翻訳論文　無線通信システムに組み込まれた真性乱数生成器法

翻訳論文

無線通信システムに組み込まれた真性乱数生成器法

A True Random Number Generator Method Embedded in Wireless Communication Systems

戸村 康汰* 鈴木 利則*
Kota TOMURA Toshinori SUZUKI

Abstract: To increase the number of wireless devices such as mobile or IoT terminals, cryptosystems are essential for secure communications. In this regard, random number generation is crucial because the appropriate function of cryptosystems relies on it to work properly. This paper proposes a true random number generator (TRNG) method capable of working in wireless communication systems. By embedding a TRNG in such systems, no additional analog circuits are required and working conditions can be limited as long as wireless communication systems are functioning properly, making TRNG method cost effective. We also present some theoretical background and considerations. We next conduct experimental verification, which strongly supports the viability of the proposed method.

Keywords: Random Number Generator, Internet of Things (IoT), Radio Frequency Identifier (RFID), Wireless Communication

本論文は,
Toshinori SUZUKI, Masahiro KAMINAGA, “A True Random Number Generator Method Embedded in Wireless Communication Systems”, IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, vol. E103-A, No.4, April.2020.
を翻訳したものであり, 併せて参照頂きたい.

1 はじめに

安全な通信にとって, 乱数の生成は重要な問題である. なぜならば, それが暗号システムに必要不可欠であり, 理想的な乱数であることが暗号システムの前提となっているからである. 暗号システムの脆弱性はしばしばランダム性が不十分な数を乱数として用いることにより生じている. 例えば, デジタル署名アルゴリズム(DSA)はすべての署名において乱数を必要とする. DSA に疑似乱数(PRN)を用いると, いくつかの署名から署名に用いた秘密鍵を復元することができる[1]. SSH ホストで用いる DSA の秘密鍵でさえ, 署名の不十分なランダム性から, その値を取り出すことができる[2]. このような状況を考えると, 乱数生成の統計的なランダム性だけでは不十分であり, 予測不能性が必要である. シード値から決定論的に生成される PRN に対して, 真正乱数(TRN; True Random Number)は決定論的ではない. それゆえ, 安全性の観点からは TRN が望ましい. 一方で, 実用性の観点からは, TRN を生成する源をどうするか(何に基づいて TRN を生成するか)がコストと性能に関係して重要な事項になる.

雑音源を使用する真性乱数生成器(True Random Number Generator (TRNG))法は, 主に(1)直接増幅, (2)発振器サンプリング, (3)離散時間カオスの 3 つのカテゴリに分類される[3]. 方法(1)は, 予測できない雑音を増幅し, それを適切なしきい値と比較して, サンプリング時に 0 もしくは 1 を割り当てる [4]. この方法(1)は, アナログ信号を広帯域増幅するため, 付加的なアナログ回路を必要とする. これらの回路はかなり高価である. 方法(2)は, 低速クロックで高周波発振器からジッタのある出力をラッチするが, 方法(3)は非線形ア

ナログマッピングと正のフィードバックを使用して雑音の不確実性を拡大する([5]などを参照). 方法(1)や(3)と比較して, 方法(2)は, 信号処理回路と統合でき, 1/f 雑音および増幅器オフセットに対して良好に機能するため, コストメリットがある[6].

ワイヤレスセンサや RFID などの小型 IoT 端末の場合, 端末のリソースに制約があるため, TRNG に必要な新たなハードウエアや電力消費をできるだけ抑える必要がある. 方法(1)および方法(2)に基づいて, 付加的なハードウエアを抑えた TRNG の検討がなされている. そのような試みの一つとして, 従来研究[7]では, DC オフセットやゆっくりと変化する雑音などの好ましくない成分を除去しても消費電力が数 μW 程度に収まる TRNG を示している. この TRNG は方法(1)に基づいているが, 雑音をサンプリングするために直接増幅器の代わりにラッチが使用されている. このようなラッチベースの TRNG は, 方法(1)の変形例である. 熱雑音に基づく同様の TRNG として, オペアンプと比較器の代わりにフィードバック回路を使用する従来研究[8]がある. Balachandran 等 [9] は, 消費電力とハードウエアの複雑度が少ない RFID を目指し, 不安定な 320kHz の内部クロックを利用して, 900MHz の RFID システムに使用される RF 信号をサンプリングしている. そこでは追加する回路として, 内部クロックにジッタを与えるために雑音バッファが導入された. これらの手法は, 付加するハードウエアを抑える取り組みであるが, それでも TRNG のために新たなハードウエアと電力消費が発生する.

別の手法では, 元々ターゲット端末に装備されていたハードウエアを利用する. 従来研究[10]は, 雑音源としてイメージセンサーによって測定された可視スペクトルを採用し, 別の研究[11]は, RNG に加速度計を採用している. 他のセンサや入力デバイス, たとえばマイク, 磁力計, ジャイロスコープ, キーボード, マウスデバイスも, ランダム性をキャプチャする候補である[12]. この手法には測定と処理が必要であり, より多くのバッテリと時間を消費する可能性がある.

無線端末の重要な構成要素は, デバイスがその意図された目的を果たすために必要な RF (radio frequency) モジュールである. TRNG(Tiny RNG) [13]は, ワイヤレスリンクのビット誤りをランダム性の源として利用する. Latifetal [14]は, 受信信号強度インジケータ(RSSI)の変動を使用したが, その欠点が後に Hennebert 等によって指定され, そしてリンク品質指標を組み込むことによって改善した[15]. ただし, これらの方法では追加の測定と処理が必要であり, TRNG のための処理によって新たな電力と時間が消費される.

RF モジュールは通常, 信号増幅器, 局部発振器, およびデジタル復調用のアナログ-デジタルコンバータ(ADC)で構成されている. この増幅器は低雑音増幅器(LPA ; Low-noise Power Amplifier)と呼ばれるものの, 増幅後の信号には雑音が含まれていて, ADC の後でもその雑音成分は残っている. 無線信号の検出は雑音との戦いであり, 無線リンクは雑音を制することで実現されている. 換言すれば無線デバイスにはかなりの量の雑音が含まれているといえる.

この論文では, ADC 後の受信信号に含まれる雑音を利用して TRNG 性能を向上させることを提案する. 追加の信号測定と処理を必要とする従来の方法[13]-[15]とは異なり, 私たちの方法は, 無線通信リンクの物理層で破棄されるデータを利用する. したがって, 効率的であり, さらには物理層のサンプリングレートに応じて TRNG のスループットも高くなる可能性がある. 実験による評価を行い, 提案された方式が無線移動端末に向けた従来方式と比較してうまく機能することを示す.

