管理番号＃１３－０３

平成１７年度
研究開発成果報告書

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

委託先：　㈱東芝

平成１８年４月

情報通信研究機構

平成１７年度　研究開発成果報告書

「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」

目　次

１　研究開発課題の背景

近い将来、あらゆるデジタル機器は携帯型のものを含め、ネットワークでつながる。さらに、携帯型デジタル機器は使い易さの観点から、小型化、高機能化が進んでいく。デジタル機器とそれに関わるインフラやサービスの進歩とともに、ネットワーク上での重要情報のやりとりや金融取引が行われる頻度が、急速に進んで行くと予想される。従って、ネットワーク上の情報を盗聴したり、改竄したり、他人になりすますことを防ぐ技術が重要度を増してくる。そのため現在では、情報セキュリティ技術が、暗号アルゴリズムや認証技術など、ソフトウエア中心に開発されている。今後はセキュリティをより一層高めるために、ハードウエア、特に半導体回路の暗号特有の機能強化が必要とされると考えられる。

半導体回路の中でも特に重要なのが、暗号鍵や署名付加情報やID情報の生成に欠かせない乱数生成回路である。何故なら、乱数に不可欠のランダム性は、ソフトウエアや既存の論理回路で作り出すのには限界があり、自然の物理現象からのランダム性から乱数を作り出すハードウエアが要求されるからである。また、乱数回路は、以前から重要性が叫ばれてきたにもかかわらず、情報セキュリティに関わる他のハードウエアの開発に比べてその開発が遅れている。これは、高度な乱数生成回路を作ることが相当困難であることを示している。

２　研究開発体の全体計画

２－１　研究開発課題の概要

本提案の目的は、近未来の高度な情報セキュリティに欠かせない、高品質の乱数を生成する集積回路を開発することである。情報セキュリティシステムで使われる乱数では、乱数の偏りの無さと、周期性の無さ等、乱数の質（以降「乱数の質」と称する）が重要となる。さらに、小型のデジタル機器に搭載されるシステムLSI内部に組み込む事を想定して、回路規模が極めて小さいことも求められる。現在使われている簡単な論理回路と数学的なアルゴリズムで作る擬似乱数は質が低く、将来的に十分な安全性を保てない。また、雑音等の物理的要因でランダム性が決まるような質の高い乱数を生成できる回路が開発されているが、小型化、集積回路化に壁がある。このように、現状では乱数の質向上と回路の小型化はトレードオフの関係にあり、２つの要素を同時に実現する方法は確立されていない。本提案では、乱数の質向上のために、ナノスケールの半導体デバイスの電気特性に見られる物理的な揺らぎ現象を利用する。回路を集積化するために論理回路の出力に揺らぎ現象が直接影響する回路を用いる。さらに、量子化された物理現象から得られる信号がデジタル信号であることに注目し、これをダイレクトにデジタル化して、究極の高品質乱数である真性乱数に近い乱数を生成することを目指す。（尚、本提案の乱数生成回路は、現状の暗号アルゴリズムに基づく情報セキュリティシステムに使用するもので、新しいアルゴリズムに基づく量子暗号通信技術とは異なる。）

２－２　研究開発目標

２－２－１　最終目標（平成１８年３月末）

以下の２点を同時に満たす乱数生成回路の開発と、関連する基盤技術の開拓。
（１）乱数の質向上：乱数の質について、熱雑音（またはショット雑音）から生成された物理乱数のレベルを上回る。乱数の質の評価にはギガビットオーダーの長さを持つ大規模な乱数を用いて、統計的検定で検証する。
（２）回路の小型化：標準 LSI 用の CMOS 論理ゲート換算で 1000 ゲート以下を達成する。

２－２－２　中間目標（平成１６年３月末）

（１）シミュレーションによる半導体デバイスの基本的な設計仕様の確定
　　（小型化と乱数の質向上の同時達成可能なデバイスと回路）
（２）乱数生成回路の原理検証用プロトタイプの動作確認
（３）ギガビットオーダーの大規模乱数の高速評価方法確立
　　（物理乱数との定量的比較が大規模な乱数を用いて多数回必要な為）

