第22回 回路とシステム
軽井沢ワークショップ
The 22nd Workshop on Circuits and Systems
in Karuizawa, April 20-21, 2009

マルコフモデルによるオシレータサンプリング方式真性乱数生成器の乱数品質解析

An Analysis of Oscillator-based True Random Number Generator with Markov Model

天木健彦 †‡　橋本昌宜 †‡　密山幸男 †‡　尾上孝雄 †‡
† 大阪大学 大学院情報科学研究科 情報システム工学専攻　‡JST CREST

Takehiko AMAKI†‡　Masanori HASHIMOTO†‡　Yukio MITSUYAMA†‡　Takao ONOYE†‡
†Dept. Information Systems Engineering, Osaka University　‡JST CREST

概要

多くの暗号システムは第三者には予測不可能な乱数を必要とするが、数学的に生成される擬似乱数は種が知られてしまうと全乱数列を再現できる弱点を持つ。そのため、熱雑音などの物理的なランダム要因から乱数を生成する真性乱数生成器が求められている。本論文では、真性乱数生成器の一方式であるオシレータサンプリング方式について、マルコフ過程を用いた乱数品質評価モデルを提案する。また、提案したモデルを用いて、オシレータの周期、周期ゆらぎ、デューティ比などの動作パラメータが乱数の品質に与える影響について解析した結果を報告する。

1　序論

暗号を用いた安全な通信への要求の高まりにともない、暗号の基盤技術である乱数についても高い品質が求められている。線形合同法などの数学的手法を用いて生成する擬似乱数は必ず周期性を持ち、アルゴリズムと種が知られてしまうと全乱数列を再現できるため暗号用途には適さない。一方、物理的なランダム要因から生成される物理乱数があるが、特に個々のビットがお互いに独立であり、1/0 の発生確率が等しいものを真性乱数という。擬似乱数のような周期性や再現性がなく、計算機的に予測不可能であるため、暗号に用いる乱数として適当である。

真性乱数を生成する真性乱数生成器 (TRNG:true random number generator) には、ユーザーのマウス操作を利用するもの [1] から、原子の放射性崩壊を専用のデバイスで観測するもの [2] まで様々あるが、スループットの高さや実装の容易性から、回路の内部雑音を利用する TRNG についての研究が比較的多くなされている。しかし、一般に内部雑音は小さいため、内部雑音を利用する TRNG から高品質の乱数を得ることは容易でない。オシレータサンプリング方式は、回路内の雑音を利用する TRNG の一つであり、既に実機での動作も報告されている [3][4][5]。しかし、方式の動作を特徴づける動作パラメータと乱数の品質の関係について詳しく解析を行った例が少なく、設計を行う上での指針に乏しい。文献 [6] では、オシレータサンプリング方式の設計上の課題を解決するために性能評価モデルを構築しているが、VCO(voltage controlled oscillator) の使用を前提とした限定的なモデルに留まっており、未解析の動作パラメータが多く残されている。そこで本論文では、マルコフ過程を用いた性能評価モデルを提案し、オシレータサンプリング方式における動作パラメータが乱数品質に与える影響について解析を行う。

本論文は以下の構成をとる。まず 2 章でオシレータサンプリング方式 TRNG の説明を行い、注目する動作パラメータを取り上げる。3 章では提案モデルの考え方を説明し、確率分布を用いた解析の一例を示す。4 章では各動作パラメータを変化させて乱数の品質評価を行った結果を示す。最後に 5 章で結論をまとめ、今後の展望について述べる。

2　オシレータサンプリング方式 TRNG

2.1　回路構造と動作原理

図 1 にオシレータサンプリング方式 TRNG の回路構造を示す。オシレータサンプリング方式では、速度差のある二つのオシレータを用意し、高速オシレー

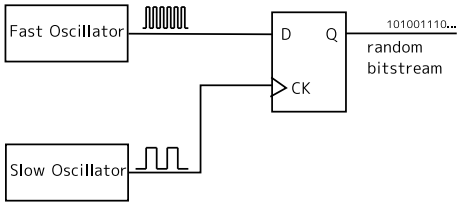

図 1: オシレータサンプリング方式 TRNG

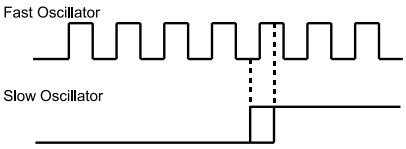

図 2: オシレータの発振波形

タの発振信号をデータ、低速オシレータの発振信号をクロックとし、D フリップフロップでサンプリングすることで乱数列を得る。図 2 に二つのオシレータの発振波形を示す。低速オシレータの発振波形には回路内雑音により周期ゆらぎが生じるため、発振波形の立上がりタイミングにもゆらぎが生じる。フリップフロップはクロックの立上がりタイミング時のデータの HIGH/LOW に従ってビット列を出力するため、ゆらぎによって 1/0 が変化する。このように、ランダムな雑音から乱数列を得ることができる。