この論文では次のように構成されている. 2 章では, 従来の TRN を生成する方法(1)の特徴と熱雑音のモデルを示す. 3 章では提案する TRN の生成方法の理論的背景と概念を, 4 章では提案手法のシステム構成と理論的評価を示す. 5 章では提案手法の実現可能性を, ソフトウェア無線(SDR)デバイスを用いて実験的に検証する. 6 章はまとめである.

2 従来の TRNG は最上位ビットの雑音源を使用する

熱雑音を使用する従来の TRNG の場合, 雑音レベルによって乱数が決まる. したがって, このような方法では, 予測できない成分が雑音の中で支配的とある. しかしながら, 一般に雑音には $1/f$ 雑音や AC ライン雑音などの好ましくない成分を持っている. 従来研究[3]では, 雑音源が好ましくない要素を含む場合に TRN を生成する方法(1)～(3)のランダム性を比較するために Fig.1 に示す雑音

モデルを使用している.

Fig. 1 において, PRNG はガウス性の疑似 RNG を指し, $n_A(t)$は結合性の正弦波雑音を意味する. $n_P(t)$はガウス分布に従い, そのパワースペクトルは Fig. 2 に示すようなグラフの形状を取る.

コーナ周波数f_{co}は実装技術に依存する. f_{co}は, JFET の場合は数十ヘルツ, MOSFET の場合は数十から数百キロヘルツのオーダーであると報告されている[16]. 特に, 幅が数百ミクロンでバイアス電流が数百マイクロアンペアの MOSFET の場合, f_{co}は 1MHz に近くなる[17]. 次に, $n_P(t)$は熱雑音成分$n_T(t)$とフリッカ雑音成分$n_F(t)$に分割される. それらのパワースペクトルをそれぞれ$N_T(t)$, $N_F(t)$とし, 形状を Fig. 2 に示す.

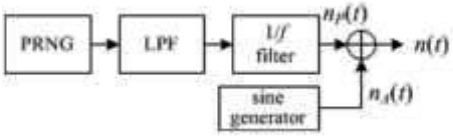

Fig. 1 Noise model for TRNG method evaluation in [3].

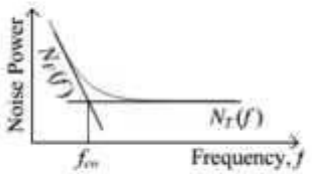

Fig. 2 Typical noise power spectrum of $n_P(t)$.

文献[6]～[9]で述べられている, 方法(1)に基づく従来の TRNG は, $n_A(t)$や$n_F(t)$などの好ましくない成分をキャンセルする, あるいは, コーナ周波数より高い周波数で雑音源から熱雑音を抽出する. いずれにせよ, これら従来の検討では, サンプリングされた雑音値の最上位ビットから乱数 0 または 1 を生成している.

3 無線信号の最下位ビットの理論考察

3.1 無線チャネルの雑音

受信機によって検出された RF 信号は, 送信された成分だけでなく, 雑音項も含む. 検出された信号を$r(t)$, 送信成分と雑音項をそれぞれ $u(t)$と$n(t)$としよう. 雑音項$n(t)$は, 熱雑音$n_T(t)$およびその他の要素, たとえば干渉雑音やショット雑音などの和$n_O(t)$で構成される. 方程式として表すと,

$$r(t) = u(t) + n(t) = u(t) + n_T(t) + n_O(t) \quad .$$

Wi-Fi やセルラーシステムなど, 多数の干渉局からの干渉は, 白色ガウス性雑音とみなすことができる. ハードウエア誤差が原因で生じる雑音の一部も, 熱雑音のように動作する場合がある. ただし, このような雑音は, 無線通信での信号検出を向上させるために, 可能な限り抑制されることになっている. 加法性白色ガウス雑音(AWGN)は通常, 静的ワイヤレスチャネルで想定され, フラットなパワースペクトルでガウス分布に従う[22].

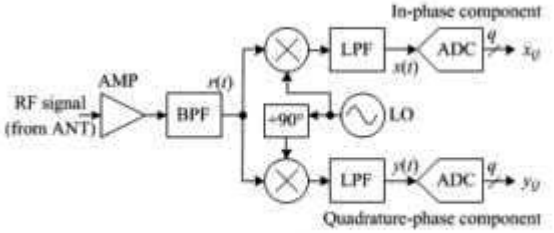

Fig. 3 Configuration of coherent demodulator.

$1/f$雑音と呼ばれるフリッカ雑音は, 特に, 受信した RF 信号を中間周波数(IF)変換なしでベースバンドに変換するダイレクトコンバージョン受信機で発生する可能性がある. 対照的に, $1/f$雑音を緩和する SiGe または BiCMOS 回路の実装, あるいは帯域幅がよりも広い広帯域通信システムでは, $1/f$雑音の効果が低下する[17]. 低周波雑音は, SDR と呼ばれるスーパーヘテロダイン受信機および IF/RF サンプリング受信機では少ないとみなすことができる

3.2 無線チャネルモデル

受信機では, 受信信号が 2 つの構成要素に分割される. コヒーレント検出の場合, $r(t)$は, 再生キャリアを基準にして同相成分と直交相成分に分解される. 同様に, インコヒーレント検出では, 互いに直交する 2 つの構成要素が存在し, 同様のモデルを適用できる.

Fig.3 は, コヒーレント受信機の構成を示している. ANT(アンテナ)からの RF 信号は AMP によって増幅され, BPF(バンドパスフィルター)でフィルター処理されて, 不要な周波数帯域をカットする. キャリア周波数をf_c, キャリアを$\cos(2\pi f_c t)$とする. 次に, $r(t)$は次のように表すことができる.

$$r(t) = x(t)\cos(2\pi f_c t) - y(t)\sin(2\pi f_c t)$$

式の右辺の最初の項は同相チャネル(I-Ch)と呼ばれ, 2 番目の項は直交位相チャネル(Q-Ch)と呼ばれる. $x(t)$と$y(t)$は雑音を含むベースバンド成分であり, 互いに直交している.

