SiリッチSiN MOSFETを用いた高速乱数生成器

High-Generation-Rate Random Number Generator Using Si-Rich SiN MOSFET

松本　麻里　■ MATSUMOTO Mari
大場　竜二　■ OHBA Ryuji
牛島　知巳　■ USHIJIMA Tomomi

ICカードやモバイル機器などでは，情報セキュリティが近年ますます重要視されており，セキュリティ技術の要と言える乱数に対し，より厳しい基準を要求されるようになっている。高度なセキュリティ基準に耐えうる予測不可能な真性乱数の生成には，物理乱数が有効である。

今回東芝は，SiN（シリコン窒化膜）MOSFET（金属酸化物半導体型電界効果トランジスタ）を新たな乱数生成源として用いることで，回路の小型化とともに高速で良質な乱数生成を可能にする乱数生成装置を開発した。

Information security has recently been playing an increasingly important role in various ubiquitous applications such as integrated circuit (IC) cards and mobile equipment. Higher level random numbers have correspondingly been required as one of the fundamental elements of secure systems. Physical random number generators are most desirable because of their unpredictable "true" random numbers.

Toshiba has developed a silicon nitride metal-oxide-semiconductor field-effect transistor (SiN MOSFET)-based random number generator that can generate high-quality random numbers at high speed and can be embedded into small circuits.

1　まえがき

乱数は，暗号技術の中で極めて重要な役割を担っており，文書の暗号化や復号化に用いる鍵の生成などに利用されている。そして，使用する乱数の質にセキュリティレベルが左右され，ハッカーなどの攻撃者から見破られない鍵を生成するためには，使用する乱数が予測不可能であることが重要である。

ICカードや携帯電話などのモバイル機器を対象とした乱数生成を行うためには，乱数の質が良いことはもちろん，回路規模が小さい乱数生成装置である必要があり，更に乱数生成速度が速いことが要求される。

今回東芝は，SiN（シリコン窒化膜）MOSFET（金属酸化物半導体型電界効果トランジスタ）を新たな乱数生成源とした小型の乱数生成回路を用いることで，小型で高速かつ良質な乱数生成装置を開発し，実用に向けて大きく近づいた。

2　乱数生成装置の現状

近年，より高度なセキュリティが求められるなか，乱数もより真性度の高いものが求められている。乱数の質の評価は，無作為性，予測不可能性，及び再現不可能性ということばで表される。後者ほど条件は厳しく，暗号技術に用いるためには，無作為性と予測不可能性は最低限満たす必要がある。従来，ICカードやモバイル機器のセキュリティ用途としては，一定のアルゴリズムで作られる算術乱数が一般的に用いられている。これらは擬似乱数と呼ばれている。擬似乱数は基本として，ある種の初期値設定が必要で，同じ初期値に対して同じ乱数を生成することから再現性がある。ソフトウェアだけでは，ソフトウェアを支えているコンピュータが有限の内部状態しか持たないために，長くても短くても必ず有限の周期を持つ。

それに対し，物理乱数は，放射線や熱雑音などハードウェアから得られた情報を元に生成されるため，再現不可能性を持つ乱数を得ることができる。よって，より高度なセキュリティを実現させるには，物理乱数を利用することが有効である。実用化されている乱数の一つとして，熱雑音を利用した乱数生成装置がある。しかし，熱雑音によるノイズ信号は非常に小さく，乱数生成のためにはその信号を増幅させる増幅回路を必要とするため，回路規模が大幅に大きくなる。

従来用いられている乱数生成装置について比較すると，質の良い乱数を求めると回路規模も増大してしまうというトレードオフが存在していることがわかる。

ICカードやモバイル機器では，実装上の制約から擬似乱数回路しか搭載ができなかったが，銀行取引や個人情報保護などの観点から，いっそうのリスク管理が必要とされている。そのため，そのセキュリティの基盤となる乱数にもいっそうの質の向上が要求されている。

そこで当社は，乱数の質と回路規模のトレードオフを破り，乱数の質と回路の小型化の両方を満たすようにSiN MOSFETを乱数生成源として用いた乱数生成装置を開発した。

物理乱数として従来用いられている熱雑音は，前述のとおりノイズ信号が小さいために，信号を増幅させる大きな増幅回路

を必要とする。しかし，大きなノイズを生成できれば，増幅回路が必要なくなり回路規模の縮小につながる。そのため，ノイズ生成源は，強いノイズ信号を生成できることが重要となる。

3　素子の特性

2章では，大きなランダムノイズを発生させることが，乱数生成装置の回路規模を小さくするのに有効であることを述べた。

今回，当社がノイズ生成源として開発したSiN MOSFETは，Siトランジスタに付随するナノスケールでの物理現象で見られる揺らぎや不確定性を利用し，増幅回路なしで乱数を作り出すことができる。