２－３　研究開発の年度別計画

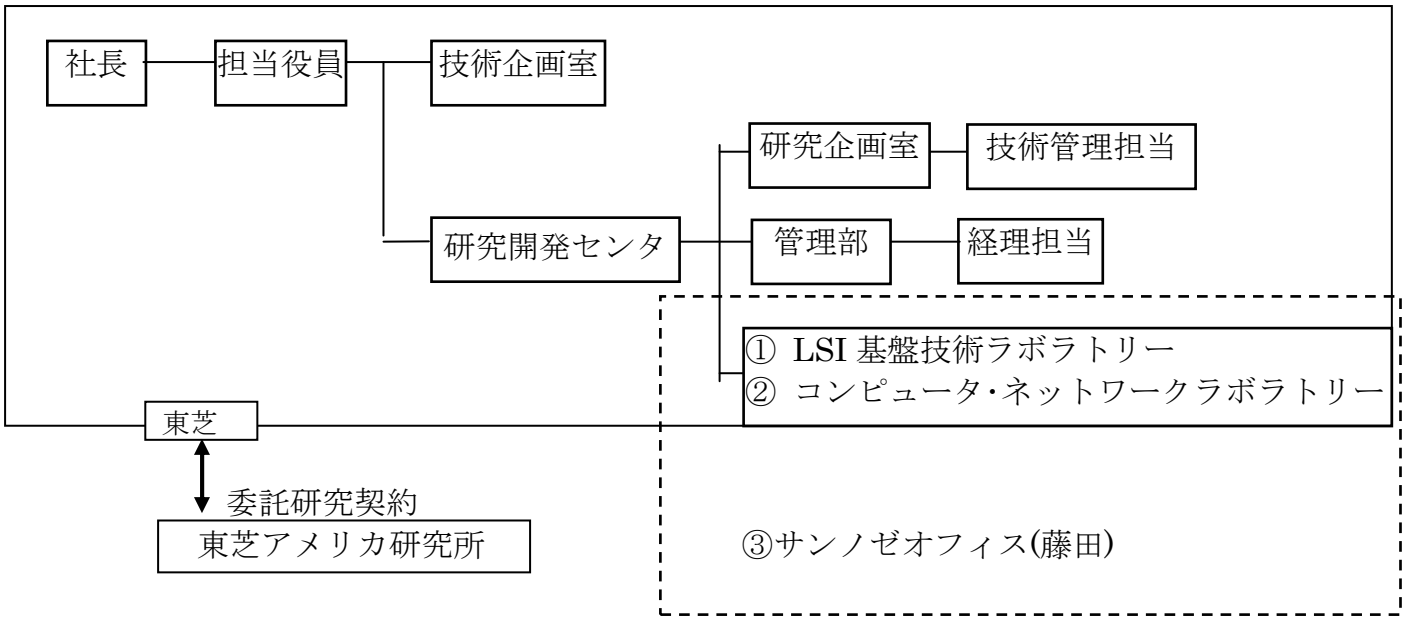
（金額は非公表）

研究開発項目	13 年度	14 年度	中間評価 15 年度	16 年度	17 年度	計	備考
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 ①デバイスシミュレーションに関わる研究開発 ②デバイス・回路試作に関わる研究開発 ③乱数評価に関わる研究開発 研究開発の方針・計画策定	→	→	→	→	→		
間接経費							
合　　計							

３　研究開発体制

３－１　研究開発実施体制

○ 研究開発管理体制



○研究開発実施体制

研究代表者
棚本　哲史
研究主務①

（１）デバイスシミュレーション担当
棚本　哲史　研究主務（主担当、研究代表者兼務）①

（２）デバイス・回路試作担当
大場　竜二　研究主務（主担当）①
安田　心一　研究員①
安部　恵子　研究員①
松本　麻里　研究員①
藤田　忍　　研究主幹③

（３）乱数評価担当
野崎　華恵　研究主務②（主担当）
棚本　哲史　研究主務①
藤田　忍　　研究主幹③

但し①LSI 基盤技術ラボラトリー
②コンピュータ･ネットワークラボラトリー
③東芝アメリカ研究所サンノゼオフィス

4　研究開発実施状況

下図に乱数生成集積回路の構成部品（１つのデバイスと３つの回路）と、対応する研究の分担（①～③）を示す。高度な真性乱数生成回路では理想的なランダム性、すなわち一様性を持つことと、周期性・規則性がないことが求められる。乱数生成回路の心臓部にあたる物理揺らぎ信号の発生源である乱数源デバイスから出たランダム信号（アナログ信号）をデジタル変換回路でデジタル信号に変換すると、単純にはデジタル乱数が得られることになる。しかし、実際には乱数源の物理揺らぎが、理想的な揺らぎ分布からずれている場合や、デジタル変換回路において一様性と非周期性が損なわれる場合が多いので、これを補正するために、一様性補正回路と周期性・規則性補正回路が必要となる。最終目標には、乱数源デバイスから周期性・規則性補正回路までの全てをシステム LSI の一部に内蔵できるような小型の LSI を作ることをあげている。

これを達成するために、①～③の３つのパートでの研究開発を進める。1 番目は乱数源デバイスのシミュレーション、２番目は乱数源デバイスと後段のデジタル回路部の試作とその評価、３番目は得られた乱数の質の高さ(真性度)を調べることである。