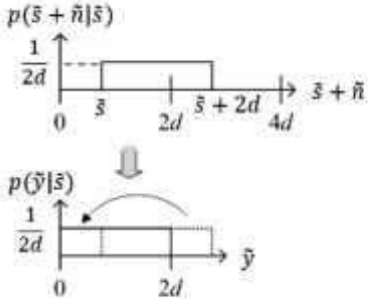

Fig. 4 The pdf of $\tilde{y}$.

Fig.3 の上側の成分$x(t)$, $r(t)$ を分離するために, LO（局部発振器）から生成された再生キャリア$\cos(2\pi f_c t)$が乗算され, LPF（ローパスフィルター）に送られる.

このプロセスを通じて, 同相ベースバンド成分$x(t)$が得られる. 同様に, Fig.3の下側に示すように$y(t)$も得られる.

通信理論では, ベースバンド信号は$x(t)+jy(t)$の複素数形式で表すことができる. これは, 等価低域表現[22](p155)と呼ばれる. 原則として, 実数成分$x(t)$と$y(t)$は統計的に同等である. 再生キャリアのハードウエア誤差または位相雑音が原因で, IQ の不均衡が発生する可能性がある. ただし, その影響は一般に非常に小さいため, 無視できると考えることができる.

Fig.3では, 両方の成分がそれぞれqビットでx_Qおよびy_Qとして量子化され, 送信された情報を復元するためにデジタル復調器に供給されている.

次の節では, $x(t)$および$y(t)$に含まれる雑音成分が ADC の後でどのように振舞うのかを, 特に雑音成分の LSB（最下位ビット）について述べる.

3.3 ADC での量子化

同じ統計的特性のため, ここでは$y(t)$を単一の構成要素の代表として用いる. 信号$y(t)$は, 周波数f_sでサンプリングされ, 量子化幅 d の q ビットで量子化される. y をサンプル値, y_Qをその量子化シンボルとする. $y_Q = \lfloor y/d \rfloor$である. これは, $y(t)$が ADC 範囲内にある限り正しい

$y(t)$が範囲外の場合, y_Qはクリップされる. $y \leq 0$の場合は$y_Q \leq 0$, y が上限を超える場合は$y_Q = (2^q - 1)$となる. ここで, $y(t)$は ADC 範囲内にあると想定する. これは通常, 無線信号を正しく受信するために必要な条件である.

3.4 十分に dが小さく qが大きいときの量子化信号

y_Qの LSB を Yとすると, Yは次のように表せる.

$$Y = \begin{cases} 0, & \text{if } (y \bmod 2d) \leq d \\ 1, & \text{if } (y \bmod 2d) > d' \end{cases}$$

ここで mod は剰余演算である. $0 \leq r < 2d$として, 整数 m に対して$y = 2md + r$が成り立つとき, $y \bmod 2d = r$となる. アナログサンプル値 y を TRNG に必要な雑音項nとそれ以外の項（残余項と呼ぶことにする）sに分割することにより, $y = s + n$として表すことができる. ここで, n は, 少なくとも熱雑音を含む予測不可能な成分であり, ガウス分布に従う. TRNG にとって好ましくない成分はsであり, これは少なくとも, 通信目的のために所望の送信機からの変調された信号を含んでいる.

アナログ剰余信号$\tilde{y} = y \bmod 2d$ は次のように表すことができる.

$$\begin{aligned} \tilde{y} &= y \bmod 2d = (s+n) \bmod 2d \\ &= [(s \bmod 2d) + (n \bmod 2d)] \bmod 2d \\ &= (\tilde{s} + \tilde{n}) \bmod 2d \end{aligned} \quad (1)$$

d は十分に小さく q が十分に大きい場合, 剰余雑音項$\tilde{n}$は[0,2d]に均一に分布する[23]. すると, Fig.4 に示すように, $\tilde{y}$も$\tilde{s}$にも関係なく一様分布に従うことがわかる. それゆえ, 次の式が成り立つ.

$$p(\tilde{y}) = \int p(\tilde{y}|\tilde{s})p(\tilde{s})d\tilde{s} = \frac{1}{2d}\int p(\tilde{s})d\tilde{s} = \frac{1}{2d}$$

結果として $p(Y) = 1/2$ となる.

3.5 十分に大きい qで量子化された信号

この節では, q を大きく保ったまま d は必ずしも十分に大きくなく, かつ, n が標準偏差σのゼロ平均ガウス分布, つまり$n \sim N(0, \sigma^2)$であると仮定し, $p(y)$の$1/2$からの偏差を明らかにする. 最初に, 量子化幅が dのとき, $\tilde{n}$の PDF（累積確率密度関数）$p_{\tilde{n}}(\tilde{n}, 2d)$ は次のように表される.

$$p_{\tilde{n}}(\tilde{n}, 2d) = \frac{1}{\sqrt{2\pi\sigma}} \sum_{l=-\infty}^{\infty} e^{-\frac{(\tilde{n}-2ld)^2}{2\sigma^2}} \quad (2)$$

この式は, テータ関数[23]で表すこともできる. $2d = 3.0$, $\sigma = 1$のときの概形を Fig.5 に示す. $p(Y \mid \tilde{s})$は次のように表される.

$$\begin{aligned} p(Y=0|\tilde{s}) &= \int_0^d p(\tilde{y}|\tilde{s})d\tilde{y} \\ &= 1 - p(Y=1|\tilde{s}) \end{aligned} \quad (3)$$

$$p(\tilde{y}|\tilde{s}) = \frac{1}{\sqrt{2\pi\sigma}} \sum_{l=-\infty}^{\infty} e^{-\frac{(\tilde{y}-\tilde{s}-2ld)^2}{2\sigma^2}} \quad (4)$$

等確率1/2からの偏差を$\Delta(\tilde{s},\ 2d)$とする.

$$\Delta(\tilde{s},2d)=\int_0^d p(\tilde{y}|\tilde{s})d\tilde{y}-\frac{1}{2}$$

前の節で見たように, $lim_{d\to 0}\Delta(\tilde{s},\ 2d)=\ 0$であることは明らかである.

dが非零の場合, $\Delta(\tilde{s},2d)$は常に0とは限らない. 例として, $\sigma=\ 1$として, $\Delta(\tilde{s},2d=3)$の概要をFig.6に示す. $\Delta(\ \tilde{s},2d\ =\ 3)$は$\tilde{s}$によって変化することがわかる.

