日本統計学会誌
第35巻，第2号，2006年3月
201頁～212頁

日本における物理乱数発生装置の現状

田村義保*，小野寺　徹†，中畑昌也‡，清水隆邦§

On Physical Number Generators in Japan

Yoshiyasu Tamura*, Onodera Toru†, Masaya Nakahata‡, Shimizu Takakuni§

乱数は科学の研究には不可欠なものである．計算が大規模になっているために，周期の長い乱数が要求されている．メルセンヌ・ツイスタのような周期性だけでなく一様性も優れた擬似乱数発生法が提案されている．しかしながら，数式を用いて発生させられている以上，真の乱数ということはできない．本論文においては，日本で現在市販されている物理乱数発生装置の発生原理を詳解している．物理乱数こそ真の乱数と呼ぶにふさわしいものであると考える．

For most of scientific studies, random numbers are indispensable. Recently many scientists need large amount of computations and so pseudo random number generators of which periods must be sufficiently long are desirable. Indeed recently a new pseudo random number generator, which is called Mersenne Twister, was proposed. Its period is too long and random number sequence generated with this method has superior statistical properties. But its random number sequence cannot be regarded as "truly random number", because it is generated with numerical expressions. In this article, physical random number generators, which can be now obtained in Japan, are explained in detail. We think that random number sequence with physical random number generators can only be regarded as "truly random number".
Key Words and Phrases: pseudo random number, physical random number

1. はじめに

乱数（random number）は確率モデル（システム）のシミュレーションには欠くべからざるものである．統計科学の分野ではシミュレーションだけでなく，MCMC（マルコフ連鎖モンテカルロ法）や粒子フィルタ（モンテカルロフィルタ）などのためにも乱数が用いられている．大規模計算が必要な解析，シミュレーションが増えているために，1回の計算で使用される乱数の個数が，乗算合同法のような簡単な手法を用いたりすると，その周期分以上になる場合が多くなっており，周期性が解に思わぬ副作用を与えることがありうることに十分に注意しておく必要がある．Matsumoto-Nishimura（1998）により，通常の応用に対しては周期（$2^{19937}-1$）をが事実上，無限大と考えてもよくかつ高次元空間における一様性も優れたメルセンヌ・ツイスタが提案され，多くの研究で用いられている．

* 〒106-8569 東京都港区南麻布4-6-7　統計数理研究所
† 〒235-8523 神奈川県横浜市磯子区新杉田町8　株式会社東芝
‡ 〒259-1304 神奈川県秦野市堀山下1　株式会社日立製作所
§ 〒972-8322 福島県いわき市常磐上湯長谷町釜の前1　FDK株式会社

しかしながら，ある数学的規則で計算されている以上，いくら優れているとは言え，真性乱数と呼ぶことはできない．物理現象を利用して発生させる，いわゆる物理乱数（石田等（1972），仁木（1980，1983），岸本-福江（1999））こそが，真性乱数と呼ばれる可能性があると考える．特許庁ホームページ（http://www.ipdl.ncipi.go.jp/）において，発明の名称に「乱数」を含むものを検索すると平成6年から平成17年の間に91件の特許が取られていることが分かる．キーワードを「物理乱数」とすると4件となるが，物理乱数についての特許でも，発明の名称に「物理」という用語を含んでいないものあり，田村が特許内容を精査した結果においては，上記の期間中に物理乱数に関係した10件の特許が認められていることが判明した．これらの中で，製品化されており，入手可能な3社の物理乱数発生装置についての仕様を本稿において解説している．解説は，各社で開発に携わった方々に執筆していただいている．その関係上，各章で説明の程度が異なったり，説明が重複したりしているが，御容赦いただければ幸いである．2節から4節に示した3社の説明により，「物理乱数」の発生方法の理解が深まれば幸いである．なお，本稿の3種の発生装置の「乱数源」は電気回路の熱雑音である．他に雑音源としては，放射線同位元素（石田正次（1956）），光子（末松等（2005））があることを述べておく．

2. ランダムマスター™における物理乱数発生法

2.1. 基本原理

ランダムマスター™においては，ツェナーダイオードの出力信号から得られるゆらぎ成分をノイズ源とし，品質の良い物理乱数を高速に生成している．ツェナーダイオードのゆらぎ成分を増幅した後，12-bit/66 M-SPS（Sample Per Sec）のADC（Analog to Digital Converter）を用いてゆらぎ成分をディジタル値に変換，変換したディジタル値の下位4ビットを用いて4系列の二値乱数列を生成している．1回のAD変換で複数の二値乱数を生成するため高速に乱数を生成していることがランダムマスター™の特徴である．しかし，使用する回路構成や素子の特性により一様性が低下する可能性がある．これを，補正し，一様性を改善している．この結果，1つのノイズ源から，品質の良い物理乱数を約167 M-byte/secという高速で生成することを可能にしている．

