論　文

可変容量パラメトロンによる物理的乱数発生法

斉藤　義明[†a)]　堀　潤一[†]　西村　浩志[††*]　木竜　徹[††]

Generation of Physical Random Number with Variable-Capacitor Parametron

Yoshiaki SAITOH[†a)], Junichi HORI[†], Hiroshi NISHIMURA[††*], and Tohru KIRYU[††]

あらまし　本論文では，周期性のない一様乱数を発生する物理乱数生成法として，パラメトロンの原理に注目した．パラメトロンは，励振した周波数の2分の1で発振を起こす回路であり，その位相は回路内に存在する雑音によって決定されるため予測することができない．この予測不可能な位相を検出することによって，乱数を発生させる装置を開発した．度数分布と統計的乱数検定より，本方式で生成された乱数が一様であることを確認した．

キーワード　物理乱数，パラメトロン，乱数生成，乱数検定

1. まえがき

完全に無秩序でかつ全体としては出現頻度が等しくなる乱数は，社会現象や物理現象の数値シミュレーションなどに広く利用されている．また，乱数は暗号技術としても重要な役割を果たしており，情報の保護の分野でもその需要が高い．現在，乱数の発生方法として様々な方法が開発されているが，そのほとんどは平均採中法や合同法などのアルゴリズムによるソフト的な擬似乱数の生成である[1]～[3]．アルゴリズムによる乱数生成は，ある程度の信頼性をもち，また高速に乱数生成を行えるという点から広く利用されている．しかし，コンピュータは有限の状態しかとらないために，生成された乱数は周期性をもつことが確認されている．そのため，正確な解や十分なセキュリティが得られない場合があり，より無秩序な乱数生成法が望まれている．

近年，ハードウェアの発展に伴う処理速度の向上と信頼性の向上から，物理的な乱数の生成方法が開発されてきた．ガンマ線を用いた乱数発生法が開発されているが，乱数生成速度が遅い，大規模の装置を必要とするなどの問題がある[4],[5]．株式会社東芝が半導体の内部熱雑音を利用した乱数生成器「ランダムマスター」を開発・生産しているが，新たなハードウェアの購入・設備などを必要とする．また，ダイオードノイズを利用して物理乱数を発生する方法も開発されている[6]～[8]．

ところで1955年，後藤によってパラメトロン（パラメータ発振）の原理が提案された[9]．これはコイルとコンデンサによる共振回路において，コイルの値を周波数 f で周期的に変化させた場合に回路が周波数 $f/2$ で発振する現象である．このパラメトロンは0相振動と π 相振動の二つの状態をもち，その状態は励振する直前に共振回路に存在する微小振動の位相によって決定される[9]～[11]．後藤は，当時この性質を利用して乱数を発生できると予言しているが，45年後の現在まで装置は実現されていない[12]．本論文でも共振回路に微小振動が存在しない場合は雑音により発振位相が制御されるためパラメトロンの状態を予測できないと考え，可変容量パラメトロンを用いて実際に乱数を発生させる装置を開発した．パラメトロンは短波帯のみならず，ミリ波帯，光の領域でも実現可能であり，既に光パラメトリック発振の技術が開発されている[13]．この光パラメトリック発振を用いて乱数を生成できれば物理的乱数生成における生成速度の問題を一挙に解決できるものと期待できる．

本論文では，パラメトロンを用いた乱数生成の基本原理について述べ，実際に短波周波数帯域で構成した乱数生成装置について述べる．次に，この乱数生成装

† 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
†† 新潟大学大学院自然科学研究科，新潟市
Graduate School of Niigata University, 8050 Ikarashi 2-nocho, Niigata-shi, 950-2181 Japan
* 現在，(株) 松下通信金沢研究所
a) E-mail: saitoh@bc.niigata-u.ac.jp

置の統計的性質を示し，生成した乱数を評価することにより，本手法の有効性を確認する．

2. 乱数生成の基本原理

2.1 パラメトロンについて

パラメトロンは，コイルとコンデンサによる共振回路において，一方のコイルまたはコンデンサの値を周波数 f で周期的に変化させた場合に回路が周波数 $f/2$ で発振する現象である．本論文では，コンデンサの値を変化させる可変容量型パラメトロンを用いる．図 1 にパラメトロンの基本回路を示す．パラメトロンの基本回路は，コイル（L），抵抗（R），バリアブルキャパシタンスダイオード（C_v）及び高周波の励振電力源（E）によって構成される．バリアブルキャパシタンスダイオードは，印加された電圧に応じて静電容量が変化する素子である．この回路において，励振電力源より周波数 f の高周波を印加するとバリアブルキャパシタンスダイオードの静電容量が周波数 f で変化する．その結果パラメトロンの原理より，回路が高周波 f に対し，2 分の 1 の周波数（$f/2$）で発振する．パラメトロンは，0 相振動と逆位相で発振する π 相振動のどちらかの状態をとる．発振していないパラメトロン回路に高周波 f を印加した場合，パラメトロンの状態が 0 相振動となるか π 相振動となるかは，発振前に共振回路に存在する周波数 $f/2$ の微小信号の位相によって決定される．パラメトロンの応用であるパラメトロンディジタル回路 [9]～[11] では，この原理を利用して位相を制御している．逆に，この微小信号が回路に流れていなければ，パラメトロンの位相は回路に存在する雑音によって決定される．雑音は不規則であるため，パラメトロンの位相を予測することはできない．本論文では，この予測不可能なパラメトロンの位相を検出し，乱数を発生させる．