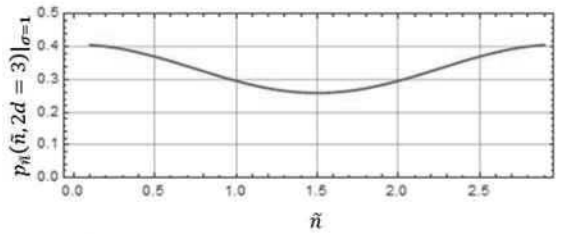

Fig. 5 Overview of $p_{\tilde{n}}(\tilde{n},2d=3)$ at $\sigma=1$.

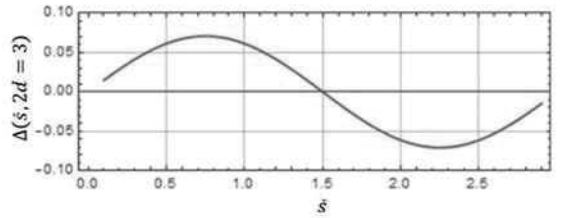

Fig. 6 Overview of $\Delta(\tilde{s},2d=3)$ at $\sigma=1$.

残余項sが送信信号または$1\ /\ f$雑音を表すことを考慮すると, サンプリング周期$1\ /\ f_s$では時不変であるように思える. したがって偏差は, 確率 1/2 からのずれの最大(最悪)値をもってその価とする. これは, $\tilde{s}\ =\ d\pm d\ /\ 2$の場合に現れる. この場合, 最大偏差$\Delta'(d\ /\sigma)$は次のように表すことができる.

$$\begin{aligned}\Delta'\left(\frac{d}{\sigma}\right)&=\Delta\left(\tilde{s}=\frac{d}{2},2d\right)\\&=\int_0^d p\left(\tilde{y}|\tilde{s}=\frac{d}{2}\right)d\tilde{y}-\frac{1}{2}\\&=\frac{1}{\sqrt{2\pi}}\sum_{l=-\infty}^{\infty}\int_0^{\frac{d}{\sigma}}e^{-\frac{\left(\tilde{y}-\frac{d}{2\sigma}-\frac{2ld}{\sigma}\right)\text{\^{}}2}{2}}d\tilde{y}\end{aligned}\qquad(5)$$

この概形をFig.7に示す. これより, たとえば, 量子化幅が熱雑音の標準偏差σに等しい場合, 偏差が0.01未満であることや, $d\ /\sigma$が3/4未満の場合偏差は約10^{-4}以下であることがわかる.

通信理論の観点から, $\tilde{s}$は量子化雑音であるから, その分布は均一であるとみなすことができる. つまり, $p(\tilde{s})=\ 1\ /(2d)$である. したがって, 長期間平均では偏差の期待値が 0 になると予想される. つまり Yは等しい確率で 0 または 1 になる.

$$\begin{aligned}p(Y=0)&=\int_0^{2d}(Y=0|\tilde{s})d\tilde{s}\\&=\frac{1}{2}+\int_0^{2d}\Delta(\tilde{s},2d)d\tilde{s}=\frac{1}{2}\end{aligned}$$

3.6 エントロピー

よく知られているシャノンエントロピーは平均的な予測不可能性を表す. これとは対照的に, 最小エントロピーは事象の予測不可能性の最小値であり, 次のように表される.

$$\begin{aligned}\min H\left(\frac{d}{\sigma}\right)&=-\log_2\max\left(\frac{1}{2}+\Delta(\tilde{s},2d)\right)\\&=-\log_2\left(\frac{1}{2}+\Delta'\left(\frac{d}{\sigma}\right)\right)\end{aligned}\qquad(6)$$

この概形を Fig.8 に示す. $d/\sigma\le 1.5$の時, 約0.8ビット以上になることがわかる.

3.7 入力アナログ値が ADC 範囲外の場合

前に説明したように, 入力アナログ信号は ADC 入力範囲内にあると想定される. つまり, 量子化されたレベル2^qの数は, 歪みなしで入力信号をデジタル化するのに十分な数である. 範囲外の場合, 最大値または最小値が量子化信号として出力される. これがかなりの程度発生すると, LSB の特性がランダム性に関して好ましくなくなる可能性がある. この場合, 一般的に信号は端末で正しく受信できない. その場合, 無線システムは, 信号の送信に必要なシステム情報を受信しないため, 端末が通信を開始できないようにする必要がある. 端末がすでに通信を開始しているときに信号が正しく受信されない場合, 端末は否定応答メッセージを送信するか, 以前に送信されたのと同じメッセージを再送信する. 端末は新しいメッセージを送信できないため, いずれの場合も新しい乱数は必要ない. 無線通信システムのこの機能は, 提案する TRNG スキームの ADC 範囲外の問題を軽減する.

4 提案する TRNG スキーム

4.1 システム概要

Fig.9 は, 無線システムにおける提案 TRNG の機能ブロック図を示している. ここで, DUP / SW は, 送信と受信の両方に単一のアンテナを使用するためのデュプレクサまたはスイッチであり, RX は受信回路, TX は送信回路として機能し, proc.は

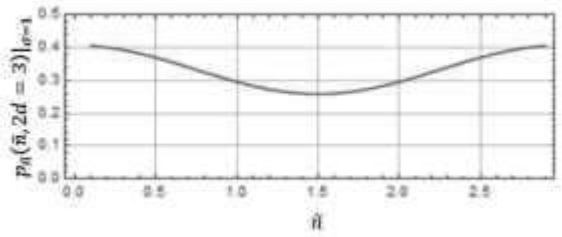

Fig. 5 Overview of $p_R(\tilde{n}, 2d = 3)$ at $\sigma = 1$.

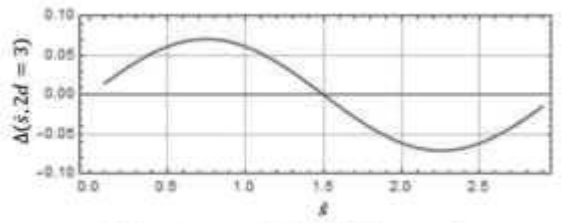

Fig. 6 Overview of $\Delta(\tilde{s}, 2d = 3)$ at $\sigma = 1$.

信号処理装置を表す． 前述のように，無線端末は，システム情報やネットワーク側からの送信許可を取得する必要があるため，一般的な無線システムでは，送信前に基地局から信号を受信する必要がある． よって TRNG は端末の受信処理中に機能するだけで事が足りる．

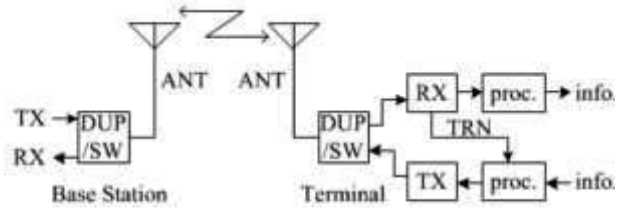

Fig. 9 System concept.

