論　文

A-D変換器の最下位ビットを用いた暗号用乱数生成法

茂呂　友子[†]　　斉藤　義明[††]　　堀　　潤一[††]　　木竜　　徹[†]

Generation of Physical Random Number Using the Lowest Bit of an A-D Converter

Tomoko MORO[†], Yoshiaki SAITOH[††], Junichi HORI[††], and Tohru KIRYU[†]

あらまし　物理乱数を生成する方法の一つとして，電気信号を用いることが挙げられる．従来は，電気信号から乱数を発生させる場合，信号のレベルに関ししきい値を設けそれを超えるか超えないかを判定し“0”，“1”を割り付ける方法などが取られてきた．本論文では，A-D変換器の最下位ビットを用いることによって，従来法では実現が困難であった乱数の高速生成が可能であることを示した．更に，特殊な雑音発生器を用いずに，発振器の揺らぎによって乱数を生成することが可能であることを示した．

キーワード　物理乱数，A-D変換器の最下位ビット，発振器，暗号用乱数

1. まえがき

高度情報通信社会が実現されつつある今日，情報の保護は最も重要視されるべき課題の一つである．現在，主に利用されている暗号方式（RSA公開鍵暗号）は，解読するのに巨大な整数を素因数分解する必要があり，現在のコンピュータの性能では莫大な時間を要する[1],[2]．このように，解読に非現実的な時間がかかることを安全性の根拠としている．しかし，ここ数年飛躍的な進歩を遂げている，ネットワークを使用した分散処理（グリッドコンピューティング）の発達や量子コンピュータの出現等によって，その計算量的安全性は崩壊の危機にさらされていると考えられる．その対策として，より無秩序な乱数による暗号化が考えられる．そのため，周期性のない一様乱数を発生する乱数生成方法が切望される[3]．

乱数には，算術乱数と物理乱数がある．算術乱数は，繰り返し演算することによって得られるため周期性をもつ可能性があり，高速計算が可能な時代の暗号化に使用するには不十分であると考えられる．一方，物理乱数は，ランダムな自然現象を用いて生成されるため周期性をもたず，十分なセキュリティが得られると期待されている．しかし，乱数の生成に放射線による雑音や，ダイオードのショット雑音などの物理的な雑音を用いた場合[4]，あるいは演算増幅器によるカオス発生器を用いた場合[5]等ではその生成速度が遅く実用に供するのは困難である．そこで本論文では，電気信号における揺らぎより発生する雑音を用いて，暗号化に用いるための物理乱数を高速に生成する工夫について述べる．

電気信号から乱数を発生させる場合，信号のレベルに関ししきい値を設けそれを超えるか超えないかを判定し“0”，“1”を割り付ける方法（この方法を以下「しきい値法」と称す.）や，位相の比較による方法[6]が取られてきた．前者の場合の問題点として，乱数生成速度を速くするためサンプリング周波数を高くしようとすると，電気信号に含まれる周波数成分も高くする必要があった．または，信号の周波数が不安定である必要があった．この問題の対処法として，筆者らは雑音で周波数変調をかけた発振信号を用いることを提案した．一方，後者の位相比較法では，高速化のためには高い励振周波数が必要となる問題点があった．

本論文で提案する方法は，電気信号に含まれる周波数成分が低くてもサンプリング周波数を高くできる方法である．A-D変換器のビット長をnとし，最下位ビットを用いることで，従来のしきい値法に比べてサンプリング周波数を2の$(n-1)$乗近くまで高くすることができる．この方法について実際に実験を行い，暗号用乱数の統計的乱数性の評価法として用いら

[†] 新潟大学大学院自然科学研究科，新潟市
Graduate School of Science and Technology, Niigata University, 8050 Ikarashi 2-nocho, Niigata-shi, 950-2181 Japan
[††] 新潟大学工学部福祉人間工学科，新潟市
Dept. of Bio-Cybernetics, Niigata University, 8050 Ikarashi 2-nocho, Niigata-shi, 950-2181 Japan

れている NIST の FIPS140-2 [7] の評価尺度を用いて検証した．現在，物理乱数発生法の速度は 250 kbits/s 位 [8] であるが本実験では 10 Mbits/s を実現した．

本論文で提案する方法の有利な点は，しきい値を設定する必要がないこと，及び特殊な雑音源を必要としないことである．

2. 乱数生成の基本原理

A–D 変換器の最下位ビットが “0”，“1” と交互に変化するための必要条件を考え，A–D 変換器に入力する信号の必要周波数を推定してみる．

12 ビット長の A–D 変換器を使用した場合の正弦波による乱数生成の原理について説明する（図 1）．なお振幅は ±5 V とする．この A–D 変換器は 12 ビット長すべてを使用したとき，波形の振幅を 4096 分割（4096 ステップ）することになる．正弦波 1 周期を 360° と表したとき，1 ステップ変化するのに必要な角度 x を求める．