2.2 注目する動作パラメータ

オシレータサンプリング方式において注目すべき代表的な動作パラメータを取り上げる。高速オシレータにおいては、平均周期とデューティ比に注目する。ここでデューティ比とは、一周期における HIGH の時間の割合として定義する。デューティ比は乱数列の 1/0 の割合に直接影響する。一方、低速オシレータにおいては、平均周期と周期ゆらぎに注目する。周期ゆらぎは、一般にオシレータサンプリング方式 TRNG の品質を決定する重要な動作パラメータと考えられている。ここでは周期ゆらぎを周期の標準偏差と定義する。低速オシレータにおいて、複数サイクルに 1 回サンプリングし、サンプリング間隔を広げることで擬似的に周期ゆらぎを大きく見せることができ、乱数の品質を向上できると考えられる。周期ゆらぎが時間に対して独立のとき、サンプリング間隔を k 倍すると周期ゆらぎは $\sqrt{k}$ 倍となる。よってサンプリング間隔にも注目する。また、低速オシレータの一周期ごとに生じる、高速オシレータとの位相差にも注目する。位相差は、低速オシレータの平均周期を高速オシレータの平均周期で割った余りとして定義する。

動作パラメータのうち、オシレータの平均周期は、設計段階でもシミュレーションにより見積もりができるため、設計者が容易に値を設定可能である。一方、周期ゆらぎは、一般に製造会社から周期ゆらぎを見積もるためのデバイス動作パラメータが提供されないため、設計段階で値を精度良く見積もることが難しく、設計者が任意の値に設定することは困難である。サンプリング間隔は、カウンタや分周器を用いることで離散的に変更できる。しかし、十分な品質を得るために必要なサンプリング間隔は周期ゆらぎの大きさに依存するため、必要十分なカウンタや分周器のサイズを設計時に見積もることは困難である。デューティ比、位相差は、製造ばらつきによって敏感に変化するため、正確な値の設定には製造後の調節が必要である。

3 マルコフ過程を用いた乱数品質評価モデル

3.1 マルコフ過程

マルコフ過程とは、離散時間の確率過程 $(X_n; n = 0, 1, 2, \cdots)$ で、状態空間 S においてすべての時刻 $n \geq 0$ とすべての状態 $j \in S$ に対して以下の条件が成り立つ確率過程である [7]。

$$P\{X_{n+1} = j | X_0, X_1, \cdots, X_n\} = P\{X_{n+1} = j | X_n\}$$

すなわち、マルコフ過程においては、次時刻の状態 X_{n+1} が現在時刻の状態 X_n のみに依存して確率的に決定され、過去の履歴 $X_0, X_1, \cdots, X_{n-1}$ とは無関係である。

3.2 モデルの考え方

提案モデルの構築にあたって、簡単のためいくつかの仮定を置く。まず、高速オシレータに周期ゆらぎは生じないものとする。次に、考慮する雑音は熱雑音やショット雑音のような白色雑音のみとし、1/f 雑音、電源雑音、基板雑音などは考慮しない。すなわち、回路内の雑音および雑音により生じる低速オシレータの周期ゆらぎは、空間的、時間的に無相関であるとする。

マルコフ過程の TRNG への適用を説明する。まず、高速オシレータの一周期分を時間的に m 分割し、各時間区分をそれぞれ一つの状態とする。得られた m 個の状態がマルコフ過程における状態空間 S に相当する。次に、低速オシレータの発振信号のある立上がりタイミングを時刻 n とし、それ以降の立上がりタイミングを順に時刻 $n+1, n+2, \cdots$ とする。低速オシレータがあるタイミングで立上がったとき、そ

