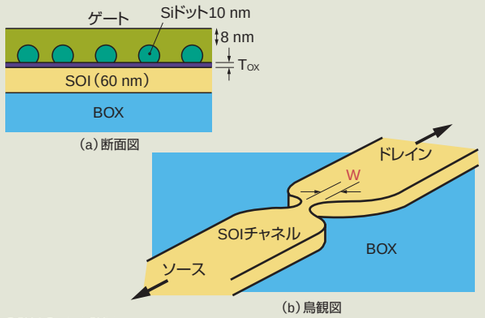
SiドットMOSFETを用いた情報セキュリティ用 高速乱数生成

ハッカーお手上げの新セキュリティ技術

近年，ネットワークにおける情報保護がますます重要視されています。強固な情報セキュリティのためには予測不能な暗号が求められ，高度な乱数生成回路が威力を発揮する場面が増えています。高度という意味は，生成した乱数列が周期性や再現性を持たない，真性度が高いものであることを意味しています。特に，モバイル機器でのネットワーク情報保護では，乱数生成回路は真性乱数の生成に加えて，小型であること，高速で生成できることも要望されます。

今回，新たな小型乱数生成源として，狭チャネルSi（シリコン）ドットMOSFET（金属酸化物半導体型電界効果トランジスタ）を提案し，高速で真性乱数を生成することを示します。これにより，小型で高速の真性乱数生成回路ができると期待されます。



BOX：Buried OXide

図1．素子構造 ― SOI基板上にSiドットMOSFETを作製する。SOIチャネル中央部には真ん中付近に幅の狭い箇所がある。

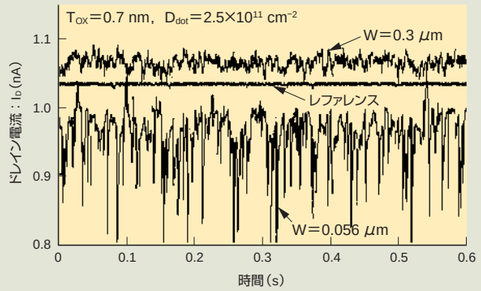


図2．I_D揺らぎのW存在性 ― SiドットMOSFETはレファレンスMOSFETより強いI_D揺らぎが出る。また，I_D揺らぎはWが狭いほど強くなる。

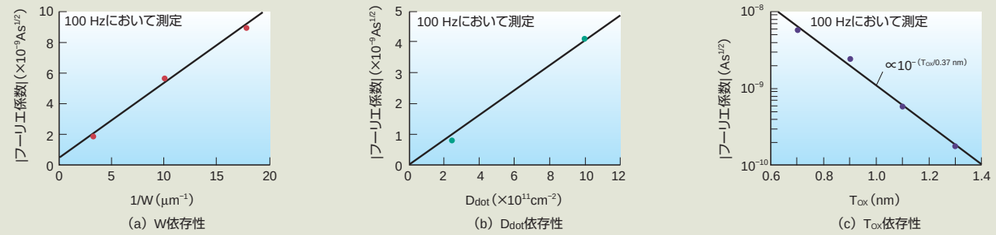


図3．フーリエ係数のW，D_{dot}，T_{OX}依存性 ― フーリエ係数はWに反比例し，D_{dot}に比例する。また，T_{OX}には指数関数的に依存する。

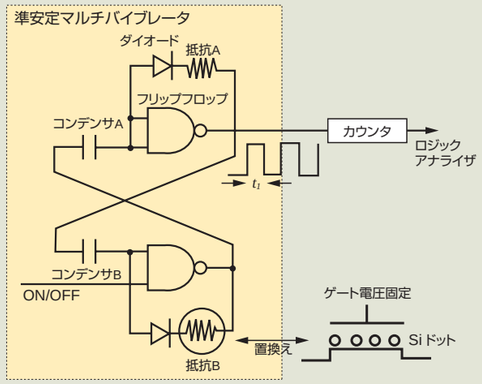


図4．乱数生成回路 ― 準安定なマルチバイブレータ回路で発振し，カウンタによりデジタル化することで乱数列化を行う。用いた素子はT_{OX}=0.7 nm，W=0.1 μm，D_{dot}= 2.5×10^11 cm^-2のものです。