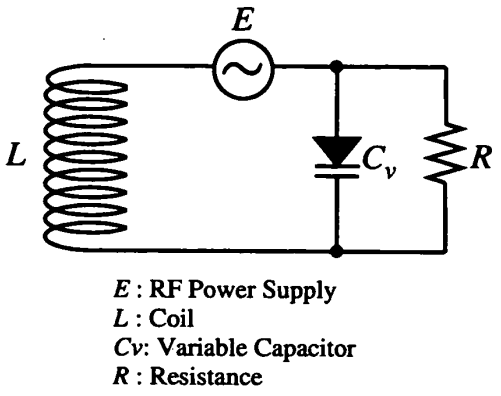


図 1 パラメトロンの基本回路
Fig. 1 Fundamental circuit of a parametron.

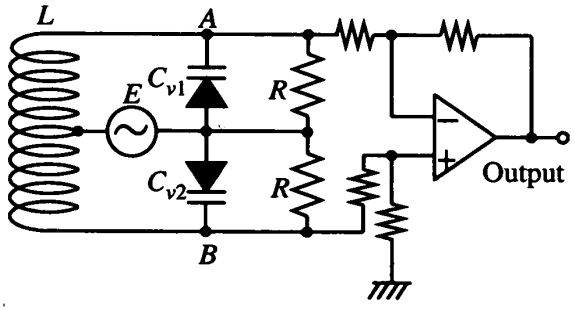


図 2 パラメトロン回路
Fig. 2 Parametron circuit.

2.2 パラメトロン回路

図 1 で示したパラメトロン基本回路の出力には，励振高周波にパラメトロン信号が重畳した波形が観測されるため，位相の判別が困難となる．そこで，励振高周波を除去し，パラメトロン信号のみを検出するように基本回路を図 2 のように変更する．変更後の回路は，励振電力源を中心として対称な二つのパラメトロンと OP アンプを用いた差動増幅器によって構成される．図 2 の回路において，励振高周波は $E \rightarrow C_{v1}(C_{v2}) \rightarrow A(B) \rightarrow L \rightarrow E$ の内周部を流れ，パラメトロン信号は $L \rightarrow A \rightarrow C_{v1} \rightarrow C_{v2} \rightarrow B \rightarrow L$ の外周部を流れる．内周部を流れる励振高周波は図 2 の A 点及び B 点において同相信号となるため，AB 間の差動増幅を行うことにより除去される．その結果，逆相信号であるパラメトロン信号のみを検出することができる．

2.3 パラメトロンによる乱数生成装置

本装置ではパラメトロンの位相情報を用いて乱数を生成する．しかし，図 2 のパラメトロン回路単独では基準となる位相がわからないため，位相情報を取り出すことが不可能である．そこで，パラメトロン回路を二つ用意し，それぞれに同位相の高周波を印加して，一方を常に発振状態にし，他方の発振をスイッチによりオンオフする．そして，二つのパラメトロン回路の位相を確認することによって位相情報を検出する．図 3 に乱数生成装置全体の構成を示す．装置は位相制御可能な二つの出力をもつ励振電力源（NF 回路設計ブロック Wave factory1946），図 2 に示したパラメトロン回路（L=21.5μH, C_v：SV101）2 台，差動増幅器（LM741），低域通過フィルタ，電子リレー，制御装置及びパーソナルコンピュータ（日本電気．PC-9801NS/E）から構成される．パラメトロン B に印加する励振高周波は電子リレーを用いて制御す

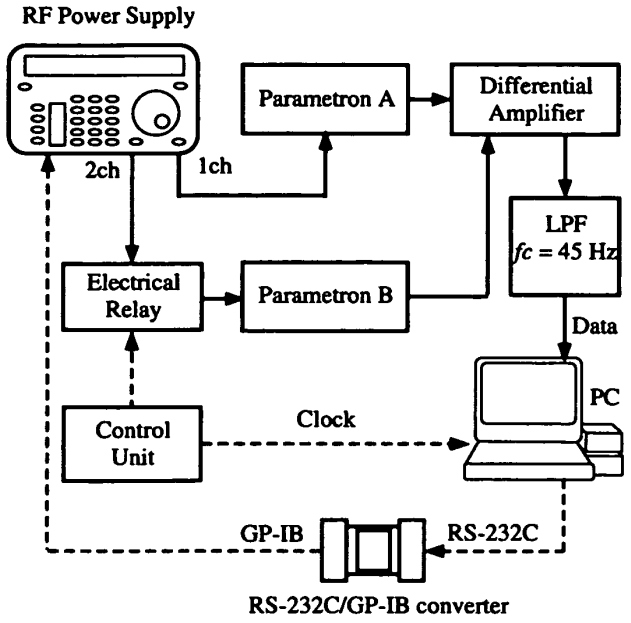


図 3　乱数生成装置のブロック図
Fig. 3　Block diagram of a random number generator.