2.2. 乱数の必要性

乱数は，ゲーム機，暗号通信，計算機シミュレーションなどさまざまな分野で利用されている．特に，統計科学分野における大規模な計算機シミュレーションでは大量の乱数が使用されている．

計算機では擬似乱数が一般に用いられているが，大量の乱数を使用する場合は，周期性，再現性が課題となる．また，最近の大型な計算機には複数のCPUが搭載されることが多く，1CPUの場合よりも周期性や再現性が問題になる可能性が高い．この対策として，使用する乱数系列の周期性や再現性を確認した上で品質が良い乱数系列のみを利用することが挙げられるが，この検定には膨大な時間が必要であり，現実的ではない．

これに対し，物理乱数は原理的に周期性や再現性を持たないため，大量の乱数を使用する場合に膨大な時間を掛けて確認する必要はない．また，周期性や再現性を改善した擬似乱数を生成するアルゴリズムは，CPUやメモリなどの計算機のリソースを多く消費する傾向にあるが，物理乱数の生成は専用のハードウェアが行うため，計算機のリソースを消費しない．

したがって，物理乱数を使用することにより，周期性や再現性の確認に要する時間の短縮，計算を実行するときの計算機リソースの効率向上が期待でき，今後の利用が高まると予想される．

ここでは，ツェナーダイオードの出力信号のゆらぎ成分を用いて品質の良い物理乱数を高速

に生成する方法について述べる．

2.3. 物理乱数の生成方法

図1に物理乱数生成回路の内部構成を示す．

図1　物理乱数生成回路の内部校正

物理乱数を生成する元になるノイズ源として，ツェナーダイオードの出力信号に含まれるゆらぎ成分を用いている．このゆらぎ成分は数μVrms程度であるため，増幅器を用いてADC（Analog to Digital Converter）の変換範囲まで増幅し，ディジタル値に変換している．ディジタル値の下位ビットは二値乱数ではあるが，ツェナーダイオードのゆらぎ成分，増幅器，ADCの特性の影響で完全な一様性は得られない．そこで，補正回路を用いて完全な一様性に近づける処理を行った後に物理乱数として取り出している．取り出した物理乱数は，PCIバスを経由して計算機に出力する．

2.4. 高速化とその課題

高速な物理乱数を生成するためには，1つのノイズ源からより多くの二値乱数列を高速に取り出せることが望ましい．そこで，アナログ回路の周波数帯域とPCIバスのクロック周波数を考慮して，12-bit/66 M-SPS（Sample Per Sec）の高速・高精度なADCを用い，ADCが出力したディジタル値の下位から4ビットを二値乱数として取り出すことを検討した．この場合の課題は，下位4ビットを乱数として取り出すことの妥当性，高速なADCのDNL（Differential Non Linearity：微分非直線性），取り出した二値乱数列間の相関である．

乱数として取り出すことができるビットは，ゆらぎ成分の振幅とそのビットの変換精度により決まる．変換範囲が1Vp-pで12-bit精度のADCの下位から4ビット目は，約2 mVの変換精度であるから，2 mVp-pよりも充分に大きなゆらぎ成分をADCの入力に加えることで，下位4ビットはいずれも乱数として利用可能である．

市販の高速ADCのDNLは$\pm$0.5LSB（Least Significant Bit）程度であり，LSB（最下位ビット）を二値乱数に用いた場合の“1”の発生確率は目標値50%に対して25〜75%である．実際には，上位ビットが異なる組み合わせでLSBを用いるため，一様性は50$\pm$0.1%程度まで向上するが，計算機で乱数を使う場合に要求される精度を考慮するとまだ不十分である．

AD変換には様々な方法があるが，高速なAD変換に用いられる逐次比較型ADCの変換結果は原理的にビット間の相関が生じるため，生成した4ビットの二値乱数は独立な乱数として扱うことができない．

ADCのDNLとビット間の相関については，個々の対策は行わず，後で述べる一様性の補正手段により解決した．

2.5. 一様性の向上

計算機で要求される乱数の一様性の目安は，単精度浮動小数点型の演算では数桁（23-bit），倍精度浮動小数点型の演算では十数桁（51-bit）の演算精度を考慮して決める必要がある．

物理乱数は，原理的に周期性や再現性がなく，擬似乱数よりも真性乱数に近い乱数を生成できると期待されるものであるが，理想的なノイズ源を採用したとしても，現実には回路構成や素子の特性が一様性に影響するので，何らかの対策が必要である．

ADCが変換したデータ速度を低下させずに一様性を向上させる方法として，論理反転による補正手法がある．たとえば，二値乱数を1 msecの間正論理で出力し，その後の1 msecの間