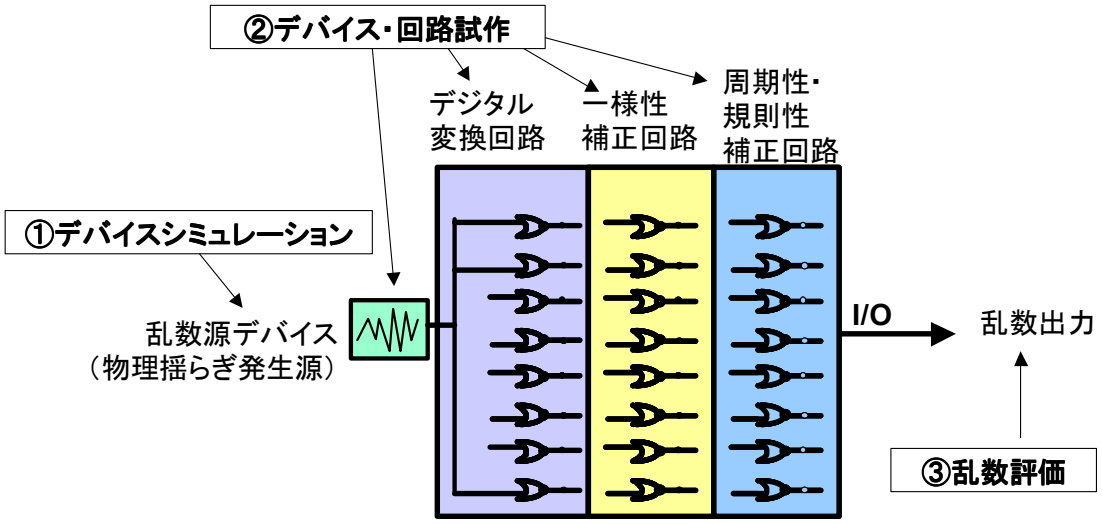


図 4-0：本計画の概要

一番重要な構成部品は、乱数生成回路の心臓部にあたる乱数源デバイスである。この開発に全体の 50%以上のリソースを投入する必要がある。まずは、ナノスケールのシリコンデバイスに見られる様々な物理的揺らぎ信号のうち、乱数源として有効なものはどれかをシミュレーションと実験との両面から選定することが必要である。平成 13 年度（平成 14 年 1 月 16 日）から平成 15 年度にかけて、この選定を行ってきて、高度な乱数を発生するための乱数源デバイスをいくつか試作し、高品質の乱数発生を実証してきた。

平成 17 年度は、②のデバイス・回路試作と、③の乱数評価に重点をおく。②のデバイスでは平成 16 年度までの研究成果を元に、候補となるデバイスを絞って開発し、そのデバイスの特性に適した乱数化回路を開発する。③の乱数の評価については、特に不正攻撃に対するセキュリティ強度という観点からの評価に重点をおきながら研究を進める。

シミュレーション、乱数源デバイス・回路の実験、乱数評価の３つのパートについて、具体的な成果を以下に記す。

４－１　デバイスシミュレーションに関わる研究開発

４－１－１　序論

全般を通して、乱数源デバイスを簡素化して、電子チャネルと、近接する単一または複数のトラップ準位（量子ドット）との間を電子がトンネリングして揺らぎを生じるというモデルの解析とまた汎用シミュレータを利用したノイズの解析を行った。

平成 13 年度、平成 14 年度は乱数源となるトラップ準位（量子ドット）が伝導チャネルの近くに存在する場合のノイズの性質を物理モデルに基づいて解析した。そしてノイズスペクトルなどを導出した。

平成 15 年度は、汎用のデバイスシミュレータを用いて、伝導チャネルの近辺に存在する量子ドットをフローティングゲートとみなして、書き込み/読み出し特性について計算した。また物理モデルを発展させて Green 関数を用いた電流の解析を行った。

平成 16 年度は、前年度までに定式化してモデルを用いて、トラップ準位のある場合の効果を電気伝導度の特性を中心に調べた。

平成 17 年度はデバイス開発で集中的に行っている SiN 乱数素子のシミュレーションを行い、実験的に得られたデータとの対応について検討した。

４－１－２　研究の実施状況

(平成 13, 14 年度)