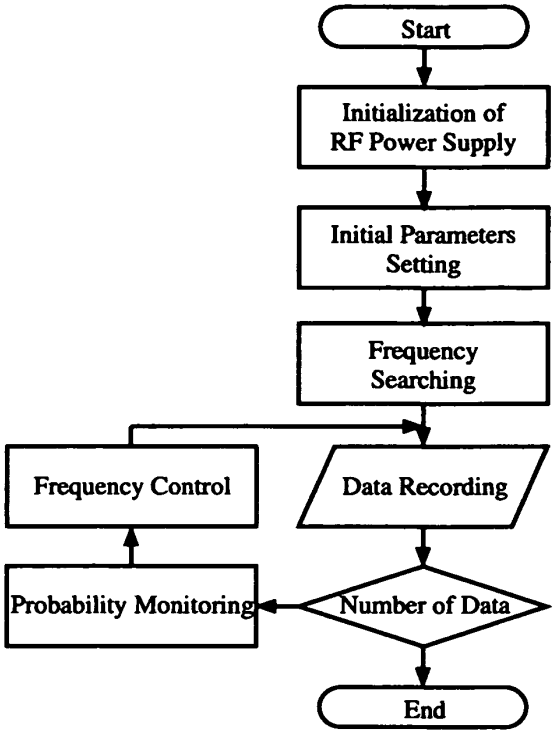


図 4　動的周波数制御アルゴリズム
Fig. 4　Algorithm of dynamic frequency control.

る．電子リレーのオンオフは制御装置より発生するクロック信号により制御する．位相情報は二つのパラメトロン出力の差動をとることによって検出する．つまり，二つのパラメトロンの位相が同相ならば出力がほぼ零，逆相ならばパラメトロンの 2 倍の振幅をもつ信号が出力される．この信号をカットオフ周波数 45 Hz の 5 次チェビシェフ型低域通過フィルタに通し，振幅成分のみを検出して，パーソナルコンピュータに入力する．本装置では 0 相振動時の出力を 2 進数の 0，π 相振動時の出力を 2 進数の 1 に対応させ乱数を生成する．パーソナルコンピュータは，制御装置より出力されるスイッチのオンオフに同期したクロック信号に合わせて検出信号の振幅を取り込み，乱数を記録するとともに，実験の自動化のため，**3.** で述べる励振電力源のパラメータを制御する．パーソナルコンピュータから転送される RS-232C 信号を励振電力源が制御できる GP-IB 信号に変換するため，RS-232C/GP-IB 変換器（Keithley. Model 500-Serial）を使用する．

2.4　装置の安定化

乱数生成装置から安定して一様乱数を生成するため，乱数の出現する確率を制御する方法を考える．今，全データ数を N，0 の出現個数を N_0 とすると，全データ中の 0 の占める割合である 0 の出現確率 P_0 を $P_0 = N_0/N$ で定義する．1 の出現確率 P_1 も同様である．乱数はこの出現確率が 1/2 になることが望ましいと考えられる．ところで，図 3 に示した乱数生成装置には励振周波数と励振端位相差という二つのパラメータがある．これらのパラメータを変化させることによって，出現確率 P_0 及び P_1 が変化する可能性がある．ここで励振端位相差とは，二つのパラメトロンに印加する直前の高周波間の位相差とし，励振電力源とパラメトロン間のケーブル長の違いから生じる位相のずれはあらかじめ修正した．また，自作したパラメトロンの構成要素として手巻きコイルを使用しているため，周囲の環境の変化によって値が変化する可能性がある．この変化に伴い発振周波数が変化し，その結果出現確率が時間とともに変化し，長期にわたり安定して乱数を生成することが困難になると考えられる．そこで，生成される 0，1 の出現確率を逐次監視し，励振周波数を動的に制御することによって装置の安定化を図る．図 4 に周波数制御アルゴリズムを示す．これによって周囲の環境が変化しても安定した乱数を得ることができると考えられる．

3.　乱数生成装置の動作特性

本章では **2.3** で述べた乱数生成装置の動作を出力波形より確認し，更に一様乱数を生成するために適した励振電力源のパラメータを求めるため，乱数生成装置の特性を明らかにする．