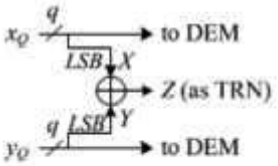

Fig. 10 Configuration for TRNG.

Table 1 Joint probability with correlation parameter, r.

	$Y=0$	$Y=1$	$p(X)$
$X=0$	$(\frac{1}{2}+\Delta_1)(\frac{1}{2}+\Delta_2)+r$	$(\frac{1}{2}+\Delta_1)(\frac{1}{2}-\Delta_2)-r$	$\frac{1}{2}+\Delta_1$
$X=1$	$(\frac{1}{2}-\Delta_1)(\frac{1}{2}+\Delta_2)-r$	$(\frac{1}{2}-\Delta_1)(\frac{1}{2}-\Delta_2)+r$	$\frac{1}{2}-\Delta_1$
$p(Y)$	$\frac{1}{2}+\Delta_2$	$\frac{1}{2}-\Delta_2$	

4.2 構成

提案方式はTRNGのために通信回路の一部を利用おり，入力信号レベルによってはd/σが小さくならない場合がある． この状況に対処するために，提案方式では，Fig.10 に示すように，X と Y の間の XOR 演算($Z = X \oplus Y$)を使用する．

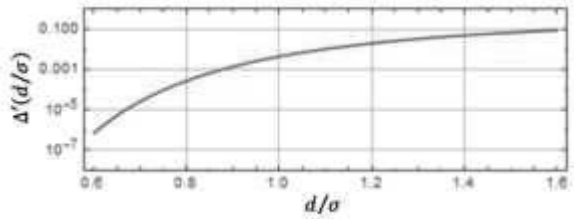

Fig. 7 Overview of $\Delta'(d/\sigma)$.

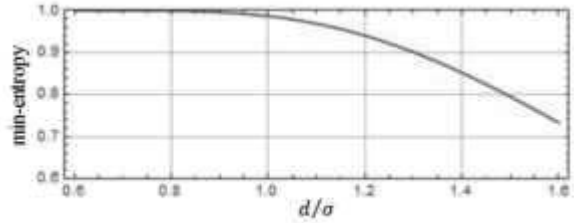

Fig. 8 Theoretical min-entropy for single channel.

独立したバイナリシーケンス間で XOR されたシーケンスは，特に論理0と1のバランスで，より優れたランダム性を持っていることが知られている[10]. I 成分と Q 成分間の独立性の原則により，X と Y は互いに独立しているため，Z はより優れた 0 と 1 のバランスを有する．入力レベルが高くクリッピングされる場合でも，I 成分と Q 成分の両方が同時に飽和することはめったに起こらないため，Z のシーケンスでの 0 と 1 のバランスはそれほど悪化しないことが期待される．

4.3 乱数の平均値

前述のように，I成分とQ成分は，理想的には独立と想定されている． ただし，特定のハードウエア誤差のために独立性が完全ではない可能性があるため，実用的な観点から，両成分間の相関が乱数 Z に与える影響を調べることは価値がある． 同時確率$p(X,Y)$を表 1 の式として定義する．

Table 1 で，$\Delta_i = \Delta(\tilde{s}_i, 2d)$， $\tilde{s}_1$および $\tilde{s}_2$は，それぞれ I-Ch および Q-Ch の残余項の成分である．項rは，X と Y の間の相関を決定する．$r = 0$の場合，X と Y の間の相関はない．X と Y の間の相関は次のとおりである．

$$\frac{E[XY]}{\sqrt{Var[X]Var[Y]}} = \frac{r}{\sqrt{(1/4-\Delta_2^2)}} \cong 4r \quad (7)$$

Z の確率は次のように表すことができる．

$$p(Z=0|\tilde{s}_1,\tilde{s}_2) = \frac{1}{2} + 2\Delta(\tilde{s}_1,2d)\Delta(\tilde{s}_2,2d) + r$$

$$p(Z=1|\tilde{s}_1,\tilde{s}_2) = \frac{1}{2} - 2\Delta(\tilde{s}_1,2d)\Delta(\tilde{s}_2,2d) - r$$

したがって，次のように，式(5)で与えられるYの最大偏差と比較して，Z の最大偏差が改善される．

$$2\Delta'^2\left(\frac{d}{\sigma}\right)+2r\,.$$

Fig.11 は, $r = 0$の場合の Z の最大偏差を破線で, $r = 10^{-4}$の場合の実線でプロットしている. どちらの場合も, $d/\sigma \le 1.5$であるため, Z の最大偏差は 0.01 未満になる.

4.4 エントロピー評価

推定される最小エントロピーは次のようになる.

$$\begin{aligned}\min H\left(\frac{d}{\sigma}\right) &= -\log_2 \max p(Z|\tilde{s}_1,\tilde{s}_2)\\ &= -\log_2\left(\frac{1}{2}+2\Delta'^2\left(\frac{d}{\sigma}\right)+2r\right)\end{aligned} \quad (7)$$

これを Fig.12 に示す. 破線は$r = 0$の場合を表し, 実線は$r = 10^{-4}$の場合を表す. 線はほぼ同じ曲線を示している. どちらの場合も, 最小エントロピーは$d/\sigma \le 1.5$のとき約 0.95 ビットである.

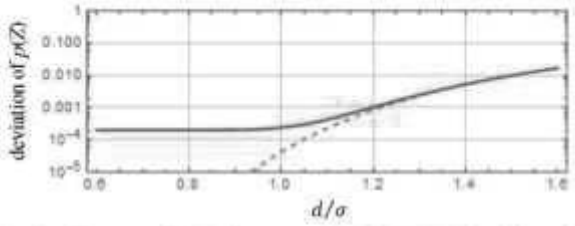

Fig. 11 Deviation of $p(Z)$ for proposed TRNG. (dashed line for $r = 0$, solid line for $r = 10^{-4}$).

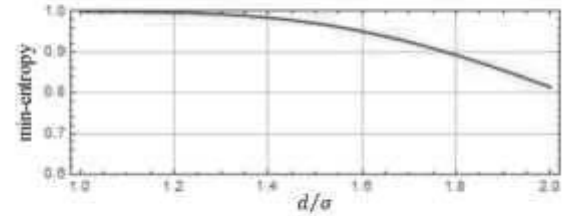

Fig. 12 Theoretical minimum entropy for proposed TRNG. (dashed line for $r = 0$, solid line for $r = 10^{-4}$).