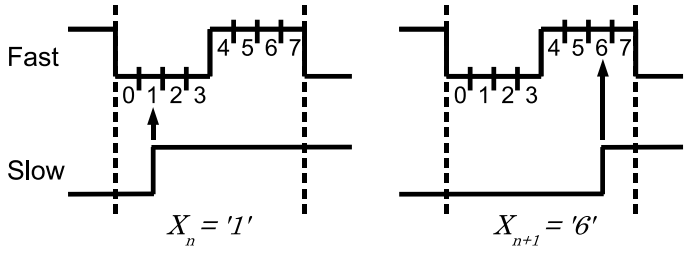

図 3: マルコフ過程の TRNG への適用例

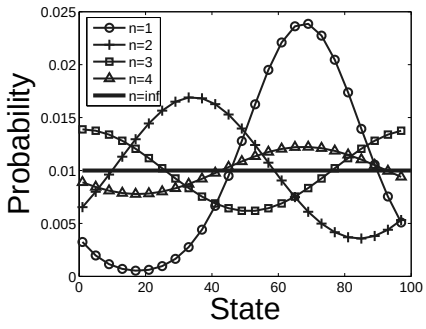

図 4: 確率分布の推移と極限分布

のタイミングは分割した高速オシレータの時間区分、つまり状態のいずれかに対応づけられる。時刻 n における状態を X_n とする。時刻 n は低速オシレータのある立上がりタイミングであり、各状態は高速オシレータの HIGH/LOW に対応しているので、TRNG は X_n に応じて n 番目のビットを出力する。

図 3 に $m = 8$ としてモデルを適用した例を示す。ある時刻 n において状態 1 にあり、次の時刻 $n + 1$ では状態 6 にある。先においた仮定から、次の時刻に移る状態は、現在の状態、位相差、および低速オシレータの周期ゆらぎの値から確率的に求めることができる。また、例の場合、デューティ比は 0.5 であり、LOW に状態 0,1,2,3 を、HIGH に状態 4,5,6,7 を割り当てているので、TRNG は n ビット目に 0、$n + 1$ ビット目に 1 を出力する。

提案モデルの考え方は、オシレータの実現方法などによらない一般的な確率過程の議論であるので、任意の回路構造をもつオシレータサンプリング方式 TRNG に用いることができる。

3.3 確率分布による解析例

提案モデルを用いた解析の一例を示す。高速オシレータ一周期の時間分割数は 100 に設定した。また、雑音から生じる周期ゆらぎは正規分布に従うものとした。ある時刻において状態確率分布が与えられている時、次の時刻における状態確率分布を求めることができる。図 4 に時刻 n=0 において状態 0 にあるとした時の、時刻 n=1,2,3,4 における確率分布を示す。また、十分な時間が経過した後 $(n = \infty)$ の極限確率分布をあわせて示す。なお、高速オシレータの平均周期を 0.3[ns]、低速オシレータの平均周期を 50[ns]、周期ゆらぎを 50[ps]、デューティ比を 0.5 とした。図 4 から、確率分布は時刻が進むにつれてフラットになり、極限確率分布に近づいていることが分かる。確率分布がフラットで偏りがないということは、次に生成されるビットが現在のビットと独立であり、かつ 1/0 の発生確率が等しいことを意味し、真性乱数としての性質を持った高品質な乱数が出力される。したがって、サンプリング間隔を広げることにより、乱数の品質向上が期待できる。

4 実験

MATLAB を用いて提案モデルを実装した。行列演算により状態確率分布を求め、各動作パラメータが乱数品質に与える影響を調べる。

4.1 評価指標

提案モデルにおける乱数の品質評価指標として R_{Prob} を導入する。R_{Prob} は確率分布の偏りの程度を表し、図 4 に示す全状態確率分布において、確率の最大と最小の差として定義する。例えば n=1 の時、$R_{Prob} = 0.0239 - 0.0005$ である。

乱数の品質を評価するための検定法として、NIST Special Publication 800-22[8] で提案されたテストセットを用いる。NIST テストセットの各テストは、対象ビット列が理想的な乱数列であるかの検定を行う。NIST テストセットは 16 種類のテストから構成されており、1/0 の比率や線形複雑度など、乱数の品質を多面的に評価することができる。

また、FIPS PUB 140-2[9] において規定されているポーカー検定も評価に用いる。ポーカー検定は 4bit を単位とした頻度に関する乱数検定法であり、結果として単一の検定値 x が出力される。検定値 x が小さいほど良い乱数とみなすことができるため、検定値 x をスコアとして品質の比較が容易になる。

4.2 評価条件

基本動作パラメータは表 1 と設定した。なお、高速リングオシレータの平均周期（高速-平均周期）の値は 90nm プロセスにおける 11 段リングオシレータのシミュレーション結果から決定し、低速オシレータの周期ゆらぎ（低速-周期ゆらぎ）、低速オシレータの平均周期（低速-平均周期）の値は 1531 段リン