表1 ADCの変換値と補正値との排他論理和

			補正値			
			0	1	2	3
	変換値	確率	ϕ	ϕ	ϕ	ϕ
ADC	0	ρ_0	$\rho_0 \cdot \phi$	$\rho_0 \cdot \phi$	$\rho_0 \cdot \phi$	$\rho_0 \cdot \phi$
			0	1	2	3
	1	ρ_1	$\rho_1 \cdot \phi$	$\rho_1 \cdot \phi$	$\rho_1 \cdot \phi$	$\rho_1 \cdot \phi$
			1	0	3	2
	2	ρ_2	$\rho_2 \cdot \phi$	$\rho_2 \cdot \phi$	$\rho_2 \cdot \phi$	$\rho_2 \cdot \phi$
			2	3	0	1
	3	ρ_3	$\rho_3 \cdot \phi$	$\rho_3 \cdot \phi$	$\rho_3 \cdot \phi$	$\rho_3 \cdot \phi$
			3	2	1	0

負論理で出力することにより，2 msecの平均で見た場合に“0”または“1”の発生頻度は50%とする方法である．

この方法を多ビットの場合に適用することで，高品質な物理乱数を高速に生成することができるようになる．原理を説明するために，ADCの下位2ビットを補正する場合について述べる．

ADCが下位2ビットの変換値として0〜3を出力し，その確率をρ_0〜ρ_3とする．発生の確率ϕが等しい補正値0〜3を生成し，ADCの出力との排他論理和を求める．表1にADCの変換値と補正値との排他論理和をおこなったときの生成確率（上段）と補正後の値（下段）を示す．たとえば，補正後の値が0となるのは，表1の対角線上に4箇所並んでいて，その4箇所の確率をすべて合計するとϕ（=25%）となる．他の補正後の値も確率はすべて25%であるから，この方法により，ADCの変換値がどのような確率であっても補正後の二値乱数は必ず25%の確率に落ち着く．説明の都合上，2ビットの場合について述べたが，ADCの変換値の下位4ビットについても同様である．

この補正方法は，一様性の改善手法であるが，2.1で述べた2つの課題（ADCのDNL，系列間の相関）のいずれに対しても有効に作用する．また，ADCの変換値の確率ρ_0〜ρ_3に変動がなければ補正後の二値乱数の一様性は向上し続ける．

2.6. 今後の発展

ツェナーダイオードの出力信号から得られるゆらぎ成分をノイズ源とし，品質の良い物理乱数を高速に生成する方法について説明した．回路構成や回路素子の影響があっても，適当な補正方法を採用することにより，高品質な物理乱数の生成が可能である．

66 MSPSのADCを使用し，2回のAD変換で8系列の二値乱数を生成することができるため，図1に示す構成で物理乱数の生成速度は33 M-byte/secである．ただし，上記補正手法だけでは短時間の品質が充分ではないことを考慮し，最初にADCの出力データを加算している．そのため，1つのノイズ源から得られる物理乱数の生成速度は約16.7 M-byte/secとなる．データ幅が64-bitのPCIバスの場合，図1に示す構成の回路を8回路ボードに搭載，特性の良いADCを採用することで加算を省略し，266 M-byte/secの物理乱数を計算機に対して供給することも可能である．

AD変換素子は，専業メーカが改良を進めており，16-bit/100 MSPSのADCが開発されてい

る．これまでは，主に 12-bit の ADC を使用して来たが，16-bit の ADC に置き換えることで，1回の AD 変換で1バイトの物理乱数を生成できるようになる．物理乱数の生成速度は，今後，さらに向上する余地がある．

3. 日立製作所製乱数発生器

3.1. 発生原理

本「物理乱数発生器」は，乱数発生源に従来から有効な熱雑音源として知られるツェナーダイオード（ZD）を使用する．そこから得られる出力電位をアナログ・デジタル・コンバータ（ADC）により量子化し，特定のビットをシリアル・パラレル変換（S—P）する一般的な方法により乱数を生成する（図2）．

図3に本「物理乱数発生器」で採用したダイオードのノイズ波形，図4にその周波数スペクトルを示す．乱数を生成するためには，雑音源からの信号がホワイトノイズである必要があるが，本ダイオードは 2 GHz（測定範囲内）まで，ほぼフラットな出力特性を持つことから，その性質を備える．

本「物理乱数発生器」では，雑音源からの信号を増幅し，100 MHz でサンプリングして乱数データを生成する．図3からサンプリング間隔内で十分な変動が確認でき，その電位についてもサンプリング毎に不確定であるといえる．