表1．25 kbpsで生成された2万ビット乱数例の統計試験結果

試験項目		真性乱数のための要求	SiドットMOSFET		レファレンスMOSFET	
monobit		9,725−10,275	9-853	○	10,582	×
Poker test		2.16−46.17	29.3184	○	662.4832	×
Long run test	“0”	1−26	13	○	11	○
	“1”		16	○	15	○
Length of run 1	“0”	2,315−2,685	2,373	○	3,804	×
	“1”		2,393	○	3,523	×
Length of run 2	“0”	1,114−1,386	1,179	○	1,242	○
	“1”		1,204	○	1,225	○
Length of run 3	“0”	527−723	633	○	528	○
	“1”		639	○	611	○
Length of run 4	“0”	240−384	312	○	217	×
	“1”		300	○	288	○
Length of run 5	“0”	103−209	167	○	60	×
	“1”		178	○	119	○
Length of run 6＋	“0”	103−209	197	○	54	×
	“1”		147	○	139	○

＊monobit：0の総数　Poker test：無作為度試験
Long run test：0又は1の最長連続ビット数
Length of run N：0又は1がN回連続して出現する回数

高速真性乱数生成とは

ネットワークセキュリティのためには絶対的に予測できないデータ列を使う必要があり，そのためには乱数生成（Random Number Generator：RNG）素子が重要となります。モバイル機器へ搭載するためにはRNGは小型化が必要ですが，現在のRNGは非常に大きな回路となっているため，セキュリティが不十分な擬似乱数を用いて小型化を実現しています。また，RNGの乱数生成速度が速いほうがより広い用途へ適用されるので，高速な生成レートも重要な要素となります。小型で真性乱数を高速生成できるRNGが，現在強く望まれています。

ここでは，新たなRNG素子として，狭チャネルSiドットMOSFETを提案します。簡単なデジタル化回路を用いて，真性乱数を25 kbpsの速度で生成できます。更に高速生成するための素子設計指針も示します。この新RNG素子により，小型で高速の真性乱数生成ができるようになります。

実　験

SiドットMOSFETはSOI（Silicon On Insulator）ウェーハ上に作製し（**図1**(a)），トンネル酸化膜厚（T_{OX}）は1 nm以下の薄いものを形成しました。SOIチャネルには真ん中付近に幅（W）が0.1 μm程度の狭い部分（狭チャネル）があります(図1(b))。Siドットは粒径10 nm程度のSiのナノ微小結晶で，その面密度（D_{dot}）は2.5×10^11 cm^-2程度です。比較のため，Siドットがない参照用（レファレンス）MOSFETも作製しました。

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ます。I_D揺らぎは，チャネル−Siドット間の電子の出入により起こるので，W，T_{OX}，D_{dot}の三つが重要なパラメータとなります。

実験結果と考察

図2は，I_D揺らぎのW依存性を示すものです。Siドットのないレファレンスでは，ほとんど揺らぎが観察されません。Wが狭いものほど揺らぎは強くなります。揺らぎの強さを示すフーリエ係数の比較から，揺らぎの強さはWに反比例することがわかります（**図3**(a)）。

D_{dot}が大きいほどI_D揺らぎは強くなると考えられます。図3(b)は，実測で得られたI_D揺らぎのフーリエ係数のD_{dot}依存性ですが，ほぼ比例して揺らぎが強まることがわかります。

T_{OX}が薄いほどI_D揺らぎは強くなると考えられます。実測で得られた結果によると，揺らぎの強度は，図3(c)に示すようにT_{OX}に指数関数的に依存して，薄いほど揺らぎが強まることがわかります。これはトンネル抵抗が，T_{OX}に指数関数的に依存するためと考えられます。以上の依存則に従って，Wを狭く，D_{dot}を大きく，T_{OX}を薄くすることで，揺らぎの強さの設計ができます。

高速乱数生成

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に変換すれば生成されます（**図4**）。

バイアス条件を調節することで，適当なI_D揺らぎ状態にすれば，高速な乱数生成ができるようになり，25 kbps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できます（**表1**）。

更なる高速化のための指針

真性乱数を更に高速で生成するには，Wを更に狭くして，D_{dot}を更に大きくしてやれば，Wに反比例し，D_{dot}に比例して高速化できます。また，現行のSi酸化膜よりもトンネルバリア高の低い薄膜絶縁体をトンネル膜にしてやれば，トンネル抵抗はバリア高にも指数関数的に依存することから，揺らぎもまだまだ指数関数的に強めることができると考えられます。

新セキュリティ技術へ向けて

新たに提案した小型RNG素子のSiドットMOSFETでは，25 kbpsのレートで真性乱数を生成でき，真性乱数の更なる高速生成にも，十分な余地が残されています。この新RNG素子により，小型で高速の真性乱数生成ができるようになります。

大場　竜二
研究開発センター
LSI基盤技術ラボラトリー研究主務