表 1: 基本動作パラメータ

高速-平均周期	0.3 [ns]
低速-周期ゆらぎ	50 [ps]
高速-デューティ比	0.5
低速-平均周期	60 [ns]

グオシレータの実測結果に基づいて決定した。なお、低速オシレータの周期ゆらぎは正規分布に従うものとした。また、高速オシレータのデューティ比（高速-デューティ比）は理想的な値を用いた。高速オシレーター周期の時間分割数 m の値は、結果の精度と関係があると考えられるが、確率分布を求める際の計算量が大きくなるため、ここでは $m = 100$ とした。NIST テストセットおよびポーカー検定については、モデルにより求められた確率分布に基づいてシミュレーションを行い、生成した 1M ビットの乱数列 1000 系列を用いた。

4.3 サンプリング間隔

フリップフロップにおいてサンプリング間隔を、低速オシレータ周期の 1 倍、4 倍、16 倍と変化させた。図 5 に R_{Prob} の変化を、図 6 にポーカー検定の検定値 x の変化を、表 2 に NIST テストセットの結果の一部を示す。図 5 から、サンプリング間隔を広げることで確率分布の偏りが小さくなっており、品質が向上していることが分かる。図 6 のポーカー検定、表 2 の NIST テストセットの結果も R_{Prob} と同様の結果を示しており、R_{Prob} が評価指標として有効であることが確認できる。サンプリング間隔の調整による品質向上を実現するためには、低速オシレータを分周すれば良いと考えられるが、分周するほど TRNG のスループットも落ちてしまうため、必要十分な分周回数を求めることが重要である。

4.4 高速-平均周期

高速オシレータの平均周期を 0.3[ns]、0.15[ns]、0.1[ns] と変化させた。R_{Prob}、ポーカー検定の検定値 x、NIST テストセットの結果の一部を、それぞれ図 7、図 8、表 3 に示す。図 7 から、高速オシレータの平均周期が小さくなるほど、確率分布の偏りが小さくなっており、品質が向上していることが分かる。図 8 のポーカー検定、表 3 の NIST テストセットの結果も同様の結果を示している。しかし、実際には高速オシレータの高速化には限界があるため、高速オシレータの平均周期を小さくすることのみで十分な品質を得ることは難しいと考えられる。

4.5 低速-周期ゆらぎ

低速オシレータの周期ゆらぎを 50[ps]、100[ps]、500[ps] と変化させた。R_{Prob}、ポーカー検定の検定値 x、NIST テストセットの結果の一部を、それぞれ図 9、図 10、表 4 に示す。図 9 から、低速オシレータの周期ゆらぎが大きくなるほど、確率分布の偏りが小さくなっており、品質が向上していることが分かる。図 10 のポーカー検定、表 4 の NIST テストセットの結果も同様の結果を示している。低速オシレータの周期ゆらぎによる品質向上の実現には、大きな段数のリングオシレータを用いるなど周期ゆらぎの大きい回路構造や動作条件を選ぶなどの方法が考えられ、他の動作パラメータよりも工夫が要求される。

4.6 高速-デューティ比

デューティ比の変化による品質劣化を明確にするため、低速オシレータの周期ゆらぎを 500[ps] とした上で、高速オシレータのデューティ比を 0.55 として解析した。NIST テストセットの結果の一部を表 5 に示す。先に述べたように、低速オシレータの周期ゆらぎ 500[ps] は高品質の乱数を得られる条件であるが、デューティ比が崩れることで大きく品質が落ちている。また、図 10 の＋印がポーカー検定の検定値 x である。ディーティー比が 0.5 の場合の検定値 x は 15.0 であるが、デューティ比が 0.55 の場合、検定値 x は 218.2 まで劣化している。これらから、高速オシレータの平均周期や低速オシレータの周期ゆらぎが良好な値であっても、高速オシレータのデューティ比が崩れていれば品質が落ちることが分かる。高速オシレータのデューティ比を整えるには、分周器を用いることや、基板バイアスにより立上がりまたは立下りの遷移時間を調整するなどが考えられる。