ここでは，より大きなランダムノイズを得るためのコンセプトと，SiN MOSFETのノイズ源としての特性について述べる。

3.1　ノイズ源素子のノイズ生成のコンセプト

大きなランダムノイズを発生させるノイズ源として，多くの局在トラップを保有する狭チャネルMOSFETを用いることを提案する。キャリア（電子）は，熱揺らぎによってSiチャネルと局在トラップ間を出入りし，ドレイン電流にノイズが発生する。更にチャネル幅を狭めることで，一つの電子の出入りが与えるドレイン電流への影響が大きくなり，ノイズ強度が増大する。このように大きなランダムノイズを生成することによって，生成回路の小型化を可能にする。そして，このようなSiチャネルとトラップ間の確率的トンネル過程という物理現象を利用することで，高い乱数の質を実現する。更に，多量のトラップを含み，薄いトンネル絶縁膜を使用することで，電子の出入りが頻繁になり，より高速なノイズが発生する。

このようにして得られたドレイン電流のランダムノイズを，乱数変換回路を通してデジタル乱数化することで，乱数を生成する。

3.2　SiN MOSFETの素子構造

SiN MOSFETの素子構造とチャネルコンセプトを**図1**に示す。基本的な構造はフローティングゲート型FETと同じで，ソース，ドレイン，及びゲート電極を持ち，ゲート絶縁膜上に通常のSiN膜（Si_3N_4）よりもSiを過剰に含む非化学量論的SiN膜を形成する。Siを多く含むSiN膜とすることで，SiN膜中にはトラップとなるダングリングボンドが原子数オーダーで多量に含まれる。ドレイン電流（I_D）揺らぎは，Siチャネルとダングリングボンド間で電子の捕獲と放出がランダムに起こることで生じる。更に，1 nm以下の薄いトンネル絶縁膜を使用することで，高速なノイズ発生を可能にする。

3.3　SiN MOSFETの特性

当社は，これまでにもICカードやモバイル機器への利用が可能な小型乱数生成装置の開発を行ってきた[1]。なかでも，Siドット群をトラップ層に用いた乱数生成素子SiドットMOSFETは，3.1節で示したコンセプトの下に作成したSiN MOSFET素子の前身のノイズ源素子である[2), (3)]。**図2**は，SiN MOSFET，SiドットMOSFET，及びトンネル絶縁膜だけでトラップを持たない通常のMOSFETのI_D揺らぎを比較したものである。ここで，SiドットMOSFETは，トラップとなるSiドットの密度がもっとも高い（粒径10 nmに対し，面密度$1.0\times10^{12}\,cm^{-2} = 1/(10\,nm)^2$）素子を使用した。しかし，図から明らかなように，SiN MOSFETのほうが大きなI_D揺らぎを発生させることがわかる。これは，SiドットMOSFETと比べ，ノイズの原因となるトラップが格段に多いため，より頻繁

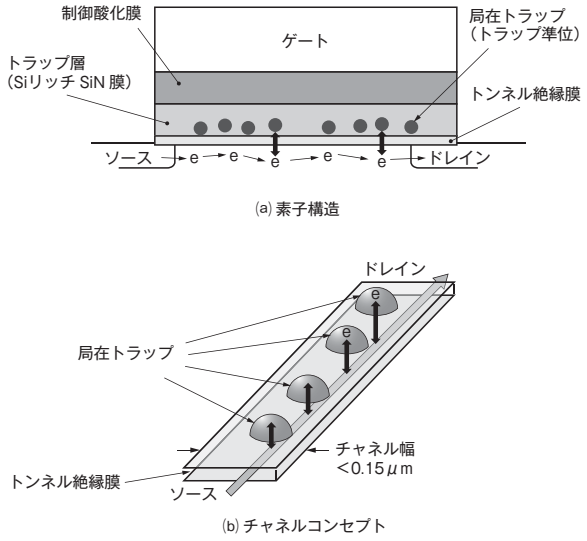


図1．SiN MOSFETの素子構造とチャネルコンセプト — Siチャネルとトラップ間での電子の捕獲／放出により，ドレイン電流に揺らぎが発生する。チャネル幅を狭くすることで，1個のキャリアの出入りがI_D揺らぎに与える影響が大きくなる。

