RL78 ファミリ

A/D コンバータによる乱数の取得

KR01AN0001JJ0001
Rev. 0.01
2018.2.12

要旨

本アプリケーションでは、A/D コンバータのノイズにより発生した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。

本方式による乱数精度は同ビット数の真性乱数よりも劣っていますが、1 ビットあたり 20usec 程度(32MHz 動作時)と高速に乱数を生成することができます。(A/D コンバータによる 24 ビットの乱数は、真性乱数 18 ビット程度に相当)。

注意事項として、A/D コンバータで発生するノイズは電源電圧や周囲温度などに強く影響されるため、特定の条件が揃うと乱数の品質が著しく劣化することがありますので、プログラム自身により定期的に乱数の品質を確認することをお勧めします。

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。

目次

1. 仕様

本アプリケーションノートでは、A/D コンバータによりオープン状態にした ANI2 端子をサンプリングすることでノイズを測定します。変換結果の最下位 1 ビットを乱数シードとして扱います。単純に最下位ビットを乱数とすると規則性を持つため、1 ビット分の乱数を生成するために 8 個の乱数シード(変換結果の最下位 1 ビット)を使用します。

※乱数シードの数を増やせば増や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、8 個程度が適当です。

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
10 ビット A/D コンバータ	ANI2 端子を利用して A/D 変換を行う。

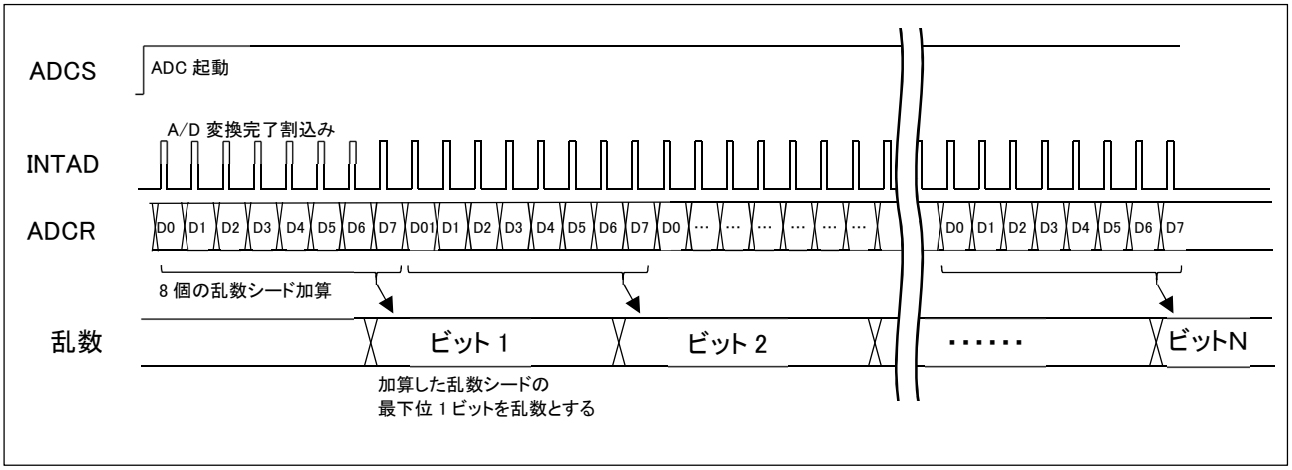

図 1-1 乱数生成の動作

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 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