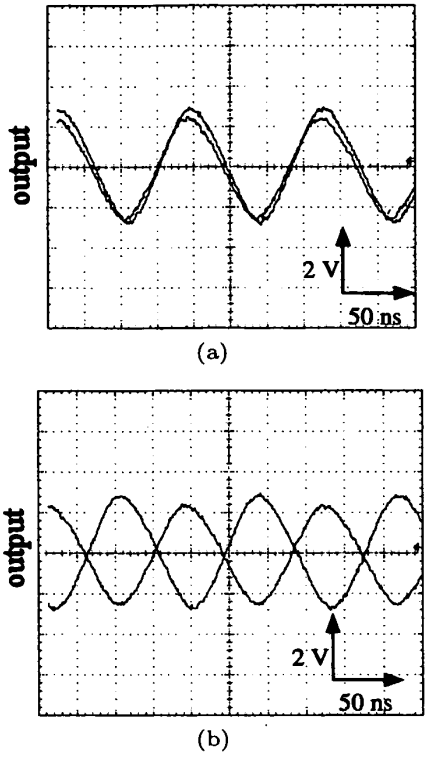


図 5 パラメトロンの例 (a) 0 相発振時の波形，(b) π 相発振時の波形

Fig. 5 Examples of waveforms in parametron. (a) Zero-phase and (b) Pi-phase oscillation.

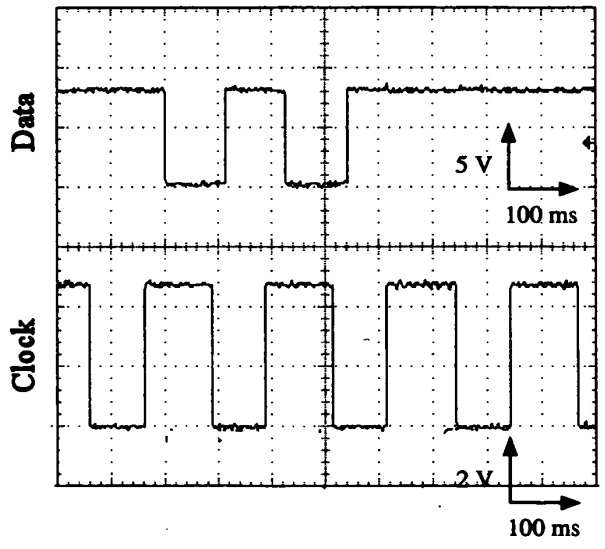


図 6 出力波形の一例

Fig. 6 An example of the output signal.

図 3 に示した乱数生成装置におけるパラメトロン A, B の出力例を図 5 に示す．常に発振しているパラメトロン A の出力に対して，(a) 0 相発振あるいは (b) π 相発振のどちらかの状態が観測できた．図 3 に示した低域通過フィルタの出力波形の一例を図 6 に示す．

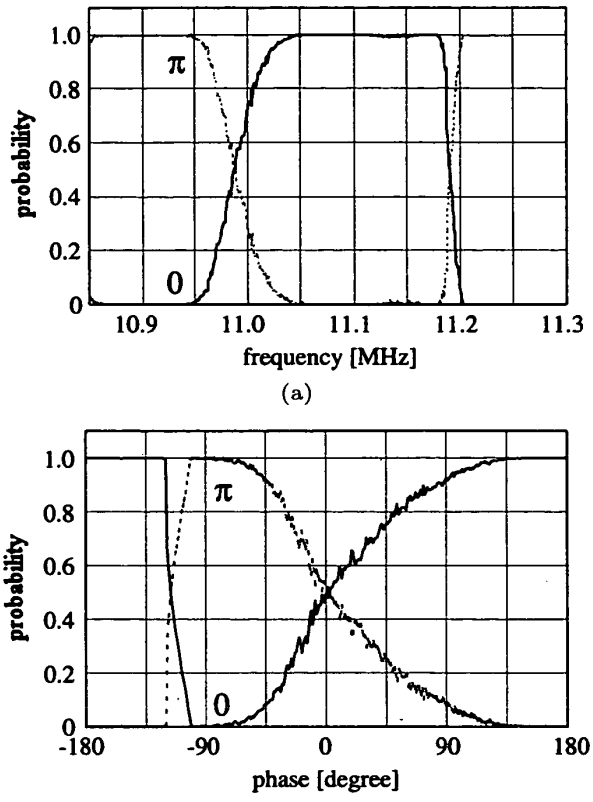


図 7 出現確率特性 (a) 励振周波数を変化させた場合 ($\theta = 0°$)，(b) 励振端位相差を変化させた場合 ($f = 10.988\,\mathrm{MHz}$)

Fig. 7 Probability characteristics of the random number generator in the case of (a) frequency and (b) phase changing.