Device structure (a) and channel concept (b) of SiN MOSFET

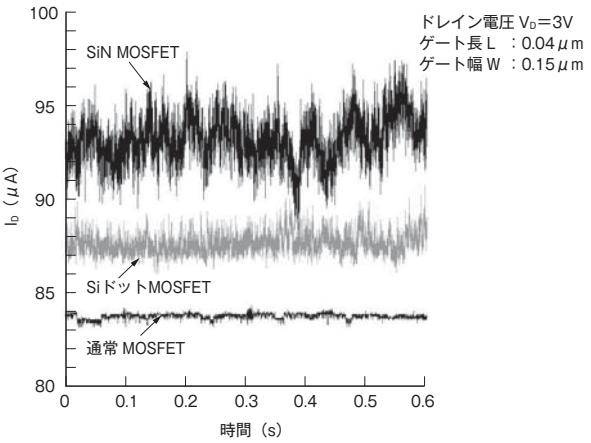


図2．ドレイン電流（I_D）揺らぎ特性 — 今回開発したSiN MOSFETのI_D揺らぎのほうが，SiドットMOSFETよりも約3倍大きな揺らぎを持つことがわかる。

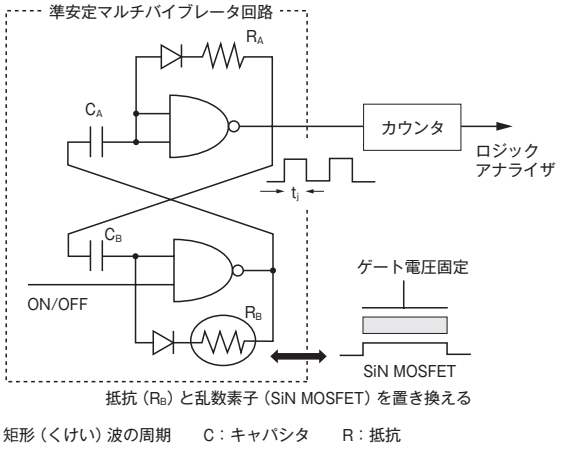
Fluctuation of drain current

にSiチャネルとトラップ間の電子の捕獲と放出が起こることから，大きなノイズ生成が可能になったと考えられる。I_D揺らぎの大きさは，$I_D = 100\,\mu A$に対して約6％の揺らぎ成分を持ち，トラップ層を持たない通常MOSFETの揺らぎ成分が約0.3％であることと比べると，かなり大きいことがわかる。

SiN MOSFETのI_D揺らぎにおいて，ゲート長L，ゲート幅W，トンネル酸化膜厚Tox，Si/N原子数比率の四つのパラメータは重要な要素であり，これらのパラメータ設計によって，より大きなランダムノイズの生成が可能になる。I_D揺らぎの大きさを示すフーリエ係数の比較から，I_D揺らぎの大きさはゲート長Lに反比例し，ゲート幅Wに対しては$W^{-0.4}$に比例することがわかった。更に，トンネル絶縁膜が薄いほど指数関数的に揺らぎが大きくなり，トラップを含む非化学量論的SiN膜中の原子数比率Si/Nは，1に近いほどI_D揺らぎが大きくなることがわかった。

4　乱数変換回路

乱数変換回路を**図3**に示す。SiN MOSFETから得られるランダムな揺らぎ成分をデジタル乱数に変換するために，発振回路であるマルチバイブレータ回路にSiN MOSFETを組み入れることで，0又は1に変換するという方法を用いた。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の非常に小型な回路構成である。マルチバイブレータの発振周期は，回路を構成する抵抗とキャパシタによって決まるので，抵抗（R_B）をSiN MOSFETに置き換え，ランダムに変化する抵抗とみなすことで，その周期はランダムに揺らぐ。この揺らいでいる周期の一つ一つをカウンタで1ビット化することで，乱数列を得た。この周期の揺らぎの大きさは，生成される乱数の質に大きく影響する。バイアス条件を調節することで，適当なI_D揺らぎとなる状態にすれば，高速な乱数生成ができるようになり，0.3Mビット/sの生成レートで，高度な統計検定試験に合格する真性度の高い乱数生成が可能になった。



t_j：矩形（くけい）波の周期　　C：キャパシタ　　R：抵抗

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。

Random number generator circuit

5　生成乱数の検定評価

すべての情報セキュリティにかかわるツールでもっとも重要な点の一つとして，使用する乱数が安全なものであること，すなわち，高いセキュリティを保てるものであることが大前提となる。物理乱数が予測不可能な現象を用いて生成されたものであっても，それが常に安全な乱数を生成しているかどうかを確かめる必要がある。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[4]。

SiN MOSFETを用いた乱数生成回路で生成した乱数列の，FIPS140-2による検定結果を**表1**に示す。比較のために，SiドットMOSFETを用いて生成した乱数と，通常のMOSFETを用いて生成した乱数の検定結果も示している。検定に用いた乱数は，それぞれ生成速度0.3MHzで生成した。表1から，すべての検定項目で合格したものはSiN MOSFETだけである。

