[Work in Progress] 研究報告

# 手頃な価格で作れるハードウェア乱数発生器の製作と評価

力武 健次[1,a)]

# Building and Evaluating Affordable Hardware Random Number Generators

Kenji Rikitake[1,a)]

情報システムのセキュリティを確保するには，物理乱数生成のためのエントロピー収集が必要である．エントロピーはアルゴリズム的に予測不能な事象から採取する必要があり，コンピュータ機器単体では困難である．一般的に OS が収集したエントロピーはシステム疑似乱数 (/dev/urandom など) の生成に定期的に費されるため，予測可能性を最小限にする必要がある暗号鍵などに直接使用するには量と速度の両面で不十分である．エントロピーの過剰消費による枯渇は生成乱数の品質低下を招き，セキュリティ上の脆弱性となり得る．この枯渇を防ぐためには，十分な速度と品質の物理乱数を生成する機器 (Hardware Random Number Generator, HRNG) を使用する必要がある．HRNG の使用にあたってはどのような乱数生成手順が採用されているかについて，脆弱性評価の面から検証できるべきである．検証可能性を高めるためには，HRNG の回路やソフトウェアを公開し，かつ安価な部品で容易に再現できる必要がある．

筆者は 2009 年に 8bit AVR を使った Arduino に逆接トランジスタによるノイズ生成回路を追加した HRNG である avrhwrng を設計製作し [*1]，そして 2015 年 9 月にこれを改良した第 2 版を発表した [*2]．この第 2 版は毎秒約 10k バイトの生成速度を持ち，TestU01 の 1M ビット乱数列に対する Rabbit/Alphabit の両テストで 1 つ以上の問題が指摘される確率は約 5%，そして FIPS 140-2（2001-10-10 版）での問題発生率は約 0.08%という精度を達成した．この実装に対応した Arduino Uno R3 は入手性も高く，追加回路も部品代は実勢価格 500 円以下で作成できる [*3] ため，普及展開は容易と考える．

同種の HRNG としては，新部 [*4] による NeuG が A/D コンバータのノイズをエントロピー源とした毎秒 80k バイト程度の質の高い物理乱数を生成している．新部は自身が開発した USB ドングルである飛石技研の FST-01 [*5] にこれを実装したが，筆者は新部の協力を得て STM32 Nucleo のデバッガ部 ST Dongle でこれを実装し実行することに成功した [*6]．ST Dongle を使ったボードは秋葉原で 1500 円程度で入手できるため [*7]，avrhwrng 同様，手軽かつ手頃な HRNG として普及展開が可能と考える．

これらの HRNG は USB のシリアルデバイスとして動作する．OS からこれらを利用するには Linux では rng-tools [*8] というツールがあるが，FreeBSD ではカーネルモードで random_harvest(9) という関数を使わなければならない．筆者はそのためのインターフェース用デバイスドライバならびにシリアルデバイスからの転送用コードを開発し公開した [*9]．このコードは FreeBSD に備わった物理乱数検定用の rndtest(4) ドライバと併せて，現在筆者の実験環境で NeuG や avrhwrng からの出力を処理し，80k バイト/秒の物理乱数列に対し Intel i3-3217U 1.8GHz にて CPU 利用率 3%程度で運用できている．

HRNG の高速化のためには，ノイズ生成回路を増やし並列化する方法や，より広帯域な USB ラジオドングル R820T によるサンプリング [*10] などが有望である．これらの手法を使えば実売数千円前後で毎秒数百 k ビットの物理乱数を得られると予想できる．

[1] 力武健次技術士事務所
Kenji Rikitake Professional Engineer's Office
[a)] http://rikitake.jp/

[*1] http://makezine.jp/blog/2009/04/random_number.html
[*2] https://github.com/jj1bdx/avrhwrng/
[*3] 秋月電子通商の部品価格より推定.
[*4] http://no-passwd.net/fst-01-neug-handbook/
[*5] http://www.gniibe.org/shop/neug_1_0_x-on-fst-01.html
[*6] http://www.gniibe.org/memo/development/gnuk/hardware/stm32-nucleo-f103.html
[*7] STM32 Nucleo F103 のボードが税別 1500 円，秋月電子通商調べ，2015 年 10 月 29 日現在.
[*8] http://sourceforge.net/projects/gkernel/files/rng-tools/
[*9] https://github.com/jj1bdx/freebsd-dev-trng/
[*10] https://github.com/pwarren/rtl-entropy/

© 2015 Information Processing Society of Japan