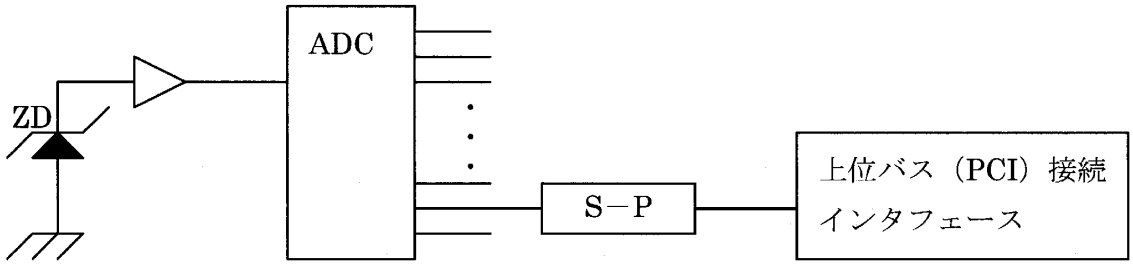


図2　物理乱数発生器の概要

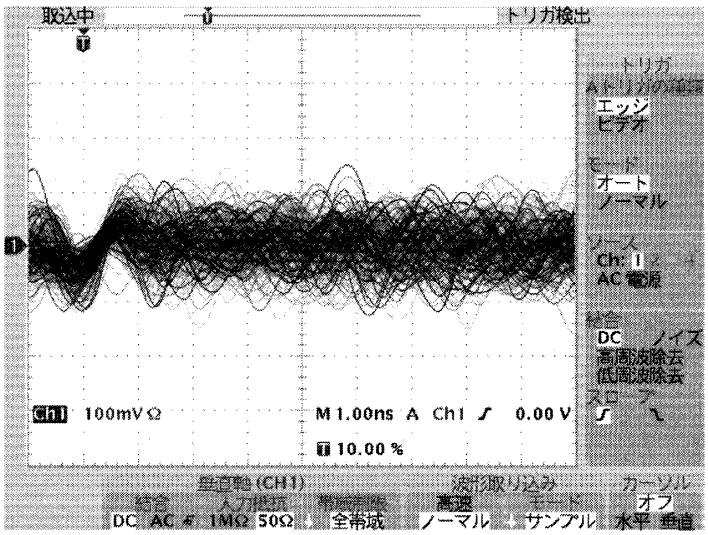


図3　ノイズ波形

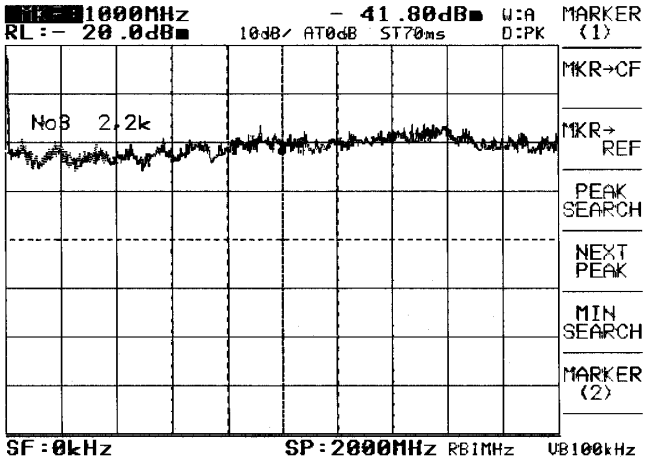


図4 周波数スペクトル

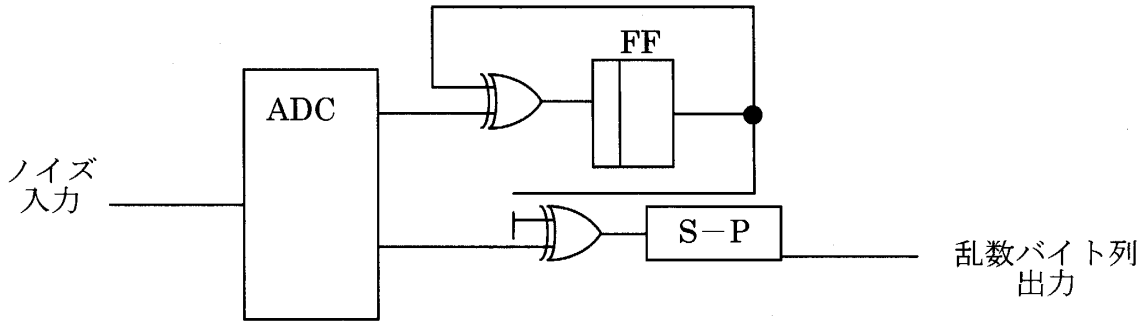


図5 積算反転とシリアル・パラレル変換

3.2. 特　　徴

本「物理乱数発生器」では，ADCによる量子化の際に生じた0と1の出現率の偏りを，論理回路により均一化する．その手段として，「特開2000—298577」に公開された積算反転方式を回路として実装した．積算反転方式は，あるビット列を，毎サイクル排他論理和で積算することで0と1の出現率が各50%である信号を作り，これによって他のビット列を反転／非反転させるものである．これを，シリアル・パラレル変換して乱数バイト列を発生する（図5）．