正弦波において最も変化が少ない部分は 90° 付近と 270° 付近であるから，この付近において 1 ステップ変化するのに必要な角度を求めればよい．そこで 90° 付近について考える．振幅が ±5 V であることから，1 ステップに相当する振幅を求める．

$$1step = \frac{10\,[\mathrm{V}]}{4096} \cong 0.00244\,[\mathrm{V}] \tag{1}$$

90° から 1 ステップ移動するための角度 y を求める．

$$y_1 = \sin^{-1}\left(\frac{5 - 0.00244}{5}\right) \cong 88.2^\circ \tag{2}$$

より，

$$y = 90^\circ - y_1 = 1.8^\circ \tag{3}$$

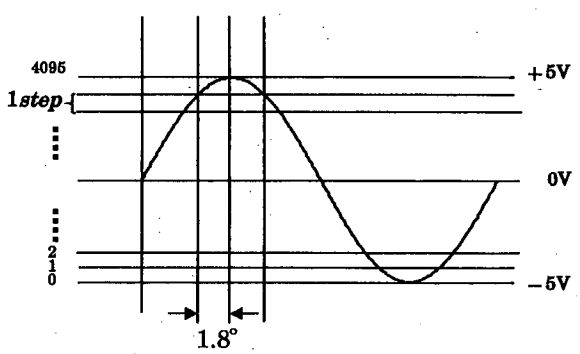


図 1　A–D 変換器の最下位ビットを使用した乱数生成の原理

Fig. 1　Principle of random number generator using the lowest bit of an A-D converter.

90° の前後について考慮が必要であるから角度 x は y の 2 倍である，

$$x = 1.8^\circ \times 2 = 3.6^\circ \tag{4}$$

となる．x は必要最小限の角度となるため，1 周期中では，

$$\frac{360^\circ}{3.6^\circ} = 100 \tag{5}$$

となり，1 周期中に約 100 回までサンプリング可能であるといえる．この原理から，サンプリング周波数 1 MHz の場合は入力信号の発振周波数を 10 kHz 以上，サンプリング周波数 10 MHz の場合は入力信号の発振周波数 100 kHz 以上の正弦波をシステムに入力し，この正弦波に揺らぎが存在すれば乱数の生成が可能であると推測できる．

3. 乱数生成システム

3.1 発振器による乱数生成

本システムは，図 2 のごとく発振器の出力を直接 A–D 変換器を用いて計算機に取り込むものである．用いた発振器は，RC 発振器（菊水電子工業株式会社製 418B）及び LC 発振回路（図 4）である．これらの発振器の短期安定度はそれぞれ約 1×10^{-5}，1×10^{-4}（ゲート時間 10 秒の実測値）である．取り込んだデータを乱数へ変換する方法については，後述の **3. 3** で示す方法を用いた．

3.2 ショット雑音発生回路による乱数生成

乱数を生成する方法として，雑音を直接取り込み，数値化する方法もある．本論文で提案する方法を検討するためにこの実験を行った．ここではダイオードのショット雑音を利用した．ショット雑音を用いた乱数生成システムを図 3 に，実際に用いたショット雑音発生回路を図 5 に示す．図 5 ではダイオードで発生させたショット雑音を約 105 dB の電圧利得で A–D 変換器の入力レンジを超えない範囲で増幅した．図 5 の回路の出力に対して A–D 変換を行い，計算機にデータを取り込んだ．取り込んだデータを乱数へ変換する方法については，後述の **3. 3** で示す方法を用いた．

3.3 2 進乱数列への変換

計算機に取り込んだデータから，乱数列を生成する方法を説明する．本システムで使用した二つの A–D 変換器 [Contec 社製，A-D12-16U (PCI)E（サブレンジング・フラッシュ方式，最高サンプリング周波数 1 MHz，以下 AD12 と略す.），及び Interface 社製，

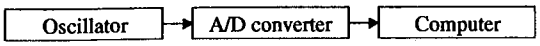


図 2 発振器を用いた乱数生成
Fig. 2 Random number generator using an oscillator.

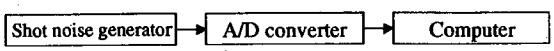


図 3 ショット雑音を用いた乱数生成
Fig. 3 Random number generator using shot noise.

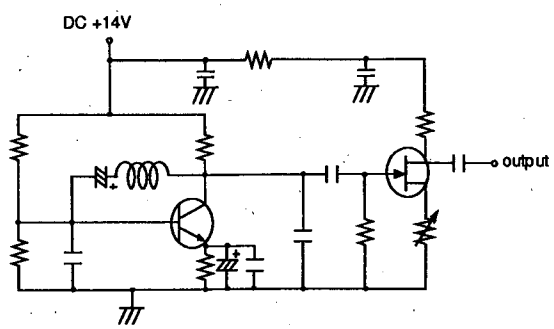


図 4 LC 発振回路
Fig. 4 LC oscillation circuit.

