超小型乱数発生素子

Ultrasmall Random Number Generator

棚本　哲史　■TANAMOTO Tetsufumi
大場　竜二　■OHBA Ryuji
藤田　忍　■FUJITA Shinobu

情報セキュリティへの要求が厳しくなるにつれて，その基盤技術の一つである乱数発生回路に対する要求も年々増加している。乱数の予測困難性の高さは安全性の根幹にかかわるために，近年，商用乱数としての統計検定項目も徐々に厳しいものが採用されるようになってきた。

東芝は，ナノスケールのシリコンデバイスを発展させることにより，より高品質で高速な乱数を生成可能な超小型乱数生成回路を開発した。

As the demand for information security becomes increasingly severe, higher level random number generators, which are one of the fundamental information technologies, are also required every year. Because the unpredictability of a random number is closely relevant to the basis of information security, significantly stricter statistical tests of commercial random numbers have been adopted in recent years.

Toshiba has developed an ultrasmall random number generation circuit that can generate high-quality and high-speed random numbers. This was achieved by the development of nano-scale Si devices.

1　まえがき

携帯電話やPDA（携帯情報端末）などのモバイル機器，あるいはICカードなどの利用が急速に拡大し，またネットワーク上を流れる情報量が年々増加するのにつれて，小規模電子回路における個人情報に関するセキュリティへの要求が厳しくなってきている。

このような状況のなかで，セキュリティ基盤技術の一つである乱数生成回路に対しても，より高品質でかつ小面積なものへの要求が年々高まっている。

乱数は，認証手続き，ID（IDentification）やパスワードの発行，あるいは暗号鍵生成などセキュリティ技術全般のなかで広く使われており，要求される本質は予測困難性にある。

ここでは，モバイル機器に搭載可能なシリコン（Si）ナノ構造を用いた超小型物理乱数生成回路について述べる。この回路は，ナノサイズのトランジスタが発生する電流のゆらぎを利用している。通常のトランジスタは，微細化に伴い生ずるこの種のゆらぎによって，正常な動作が困難となる問題に直面しつつある。東芝はこのゆらぎを逆に利用することによって，高品質な乱数の発生に成功した。

2　乱数生成回路の現状

従来，ICカードや，携帯電話，PDAなどの小型機器では，一定のアルゴリズムで作られる算術乱数が用いられてきた。この手法ではまず，シードと呼ばれる初期値をフィードバックレジスタ回路などで一定の周期（線形最大周期列）で繰り返す方式が用いられてきた。これらは擬似乱数と呼ばれ，線形最大周期列の範囲内で乱数として用いられてきた。しかし，最近では擬似乱数であるための限界が指摘されつつある。

2.1　乱数性に対する要求

乱数には要求度に対応した質を統計的に検定する基準が設けられてきた。従来，米国商務省国立標準技術研究所（NIST）が作成した，四つの乱数データ検定項目から成るFIPS（Federal Information Processing Standard）140-2に合格することが商用乱数としての信頼の基準となってきた。その検定項目を以下に示す。

⑴　monobit test　　0と1の出現回数がそれぞれ50％に近いか

⑵　run test　　000.., 11..などの同じ値の連の数が数学的に期待される確率で適度に分布しているか

⑶　poker test　　四つの連続数を10進法に直したとき（例えば0101なら5），その値が0から15の間で一様に分布しているか

⑷　long run test　　連続した同じ値の数の最大が26以下であるか

しかし現在では，16個の更に厳しい検定項目から成るNIST SP（Special Publication）800-22が商用乱数の基準となりつつある[1]。

将来的には，より乱数性の高いと期待される物理乱数をシードとして用いることが必須要求項目となる可能性も出てきており，それに伴って，物理乱数生成回路に対する要求項

目も整備されつつある。質の高い乱数生成に対する要求は増える一方なのである。

2.2 物理乱数

従来広く利用されている物理乱数として，電気回路の熱雑音（ジョンソンノイズ）を増幅した回路がある。熱雑音は大きい場合でも数十 μV で，演算増幅器や差動アンプを使い，4～5けた増幅して，更に0と1のバランスを調整する回路が付加されるため，回路規模は大きくなる。ジョンソンノイズを用いた物理乱数は，パソコンやサーバなどのサイズで使用されており，当社でも既に製品化されている。これより小さい乱数回路としては発振回路を利用するものがある。これは，高速で発振する回路部分と，非周期の低速カウンタで1ビットずつ読み込み0と1を均等化する平滑化回路部分から成る。増幅が不要なため前記の熱雑音乱数回路より小さいが，発振回路が持つ周期性が乱数に残ってしまう傾向があることと，消費電流が大きいという欠点があるため，低消費動作が求められるICカードやモバイル機器では搭載が難しい。