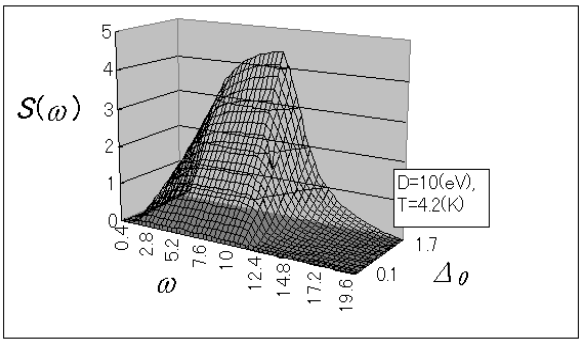
トラップ準位のノイズスペクトルの計算

シリコンの量子ドット（量子効果を示す微結晶）を内包するシリコンデバイスは、乱数源デバイスの有力候補である。また、シリコンデバイスのチャネル近辺の電気的不純物準位は通常のデバイスにとっては有害な雑音の原因の一つと考えられている。今回、伝導チャネルのそばに位置し、伝導チャネルと電子がトンネリングで行き来できるトラップ準位を一つ設けたモデルと多数設けたモデルを考え、そのノイズ特性をノイズパワースペクトラムから計算することにより調べた。この際、準位は量子ドットとしても不純物準位としてもみなすことができるものと考えられる。トラップ準位には上向きスピンと下向きスピンの両方が入ることができるが、電子間にはクーロン相互作用が働くために、一つの電子が入った場合に、二つ目の電子が同じ準位に入ろうとするとクーロン力分のエネルギーが上昇する。この状況は理論的にはアンダーソンハミルトニアンで記述できる。しかしながら、このモデルの解は一般的にはかなり複雑で扱いにくい。そこで我々は上記のクーロン力が十分大きく、トラップ準位に電子は一つしか入らないとした状況をスレーブボソンという演算子を用いて表し、さらにこのモデルを平均場理論の枠内で解いた。平均場を用いることで、ハミルトニアンは対角化でき、ノイズパワースペクトラムを解析的に導出できる。

ここでは Coleman boson b を導入した slave-boson 平均場理論を用いる(Coleman(1983))とハミルトニアンは以下のようになる：

$$H = H_{\text{band}} + \sum_m E_D f_m^+ f_m + V \sum_{km} \left(f_m^+ c_{km} b + \text{H.c.} \right)$$

ここで H_{band} がチャネル電流： $H_{\text{band}} = \sum_{km} E_k c_{km}^+ c_{km}$ 、E_D がトラップ準位のエネルギー、V がトラップ準位へのトンネル結合の強さを表す。b はスレーブボソンであり平均場を仮定し、自己無撞着方程式が導かれる。平均場を用いたハミルトニアン(1)は対角化でき、電流及びノイズパワーが計算できる。今回はじめてノイズパワーの表式を導いた。そして数値計算した結果が図 4-1-A-1 である。



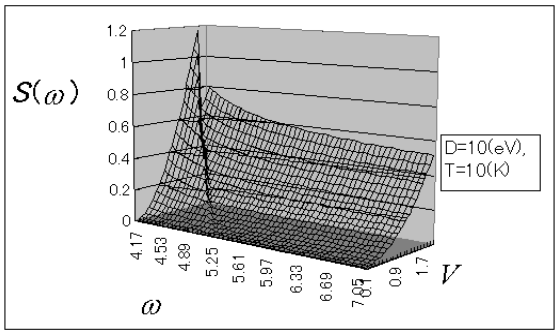


図 4-1-A-1：トラップ一つの場合のノイズスペクトル。図 4-1-A-2：多数トラップのノイズスペクトル

これよりトラップ準位と伝導チャネルとの結合が弱いうちは、ノイズパワーは平坦な構造を持つが結合が強くなるにつれて、ノイズパワーはピーク構造を持つようになることがわかる。

上記のハミルトニアンを拡張し、多数のトラップ準位がある場合について同じようにスレーブボソンの平均場を導入するとハミルトニアンは対角化できる。ノイズパワーは下記のようになる。

$$S(\omega) = \frac{\pi e^2 V^2}{2D}\left(\coth\frac{\beta\omega}{2}\right)\frac{\omega}{\sqrt{\omega^2 - 4V^2}}B(T)$$

ここで $B(T)$ はフェルミ分布関数を含む温度関数であり、絶対零度で近似的に $B(T)$ ～1 となる。この関数は $\omega \to 0$（低周波）では $S(\omega) \approx 1/\sqrt{\omega^2}$ のように振る舞い、$\omega \to \infty$（高周波）では $S(\omega) \approx 1/\omega^2$ のように振舞う。図 4-1-A-2 に示した計算結果はこの傾向を示している。