4.7 低速-平均周期

低速オシレータの平均周期を 60[ns]、600[ns]、6000[ns] と変化させた。R_{Prob}、ポーカー検定の検定値 x、NIST テストセットの結果の一部を、それぞれ図 11、図 12、表 6 に示す。低速オシレータの平均周期の桁が変わっても、乱数の品質に影響が無いことが分かる。このことから、低速オシレータにおいて品質に影響を及ぼす動作パラメータは周期ゆらぎであり、平均周期は品質と直接関係がないことが分かる。直感的にはスループットを落とすことで乱数の

品質を向上させることができると思われるが、本節の結果から、スループットと品質は必ずしもトレードオフの関係にあるわけではないと言える。

4.8 位相差

低速オシレータの一周期ごとに生じる位相差を変化させた。位相差は低速オシレータの平均周期を高速オシレータの平均周期で割った余りとして定義したので、低速オシレータの平均周期を変えることで位相差を変化させることができる。また、4.7 節で述べたように、低速オシレータの平均周期は品質に影響を及ぼさないので、位相差から生じた結果のみを得ることができる。低速オシレータの平均周期を 60∼60.3[ns] まで 0.0375(= 0.3/8)[ns] ずつ変化させた。R_{Prob}、ポーカー検定の検定値 x、それぞれ図 13、図 14 に示す。図 13 から、R_{Prob} は位相差によらないことが分かる。一方、図 14 から、ポーカー検定の結果は位相差に依存し、高速オシレータの平均周期の半分を周期とする、周期的な値をとると考えられる。このことから、周期ゆらぎなどの条件が整わない場合、低速オシレータの速度を微調整することで、乱数の品質が改善できる可能性がある。

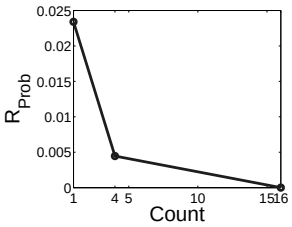

図 5: サンプリング間隔と R_{Prob}の関係

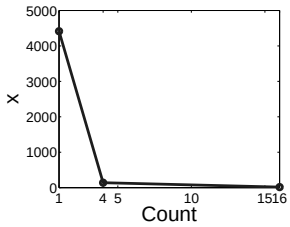

図 6: サンプリング間隔とポーカー検定結果の関係

表 2: サンプリング間隔と NIST テスト結果の関係

テスト名	サンプリング間隔		
	1	4	16
Frequency	FAIL	PASS	PASS
BlockFrequency	FAIL	FAIL	PASS
Runs	FAIL	FAIL	PASS
ApproximateEntropy	FAIL	FAIL	PASS

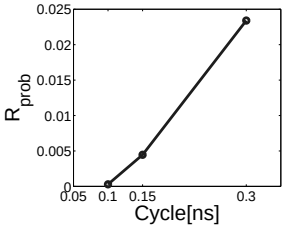

図 7: 高速-平均周期と R_{Prob}の関係

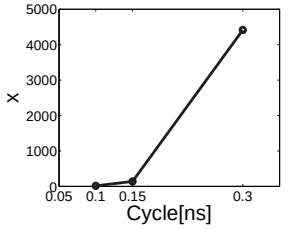

図 8: 高速-平均周期とポーカー検定結果の関係

表 3: 高速-平均周期と NIST テスト結果の関係

テスト名	高速-平均周期 [ns]		
	0.3	0.15	0.1
Frequency	FAIL	PASS	PASS
BlockFrequency	FAIL	FAIL	PASS
Runs	FAIL	FAIL	FAIL
ApproximateEntropy	FAIL	FAIL	FAIL

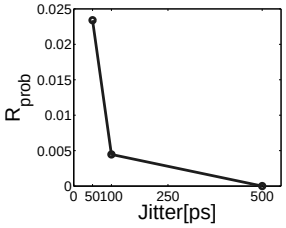

図 9: 低速-周期ゆらぎと R_{Prob}の関係

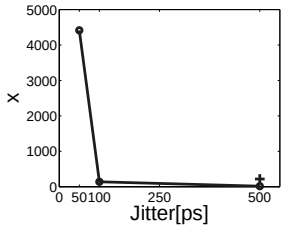

図 10: 低速-周期ゆらぎとポーカー検定結果の関係

表 4: 低速-周期ゆらぎと NIST テスト結果の関係

テスト名	低速-周期ゆらぎ [ps]		
	50	100	500
Frequency	FAIL	PASS	PASS
BlockFrequency	FAIL	FAIL	PASS
Runs	FAIL	FAIL	PASS
ApproximateEntropy	FAIL	FAIL	PASS