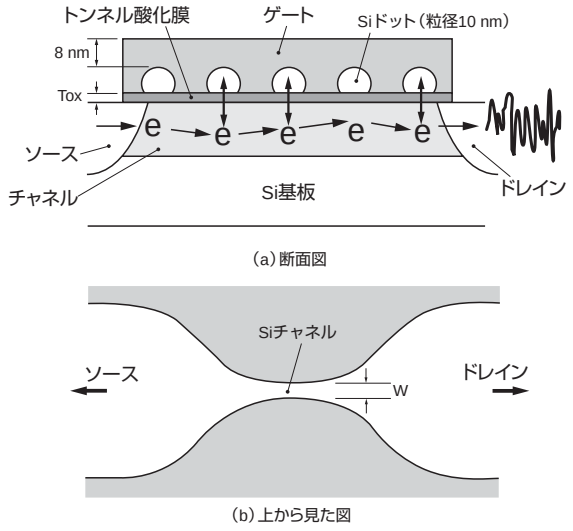


図1．乱数発生素子構造 — Siドット MOSFET 素子構造を断面図と上から見た図で示す。

Structure of newly developed random number generator

3 小型乱数生成回路の開発

前述のように，一般的に乱数の質を高くしようとすると回路面積が増加し，逆に回路面積を減らそうとすると乱数の質が悪くなるというトレードオフがある。従来の算術乱数の場合，周期を十分長くしたり，初期値自身を毎回変更したり，また生成した乱数を再度暗号モジュールで再かくはんしたりするなどの必要があったが，これらの付属回路は算術乱数回路よりも大きいため，乱数の質を高めようとすると，結局は回路規模が大きなものになってしまう。

当社はこのトレードオフを破る技術として，超小型の物理乱数生成回路を開発した。ポイントとなるのは，Siトランジスタに付随するナノスケール物理現象で見られる“揺らぎ”や“不確定性”を利用して，増幅回路なしで乱数を作り出すところにある。一般的に，トランジスタは微細にするほど揺らぎが大きくなる。この揺らぎが十分大きければ，回路内で大きな面積を占める余分な付属回路が不要になるため，小型で高度な乱数が利用できることになる。ここでは，単一電子素子を用いた乱数生成について紹介する。

3.1 高速乱数生成可能なSiドットMOSFET

単一電子現象は，ナノスケールの領域に電子を閉じ込めたとき，電子間のクーロン反発力が大きくなり，室温でも電子の一つ一つの挙動が観測される現象である。

当社は，ナノスケールのトランジスタ構造において特徴的に現れるこの単一電子現象を利用することで，統計的にランダムでかつ巨大な揺らぎ信号を発生させることができることを見いだし，高品質の乱数生成を実証してきた[(2)]。

ここでは，単一電子素子のなかでも特に高速な乱数を生成することのできる，SiドットMOSFET（金属酸化物半導体型電界効果トランジスタ）について解説する[(3), (4)]。

素子構造を**図1**に示す。基本的な構造はフローティングゲート型電界効果トランジスタと同じで，ソース，ドレイン，及びゲート電極を持ち，ゲート絶縁膜中に通常のフローティングゲートのSiドット領域を持つ。SiドットMOSFETはバルクSi基板上に作製した（図1（a））。これはSOI（Silicon On Insulator）基板に比べて，Siドットへ入る電子数が増えることを期待したものである。トンネル酸化膜厚（T_{OX}）は1 nm以下の薄いものを使用した。Siチャネルは真ん中付近に幅（W）0.15 μm程度の狭い部分を持つ（図1（b））。Siドットは粒径10 nm程度のSiナノ微小結晶で，Siドットの面密度（D_{dot}）は $2.5 \times 10^{11}\,cm^{-2}$ 程度である。比較のためSiドットを持たない参照用のMOSFETも作製した。乱数列は固定バイアス条件でのドレイン電流（I_D）の揺らぎを用いて生成される。I_D 揺らぎはチャネル～Siドット間の電子の捕捉（ほそく）と放出により誘起されるので，W，T_{OX}，及び D_{dot} の三つが重要なパラメータとなる。

3.2 素子の動作特性

図2は，バルクSi基板上に生成したSiドットMOSFET素子と，SOI基板上に生成したSiドットMOSFET素子の I_D 揺らぎを同時にプロットしたものである。図から明らかなように，バルクSi基板上に形成した素子の方が大きな揺らぎ電流を発生させていることがわかる。これは前述したように，バルク基板の方がSiドットへの電子の出入りが多いことを示している。SOI基板を用いた場合，I_D 揺らぎの強さを示すフーリエ係数の比較から，I_D 揺らぎの強さはWに反比例し，T_{OX} が薄