（平成 15 年度）

フローティングゲート構造のシミュレーション

平成 14 年度はソースとドレインがない、つまり電子伝導チャネルに電位差が無い平衡状態を取り扱った。これはノイズ特性を表すノイズパワースペクトルが電流の時間相関であるため、一般的な非平衡状態の取り扱いはとても煩雑で、ほとんどの場合にノイズパワーの周波数依存性までは事実上計算できないからである。しかし、伝導体にソース・ドレインをつないだ非平衡状態についての解析を進めたいと考え、平成 15 年度は、その基礎となる計算をいくつか行った。結果は平成 16 年度に引き継いだので省略する。ここでデバイスシミュレーションについて述べる。

通常使用されているデバイスシミュレータでトラップの影響をどの程度まで取り入れることができるかについて分析した。三端子素子、例えば MOS トランジスタ構造においてトラップ準位が存在する状況はトラップをフローティングゲートとしたフローティングゲートメモリ素子と構造が類似していることがわかる。今期は汎用のシミュレータにおいて、特に結合したフローティングゲート二つを下記のように MOSFET 内ゲート絶縁膜内のトラップとみなし、通常のフローティングゲート構造と比較し、その効果を調べた。

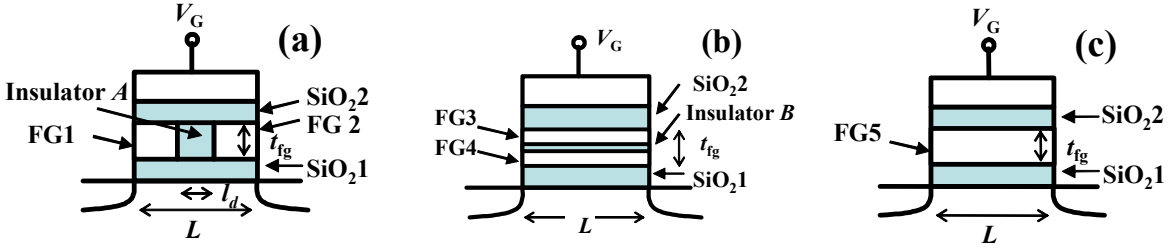


図 4-1-B-1 (a)：横型フローティングゲート(floating gate：FG)構造。FG1 と FG2 はポリシリコンを仮定。(b)：縦型 FG 構造。(c)：(a)(b)と比較するための通常の FG 構造。絶縁物 A, B は SiO_2 を含め、high-k 材料を視野に入れ、誘電率を変化させる。

ゲート長は（L=0.2μm), SiO_2 膜厚($SiO_2$1: 9x10^{-3} μm, $SiO_2$2: 6x10^{-3} μm), 二つの SiO_2 間の距離(t_{fg}=0.1 μm)はすべての構造で共通と仮定する。基盤の不純物濃度は 5x10^{17} cm^{-3}. 書き込みプロセスは起点時間(time=0)に 20V の正バイアスをゲート V_G にかけ、このとき、FG の初期電位が 1.5V から始まると仮定する。ここでは電荷の FG の保持時間そのものを現実的なデバイスパラメータで計算する代わりに、バイアスをかけて消去過程を加速した場合の FG の時間発展依存性を比較した。FG 電位がよりゆっくり変化すれば電荷の保持能力がより高いと考え、保持時間がより長いメモリ構造であると考えたのである。ここで消去過程は起点時間(time=0)で-19V の負バイアスをゲートに駆けることにする。このとき FG の電位は-1.5V にセットした。