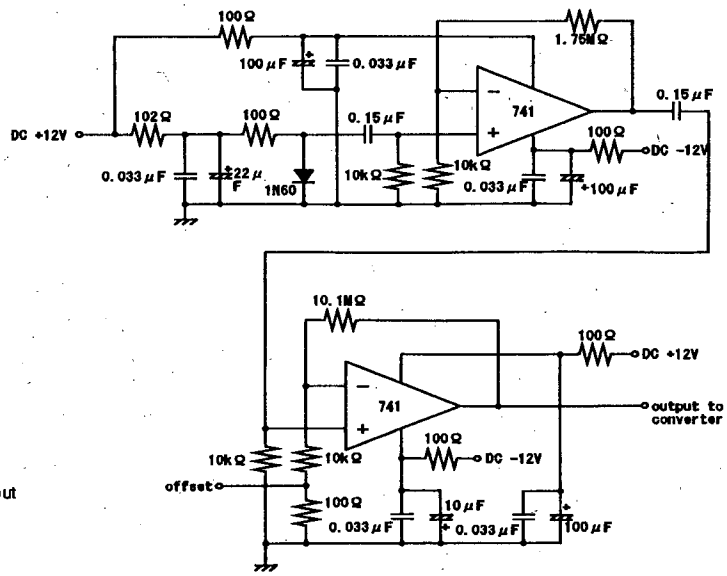


図 5 ショット雑音発生回路
Fig. 5 Shot noise generator.

表 1 ランの分布
Table 1 The distribution of run.

ランの長さ	要求される個数検定
1	2,315～2,685
2	1,114～1,386
3	527～723
4	240～384
5	103～209
6 以上	103～209

PCI3163（フラッシュ型パイプライン方式，最高サンプリング周波数 10 MHz，以下 PCI と略す.)］のビット長は，12 ビットである．本システムでは，−5～+5 V の範囲を 2^{12} つまり 4096 分割することになる（1 ステップ約 2.44 mV)．取り込んだ 2 進データの最下位ビットの値を用い，FIPS140-2 の検定法に合わせて 20,000 個を 1 組とし，各組に対して検定を行った．全組に対して FIPS140-2 の検定を行い，全組数に対する検定を通過した組数の割合を検定通過率と呼ぶ．検定法の詳細は **3. 4** で示す．

3. 4 乱数の評価

暗号用乱数を使用するには，暗号学的強度評価を行う必要がある．暗号学的に安全な乱数の必要条件の一つとして，統計的乱数性が挙げられる [9]．ここで，統計的乱数性とは，統計的な意味で乱数とみなせるか否かの評価である．この評価には，現在最も厳しいとされる NIST（National Institute of Standards and Technology）の FIPS140-2 に示される統計学的乱数生成テストを採用する．以下に FIPS140-2 の四つの検定について説明する．

3. 4. 1 モノビットテスト

系列中の 1 の個数 X は $9{,}725 < X < 10{,}275$ を満たす．

3. 4. 2 ポーカーテスト

系列を 4 ビットずつ分割して 5,000 個のブロックに分ける．ブロック内の 4 ビットを 16 進数としたとき，値が i となるブロックの個数を $f(i)$ とする（$0 \leq i \leq 15$)．このとき，$f(i)$ は次の不等式を満たす．

$$2.16 < \frac{16}{5000}\sum_{i=0}^{15} f(i)^2 - 5000 < 46.17 \qquad (6)$$

3. 4. 3 ランテスト

0 のラン及び 1 のランの分布が表 1 の条件を満たす．

3. 4. 4 長ランテスト

26 ビット以上のランを含まない．

4. 実験結果

A–D 変換器に入力する信号の周波数に対する低域特性について述べ，次に高域特性を述べる．更にショット雑音入力の場合についても述べる．

4. 1 低域特性について

4. 1. 1 RC 発振器による乱数生成

(a) 入力信号として RC 発振器の出力を正弦波としたものを用い，A–D 変換器（PCI）により A–D 変換

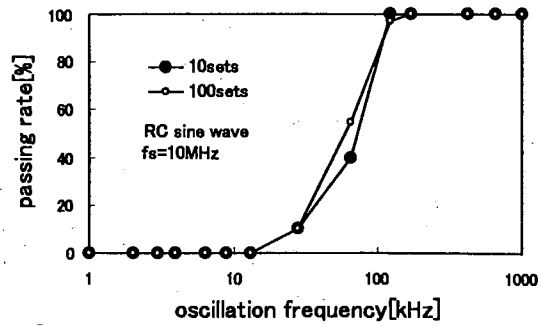


図 6　RC 発振器の正弦波を用いた場合の各発振周波数における検定通過率

Fig. 6　Relationship between passing rates and oscillation frequency for a RC sine wave.