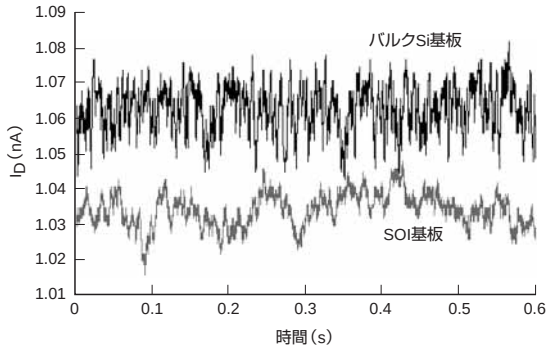


図2．I_D揺らぎ特性 ― SOI基板を用いたSiドット乱数発生素子と今回開発したバルクSi基板を用いたSiドット乱数発生素子のノイズ電流の比較を示す。バルクSi基板を用いた方が電流揺らぎが大きいことがわかる。

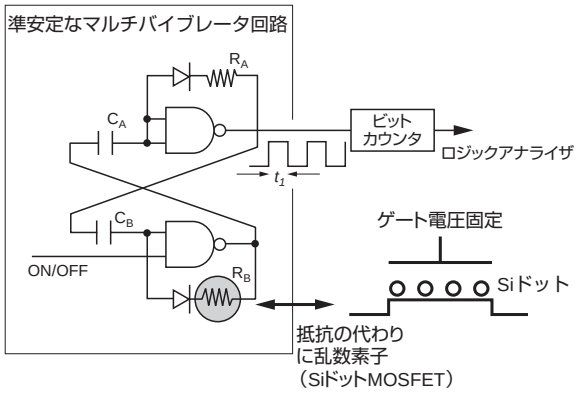
Fluctuation of current I_D

いほど指数関数的に，また，D_{dot}が大きいほど，I_D揺らぎは速くなることを示した[3]。今回，バルクSi基板でも同様にWを狭く，T_{OX}を薄くし，またD_{dot}を大きくすることで，揺らぎをより強くすることが可能であることもわかった。

3.3 乱数変換回路

乱数列は，マルチバイブレータ回路にSiドットMOSFETを組み入れて，I_D揺らぎにより揺らぐ発振周期をビットカウンタで0又は1に変換すると生成される（**図3**）。この回路は，20程度の論理ゲートといくつかの受動素子だけで形成される小型なものである。用いた素子は，T_{OX}=0.7 nm，W=0.1 μm，$D_{dot}=2.5\times10^{11}\,cm^{-2}$のものである。

バイアス条件を調節して適当なI_D揺らぎ状態にすると高速な乱数生成が可能になり，250 kビット/sの生成レートで，高度な統計検定試験をパスする真性乱数に近い乱数が生成



R：抵抗　C：コンデンサ　t_1：発振時間

図3．乱数生成マルチバイブレータ回路 ― 準安定なマルチバイブレータ回路を改良し，抵抗の一部分を乱数生成素子で置き換えることにより，素子抵抗の揺らぎをデジタル信号に変換することができる。

Digital circuit for random number generator

可能である。これは，SOI基板をベースとした乱数生成回路の10倍の速さである。

3.4 乱数データの統計評価

バルクSiドット乱数素子においても，FIPS140-2はもちろん，NIST SP800-22に合格する。しかし，このような従来の検定方法では，データの期待値からのズレに関係して定義されるカイ二乗値(注1)を1点だけ計算して，その値がカイ二乗分布曲線の信頼区間内にあれば合格とするので，ある意味で不十分な検定である。例えば，棄却率を5％とすれば，カイ二乗値がカイ二乗分布曲線の95％以内の値に入っていればよいのである。

当社は，より高品質の乱数を目指すため，乱数検定方法についても検討を行ってきた。統計的に高品質な乱数とは，多数のデータの分布が数学的なカイ二乗分布曲線により近接していることである。