○(a). 横型結合 FG 構造

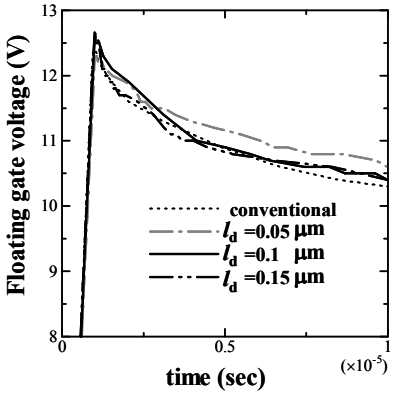


図 4-1-B-2：横型 FG 構造(図 1(a))の書き込み特性。

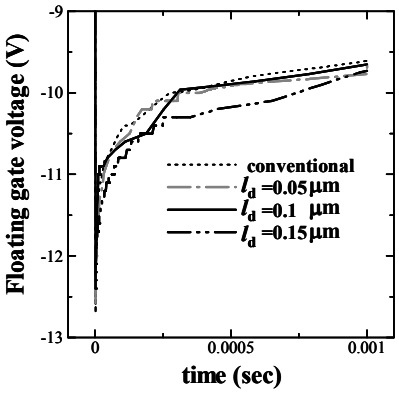


図 4-1-B-3：横型 FG 構造(図 1(a))の消去特性。

図 4-1-B-2 と図 4-1-B-3 はそれぞれ、横型 FG 構造(図 4-1-B-1(a))の書き込みと消去過程の計算結果である。書き込過程においては FG 間の距離 l_d=0.05μm の素子のみが他とは違う特性を示し、一方消去過程においては、二つの FG 間の距離が増加するについて、FG の電位が減少することを示している。そして l_d=0.15μm.素子では約 0.5V のシフトが得られる。下側の FG における電荷の保持特性がメモリ全体の特性を決めると考えられるため、以上の結果は横型結合 FG 構造においては通常の構造(図 4-1-B-1(c))よりも電荷保持時間を長くできるものと考えられる。図 4-1-B-4 は横型結合 FG 構造の電位ポテンシャルの図である。この図から挿入された絶縁体 A がデバイス内の電位分布を変化させていることがわかる。この新しい電位ポテンシャル分布が電荷蓄積をより安定なものにしているものと考えられる。さらに面白い点は二つの FG 間の距離が l_d>0.1μm の場合、FG の面積がゲートの半分以下になるにも係らず、書き込み時間があまり変化しない点である。さらに絶縁体 A の誘電率を 3.9 (SiO_2) からずらしても上記の結果に変化はないことがわかった。

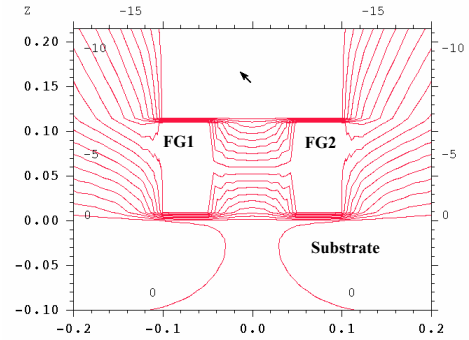


図 4-1-B-4：横型 FG 構造の電位ポテンシャル分布。l_d=0.1um の素子。

○ (b). 縦型結合 FG 構造

縦型結合 FG 構造(図 4-1-B-1(b))においては、より長い電荷保持時間が期待できる。これは上側の FG に蓄積された電荷が基盤に到達するのに二重のトンネル障壁を越えなければならないからであり、大場らの結合量子ドット構造において実験的にも確かめられている[5]。

図 4-1-B-5 と図 4-1-B-6 は絶縁体 B の誘電率を変化させたときの縦型結合 FG 構造の書き込み、消去過程を計算したものである。誘電率が大きくなるに従って、書き込み時間が増え、電荷保持特性も通常の FG 構造の特性に近づくことがわかる。誘電率ε_i=7.5(SiN)の特性がもっとも通常の FG 構造から離れており、長い電荷保持時間が期待できることがわかる。

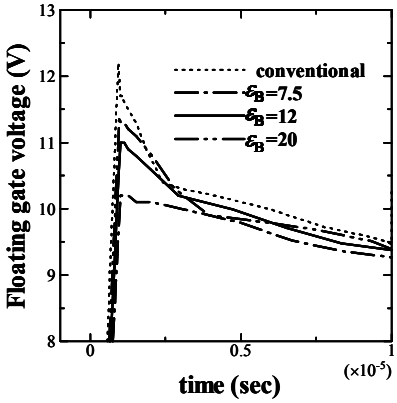


図4-1-B-5：縦型FG構造(図4-1-B-1(b))の書き込み。

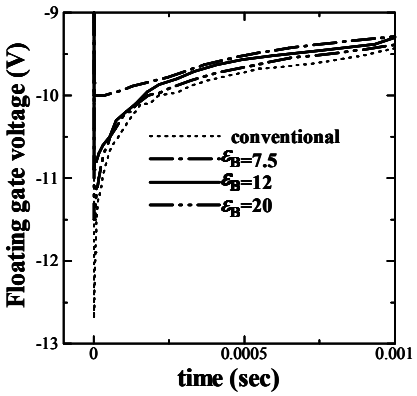


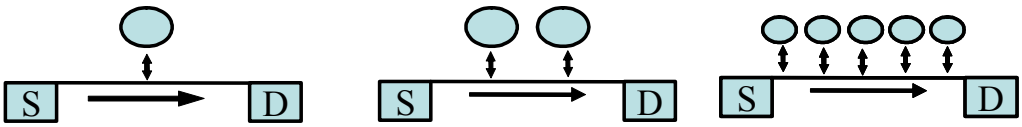
図4-1-B-6：縦型FG構造(図4-1-B-1(b))の消去特性。

(平成 16 年度)