パラメトロン B を制御することによって，常に発振しているパラメトロン A の出力に対し，0 相振動若しくは π 相振動のどちらかの状態が観測できた．

次に，一様乱数を生成するために，乱数生成装置のパラメータである励振周波数と励振端位相差を変化させたときの 0，1 の出現確率を調べることにする．励振端位相差を一定とし，励振周波数を変化させた場合の 0，1 の出現確率を図 7 (a) に示す．室温 23.5°C，励振高周波の振幅 0.2 Vp-p，励振端位相差 0° 一定とし，制御装置のクロック周波数は 45 Hz とした．励振周波数は 10.85～11.30 MHz まで 0.001 MHz 間隔で変化させ，励振端位相差を各周波数における 0, 1 の出現確率を記録した．出現確率は再現性を確認するために同一周波数ごとに 3 回測定し，その平均値を記録した．図 7 (a) より，0 の出現確率は周波数が高くなるにつれて増加し，10.988 MHz の付近で 1/2 になった．更に周波数が増加すると 0 の出現確率は 11.177 MHz から急激に減少し始め，112.030 MHz で 0 となった．

更に，励振周波数を固定し，励振端位相差を変化させた場合の出現確率の変化を図 7(b) に示す．励振周波数は 10.988 MHz 一定とし，励振端位相差は $-180°$ ～$180°$ まで $0.1°$ 間隔で変化させ，各位相差における 0, 1 の出現確率を記録した．0 の出現確率は $-125°$ から急激に減少し始め，$-94°$ で 0 となった．その後，励振端位相差が大きくなるにつれて増加し，$0°$ の付近で出現確率が 1/2 になった．

4. 乱数の評価

3. で求めたパラメータを用いて実際にデータを生成し，そのデータが乱数であるかを検証した．まず **2.3** で示した乱数生成装置で生成した 2 進数データ 32768 個を $M = 8$ ビットずつ数値化し，$N = 4096$ 個の数値データを生成した．比較対象として，C 言語 (Borland Turbo C Ver2.0) の標準ライブラリ rand 関数で生成した 8 ビット数値データの乱数 4096 個を用意した．本方法のアルゴリズムは線形合同法である．**1.** で述べたように，コンピュータで生成した乱数は周期をもつが，C 言語のランダム関数で生成したデータの数がその周期である 2^{32} に比べ十分少ないことから一様乱数とみなすことができる．2 次元及び 3 次元度数分布と統計学的乱数検定法を使用し，乱数の検証を行った．

4.1 2 次元及び 3 次元度数分布による比較

図 3 の乱数生成装置の基本構成で生成されたデータを 2 次元及び 3 次元度数分布で表示し，確認した．はじめに，生成された $N = 4096$ 個の $M = 8$ ビットデータを 2 個あるいは 3 個ずつ組み分けし，2 次元及び 3 次元座標データとする．これより 2 次元の場合は 2048 組，3 次元の場合は 1365 組のデータが生成される．次に各組を 2 次元あるいは 3 次元空間にプロットする．図 8(a) に 2 次元度数分布の結果を，図 8(b) に 3 次元度数分布の結果を示す．C 言語のランダム関数より生成したデータ及び本方法により生成したデータの結果ともに，2 次元空間及び 3 次元空間にデータが一様に分布し，周期性が見られないことから，生成されたデータは乱数であることが確認できる．

4.2 統計学的乱数検定法による比較

次に，統計学的乱数検定法として頻度検定，連の検定，及び組合せ検定を用いて生成された $N = 4096$ 個の $M = 8$ ビットデータを評価する．

(A) 頻度検定

生成された N 個の数値データのうち，値 k が出現

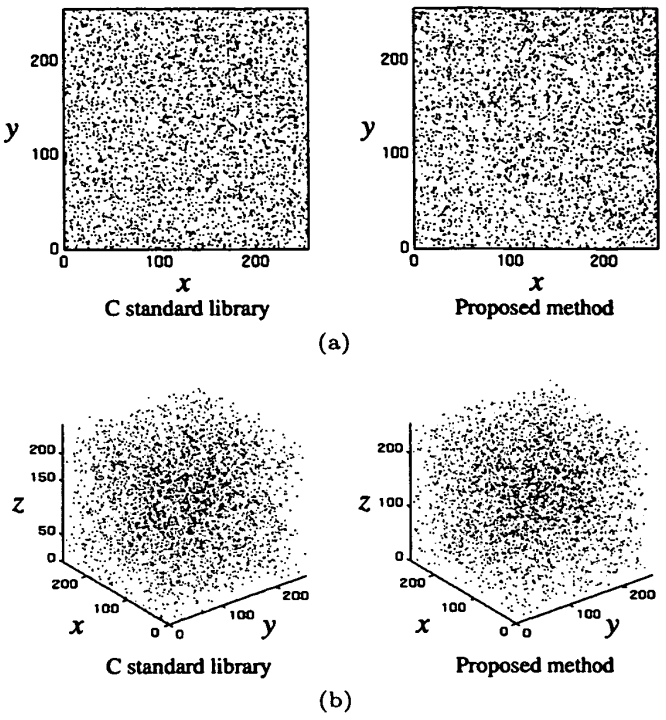


図 8 度数分布による比較 (a) 2 次元度数分布，(b) 3 次元度数分布

Fig. 8 Comparison in frequency distribution. (a) Two- and (b) Three-dimensional frequency distribution.