頻度検定と系列検定における，数学的カイニ乗分布曲線と発生させた乱数データとの比較を**図4**に示す。頻度検定

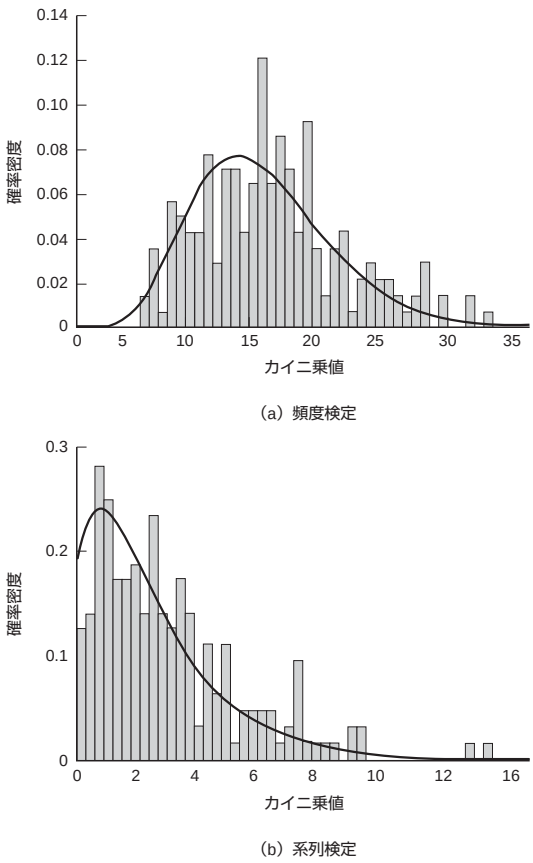


図4．乱数性のより高度な評価 ― 頻度検定及び系列検定において，数学的カイ二乗分布曲線と発生させた乱数データとの比較を示す。乱数として質の高いことがわかる。

Higher level test of random number generation

（注1）　カイニ乗値＝((観測度数－期待度数)^2÷期待度数)の総和で算出する。

は，0と1が一様に分布しているかどうかを見るため，連続した0と1のデータを決められた数ずつ区切り（ここでは四つずつ），それを10進数に変換してカイ二乗分布を見るものである（ここでは0から15の分布）。系列検定は，連続した数のペアが一様に分布しているかどうかを検定する。ここでは(0,0)，(0,1)，(1,0)，(1,1)のパターンが出現する数をカウントし，これらがどのように分布しているかを検定した。データの数は60,000点である。データのばらつきを補正する様々な平滑化の工程を経ない乱数データとしては数学的分布曲線に近く，乱数として質の高いものであることがわかる。更に，より乱数の質が高いかどうかはこの数学的分布曲線にどれだけ近づくことができるかで判断できる。

3.5　高速化のための指針

より高品質な乱数をより高速で生成するには，更にI_D揺らぎを強くする必要がある。チャネル幅Wを更に細くし，D_{dot}を更に増やすと，Wに反比例し，D_{dot}に比例して強めることができる。また，現状のSi酸化膜よりもトンネルバリアの低い薄膜絶縁体をトンネル膜にすると，トンネル抵抗はトンネルバリアにも指数関数依存することから，揺らぎもまだまだ指数関数的に強められると考えられる。今後は，より厳しい乱数検定と合わせて素子設計を行っていく。

4　あとがき

当社はSiナノ構造を利用して，コア部分の回路規模が100程度という超小型物理乱数生成回路のプロトタイプを開発した。乱数源となる素子はナノテクノロジーの進歩につれて，更に信号の強度の増大及び速度の向上が可能である。組込み回路の改良と合わせて，より厳しいセキュリティ基準に対応可能な超小型乱数回路を開発していく。

謝　辞

Siドット MOSFETを利用した乱数生成に関する研究の一部は，独立行政法人 情報通信研究機構の委託により実施している“高度情報セキュリティに向けた真性乱数生成用集積回路の研究開発”に関するものである。

ここに，ご支援いただいた関係各位に深く感謝の意を表します。

文　献

(1) NIST.“NIST Special Publication 800-22.Revised May 15, 2001”. Computer Security Resource Center（CSRC） Home page. <http://csrc.nist.gov/publications/nistpubs/>（accessed 2005-11-21）.

(2) 藤田忍，ほか．高度情報セキュリティ向け超小型乱数生成回路．東芝レビュー．**58**，8，2003，p.47－51.

(3) 大場竜二．Siドット MOSFETを用いた情報セキュリティ用高速乱数生成．東芝レビュー．59，11，2004，p.60－61.

(4) Ohba, R., et al. Narrow-channel-MOSFET having Si-dots for High-rate Generation of Random Numbers. IEEE International Electron Devices Meeting Technological Digest. 2003, p.745－748.

棚本　哲史　TANAMOTO Tetsufumi, D.Sc.

研究開発センター LSI基盤技術ラボラトリー 研究主務，理博。システムLSI用半導体ナノデバイスの研究・開発に従事。日本物理学会，応用物理学会会員。
Advanced LSI Technology Lab.

大場　竜二　OHBA Ryuji

研究開発センター LSI基盤技術ラボラトリー 研究主務。システムLSI用半導体ナノデバイスの研究・開発に従事。日本物理学会，応用物理学会会員。
Advanced LSI Technology Lab.

藤田　　忍　FUJITA Shinobu, D.Eng.

研究開発センター フロンティア・リサーチラボラトリー 研究主幹，工博。システムLSI用半導体ナノデバイスの研究・開発に従事。応用物理学会，IEEE会員。
Frontier Research Lab.