トラップ準位の電気伝導度への効果

まず電極がない場合についてこれまで知られていることを説明する。伝導領域にトラップなどの局在準位がある場合、この局在準位の存在での電気抵抗の変化は固体物理学での重要な問題であり、近藤効果として知られている。伝導領域内に局在準位があるのか、伝導領域脇（MOSFET では絶縁膜中）に局在準位があるかで、電気伝導は異なってくる。局在トラップ準位が伝導領域内にある場合には通常の近藤効果が起こり、電気伝導度は $G=(2e^2/h)\sin^2\pi\langle n_d\rangle$ と表される。ここで$\langle n_d\rangle$はトラップされた平均電子数である。一方、伝導領域外にトラップ準位がある場合、反近藤効果が起こる事が知られていて、その電気伝導度は $G=(2e^2/h)\cos^2\pi\langle n_d\rangle$ となる。

本報告では昨年ノイズ特性のみ調べた図 4-1-C-1 の３つの場合について、特に上記の近藤効果という観点から電極がある場合の電気伝導を調べた。



(a) one trap site　　(b) two trap sites　　(c) many trap sites

図 4-1-C-1：電気伝導を計算した 3 つのトラップの配置

電気伝導度については一般化された Landauer 公式を用いた。

$$G = \frac{2e^2}{h}\int d\varepsilon \sum_{ks} \frac{\partial f(\varepsilon)}{\partial \varepsilon} \frac{\Gamma_L \Gamma_R}{\Gamma_L + \Gamma_R}(-\mathrm{Im}\, G_k^r(\varepsilon + i\delta)) \qquad (1)$$

ここで f(ε)は Fermi 分布関数、s=↓、↑はスピン自由度，Γ_L, Γ_R は伝導領域と電極との電子のトンネリング率である。これから伝導領域の Green 関数の複素数部分を求めれば、電気伝導度を得ることができる。なお、トラップ準位内クーロン相互作用が無限大として、トラップ準位内には電子は一つしか入れないと仮定する。そして Slave-boson の平均場近似を行なう。ここで D はバンド幅、$\gamma = (\Gamma_L + \Gamma_R)/2$ が電極の効果を表す。絶対零度における電気伝導度はパラメータの温度依存性を除いて下記のようになる：

$$G = \frac{4e^2}{h} \frac{\Gamma_L \Gamma_R}{(\Gamma_L + \Gamma_R)(D + \gamma)} \frac{(\varepsilon_f - E_F)^2}{(\varepsilon_f - E_F)^2 + \Delta_1^2} \qquad (2)$$

これは Fermi 付近でのトラップ準位の密度をあわせると、反近藤効果の式 $G = (2e^2/h)\cos^2 \pi \langle n_d \rangle$ を再現する。ゲートバイアス依存性の数値計算結果は図 4-1-C-2 のようになる。

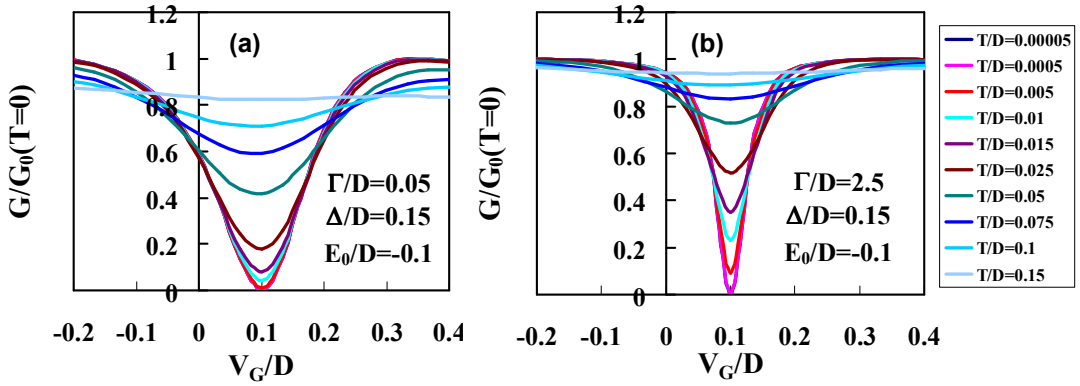


図 4-1-C-2：トラップが一つの場合のゲートバイアス依存性。(a) $\gamma < D$。(b) $\gamma > D$

まず、二つの図とも、トラップ準位のエネルギー近傍で、電気伝導度が減少することがよくわかる。これは反近藤効果における一種の干渉効果であり、伝導チャネルを直進する電荷とトラップ準位にトラップされた電荷との干渉効果が電気伝導度の減少という形で現れるのである。特に図 4-1-C-2 に示すように電極の効果が大きくなる(b)の場合には、電気伝導度の現象が抑制されることがわかる。これは電極との相互作用が強いため、電荷がトラップされないで電極間を通過する確率が大きくなる結果と考えられる。