表1．0.3Mビット/sで生成された乱数列の統計試験結果

Results of standard statistical tests

検定項目	合格必要条件	SiN MOSFET		Siドット MOSFET		通常 MOSFET	
Monobit	9725-10275	9795	○	10175	○	10030	○
Poker test	2.16-46.17	30.9184	○	531.4944	×	12978.336	×
Long run test “0”	1.0-26	12	○	13	○	6	○
Long run test “1”		15	○	10	○	6	○
Length of run 1 “0”	2315-2685	2319	○	2250	×	7537	×
Length of run 1 “1”		2416	○	2097	×	7495	×
Length of run 2 “0”	1114-1386	1218	○	1946	×	1055	×
Length of run 2 “1”		1231	○	1993	×	1085	×
Length of run 3 “0”	527-723	629	○	645	○	62	×
Length of run 3 “1”		597	○	695	○	72	×
Length of run 4 “0”	240-384	350	○	217	×	19	×
Length of run 4 “1”		306	○	266	○	22	×
Length of run 5 “0”	103-209	156	○	98	×	7	×
Length of run 5 “1”		171	○	93	×	5	×
Length of run 6 “0”	103-209	198	○	57	×	4	×
Length of run 6 “1”		149	○	69	×	6	×

また，**図4**は，乱数列を8ビットずつに区切って，前後の相関をプロットしたものである。乱数列が一様であるほど均等かつ密に点がグラフを埋める。(a)はSiN MOSFET，(b)はSiドットMOSFET，(c)は通常のMOSFETを用いた乱数生成回路で生成した乱数の結果である。(a)は規則性を持たない乱数

列となっていることがわかる。一方，(b)はやや格子状の規則性が見られ，(c)はプロットが一部にしか見られず，はっきりとした規則性が見られる。これより，SiN MOSFETは規則性のない高品質な乱数であることがわかる。

SiドットMOSFETを用いてこれらの検定に合格する乱数列を生成するには，生成レートは0.12 Mビット/sが最速であった。乱数源をSiN MOSFETにすることで，生成レートはSiドットMOSFETに比べ2倍以上上回り，汎用性の高い1 MHzオーダーに大きく近づいた。

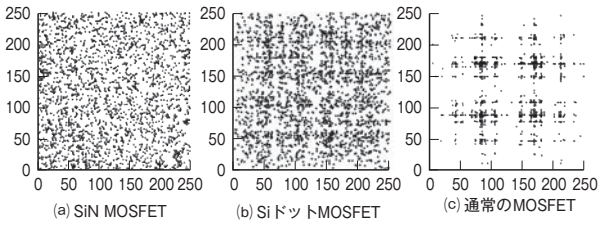


図4．乱数の相関性の比較 ― (a)のSiN MOSFETを用いて生成した乱数は，相関性は見られないが，(b)のSiドットMOSFET及び(c)の通常のMOSFETで生成した乱数では相関性が見られる。

Comparison of correlations among random numbers

6　更なる高速化に向けた指針

乱数を高速に生成するためには，高周波成分のノイズを増大させることが有効である。まずは，ゲート長などの素子の設計パラメータを見直すことが効果的であり，例えば，絶縁膜の膜厚はトンネル抵抗に指数関数的に依存することから，現行のトンネル絶縁膜であるSi酸化膜よりバリア高の低いトンネル絶縁膜にすることで，回路の更なる小型化に有効な，より大きな揺らぎを得られる。また，マルチバイブレータに限らず，乱数変換回路の改良も必要である。

7　あとがき

当社は，真性度の高い乱数を高速生成できる小型の乱数生成回路の実現を目的とし，乱数源となるSiN MOSFET素子の開発を行った。従来使用されている物理乱数の乱数源と比べ，非常に大きなランダムノイズが生成でき，真性度の高い高速乱数生成ができる。乱数源となる素子は，ナノテクノロジーの進歩につれて，ノイズ信号のよりいっそうの増幅と乱数生成速度のより高速化が期待できる。

今後は更に，乱数変換回路の改良も含めて，より厳しいセキュリティ基準に対応できるような乱数生成回路の開発を進めていく。

謝　辞

SiN MOSFETを用い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た“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) 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.
(2) 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.
(3) 棚本哲史，ほか．超小型乱数発生素子．東芝レビュー．61，2，2006，p.15－18.
(4) National Institute of Standard Technology. FIPS PUB 140-2 Security Requirements for Cryptographic Modules. May 25, 2001, p.61.

松本　麻里　MATSUMOTO Mari
研究開発センター　LSI基盤技術ラボラトリー。
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。
応用物理学会会員。
Advanced LSI Technology Lab.

牛島　知巳　USHIJIMA Tomomi
セミコンダクター社　システムLSI事業部　通信・映像LSI開発技術部主務。
通信システム用LSI製品の開発に従事。
System LSI Div.