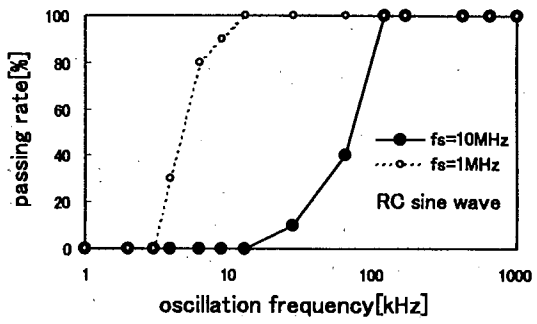


図 7　RC 発振器の正弦波を用いた場合のサンプリング周波数による違い

Fig. 7　Comparison of passing rates using difference in sampling frequency.

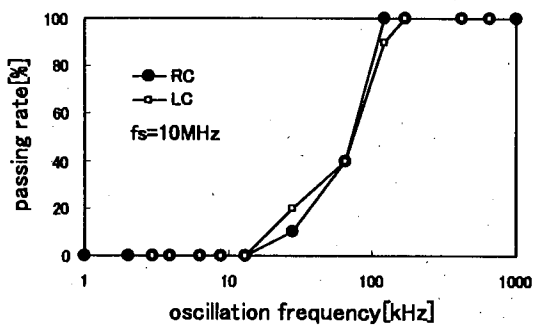


図 8　LC 発振回路と RC 発振器の比較

Fig. 8　Comparison of LC oscillation circuit and RC oscillator.

後，計算機に取り込むことによって乱数の生成実験を行った．このとき A–D 変換器の入力レンジを −5〜+5 V とし，RC 発振器の出力の波高値は A–D 変換器の入力レンジを超えない最大とした．サンプリング周波数 f_s はここで用いた A–D 変換器（PCI）の最高値である 10 MHz とし，RC 発振器の発振周波数を変化させたときの検定通過率を調べた．また，各発振周波数のデータ数が 10 組の場合と 100 組の場合とで比較を行った．結果を図 6 に示す．なお図 6 の横軸は発振周波数，縦軸は検定通過率を示す．

図 6 より，入力信号の発振周波数が約 100 kHz 以上であれば，ほぼ 100%検定を通過している．また，各発振周波数におけるデータ数 10 組と 100 組では，結果がほぼ一致しており，10 組でも十分傾向がとらえられる．よって，これ以後は各データ数を 10 組として測定を行った．

(b) サンプリング周波数と必要な入力信号の発振周波数の関係を調べるために，サンプリング周波数を 1 MHz とし，その他の条件は **4.1.1** (a) と同様として実験を行った．結果を図 7 に示す．なお，比較のために図 6 のサンプリング周波数 10 MHz の場合の値を併記した．

図 7 より，サンプリング周波数 1 MHz の場合，入力信号の発振周波数が約 10 kHz 以上でほぼ 100%検定を通過している．また，サンプリング周波数 10 MHz の場合が入力信号の発振周波数 100 kHz 以上必要であったことと比較すると，入力信号の発振周波数がサンプリング周波数の約 1/100 以上で乱数の生成が可能であることが分かる．

4.1.2　LC 発振回路による乱数生成

(a) 本論文で提案する方法が，異なる発振器についても適用できることを確認するために，LC 発振回路を用いて実験を行った．実際に用いた LC 発振回路を図 4 に示す．図 4 からの正弦波出力を，A–D 変換器（PCI）により A–D 変換後，計算機に取り込むことによって乱数の生成実験を行った．このとき A–D 変換器の入力レンジを −5〜+5 V とし，LC 発振回路の出力の波高値は A–D 変換器の入力レンジを超えない最大とした．サンプリング周波数はここで用いた A–D 変換器（PCI）の最高値である 10 MHz とし，LC 発振器の発振周波数を変化させたときの検定通過率を調べた．結果を図 8 に示す．なお，比較のために RC 発振器を用いた場合の結果を併記した．

図 8 より，LC 発振回路を用いた場合でも発振周波数約 100 kHz 以上でほぼ検定通過率が 100%になっていることが確認できた．RC 発振器を用いた場合の結果とほぼ一致した．

(b) RC 発振器の場合と同様の理由でサンプリング周波数を 1 MHz とし，その他の条件は **4.1.1** (a) と同様として実験を行った．結果を図 9 に示す．なお，比較のためにサンプリング周波数 10 MHz の場合の値を併記した．

図 9 より，サンプリング周波数 1 MHz の場合，発

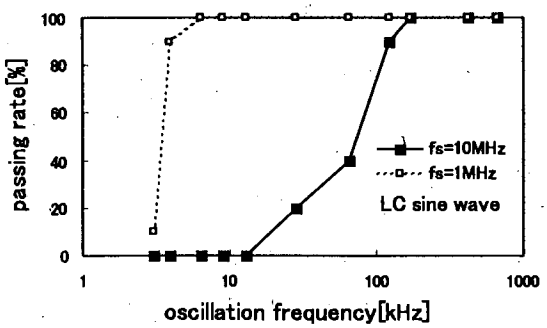


図 9 LC 発振回路の正弦波を用いた場合のサンプリング周波数による違い
Fig. 9 Comparison of passing rates using difference in sampling frequency for a LC sine wave.