5 実験的検証

5.1 実験システム

この節では, 多目的受信機を用いて, 提案スキームの実現可能性を検証する. この受信機は, Fig.3 のx_Qとy_Qのシーケンスをパソコン(PC)に出力する. Fig.13 の実験システムは, 通信の所望信号を模擬する信号発生器, シールドボックス内の送受信用に近接して配置された 2 つのアンテナ, および多目的受信機で構成されている. 主な条件は Table2 にまとめてある.

受信機はスーパーヘテロダイン構成を採用しており, 信号は中心周波数 3.57MHz の IF 帯域でサンプリングされ, デジタル処理を使用して I および Q ベースバンド成分に変換される. 所望信号として PN9 シーケンスが, シンボルレート 128kbaud の QPSK 変調で生成される. その中心周波数は, 日本のテレメータ, テレコントロール, およびデータ伝送設備に使用される 920MHz 帯域である[27]. サンプリング周波数は送信信号の 2 倍オーバーサンプルを想定している. なお, rtl_test コマンド[26]を使用すると, PC に測定データがドロップされていないことが確認された. 固定出力電力のキャプチャされたファイルには, $2\,[Byte] \times 256\,[kHz] \times 600\,[秒] = 307{,}200\,[kByte] = 300{,}000\,[KB]$のデータがある. ここで, 接頭辞「k」は 1,000 倍を意味し, 単位「KB」は 1,024 [バイト]である.

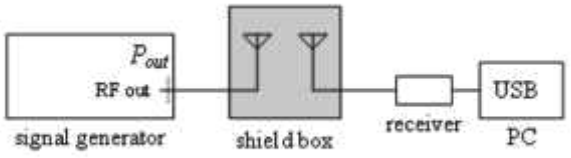

Fig. 13 Experimental system.

Table 2 Test conditions.

Transmitter	
Signal generator	Agilent E4432B [24]
Center frequency	923.6 MHz
Baseband signal	PN9
Bandpass filter	Root Nyquist with 0.5 roll-off
Modulation	QPSK
Symbol rate	128 kbaud
Output power P_{out}	$-\infty$ dBm ~ 0 dBm
Receiver	
Device	R820T [28]
Sampling frequency	256 kHz
Number of quantizing bits	8 for each channel
Environment	
Temperature	24°C
Measurement duration	600 [s] each for a fixed output power

4.2 節で提案したスキームに従って, バイナリ乱数 Z のシーケンスがそのファイルから生成される. さらに, 元のバイナリ雑音特性を観察するために, I-Ch からの X と Q-Ch からの Y の 2 つのシーケンスファイルも生成される. これらの 3 つのファイルのサイズは同じ 18,750 [KB] (= 300,000 [KB] / 16) である.

5.2 フルビット特性

実験構成の利得特性を確認するために, Fig.13 に示す信号発生器の出力レベルP_{out}と量子化されたシンボルの平均二乗との関係を求めた. 参考までに, 目的の信号がない場合, つまり

$P_{out} = -\infty\ dBm$も測定されている. 増幅利得は, 雑音成分を収集する TRNG の重要なパラメータである. 受信機は自動的に利得を制御して, ADC 範囲内の入力信号を適切に増幅する. 入力信号レベルが高い場合, 利得は低くなる. その後, 雑音が抑制され, d /σ が高くなるため, 生成される乱数のランダム性が悪化する可能性がある. 入力信号レベルがかなり高い場合, 端末は信号を正しく受信できないため, 通常, 新しいメッセージを送信することは許可されない. このような場合, 端末は新しい乱数を必要としない可能性が高い.

Fig.14 は, RF 出力が変化したときの量子化および 2 乗サンプル値の平均 $\overline{|x_Q|^2 + |y_Q|^2}$をプロットしている. 各チャネルに 8 ビット ADC があるため, 最大値は$2^{7\times2} = 16384$である. この図によると, 量子化された信号は, $P_{out} \geq -20dBm$のときに飽和する.

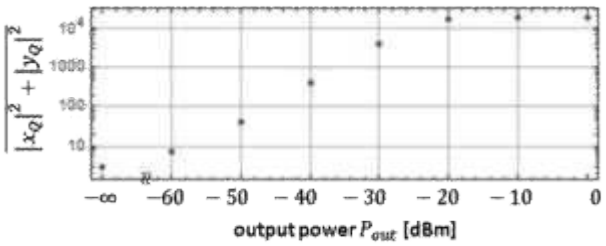

Fig. 14 Average squared signal property.

5.3 NIST 統計検定

NIST 統計検定は, ランダムシーケンスのランダム性を評価するための 15 のテスト項目で構成され, 複数のストリームが必要である. 参考文献[30](p.2-23) によると, 少なくとも Maurer の"Universal Statistical"検定では, 各ストリームの長さは 387,840 ビットである必要がある. 一部のテストでは, 各ストリームの長さが 10^6 ビット以上であることも推奨している[30](p.2-26, p.2-37).

Table 3 Block length for statistical tests.

Block Frequency, M	128
Non-Overlapping Template, m	9
Overlapping Template, m	9
Approximate Entropy, m	10
Serial, m	16
Linear Complexity, M	500

さらに, 各テスト項目の P 値の分布の均一性を確認するために, P 値の P 値も評価される. P 値 ≥ 0.0001の場合, シーケンスは均一に分布していると見なすことができるが, 統計的に意味のある結果を得るには, 少なくとも 55 のストリームを処理する必要がある[30](p.4-3).

Table 4 NIST statical test results for sequences of X, Y and Z.

P_{out}	−∞	−60	−50	−40	−30	−20	−10	0
Seq. X	Fail	Pass	Pass	Pass	Pass	Fail	Fail	Fail
Seq. Y	Fail	Pass	Pass	Pass	Pass	Fail	Fail	Fail
Seq. Z	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass

Table 5 Pass rate of failed statistical tests at P_{out} = −∞ dBm for sequences of X and Y, with the sequence of Z for reference.