表 3-1 に本アプリケーションノートで使用するハードウェア構成例を示します。

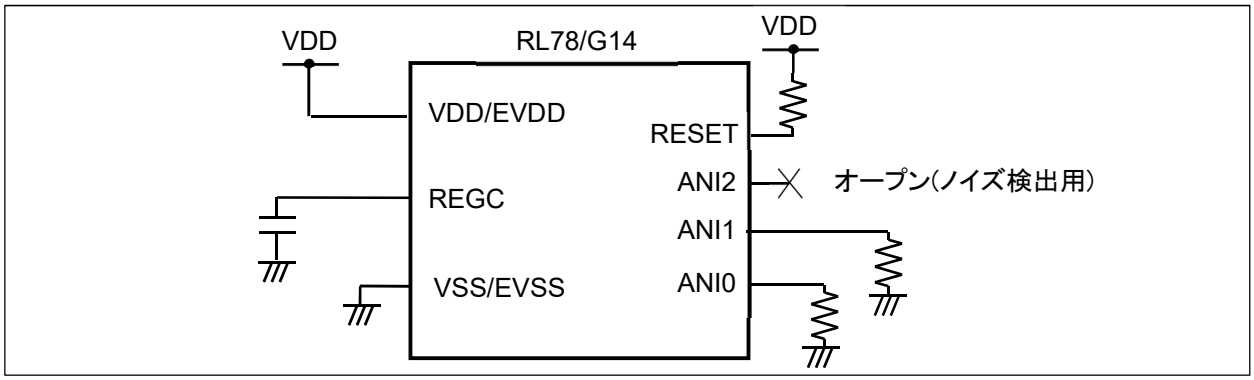

表 3-1　ハードウェア構成

注意

1　この回路イメージは接続の概要を示す為に簡略化しています。実際に回路を作成する場合は、端子処理などを適切に行い、電気的特性を満たすように設計してください。

2　乱数生成用以外のアナログチャンネルで AD 変換中に、オープンになっている乱数生成用のアナログチャンネルに外来ノイズが発生すると、稀に AD 変換精度が数 LSB～数十 LSB 劣化することがあります。乱数生成用以外のアナログチャンネル使用時は、乱数生成用のポートをデジタルポートに切り替え出力モードに設定してください。

3　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

表 3-2 に使用端子と機能を示します。

表 3-2　使用端子と機能

端子名	入出力	内容
ANI2	入力	A/D 変換用端子 ※ANI0,ANI1 端子は AVREFP,AVREFM からのリーク電流があるため乱数生成には不適です。ANI2 以降のアナログチャンネルを使用してください。
ANI0, ANI1	入力	未使用 ※ANI0,ANI1 端子は乱数生成としては未使用ですが、ANI2 を A/D コンバータで使用する際はアナログ専用端子となるため、ANI0,ANI1 未使用の場合は抵抗を介してグラウンドに接続する等の端子処理がお勧めです。AVREFP,AVREFM として使用することも可能です。

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、A/D コンバータでサンプリングしたノイズをシードと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）A/D コンバータの初期設定を行います。

＜A/D コンバータの設定条件＞

- アナログチャンネル ANI2 を使用します。
- A/D 電源安定待ち時間なし　標準モード 1、変換時間 2.375usec(76/fclk)を使用します。
- セレクト・モード、A/D 電圧コンパレータの動作許可を使用します。
- ソフトウエア・トリガ・モード、連続変換モードを使用します。
- A/D コンバータの+側の基準電圧源は VDD を使用します。
- A/D コンバータの－側の基準電圧は VSS を使用します。
- 変換結果上限／下限値チェックは使用しません。すべての変換値による割込みを有効にします。
- 10 ビット分解能を使用します。

（2）乱数生成を行います。
　A/D 変換によりノイズを測定し、8 回分の排他的理論和を取り、最下位 1 ビットを乱数とします。

（3）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
NUMBER_OF_SEEDS	8	乱数 1 ビットあたりに使用するシード(AD 変換結果の最下位 1 ビット)の数

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	ADC により生成した 24bit 乱数	main
8 ビット	level	ADC 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_adc	ADC 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_adc

概要	ADC の初期化
説明	ADC のチャンネル 2 を乱数発生用に選択します。AD 変換クロック fad を fclk/4 に設定します。AD 変換を開始します。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	乱数 1 ビットあたり AD 変換を 8 回行い、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 ADC 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