単一のノイズ源の出力を100 MHzでサンプリングした12ビットのADCの出力から，4ビットを乱数源として使用し，それぞれをS—P変換して4並列の乱数バイト列を発生する．この4並列の出力を，別ビットから生成した乱数により毎回並べ替えて4バイトデータとし，規則性および連続性を持たせないものとした．

本「物理乱数発生器」では，上記構成を4個並列で動作させる．4つの4バイトデータの出力順序を，再度乱数により入れ替えることで，固定したノイズ源からのデータがあるビットに定常的，周期的に出力されない構成とした．

3.3. 性　　能

本「物理乱数発生器」は，前述のように1つの発生源から4ビットの乱数列を生成する．これを1構成として4個並列構成として，合計で16ビットの乱数を1クロックで生成するため，200 MB/Sec（1 M＝10^6）の理論性能を持つ．

ただし，ADCに入力されるノイズ電位は，瞬間的にADCの変換範囲を外れ，正常な変換値を得られないことがある．これは，乱数の一様性に影響することから，変換範囲を外れた場合

は出力乱数から除外している．このため，実際の発生速度は 200 MB/Sec に僅かに及ばない．

上位インタフェースには，64 bit 幅の PCI バス（バスクロック：66 MHz）を採用し，データ伝送帯域として 533 MB/Sec を確保した．これにより，発生データをバッファオーバ等で失うことなく上位メモリ空間へ転送することが可能である．

4. 物理乱数生成 IC RPG100

4.1. はじめに

物理乱数は擬似乱数（Knuth（1997），渋谷(1981)，伏見（1989））のような周期性や再現性などは無く，無作為に選ばれる数列である真正乱数が持つべき性質を備えている．それゆえに貴重な存在として認められつつあるが，コストが高く付き，まだ気軽に導入できるものであるとは言えない状況である．また，乱数発生器として形状が大きいと，小型製品への応用ができなくなり市場を広げることが難しくなる．とくにセキュリティ製品は小型のものが多いので，物理乱数発生器が大きいのはデメリットとなる．

我々は，これらの問題を改善するため，「小型」で「低価格」の物理乱数生成 IC を開発した．また，この IC を利用し，物理乱数を簡単にパソコンに取り込めるよう，USB モジュールも提供している．

4.2. 物理乱数生成 IC RPG100 の構成と原理

「小型」で「低価格」を実現するため，ワンチップ IC として物理乱数生成 IC RPG100 を開発した（写真 1，RPG100：9.0×9.0×1.5，RPG100B：5.0×5.0×0.8）．このチップの内部回路は，すべてが CMOS で構成されている．