した回数を $f_k(k = 0, 1, \cdots, K-1)$ とすると，数値 k の出現確率は $P(k) = f_k/N(k = 0, 1, \cdots, K-1)$ となる．乱数の場合，各数値の出現確率が等しくなるので出現確率の理論値は $P(k)^* = 1/K$ となる．このとき

$$\chi^2_{K-1} = \sum_{k=0}^{K-1} \frac{\{P(k) - P(k)^*\}^2}{P(k)^*} \qquad (1)$$

より，算出した値が自由度 $K-1$，有意水準 5% または 1% の χ^2 分布の値より小さければ，頻度検定に関してデータが乱数であるということができる [1]．本論文では，$K = 2^M = 256$，$N = 4096$ で検定を行う．

(B) 連の検定

連とはデータ列の隣り合う数値を比較し，単調増加または単調減少がどれだけ続いたかを示す [3]．また，このとき一つの単調増加または単調減少の間に含まれる数値の個数を連の長さと呼ぶ．本論文では，修正された連の検定法 [1] より χ^2_4 を算出する．その値が自由度 4, 有意水準 5% または 1% の χ^2 分布の値より小さければ，連の検定に関してデータが乱数であるということができる．

(C) 組合せ検定

表 1 各検定法による評価結果
Table 1 The results of random tests.

検定法	パラメトロン	C 言語 rand 関数	棄却しきい (有意水準 5%)
頻度検定	272.325	245.750	293.248
連の検定	6.523	6.560	9.488
組合せ検定	7.310	6.949	15.507

M けたの 2 進数 N 個の系列を考える．データが乱数の場合，N 個の系列の中で 1 の個数が k 個となる M けたの出現確率の理論値は $P(k)^* = N_M C_k (1/2)^M (k = 0, 1, \cdots, M-1)$ となる [1]．ただし，${}_M C_k$ は M けたの 2 進数の中に 1 が k 個含まれるすべての組合せの数である．このとき，χ^2_{M-1} $(M = 8)$ より算出された数値が自由度 7，有意水準 5% または 1% の χ^2 分布の値より小さければ，組合せ検定に関してデータが乱数であるということができる．

生成したデータに頻度検定，連の検定，及び組合せ検定の三つの統計学的乱数検定法を適用した結果を表 1 に示す．ただし，棄却しきいとして有意水準 5% の χ^2 分布の値を示す．結果として，頻度検定と組合せ検定に関しては本装置で生成したデータの結果が rand 関数の結果より大きい値となったが，連の検定に関しては rand 関数より小さい値となった．しかし，どの検定法においても計算した棄却しきい値よりも小さい値となったため，今回の検定に関してはデータが乱数であるといえる．

5. 考　　察

5.1 乱数生成装置の特性について

本論文では，周期性のない一様乱数を発生する物理乱数生成法として，パラメトロンの原理に注目した．パラメトロンは，励振した周波数の 2 分の 1 で発振を起こす回路であるが，その位相は回路内で発生する雑音によって決定されるため予測するができない．この予測不可能な位相を検出することによって，乱数を発生させる装置を開発した．

図 7 で示したようにパラメトロンを用いた乱数生成装置では，励振周波数及び励振端位相差の変化によって乱数の出現確率が変化した．実験に用いたコイル，コンデンサの値では，図 7 (a) により出現確率が 1/2 になる周波数は 10.988 ± 0.001 MHz あることが確認できた．また，図 7 (b) により励振端位相差が 0° からずれると出現確率が大きく変化することを確認した．周囲の温度などの環境によって出現確率が 1/2 になる励振周波数が変化する可能性がある．そこで，一様乱数を生成するためには，励振端位相差を 0° に固定し，出現確率によって励振周波数を調節すればよいと考えられる．乱数の生成速度は，現在のところ最大で 1 秒間 45 個と遅い．この理由は，パラメトロン発振の立上り，立下りに各 10 周期を必要とし，更に安定期で位相を比較しているためである．励振周波数及びクロック周波数を高めれば高速化も可能である．また，パラメトロン発振は光の領域でも実現可能であるので，光パラメトロンによって乱数を生成できれば，格段の高速化が期待できる．