Test item	Frequency	Cum. Sums (F)	Cum. Sums (R)
Seq. X	139/150	141/150	138/150
Seq. Y	133/150	135/150	135/150
Seq. Z	148/150	147/150	148/150

これらの要件と推奨事項を考慮して, バイナリシーケンスは 150 [ストリーム]と 1,024,000 [ビット/ストリーム]または 125 [KB /ストリーム]に分割される. テストで定義されたブロック長の変数は, すべての値が推奨範囲内になるように表 3 に示すように設定される.

重複しないテンプレートマッチングテストの場合, $m = 9$の場合に最大 148 個のテンプレートが提供され, 各テンプレートがすべてのストリームに対して評価される. 148 個のテンプレートすべてがテストシーケンスに適用されると, ストリームが本当にランダムであっても, 失敗する確率が存在することに注意する. 確率は, テンプレートごとに 0.0027 と推定される. したがって, ストリームが本

Table 6 Minimum entropy with non-IID assumption results.

P_{out} dBm	−∞	−60	−50	−40	−30	−20	−10	0
Most Common Value	0.998798	0.998768	0.998575	0.998845	0.999083	0.998671	0.999132	0.998974
Collision	0.966577	0.966577	0.966577	0.977632	0.955606	0.955606	0.955606	0.977632
Markov	0.999036	0.999109	0.998852	0.998803	0.999193	0.998847	0.999475	0.999327
Compression	1.000000	1.000000	1.000000	1.000000	1.000000	1.000000	1.000000	1.000000
t-Tuple	0.936758	0.936758	0.940114	0.938417	0.936758	0.933552	0.936758	0.940114
LRS	0.999989	0.995650	0.999112	0.997434	0.999961	0.999848	0.987004	0.995447
Multi MCW	0.999621	0.999470	0.999005	0.999895	0.999466	0.998892	0.999143	0.999275
Lag	0.999121	0.999302	0.999151	0.998891	0.999277	0.998659	0.999282	0.998915
Multi MMC	0.999043	0.999382	0.999266	0.999249	0.998962	0.999110	0.999394	0.999665
LZ78Y	0.998979	0.998940	0.998752	0.998704	0.998861	0.998876	0.999734	0.999259
Min-entropy	0.936758	0.936758	0.940114	0.938417	0.936758	0.933552	0.936758	0.940114

当にランダムであっても，148 個のテンプレートすべてが適用されると，いくつかのテンプレートテストが失敗する可能性がある[31]． ここでは，このような状況にもかかわらず，念のため，統計的検定に 148 個のテンプレートすべてを使用した．

統計的検定では，148 個の重複しないテンプレートマッチングテストを含む 13 個のテスト項目の 150 個のストリームのうち少なくとも 144 個のストリームに合格する必要があり，ランダムエクスカーションテストとランダムエクスカーションバリアントテストの他の 2 つのテストには別の基準がある． 乱数 X, Y, Z の結果を表 4 にまとめた．ここで，「合格」は 15 のテスト項目すべてが解決されたことを意味し，それ以外の場合は「不合格」と判断される．

$P_{out} = -\infty dBm$の場合，同じ 2 つのテスト項目（周波数（モノビット）テストと累積合計テスト）が原因で，X と Y のシーケンスが失敗した． それらの合格率を表 5 に示し，参照用に Z のシーケンスを示す．

信号が送信された後($P_{out} > -\infty dBm$)，$P_{out} \geq -20dBm$の場合，上記の 2 つのテスト項目を含む 12 のテスト項目で X と Y の 2 つのシーケンスが再び失敗した． $P_{out} = -\infty dBm$の場合の X と Y のシーケンスの失敗の理由は，レシーバの ADC での低入力レベルであると推測される． 信号レベル $\overline{|x_Q|^2}$と $\overline{|y_Q|^2}$は，Fig.14 に示すそれらの合計のほぼ半分である． 具体的には，$P_{out} = -\infty dBm$ で $\overline{|x_Q|^2} \sim \overline{|y_Q|^2}$~1.44である． これは，この場合，有効ビットサイズが小さすぎて単一チャネルによるテストに対応できないことを意味する． 一方，ADC での入力信号レベルが飽和しているため，P_{out}が高い場合の障害が考慮される． Z のシーケンスに関しては，NIST 統計検定はすべてのP_{out}条件に合格している．

また，各テスト項目の P 値の均一性を評価するために P 値を確認した． この節の冒頭で述べたように，P 値が 0.0001 以上の場合は均一であると見なされる． その結果，シーケンス Z は，1 つの場合を除いてこの条件を満たす．148 の非重複テンプレートマッチングテストの 1 つは，$P_{out} = -20dBm$ の場合にのみ失敗する． この場合，2 つの理由が考えられる． 最初の理由は入力レベルの飽和だが，$P_{out} = -10$および$0dBm$の場合でも均一性テストに合格している． 2 つ目は，前述のように，シーケンスが本当にランダムであっても，148 個のテンプレートすべてを満たさない可能性が少しある．結果として，致命的なエラーではないと言えるが，入力レベルが飽和している場合は注意が必要である． RF 信号はそれほど強くないため，通常の使用では飽和は発生しないが，意図的に実現される場合がある．

5.4 最小エントロピー評価

NIST SP800-90B [32]に続いて，生成された乱数シーケンス Z の最小エントロピーも 10 の推定方法で非 IID 仮定を用いて評価した．表 6 に結果を示す． すべてのP_{out}値について，最小エントロピーは t-Tuple 推定によって記録される． 以前の研究[10]の表 7 によると，従来の方法の最小エントロピーは 0.47 から 0.93 の範囲であると推定されている． このことから，我々の結果は満足できる．

6 結論

雑音レベルの MSB を使用する従来の TRNG は，予測可能な構成要素を可能な限り除外する必要がある． 対照的に，本論文では，無線システムの端末の雑音レベルの LSB に基づく TRNG 法を提案し，理論的な AWGN モデルでこの方法を議論し，一般的な受信機を使用した実用的な観点からいくつかの統計的検定でその最小エントロピーを評価した．

提案された方法は，追加の回路と処理がほとんどないため，無線端末への埋め込みに適している．ユーザー端末だけでなく，無線センサやマシンツーマシン通信用の小型 IoT 端末も，提案された方法の好ましいアプリケーションの例である． 受信信号レベルに注意を払う必要があるが，NIST 統計テストと最小エントロピー推定の結果はかなり良好なパフォーマンスを示した． 入力信号レベルがかなり高い場合（意図的に発生する可能性がある），信号は受信機で歪んでおり，復調できない． この場合，無線通信システムの一般的な操作として，端末は更新された情報を送信しないため，端末は新しい乱数を必要としない． これらの結果は，提案された TRNG スキームが合理的に効果的かつ効率的であることを示している．

謝辞

この研究は，日本学術振興会科研費助成番号 25330157 の支援を受けました．著者は，XOR 操

作を排除することによる評価方法と「ハイスループットモード」の可能性について貴重なコメントを提案した匿名の査読者に感謝します.