振周波数が約 10 kHz 以上でほぼ 100%検定を通過している．また，サンプリング周波数 10 MHz の場合が発振周波数 100 kHz 以上必要であったことと比較すると，発振周波数がサンプリング周波数の約 1/100 以上で乱数の生成が可能であることが分かる．

4.1.3 A–D 変換器による違い

他の A–D 変換器でも本論文で提案する方法が利用できるか否かを調べるために，別の A–D 変換器を用いて実験を行った．**4.1.1** 及び **4.1.2** と同様の実験を，最高サンプリング周波数 10 MHz の A–D 変換器（PCI）と 1 MHz の A–D 変換器（AD12）を用いて行った．サンプリング周波数は AD12 の最高値である 1 MHz とした．結果を図 10 に示す．

図 10 より，RC 発振器，LC 発振回路の双方とも，PCI と AD12 での結果がほぼ一致した．

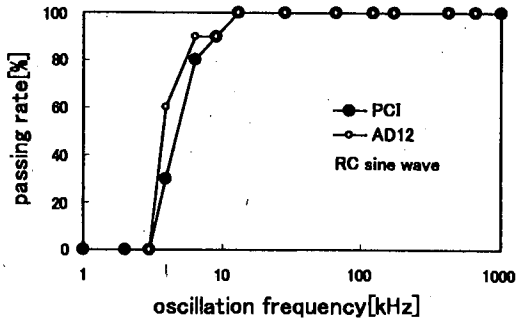
4.2 高域特性について

LC 発振回路を用いて，入力信号周波数の高域に対するシステムの特性を調べた．LC 発振回路からの高周波出力を，A–D 変換器（PCI 及び AD12）により A–D 変換後，計算機に取り込み乱数の生成実験を行った．このときの A–D 変換器の入力レンジと，LC 発振回路からの出力信号の波高値は **4.1** と同様とした．結果を図 11 に示す．

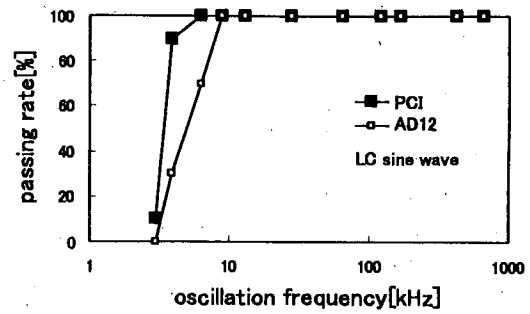
図 11 より，AD12 を用いた場合は発振周波数 10 MHz まで 100%検定を通過するのに対し，PCI を用いた場合は発振周波数 10 MHz 付近で検定通過率が急激に下降していることが分かる．

4.3 ショット雑音発生回路による乱数生成

3.2 で述べたシステムを用いて実験を行った．図 5 のショット雑音発生回路からの出力を A–D 変換器に取り込み，取り込んだデータの下位ビットから順に，$r_0, r_1, r_2, \cdots$ とした．これらのデータ列について，サンプリング周波数を変化させた場合の，サンプリング周波数と検定通過率の関係を図 12 に示す．なお図の見やすさを考慮し，図 12 には r_0 及びしきい値法の結果のみを示したが，実際には $r_1, r_2, \cdots, r_{11}$ についても実験を行った．各点には 10 組のデータ列を用いた．図 12 より，最下位ビット法を用いればサンプリング周波数約 1.25 MHz まで検定通過率 100%であるのに対して，しきい値法ではサンプリング周波数約 700 Hz 以下で検定通過率 100%となっていることが分かる．



(a) RC oscillator.



(b) LC oscillation circuit.

図 10 A–D 変換器の違いによる検定通過率の比較
(a) RC 発振器の場合，(b) LC 発振回路の場合
Fig. 10 Comparison of passing rates using difference in the A-D converters: (a) for a RC oscillator and (b) for a LC oscillation circuit.

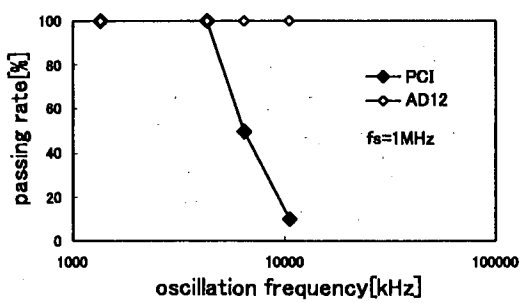


図 11 高域周波数特性
Fig. 11 Characteristics of high frequency region.