5.2 装置の安定化について

5.1 で述べたように，我々の提案した乱数生成装置の出力の出現確率は，周囲の環境によって変化する可能性がある．本論文では，出現確率が一定になるように装置の安定化を行うため，出現確率を逐次監視しその変動に応じて励振周波数を制御した．現システムでは，励振周波数の変化量の実測値で制御しているが，より高速に一様な乱数を生成するためには，更なる改良が必要である．具体的には，PID 制御を用いたより高度な周波数制御が必要になると考える．また，出現確率以外の一様乱数の性質を考慮した制御法についても検討できると考えられる．更に，周囲の環境が本装置に与える影響についても調べる必要がある．例えば，周囲にコンピュータなどの高周波雑音源をおいた場合の出現確率の変化などである．更に，乱数生成速度の高速化についても検討する必要があると考える．

5.3 装置の簡略化について

図 3 で示した乱数生成装置の基本構成では位相の相対制御可能な出力をもつ特殊な 2 出力励振電力源が必要となる．周波数制御のみを行う場合，出力を 1 チャンネルしかもたない励振電力源を用いることにより，装置の簡略化を実現できる．簡略化した装置の構成として，図 9 (a) に示すように，励振高周波を電子リレーの前で分岐し，零振端位相差が零になるように同じ電子リレーを二つのパラメトロン回路の前に接続した．また，二つのパラメトロンが電子リレーにより分離されているため，それぞれのパラメトロン回路に存在する雑音が独立し，発振した時点でそれぞれのパラメトロンが独立した位相で生じるように構成した．簡略化した乱数生成装置の励振周波数を変化させた場合の出現確率特性を図 9 (b) に示す．ただし，1 の出現確率のグラフのみを示す．出現確率特性をみると，図 7 (a) で示した基本構成の場合の出現確率特性に比

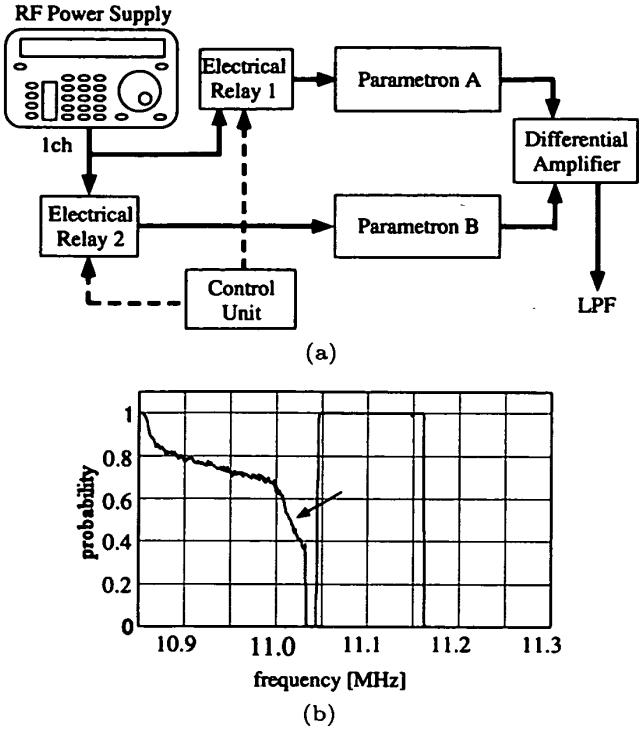


図 9 簡略化した乱数生成装置 (a) 構成，(b) 出現確率特性

Fig. 9 Simplified random number generators. (a) Block diagram, (b) Probability characteristics.

べて 0 相，π 相に大きく変化した．しかし，出現確率が 1/2 となる 11.02 MHz 付近の周波数帯域（図 9 (b) 中の矢印）に注目すると，周波数変化に対する出現確率の変化は，ほぼ図 7 (a) の基本回路の特性と同様であった．簡略化した装置でも，十分出現確率の制御が可能であると考えられる．

5.4 乱数の評価について

乱数を用いた暗号化の応用例を考えた場合，コンピュータで生成された乱数は数式で算出されているため，乱数の導出式とパラメータがわかれば同じ鍵データを作り出すことができると考えられる．それに対して，本装置のように物理的に生成された乱数は，同じ方法を用いたとしても同じ鍵データを生成することが不可能であるため，より高度なセキュリティを実現することができる．また，様々な計算機シミュレーションへの応用を考えた場合，物理乱数を用いることでより正確なシミュレーションを実行できると考えられる．

本装置で生成した乱数について 2 次元，3 次元度数分布，及び統計学的乱数検定法を用いて乱数を評価した．2 次元，3 次元度数分布では，どちらの場合でも図 8 に示したように 2 次元及び 3 次元空間中にデータが一様に分布した．統計学的乱数検定法では，今回行ったどの検定方法に対しても有意水準の理論値よりも小さな計算値が得られた．以上より，今回行ったすべての評価方法において本装置で得られたデータが乱数であるということが確認できた．ところで，統計学的乱数検定法において本装置で生成した乱数により得られた値が C の標準ライブラリ rand 関数で生成した値より大きくなるという結果が得られているが，これは，データ計測中に出現確率が 1/2 となる周波数が変化して，0 あるいは 1 の出現確率が高くなったことが原因と考えられる．また，評価するデータの数が rand 関数の周期である 2^{32} より少ないため，rand 関数の結果がよくなって見える．これを確かめるためにはデータ数あるいは数値化時のビット数を増やして，データを検定する必要があると考える．