表 5: NIST テスト結果の比較 (周期ゆらぎ=500[ps])

テスト名	高速-デューティ比	
	0.5	0.55
Frequency	PASS	FAIL
BlockFrequency	PASS	FAIL
Runs	PASS	FAIL
ApproximateEntropy	PASS	FAIL

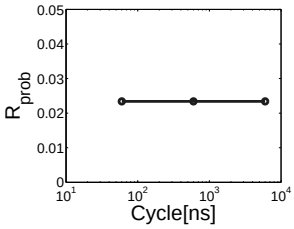

図 11: 低速-平均周期と R_{Prob}の関係

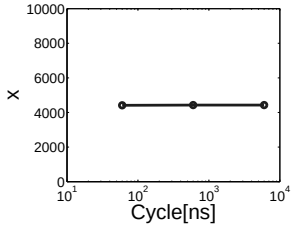

図 12: 低速-平均周期とポーカー検定結果の関係

表 6: 低速-平均周期と NIST テスト結果の関係

テスト名	低速-平均周期 [ns]		
	60	600	6000
Frequency	FAIL	FAIL	FAIL
BlockFrequency	FAIL	FAIL	FAIL
Runs	FAIL	FAIL	FAIL
ApproximateEntropy	FAIL	FAIL	FAIL

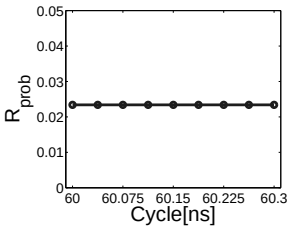

図 13: 位相差と R_{Prob}の関係

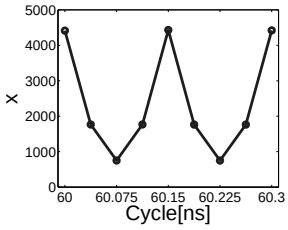

図 14: 位相差とポーカー検定結果の関係

5 結論

マルコフ過程を用いたオシレータサンプリング方式 TRNG の乱数品質評価モデルを提案した。提案モデルは一般的な確率過程の議論だけで成り立っており、新規のオシレータサンプリング方式 TRNG の乱数品質評価にも適用可能である。提案モデルを用いて各動作パラメータが乱数品質に及ぼす影響を調べた結果、1) サンプリング間隔を広げる、2) 高速オシレータの周期を小さくする、3) 高速オシレータのデューティ比を整える、4) 低速オシレータの周期ゆらぎを大きくする、5) 適切な位相差になるよう低速オシレータの周期を調整することで品質を向上させられるという結果が得られた。また、低速オシレータの平均周期は品質に直接関係が無いという結果が得られた。

今後は、実機の測定により提案モデルの正当性を確認する予定である。また、提案モデルに残された課題として、白色雑音のみを考慮している点や高速オシレータに生じる周期ゆらぎを考慮していない点が挙げられる。そのため、時間的相関のある雑音への対応や、高速オシレータに生じる周期ゆらぎの影響についても検討する。

参考文献

[1] Y. Hu, X. Liao, K. Wong and Q. Zhou, "A true random number generator based on mouse movement and chaotic cryptography," *Chaos, Solitons & Fractals*, Oct., 2007.

[2] M. Rohe, "RANDy-A true-random generator based on radioactive decay," Technical report, Saarland University, 2003.

[3] B. Jun and P. Kocher,"The Intel random number generator," Cryptography research, inc. white paper for Intel corporation, Apr., 1999.

[4] C. S. Petrie and J. A. Connelly, "A noise-based IC random number generator for applications in cryptography," *IEEE transactions on circuits and systems*, Vol. 47, No. 5, May, 2000.

[5] M. Bucci, L. Germani, R. Luzzi, A. Trifiletti, and M. Varanonuovo, "A high-speed oscillator-based truly random number source for cryptographic applications on a smart card IC," *IEEE transactions on computers*, Vol. 52, No. 4, Apr., 2003.

[6] C. S. Petrie and J. A. Connelly, "Modeling and simulation of oscillator-based random number generators," *in Proc. IEEE International Symposium on Circuits and Systems*, Vol. 4, pp.324-327, May, 1996.

[7] 伏見正則, **確率と確率過程**, 朝倉書店, 2004.

[8] "A statistical test suite for the validation of random number generators and pseudorandom number generators for cryptographic applications," NIST, Pub. 800-22, May, 2001.

[9] "Security requirements for cryptographic modules," FIPS Pub. 140-2, May 2001.