参考文献

[1] N.Heninger, Z.Durumeric, E.Wustrow, and J.A.Halderman, “Mining your Ps and Qs: Det-ection of widespread weak keys in network de-vices,” Proc. 21st USENIX Security Symposi-um, Aug. 2012,Rev.2, July 11 2012.

[2] M.Bellare, S.Goldwasser, and Micciancio, , “Pseudo-random” number generation within cryptographic algorithms: The DSS case,” Proc. Crypto’97, LNCS 1294, IACR, Palo Alto, CA, Springer-Verlag, Berlin 1997.

[3] C.S. Petrie and A. Connelly, “A noise-based IC random number generator for applications in cryptography,” IEEE Trans. Circuits Syst. I, Fundam. Theory Appl., vol.47, no.5, pp.615–621, 2000.

[4] W.T. Holman, J.A. Connelly, and A. Dowlataba-di, “An integrated analog/digital random noise source,” IEEE Trans. Circuits Syst. I, Fundam. Theory Appl., vol.44, no.6, pp.521–528, June 1997.

[5] S. Callegari, R. Rovatti, and G. Setti, “Embedd-able ADC-based true random number genera-tor for cryptographic applications exploiting nonlinear signal processing and chaos,” IEEE Trans. Signal Process., vol.53, no.2, pp.793–805, Feb. 2005.

[6] W. Chen, W. Che, Z. Bi, J. Wang, N. Yan, X. Tan, J. Wang, H. Min, and J. Tan, “A 1.04μW truly random number generator for Gen2 RFID tag,” Solid-State Circuits Conference, 2009. A-SSCC 2009.IEEE Asian, pp.117–120, Nov. 2009.

[7] J. Holleman, S. Bridges, B.P. Otis, and C. Diorio, “A 3μW CMOS true random number generator with adaptive floating-gate offset cancellation,” IEEE J. Solid-State Circuits, vol.43, no.5, pp.1324–1336, 2008.

[8] H. Zhun and C. Hongyi, “A truly random num-ber generator based on thermal noise,” Proc. International Conference on ASIC, pp.862–864, 2001.

[9] G.K. Balachandran and R.E. Barnett, “A 440-nA true random number generator for passive RFID tags,” IEEE Trans. Circuits Syst. I, Reg. Papers, vol.55, no.11, pp.3723–3732, 2008.

[10] K. Lee, S. Lee, C. Seo, and K. Yim, “TRNG (true random number generator) method usi-ng visible spectrum for secure communication on 5G network,” IEEE Access, vol.6, pp.12838–12847, 2018, DOI10.1109/ACCESS. 2018.2799682.

[11] J. Voris, N. Saxena, and T. Halevi, “Accelerom-eters and randomness: Perfect together,” Se-curity - WISEC 2011, pp.115–126, ACM, H-amburg, Germany, June 2011.

[12] K. Wallace, K. Moran, E. Novak, G. Zhou, and K. Sun, “Toward sensor-based random num-ber generation for mobile and IoT devi-ces, ”IEEE Internet Things J., vol.3, no.6, pp.1189–1201, Dec. 2016.

[13] A. Francillon and C. Castelluccia, “TinyRNG: A cryptographic random number generator for wireless sensor network nodes,” Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks, IEEE, Limassol, Cyprus, April 2007.

[14] R. Latif and M. Hussain, “Hardware-based random number generation in wireless sensor networks (WSNs),” Advances in Information Security and Assurance, pp.732–740, 2009.

[15] C. Hennebert, H. Hicham, and L. Cedric, “The entropy of wireless statistics,” Proc. 2014 European Conference on Networks and Com-munications (EuCNC), pp.1–5, 2014.

[16] F.A. Levinzon and L.K.J. Vandamme, “Comparison of 1/f noise in JFETs and MOSFETs with several figures of merit,” Fluct. Noise Lett., vol.10, no.4, pp.447–465, 2011.

[17] Q. Gu, RF System Design of Transceivers for Wireless Communications, pp.154–155, Spri-nger, 2005.

[18]http://www.fdk.com/cybere/pi_ic_rpg100.html
[19]http://www.silego.com/products/668/312/TrueRandom-Number-Generator-Hardware.html
[20] K. Yamaguchi and K. Nakamura, “HW-based random bit sequence generation method using gettime function,” Proc. International Sympo-sium on Information Theory and its App-licationsIn (ISITA), Auckland, New Zealand, Dec. 2008.
[21] C. Hennebert, H. Hossayni, and C. Lauradoux, “The entropy of wireless statistics,” Proc. 2014 European Conference on Networks and Communications (EuCNC), pp.1–5, 2014.
[22] J.G. Proakis, Digital Communications, 3rd Ed., McGraw-Hill, 1995.
[23] N.I. Koblitz, Introduction to Elliptic Curves and Modular Forms, 2nded., eq. (4.11) in p.73, Springer, 1993.
[24]http://literature.cdn.keysight.com/litweb/pdf/59661010J.pdf
[25] C. Laufer, The Hobbyist’s Guide to the RTL-SDR: Really Cheap Software Defined Radio, 3rd ed., Createspace Independent Pub, 2015.
[26] https://osmocom.org/projects/sdr/wiki/rtl-sdr
[27]https://www.arib.or.jp/english/html/overview/doc/5-STD-T108v1_0-E1.pdf
[28]https://www.rtl-sdr.com/buy-rtl-sdr-dvb-t-dongles/
[29] R.W. Stewart, K.W. Barlee, and D.S.W. Atkinson, Software Defined Radio Using MA-TLAB & Simulink and the RTL-SDR, pp.10–19, Strathclyde Academic Media, 2015.
[30] NIST, “A statistical test suite for random and pseudorandom number generators for cryptographic applications,”
http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-22r1a.pdf
[31] Ken Umeno, http://www.chaosware.com/rans-ure/pdf/ransure2.pdf
[32] NIST, “Recommendation for the Entropy Sou-rces Used for Random Bit Generation,”
https://csrc.nist.gov/csrc/media/publications/sp/800-90b/draft/documents/sp800-90b_second_draft.pdf