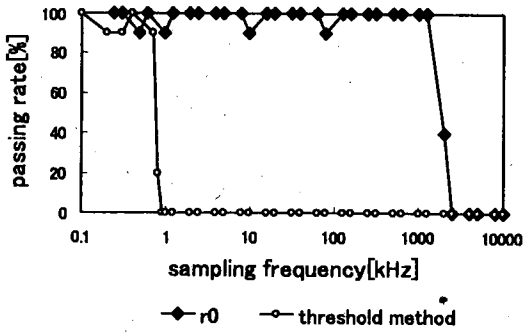


図 12　ショット雑音の場合の検定通過率
Fig. 12　Passing rates of random number test for a shot noise generator.

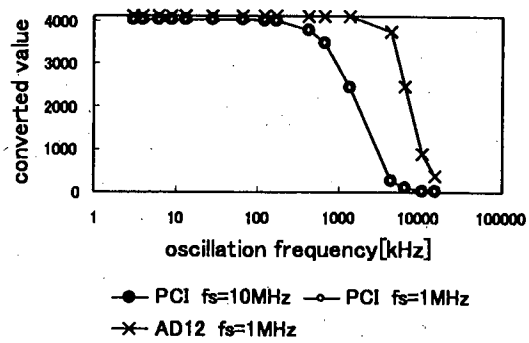


図 13　A–D 変換器の周波数特性
Fig. 13　Frequency characteristics of A-D converters.

5. 考　　察

まず，**2.** で述べた基本原理と実験結果を比較・考察する．**2.** の基本原理では，乱数生成の必要条件としてサンプリング周波数 10 MHz の場合には発振周波数 100 kHz 以上，サンプリング周波数 1 MHz の場合には発振周波数 10 kHz 以上の正弦波をシステムに入力することを述べた．これを RC 発振器を用いて検証した結果が図 7 である．図 7 の結果では，サンプリング周波数 10 MHz の場合，発振周波数 10 kHz 付近で検定通過率が上がり始め，100 kHz 付近で検定通過率が 100%になっており，それ以上の発振周波数で 100%のまま検定通過率を維持している．サンプリング周波数 1 MHz の場合は，発振周波数 10 kHz 以上で 100%のまま検定通過率を維持している．このことから，基本原理の必要条件と実験結果がほぼ一致したと考えられる．

次に，発振器の種類の違いについて考察する．LC 発振回路と RC 発振器の場合を比較した結果が図 8 である．図 8 の結果から，2 種類の発振器で結果がほぼ一致している．よって，本論文で提案するシステムはアナログ発振器を用いて乱数の生成が可能であるといえる．

A–D 変換器の違いについて考察する．PCI と AD12 を使用した場合を比較した結果が図 10 である．図 10 より，RC 発振器，LC 発振回路のどちらを使用した場合でも 2 種類の A–D 変換器で結果がほぼ一致したといえる．よって，本論文で提案するシステムはフラッシュ型の A–D 変換器の場合は，必要な信号が入力されれば乱数生成が可能であると考えられる．なお，A–D 変換器の基準発振器の安定度は約 4×10^{-8} [ゲート時間 10 秒の実測値，ルビジウム周波数標準発振器（EG&G 社製 RFS-10-102）を基準として使用]であり，入力信号の周波数安定度に比べると 250 倍程度安定であるので，本実験で用いたシステムの揺らぎは入力信号で決まると考えられる．

LC 発振回路の高周波信号を用いて行った **4.2** の実験結果（図 11）の，PCI の結果に注目すると発振周波数 10 MHz 付近で検定通過率が急激に下降している．この理由について考察する．図 11 の AD12 の結果は PCI とは異なり，発振周波数 10 MHz 付近まで検定通過率 100%を維持し続けている．これは，A–D 変換器の入力信号に対する周波数特性によるものと考えられる．PCI 及び AD12 の周波数特性を図 13 に示す．図 13 は，PCI 及び AD12 の入力レンジを −5〜+5 V の範囲とし，入力信号の振幅も −5〜+5 V とした場合の，発振周波数を変化させたときの A–D 変換後の値を表示したものである．図 13 から，入力信号の周波数がある一定値以上になると A–D 変換器の周波数特性が悪くなる傾向があることが分かる．特に，PCI ではサンプリング周波数 1 MHz を超えると周波数特性が悪くなっている．入力信号が減衰され，収集されたデータ値が小さくなると最下位ビットを用いても揺らぎの影響が現れ難くなる．**4.2** で述べた実験結果（図 11）の，PCI と AD12 の違いはこの周波数特性の差から生じるものと考えられる．**2.** の乱数生成の基本原理で述べた必要周波数は下限のみを考慮しているが，乱数生成のための上限はこの A–D 変換器の周波数特性で決まるといえる．

次に，ショット雑音発生回路を用いた実験について考察する．この実験は本論文で提案する方法の妥当性，すなわち長いビット長での高速乱数生成の有効性を示すために行ったものである．ショット雑音は白色雑音であるから，ショット雑音発生回路の出力も，白色雑音ですべての周波数帯域を含んでいることが理想であ