4.2.1. RPG100 の基本的な構成

RPG100 は，図 6 のようにシンプルな構成をとっている．

a）ノイズ源（Noise Source）

乱数生成の基となるノイズは，CMOS に微小電流を流したときに発生するものを利用している．発生したノイズはいく段かのアンプによって増幅される．

b）CR 積分回路（CR Integration Circuit）

抵抗とコンデンサによる積分回路であり，乱数生成信号の遅延時間分布を広げるように波形整形する．

c）ミキサー（Mixer）

乱数生成の基準となる乱数生成信号とノイズ源からのランダムな電圧変動をミキシングする．

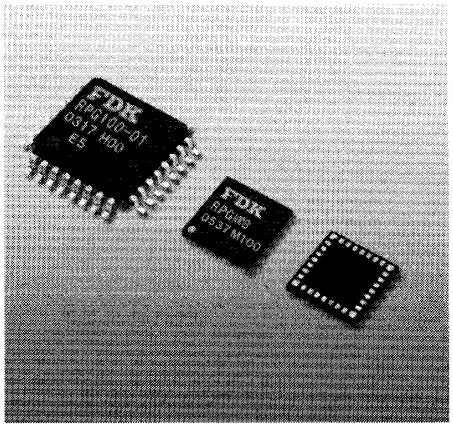


写真 1　物理乱数生成 IC RPG100，RPG100B

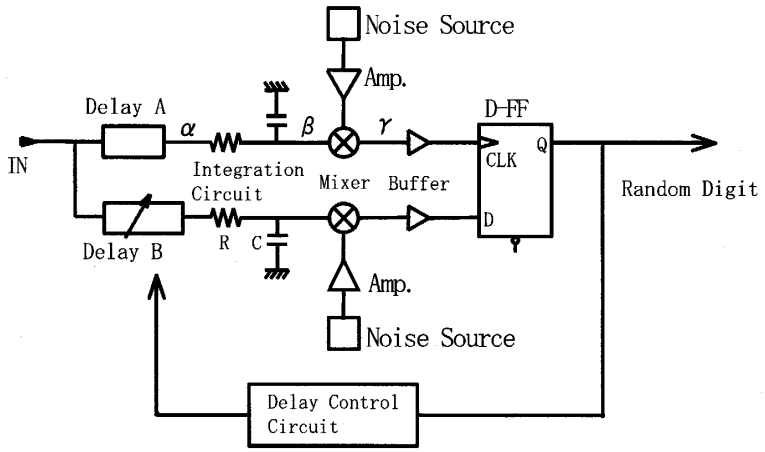


図6 乱数生成の基本構成

これにより，乱数生成クロックからの遅延時間がランダムに揺らぐようになる．

d）ディレー（Delay）

2つのDelayのうち，片方は可変できるものである．常に良い状態で乱数生成ができるように，自動的に調整される．

e）Dタイプーフリップフロップ（D-FF）

ノイズをミキシングした2つの乱数生成信号のうち，どちらが先に来たのかによって，“1”または“0”を出力する．

4.2.2. 乱数が生成されるまでの流れ

乱数の生成は，図6のINから入力する乱数生成クロックが基準となり，2つの乱数生成信号として分岐され，後段のDelay AとBによって遅延される．その後，乱数生成信号は積分回路を通って緩やかな波形に整形され，ミキサーによってノイズとミキシングされる．ここで，Delay，積分回路，およびミキサー通過後のポイント（図6のα，β，γ）の波形を図7に示す．Delayを通過した直後の乱数生成信号は，波形αのように急激な立ち上がりを持つ矩形波となっているが，その後の積分回路を通ることにより，波形βのようにゆっくりと立ち上がる．

ミキサーでは，波形βが立ち上がる途中に，波形γとして信号が伝わるタイミングを決めるしきい電圧がノイズ電圧に応じて常に変動するようになっている．したがって，ノイズによって引き起こされるランダムなしきい電圧の変動は，γにおける乱数生成信号の遅延時間を変動させる．また，波形βの立ち上がりが緩やかであるほど，その遅延時間の変動幅は大きくなる．積分回路による波形整形は，遅延時間の変動幅を適切な値に広げるためのものである．点γにおけるの乱数生成信号の，乱数生成クロックに対する遅延時間分布はグラフ1の通りである．

乱数は図6のD-FFから出力されるが，乱数値として“0”なのか“1”なのかは，乱数生

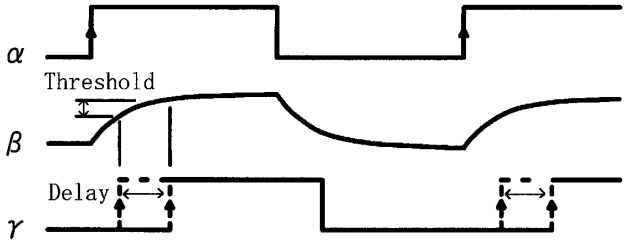
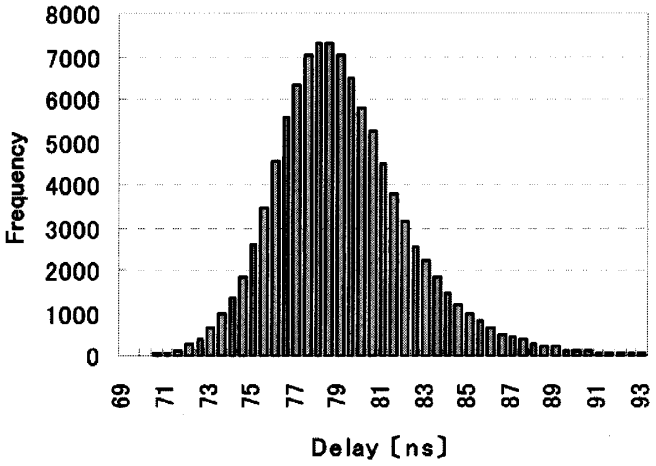


図7 ノイズのミキシングと信号のタイミング



グラフ1　乱数生成信号の遅延時間分布

成クロックから分岐された2つの乱数生成信号のうち，どちらが先にD-FFに到達するかで決まる．D-FFに入力される2つの乱数生成信号は，グラフ1の分布をもって独立に変動するので，出力はランダムとなる．

なお，良質の乱数を生成するためには，2つの乱数生成信号の遅延時間平均が一致していることが望まれる．固定Delay Aと可変Delay Bは，この遅延時間を調節するために設けられており，可変Delay Bによる遅延はコントロール回路によって自動調整が行われている．

