一定周期内の高速 OCO クロックのカウント数をもとに乱数を生成します。2 つの独立した発振器のジッターにより周期毎にカウント誤差が発生するため、これが乱数となります。

※インターバル期間を延ばせば延ばすほど乱数の品質は高くなりますが、効果は対数関数的になるため、1 ビットあたり 1msec 程度までが現実的な設定になります。最短時間の 130usec 程度でも十分な精度を持ちます。

表 1-1 に使用する周辺機能と用途を、図 1-1 に乱数生成の動作を示します。

表 1-1 使用する周辺機能と用途

周辺機能	用途
TAU0	高速 OCO のカウント数の測定
12 ビット・インターバル・タイマ	一定周周期の計測

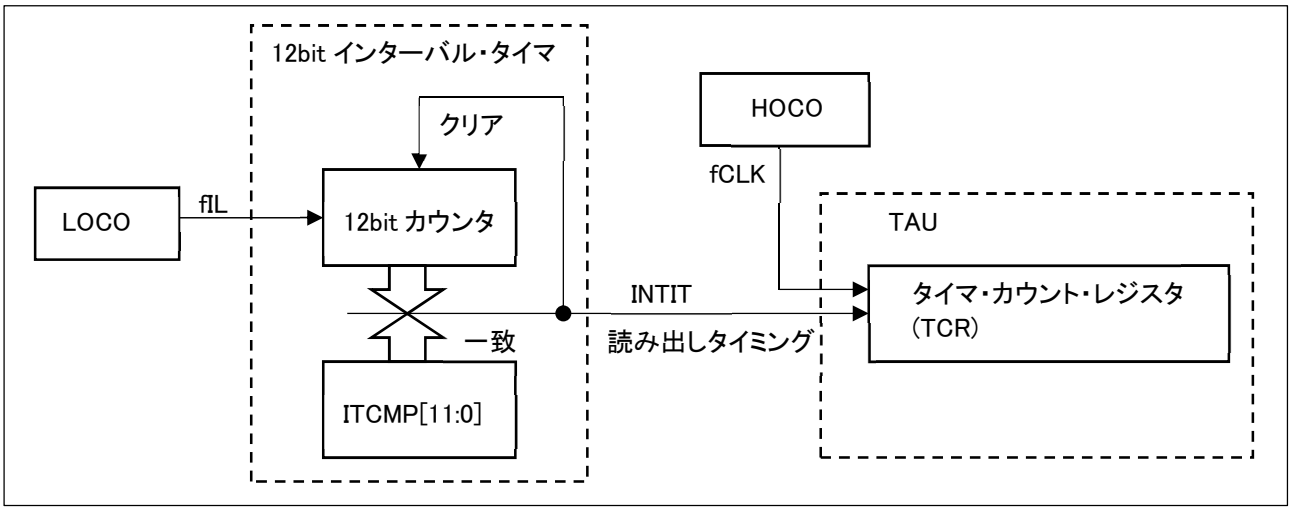

図 1-1 乱数生成のハード構成イメージ

2. 動作確認条件

本アプリケーションノートのサンプルコードは、下記の条件で動作を確認しています。

表 2.1 動作確認条件

項目	内容
使用マイコン	RL78/G14（R5F104PJ）
動作周波数	高速オンチップ・オシレータ（HOCO）クロック： 32MHz 低速オンチップ・オシレータ（LOCO）クロック： 15KHz CPU／周辺ハードウエア・クロック： 32MHz
動作電圧	3.3V（2.7V～5.5V で動作可能） LVD 動作：リセット・モード 2.81V (2.75V～2.81V)
統合開発環境	ルネサス エレクトロニクス製 CS+ for CC V6.01.00
使用ボード	RL78/G14 ターゲット・ボード（QB-R5F104PJ-TB）

3. ハードウェア説明

3.1 ハードウェア構成例

本サンプルプログラムはハードウェア構成に依存しません。

注意

1 VDD は LVD にて設定したリセット解除電圧以上にしてください。

3.2 使用端子一覧

本サンプルプログラムでは端子を使用しません。

4. ソフトウェア説明

4.1 動作概要

本サンプルコードでは、2 つのタイマーを使用して乱数を生成します。

さらに、生成した乱数の品質を測定します。

(1) TAU0 の初期設定を行います。

＜TAU0 の設定条件＞

- チャンネル 0 を使用します。
- インターバル・タイマモード、カウントクロックに fCLK を使用します。
- カウント範囲を最大値 0xFFFF とします。

(2) 12 ビット・インターバル・タイマの初期設定を行います。

＜12 ビット・インターバル・タイマ の設定条件＞

- カウントクロックに低速 OCO(15KHz)を使用します。
- カウント周期を 2 クロック(133usec)に設定します。

(3) 乱数生成を行います。

低速 OCO の動作周期(12bit タイマー)と高速 OCO の(TAU)のジッターによるカウント誤差から乱数を生成します。

(4) 乱数の品質確認を行います。

生成した乱数の統計量(χ^2値)を観測します。

4.2 オプション・バイトの設定一覧

表 4-1 にオプション・バイト設定を示します。

表 4-1 オプション・バイト設定

アドレス	設定値	内容
000C0H	11101111B	ウォッチドッグ・タイマ 動作停止 （リセット解除後、カウント停止）
000C1H	01111111B	LVD リセット・モード 2.81V (2.75V～2.81V)
000C2H	11101000B	HS モード、HOCO：32MHz
000C3H	10000101B	オンチップ・デバッグ許可

4.3 定数一覧

表 4-2 にサンプルコードで使用する定数を示します。

表 4-2 サンプルコードで使用する定数

定数名	設定値	内容
TIME_INTERVAL	1	乱数 1 ビットあたりを生成する時間 (66.7usec×(N+1))

4.4 変数一覧

表 4-3 にグローバル変数を示します。

表 4-3 グローバル変数

Type	Variable Name	Contents	Function Used
32 ビット	id	タイマー値により生成した 24bit 乱数	main
8 ビット	level	タイマーによる 24bit 乱数の 真性乱数換算の品質(8～24) 8：8bit 真性乱数相当 ・・・・ 24：24bit 真性乱数相当	main
8 ビット×8 配列	bitmask	ビットマスクのための定数	rng, rn_test

4.5 関数(サブルーチン)一覧

表 4-4 に関数(サブルーチン)一覧を示します。

表 4-4 関数(サブルーチン)一覧

関数名	概要
init_tm	タイマーの初期化
rng	8bit 単位での乱数生成
rn_test	乱数の品質測定

4.6 関数(サブルーチン)仕様

サンプルコードの関数(サブルーチン)仕様を示します。

[関数名] init_tm

概要	タイマーの初期化
説明	TAU0 チャンネル 0 のフリーランし、カウントクロックに Fclk を選択します。割込みベクタは使用しません。12bit タイマーのカウントクロックに内蔵低速 OCO を選択し、66.7usec 周期に設定します。割込みベクタは使用しません。
引数	なし
リターン値	なし

[関数名] rng

概要	8bit 単位での乱数生成
説明	12bit タイマーの割込み周期毎に乱数 1 ビットの生成を行い、これを 8 ビット分繰り返します。
引数	なし
リターン値	8bit 乱数

[関数名] rn_teset

概要	乱数の品質測定
説明	20,000bit 分の乱数を生成し FIPS140-2 相当のアルゴリズムから統計検定量を元に乱数のバラつき品質を簡易的に算出します。出力値はタイマーによる 24bit 乱数が相当する真性乱数のビット数になります。
引数	なし。
リターン値	真性乱数換算のビット数