る．しかし，実際はアナログ増幅回路を用いているので，ショット雑音の一部の周波数成分（利得帯域幅積で決まる周波数帯域：約 1 kHz）しか含まれていない．従来のしきい値法では，このような限られた周波数帯域においては，乱数の高速生成を行うことは困難であった．図 12 で比較すると，従来のしきい値法を用いた場合はサンプリング周波数が約 700 Hz まで検定通過率が 100%であるのに対し，最下位ビットを使用すればサンプリング周波数は約 1.25 MHz まで検定通過率が 100%になっている．つまり，本論文で提案した最下位ビットを使用することで，約 1,800 倍高速化している．このことから，雑音の周波数成分が低い場合でも高速乱数生成が可能であるといえる．図示していないが測定の結果では $r_{11}, r_{10}, \cdots, r_1, r_0$ と，ビット長が長いほど高いサンプリング周波数まで検定通過データを取得できている．

本論文で提案するシステムは，発振器より出力される信号の周波数の揺らぎを用いて乱数を生成するものである．この入力信号の揺らぎの性質と，出力される乱数の性質の関係について考察する．入力信号の揺らぎの性質を図 14 に示す．図 14 は RC 発振器について発振周波数 200 kHz，サンプリング周波数 10 MHz とした場合のデータ 20,000 個の値を，計算機で生成した理論的な正弦波との差の分布を表したものである．なお，ここで用いた理論的な正弦波は $2047 + 1955.5\sin(2\pi \times 200011.1 \times t - 0.019)$ とした．この式は，実測値と理論値との残差平方和が最小になるように各パラメータを定めたものである．この図 14 から，分布はほぼ $\sigma = 3.1$ の正規分布をとるものとみなせる．次に，出力される乱数の性質を図 15 に示す．図 15 は，RC 発振器より取得したデータ 5,000 組を使用し，FIPS140-2 におけるモノビットテスト及びポーカーテストの二つの検定を行った結果である．図 15 (a) より，生成したデータの 1 の個数はすべて，モノビットテストの規格である $9{,}725 < x < 10{,}275$ の範囲を満たしていることが分かる．図 15 (b) は，ポーカーテストの実測と理論分布の適合度の検定を行った結果である．χ^2 検定の計算結果は 20.35 となり，有意水準 5%の棄却域 $\chi^2 > 48.57$ に含まれない．したがって有意水準 5%で理論分布との有意差は見られない．以上のことより，本システムは正規分布をとる揺らぎの性質を有する入力信号を FIPS140-2 の検定を合格する暗号用乱数に変換するシステムであると言い換えることができると考える．

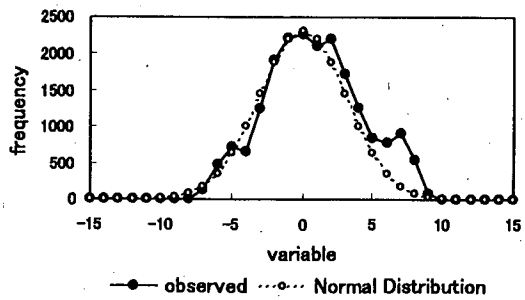
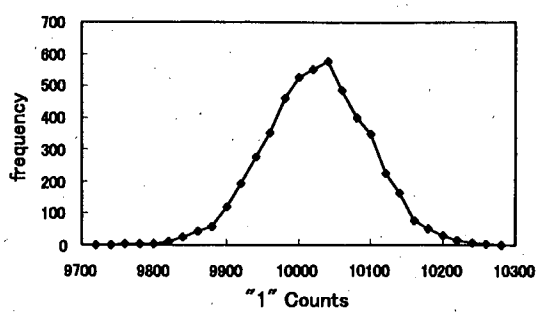
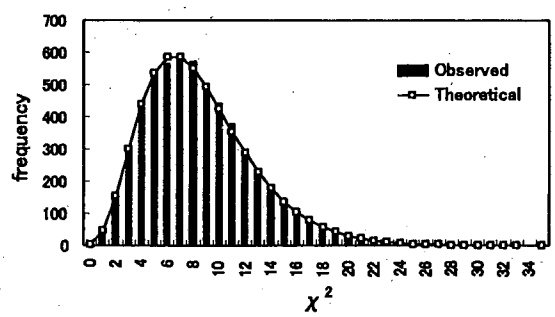


図 14　入力信号の揺らぎの性質
Fig. 14　Characteristic of fluctuation.



(a) Monobit test.



(b) Poker test.

図 15　FIPS140-2 (a) モノビットテスト (b) ポーカーテスト
Fig. 15　FIPS140-2. (a) Monobit test. (b) Poker test.