4.2.3. 高品質の乱数生成に関わる仕組み

a）外来ノイズの影響を打ち消す構造

乱数の生成は，乱数生成クロックを基準としている．同じ乱数生成クロックに対して，独立した2つのノイズを合成し，それらの差分を乱数生成に用いているため，電源などに乗った不要なノイズの影響は相殺される．さらに，ノイズ源に要求されるノイズの条件は，乱数生成クロックより高い周波数帯域であればよいというだけで，その種類は問われない．ホワイトノイズであっても1/fノイズであっても問題なく乱数を生成することができる．

b）Delay Control Circuit

乱数値は，分岐させた乱数生成クロックがD-FFに到達する時間差で決まるが，製造誤差，温度および電圧変動などにより，乱数生成クロックの片側だけ早く到達する割合が多いなどの偏りが生じ，良好な乱数生成ができなくなることが考えられる．この問題の対策として，分岐させたそれぞれの乱数生成クロックの経路にDelayを設け，その片方を可変Delayにして遅延時間を調節する方法をとっている（図7）．Delayの調節は，D-FFからの乱数をカウントして，“0”が多ければそれが少なくなる方向に，少なければ増やす方向にDelay時間を変化させることで行う．そして，Delay調節周期は，自ら出力する乱数でランダムに決定される．これは，定期的なDelayの調節による周期的な影響が乱数に及ぶことを防ぐためである．

このように，逐次最適なポイントにDelayを調節することで，製造誤差，電源電圧や温度の変動に影響されず良質の乱数を生成できるようになる．

c）乱数の一様化

この方式の乱数生成において核となっているのは，半導体のノイズという不安定なアナログ要素である．そのため，瞬間的に上記の方法で対応しきれない大きな環境変化の影響を受けることも想定され，突然乱数らしくない出力をしてしまうことも考えられる．このようなことが起こらないよう，安定して良質の乱数を出力するために，乱数の一様化を図る回路が設けられ

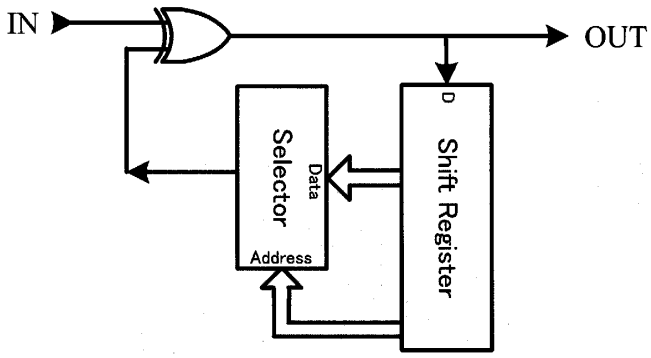


図8 乱数一様化回路

ている．一様化回路の構成を図8に示す．乱数はシフトレジスタに順次シフトしながら格納され，各ビットはセレクタの入力とアドレスに割り当てられる．したがって，シフトレジスタに蓄えられている乱数値によって，同じくシフトレジスタに蓄えられている乱数がランダムに選択される．選択された乱数は新しい乱数と排他的論理和が取られ，出力される．一様化には乱数テーブルなどとの合成は行わず，あくまで自身の乱数によってのみ乱数の攪拌を行うよう構成されている．

4.3. RPG100の仕様

これまで述べてきたように，RPG100はできるだけ外部の影響を受けないように工夫されているが，これは乱数の生成スピードを落とさない条件でもある．これにより，RPG100の乱数生成スピードは，物理乱数生成ICとして高速な250 Kbit/secを実現している．乱数は外部から入力する乱数生成クロックに同期して生成されるが，その取り出し方は，1 bitのシリアルで出力する方法と，16 bitのパラレルで出力する2つの方法がある．パラレル出力の場合は，RPG100の内部に設けられた32段の16 bitレジスタに乱数が蓄えられる仕組みになっており，乱数を使用していない時に貯めておき，必要な時に高速に取り出すことができる．なお，乱数生成の必要がないときには，パワーセーブモードによって省電力化を図ることもできる．

また，RPG100は生成した乱数を検定する機能も持っており，必要時に乱数の質を確認することができる．乱数検定の仕様は，米国の暗号モジュール標準であるFIPS140-2（Change Notice 1）に基づいている（Evans et al.（2001））．

RPG100の仕様を表1に示す．

4.4. 物理乱数生成USBモジュール

物理乱数を簡単にパソコンに取り込めるよう，RPG100を搭載したUSBモジュールが

表1 RPG100仕様

乱数生成クロック	250 K Hz
シリアル出力	乱数生成クロックに同期
パラレル出力	16bit
電源電圧	+3.0 ～ 3.6 V
電源電流	通常時 Typ. 2.30 mA
	パワーセーブ Typ. 1 μA
動作温度	−40 ～ 85 ℃
乱数自己検定機能	FIPS140-2 (Change Notice 1)

