SiN MOSFETを用いた乱数生成素子の長寿命化技術

使用法の工夫で高い安全性と長期信頼性を備えた乱数生成回路を実現

乱数は，セキュリティ技術の信頼性を決める暗号化技術の要です。これまでモバイル機器やICカードでは擬似乱数を用いてきましたが，近年，より高度なセキュリティ環境を構築するために，再現が不可能な物理現象を利用して生成する真性乱数の必要性が高まっています。

これまで東芝は，SiN膜（シリコン窒化膜）を蓄積層とするMOSFET（金属酸化膜半導体型電界効果トランジスタ）をノイズ源素子とした物理乱数生成回路を開発し，高い安全性を持つ乱数生成回路を実現してきました。更に，今回ノイズ特性の経年変化を抑制するメカニズムを解明して，10年間の長期使用に耐えうる素子動作技術を開発しました。

安全性の高い乱数

銀行取引などが携帯電話を用いて気軽にできるようになった一方，セキュリティに関する問題も近年多く発生しています。このため，どんなときでも高いセキュリティレベルを維持できることが，ネットセキュリティでの最重要事項です。従来，モバイル機器では擬似乱数が多く利用されていますが，近年，乱数の基準は厳しくなる傾向にあり，より安全性の高い物理乱数が必要になってきました。

しかし物理乱数生成回路には，回路規模の拡大や性能のばらつきなどの課題があります。性能のばらつきはセキュリティの穴となり，ハッカーなどの標的となります。東芝がノイズ源として開発したSiN MOSFET[(1)]は，従来のトランジスタと異なり，多量のトラップを内蔵し，かつ，高い頻度で捕獲と放出を繰り返すため，長期信頼性の確保が課題となっていました。

乱数生成の仕組み

SiN MOSFETの基本構造はフローティングゲート型FETと同様で，ゲート絶縁膜上に通常のSiN膜（Si_3N_4）よりも過剰にSiを含む非化学量論的SiN膜を用いることにより，膜中のダングリングボンドがトラップとして働きます。直接トンネル効果によって，Siチャネルとダングリングボンド間でキャリア（e：電子）の捕獲と放出が高速かつランダムに起こり，ドレイン電流（I_D）にノイズが生じます（**図1**）。このI_Dのランダムノイズを乱数変換回路でデジタル変換して，乱数を生成します。擬似乱数では生成できない予測不可能性を持つ乱数が得られ，安全性の高い乱数を高速生成することが可能なことから，モバイル機器に最適な小型回路を実現できます。

I_Dの経年変化と乱数の質

SiN MOSFETは，トラップとなる欠陥がSiN膜中に多量に含まれ，かつ欠陥が高い頻度で発生するため，一定電圧を印加し続けた場合，I_Dはランダムな揺らぎを持ちながら，素子のしきい値が経年変化します（**図2**）。乱数変換回路で“1”又は“0”に振り分ける基準値からI_Dが大きく外れると，1と0の発生頻度のバランスが崩れ，生成される乱数の質を劣化させるおそれがあります。そこで当社は，経年変化を抑制するため，素子を断続的に使用する技術を開発しました。素子はどのタイミングでもオンとオフができ，用途に応じて自由に変更できるという特長があります。

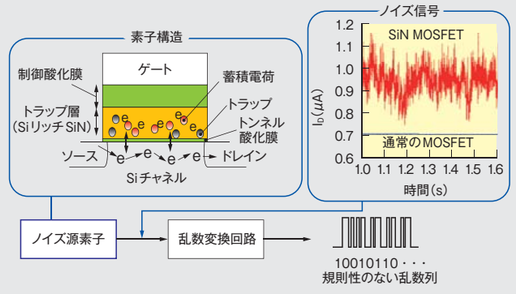


図1．乱数生成の仕組み — ノイズ源素子のSiN MOSFETで生成されたノイズ信号を乱数変換回路でデジタル化します。

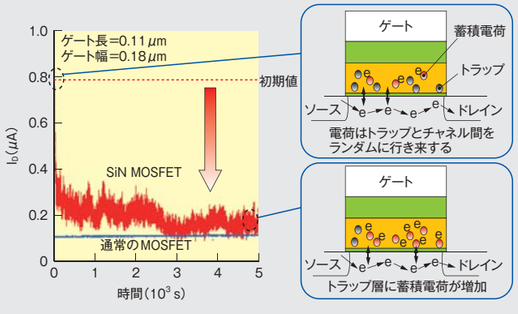
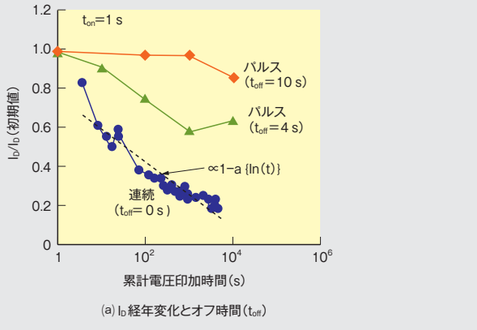