エイリアシングについて検討する．本論文ではすべての実験を通して A–D 変換器のサンプリング周波数が発振周波数を下回る部分があり，エイリアシングが生じている．しかし，本論文で提案する方法は，エイリアシングの生じないサンプリング周波数の 1/100 程度の入力信号から検定通過データが取得可能であり，発振周波数の上限は A–D 変換器の周波数特性によって決まる．このことから，乱数生成にはエイリアシングは影響していないと考えられる．

本論文で提案するシステムは 10 MHz のサンプリング周波数でのデータ収集が可能であり，10 Mbits/s で乱数を生成している．従来の方法と比較すると 40 倍の高速化が実現できた．算術乱数発生方法に比べれば

現時点では乱数生成速度は遅いが，高速の A–D 変換器 [10] も実現されてきており，より高速な乱数生成が可能となると考える．

6. むすび

本論文では，正弦波発振器の出力を直接 A–D 変換し，そのデータの最下位ビットを使用することで乱数の高速生成が可能であることを示した．本論文で提案する方法を利用すれば，雑音発生回路など特殊な回路を用いずに乱数の生成が可能である．正弦波を用いた場合乱数の生成速度は，ほぼ基本原理の必要条件の計算と一致した．また，フラッシュ型であれば A–D 変換器の違いによらず安定した乱数生成が可能であることを確認した．更に，ショット雑音発生回路からの出力により乱数を生成し，最下位ビット法としきい値法による乱数生成速度の比較を行った結果，最下位ビット法では，サンプリング周波数をしきい値法を用いた場合の約 1,800 倍まで高くできることを確認した．A–D 変換器のビット長を n とすると，1,800 倍はほぼ 2 の $(n-1)$ 乗に相当する．

謝辞 本研究を進めるにあたり，実験を実施した前川治子君，大塚拓也君に謝意を表す．

文　献

[1] 池野信一，小山謙二，現代暗号理論，電子情報通信学会，1986.
[2] D.R. Stinson，櫻井幸一（監訳），暗号理論の基礎，共立出版，1996.
[3] 宮武　修，脇本和昌，乱数とモンテカルロ法，森北出版，1978.
[4] 斉藤義明，堀　潤一，木竜　徹，“ショット雑音で周波数変調した LC 発振回路による物理乱数発生法，” 信学論（A），vol.J87-A, no.7, pp.930–937, July 2004.
[5] M.E. Yalcin, J.A.K. Suykens, and J. Vandewalle, “True random bit generation from a double-scroll attractor,” IEEE Trans. Circuits Syst. I, Fundam. Theory Appl., vol.51, no.7, pp.1395–1404, July 2004.
[6] 斉藤義明，堀　潤一，西村浩志，木竜　徹，“可変容量パラメトロンによる物理的乱数発生法，” 信学論（A），vol.J85-A, no.2, pp.181–188, Feb. 2002.
[7] National Institute of Standards and Technology, “Security requirements for cryptographic modules,” FIPS 140–2, 2001.
[8] 山本博康，清水隆邦，“CMOS 素子を用いた高速物理乱数発生器—高速性と汎用性の両立，” 信学技報，NLP2003-36, July 2003.
[9] 岡本栄司，暗号理論入門，第 2 版，共立出版，2002.
[10] O.A. Mukhanov, D. Gupta, A.M. Kadin, and V.K. Stemenov, “Superconductor analog-to-digital converters,” Proc. IEEE, vol.92, no.10, pp.1564–1584, Oct. 2004.

（平成 16 年 10 月 21 日受付，12 月 29 日再受付，17 年 1 月 31 日最終原稿受付）

茂呂　友子　（学生員）

2004 新潟大・工卒．現在，同大大学院自然科学研究科博士前期課程在学中．

斉藤　義明　（正員）

1965 北海道大学大学院工学研究科修士課程了．1970 工博．1965 から新潟大学工学部勤務，現在，同学部福祉人間工学科教授．生体情報，医療情報の収集，解析装置，治療装置の開発研究に従事．IEEE シニアメンバ，日本エム・イー学会，日本ハイパーサーミア学会，情報処理学会各会員．

堀　潤一　（正員）

1986 新潟大・工卒．1988 同大大学院工学研究科修士課程了．同年新潟大学工学部助手．現在，同大学工学部福祉人間工学科助教授．博士（工学）．1999～2000 イリノイ大学シカゴ校客員研究員．高精度生体計測，生体信号・医療画像の復元，脳機能解析と逆問題の研究に従事．IEEE，日本エム・イー学会，日本ハイパーサーミア学会，日本生活支援工学会各会員．

木竜　徹　（正員）

昭 50 新潟大・工・電子卒．昭 52 同大大学院修士課程了．昭 61 同大助教授，平 7 同大大学院教授，平 8 筑波大学 TARA センター客員研究員，現在に至る．工博．非定常生体信号処理を目的とし，非定常性の特徴分類，時変性パラメータ推定等研究に従事．最近では，動的筋活動の解析を進めている．日本エム・イー学会評議員，バイオメカニズム学会，IEEE 各会員．