表 2　Random Streamer RPG102 仕様

対応機種	純正 USBポートを持つ IBM PC/AT 互換機
対応OS	Windows 2000 / XP
乱数源	RPG100
平均転送速度	247Kbit/sec
乱数自己検定機能	FIPS140-2 (Change Notice 1)
電源電圧	DC 5 V （USBより供給）
電源電流	通常時　Typ. 43 mA
	サスペンド時　Typ. 390 μ A
動作温度	0 ～ 40 ℃

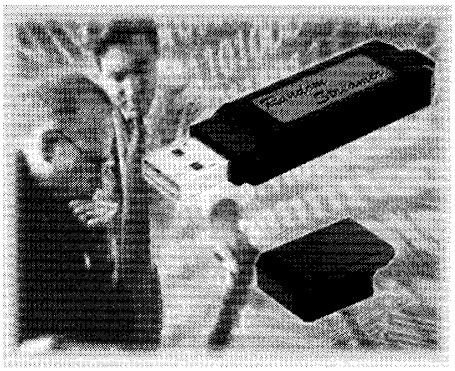


写真 2　物理乱数生成 USB モジュール
Random Streamer RPG102

Random Streamer である（写真 2）.

Random Streamer はプログラミングしやすい環境が用意されており，数学や統計をはじめとする様々なソフトで物理乱数の利用を可能としている.

4.5. ま と め

ランダムなノイズを利用した物理乱数を開発するうえで重要なのは，外来ノイズを含め，いかに外部環境の影響を受けないようにするかということと，いかに高い周波数のノイズを増幅するかということである．我々が開発した RPG100 は，これらの問題に対処する工夫を入れ，物理乱数生成 IC という形で製品化したものである．これにより，物理乱数生成器としてはたいへん高いコストパフォーマンスを得ることができた．今後，さらなる高速化と低価格化と，他の様々な機能とのワンチップ化を実現することにより，物理乱数がより身近な存在となり，市場も拡大していくと思われる．また，現在複雑な手法で行われている暗号の鍵生成は，物理乱数によって置き換えられていくと考えられる.

5. 終わりに

日本で開発され，現時点で入手可能な物理乱数発生装置の発生のしくみについて，説明してきた．学術誌である日本統計学会和文誌にはそぐわない内容であるとも思われるが，物理乱数の発生方法についてあまり知らないまま使っていることが多いと思われるので，何らかの参考になれば幸いである.

統計数理研究所においては物理乱数のみならず乱数に関係するポータルサイトを2006年4月中に立ち上げる予定である．乱数発生法や検定法について解説を掲載するのみならず，擬似乱数や物理乱数をダウンロードできるようにする計画を有している．公開の際には多くのユーザの利用があることを願っている．さらなる，物理乱数発生速度の高速化のために，発生方法を第一段階から見直すための研究も同時に行っている．PCIサイズのボードで200 MB/秒以上の発生速度にする予定である．

参考文献

[1] D. L. Evans, P. J. Bond and A. L. Bement (2001). Security Requirements for Cryptographic Modules, *FIPS PUB 140-2 (Change Notice 1)*.

[2] 伏見正則 (1989). 乱数，東京大学出版会.

[3] 石田正次 (1956). 放射能のランダム性について, 統計数理研究所彙報, **4**, 31-33.

[4] 石田正次，佐藤利男，鈴木亀二郎，下田昭一郎，川瀬哲郎 (1972). ダイオードノイズを利用した乱数発生装置，日立評論，**54**, 894-898.

[5] 岸本俊祐，福江万寿夫 (1999). ダイオードノイズを利用した物理乱数の発生とその評価，電子情報通信学会誌，**J82-A**, 1704-1709.

[6] D. E. Knuth (1997). The Art of Computer Programming. Vol. 2, Seminumerical Algorithms 3rd Ed., Addison-Wesley.

[7] M. Matsumoto and T. Nishimura (1998). Mersenne Twister: A 623-dimensionally equidistributed uniform pseudorandom number generator, *ACM Transactions on Modeling and Computer Simulations*, **8**, 3-30.

[8] 仁木直人 (1980). 工学的乱数発生, 統計数理研究所彙報，**27**, 115-132.

[9] 仁木直人 (1983). パーソナル・コンピュータのための物理乱数発生器，統計数理研究所彙報，**31**, 33-50.

[10] 渋谷政昭 (1981). 準数値算法／乱数，サイエンス社 (The Art of Computer Programming. Vol. 2, Seminumerical Algorithms 2nd Ed., Addison-Wesley, 1981の訳書).

[11] 末松知恵，行方直人，島田一平，井上修一郎 (2005). 光子検出による物理乱数発生とその評価，電子情報通信学会誌，**J88-A**, 1063-1070.