5.5 他の乱数生成法との比較

まず，アルゴリズムによる乱数生成法と提案法を比較すると，アルゴリズムよる方法で大量の乱数を生成させた場合，周期性の問題を避けることはできない．それに対して，提案法で取り上げている物理的乱数生成法では自然現象より発生するランダム性を利用しているので，非周期性という点で優れていると考えられる．よって，乱数の性質という意味では，従来から提案されている物理的乱数生成法 [4]～[8] と同じであると考えられる．

他の物理的乱数生成法として放射能を用いた方法が提案されているが，良質な乱数を生成できる一方，放射能物質の生成，検出を実現するための特殊な材料，装置を必要とした [4], [5]．本提案法では，励振電力源と，抵抗，コイル，バリアブルキャパシタンスダイオードという基本構成で良質の乱数を生成でき，特殊なハードウェアを必要としない．

また，半導体やダイオードなどから発生する雑音源をもとに物理的に乱数を生成する方法も提案されている [6]～[8]．これらの方法の場合，特殊な装置を必要とせず，将来的にコンピュータへの実装なども考えられているが，乱数の生成速度に関しては限界がある．これらと比較して，本提案法は，現時点では短波帯の周波数で実験したため乱数生成速度が制限され，従来法の生成速度より 1/100 程度劣っているが，将来的に光パラメトロンに乱数生成技術を応用すれば，格段に乱数生成速度の高速化が期待できる．本論文は，その可能性を示したことに意義があると考える．

6. むすび

パラメトロンを用いて物理的に乱数を生成する方法を開発した．この乱数生成装置によって一様な乱数を安定に生成するために，励振端位相差，励振周波数による出現確率の特性を求め，出現確率によりこれらを制御する方法を示した．また，乱数生成装置の簡略化の可能性を示した．本装置で生成した乱数を度数分布と各種乱数検定方法を用いて検証した結果，一様な乱数を生成できることを確認した．今後の課題として，装置の小型化，乱数生成速度の向上，周囲の環境が本装置に与える影響についての考察などが挙げられる．この論文では，短波帯の周波数で実験したため乱数生成速度が遅かったが，ミリ波帯または光パラメトロンにこの原理を応用すれば，飛躍的に生成速度は向上すると考えられる．

文　献

[1] 宮武　修，脇本和昌，乱数とモンテカルロ法，森北出版，1978.

[2] D.E. Knuth,（渋谷政昭訳），準数値算法/乱数，サイエンス社，1981.

[3] 伏見正則，乱数，東京大学出版会，1989.

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

[5] O. Miyatake, H. Inoue, and Y. Yoshizawa, "Generation of physical random number," Math. Jap., vol.20, pp.207–217, 1975.

[6] 仁木直人，"工学的乱数発生，" 統計数理研究所彙報，vol.27, no.1, pp.115–131, 1980.

[7] 仁木直人，"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，vol.31, no.1, pp.31–49, 1983.

[8] 岸本俊祐，福江万寿夫，"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，" 信学論（A），vol.J82-A, no.11, pp.1704–1709, Nov. 1999.

[9] 後藤英一，"非線型共振子のパラメータ励振とその応用，" 信学誌，vol.38, no.10, pp.770–775, Oct. 1955.

[10] 高橋秀俊，"パラメトロンについて，" 信学誌，vol.39, no.6, pp.586–590, June 1956.

[11] H. Takahashi, "Information theory of quantum-mechanical channels," Advanced in Communication Systems, vol.1, pp.227–310, Academic Press, New York, 1965.

[12] 後藤英一氏からの私信，平成10年10月7日.

[13] 稲場文男，霜田光一，レーザハンドブック，朝倉書店，1973.

（平成13年4月16日受付，9月5日再受付，
10月18日最終原稿受付）

斉藤　義明　（正員）

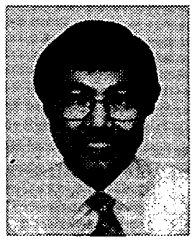
1965 北大大学院工学研究科修士課程了．1970 工博．1965 から新潟大学工学部勤務，現在同学部福祉人間工学科教授．生体情報，医療情報の収集，解析装置，治療装置の開発研究に従事．IEEE，日本 ME 学会，日本ハイパーサーミア学会，情報処理学会各会員．

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・医療画像の逆問題，脳機能解析と逆問題の研究に従事．IEEE，日本 ME 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．

西村　浩志　（正員）

1997 新潟大・工卒．1999 同大大学院自然科学研究科修士課程了．現在株式会社松下通信金沢研究所に所属．移動体通信に関する研究に従事．



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 ME 学会評議員，バイオメカニズム学会，IEEE 各会員．