図2．I_Dと素子中トラップの経年変化 — トラップ層に電荷が蓄積することで，しきい値がシフトし，I_Dが時間とともに減少します。



(a) I_D経年変化とオフ時間(t_{off})

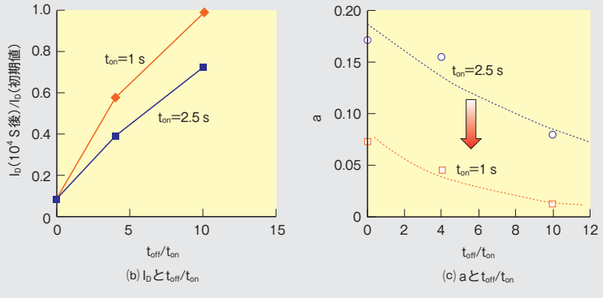


図3．経年変化によるI_Dの減少 — I_Dは時間経過とともに指数関数的に減少します。累計動作時間が同じでもt_{on}が小さいほどI_Dの経年変化は小さくなり，aも小さくなります。

乱数の使用頻度と素子寿命の関係

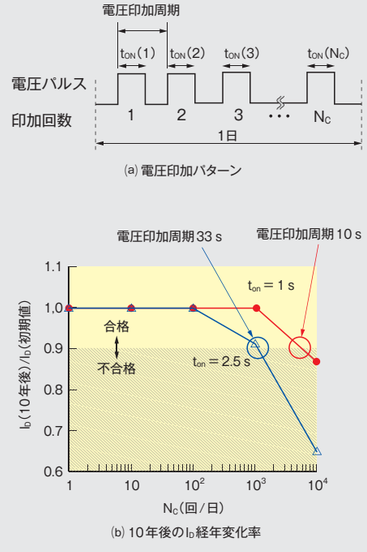
電圧印加時には，時折深い準位に電子が捕獲されて放出されにくくなるとともに，電圧印加時間が長いほど浅い準位にトラップされていた電子も深い準位に移行しやすくなり，蓄積電荷が増加します。しかし，印加電圧を適宜オフにすることで，トラップに捕獲された電子はSiチャネルへ放出され，ノイズ源素子のしきい値は初期に近い状態へ戻ります。

電圧印加周期をパラメータとして，このメカニズムによって，経年変化によるI_Dの減少レートがどのように変化するかを**図3**に示します。I_D（初期値）をI_Dの初期値，aを経年変化レートとすると，I_Dは時間（t）が経過するにつれて式(1)で示すように指数関数的に減少します。

$$(|I_D|/|I_D(\text{初期値})| = 1 - a\{\ln(t)\} \quad (1)$$

図3(b)，(c)から，1回当たりのオン時間（t_{on}）が短いほうが，累計電圧印加時間は同じであってもI_Dの経年変化は小さくなることがわかります。これは，SiN MOSFETが多量のトラップを含んでおり，長時間の電圧印加により，I_Dが対数的に減少するという特性のためです。更に解析により，各パルス周期でのI_Dの経年変化を予測した結果，1パルスのt_{on}が1 sのとき，周期10 sで10年間使用してもI_Dの経年変化は10 %以下にできることを確認しました（**図4**）。

これは，連続的に使用したときにI_Dの経年変化が90 %以上になることと比較すると，I_Dの変化を大幅に抑制できたことになります。また，I_D平均値の変化が10 %以下であれば，出力乱数に影響を及ぼすこともなく，この物理乱数生成回路を用いることにより，10年間の長期信頼性を確保することができます。



N_C：1日当たりの使用回数

図4．I_D経年変化率の電圧印加周期依存性 — 1パルスのt_{on}が1 sのとき，周期10 sで10年間使用してもI_Dの経年変化は10 %以下にできます。

今後の展望

その他には，1パルスのt_{on}が1 sより長い場合でも，オフ時間（t_{off}）を長くすることでI_Dの経年変化を軽減できます。更に，電圧を調整することでいっそうの軽減が見込まれます。これらの結果は，高い安全性と長期信頼性を兼ね備えた物理乱数生成回路の実現に大きく寄与すると期待されます。

文　献

(1) 松本麻里 他．SiリッチSiN MOSFETを用いた高速乱数生成器．東芝レビュー．62，7，2007，p.39－42.

松本　麻里
研究開発センター
LSI基盤技術ラボラトリー