次に図 4-1-C-1(b)に示すトラップ準位が二つの場合についてであるが、電気伝導度はその独立部分に対する式(2)と同様な式の和で表されることがわかった。

最後に図 4-1-C-1(c)で表される多数トラップがある場合の電気伝導について述べる。この場合は Hamiltonian として Anderson 格子模型を用いる。その結果得られた数値計算は図 4-1-C-2 と同じようになる。ここで別の角度からみるため、トラップ準位のエネルギー依存性を示す。

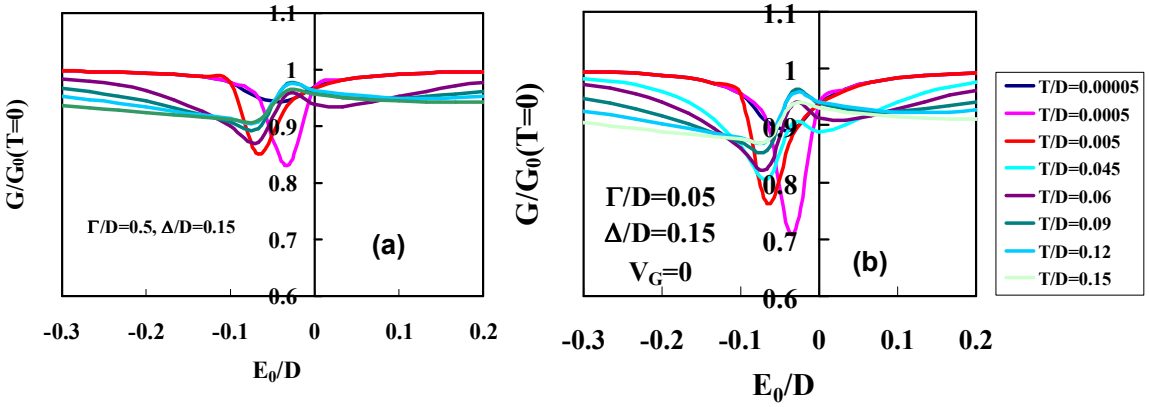


図 4-1-C-3：トラップが多数(図 1(c))場合のゲートバイアス依存性。(a) $\gamma < D$。(b) $\gamma > D$。

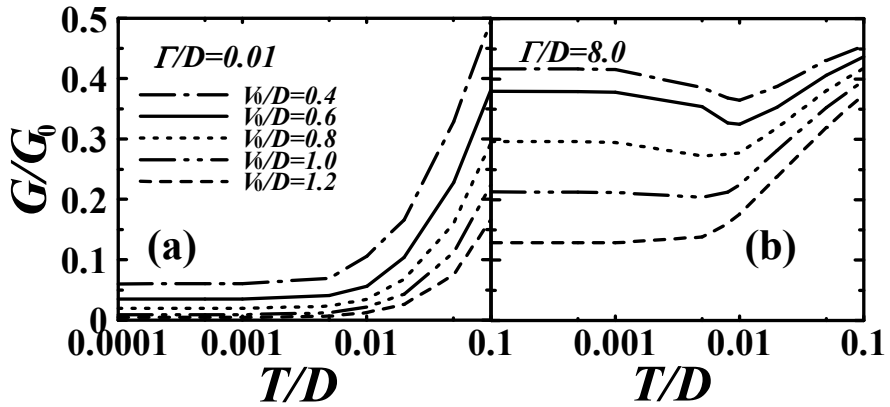


図 4-1-C-4：電気伝導度の温度依存性。V_0 はトラップと伝導体との結合の強さを表す($\Delta_1 = V_0^2/D$)。(a) $\gamma < D$。(b) $\gamma > D$ ($\gamma \propto \Gamma$)。

平成 16 年度下期においては上記のトラップの影響をさらに詳細に調べた。まず温度依存性について示したのがした図 4-1-C-4 である。図 4-1-C-4 に示したのは電気伝導度の温度依存性である。ここで電気伝導度の値は図 4-1-C-2 で電気伝導が最小となるようなゲート電圧で調べている。つまり V_0 の値によって電気伝導が最小となるゲート電圧は異なっている。電極との結合が弱い場合((a))の場合には温度が低くなるにつれて近藤効果が見えていることを示している。近藤効果はトラップ準位と伝導電子のスピン一重項を介した 2 次過程の繰り返しで起こるため、低温でコヒーレンスが増すほど顕著になると考えられる。従って、図のような温度変化が特徴的である。これに比べて(b)の電極との結合が強い場合は図(a)と違った振る舞いを示す。これは電極との相互作用が強いため、電子がトラップ準位に留まりきらない状態を示している。

また平均場のパラメータが一つのトラップ準位のときにくらべ、多数トラップのときにはバイアス依存性が大きいことも明らかにした。

(平成 17 年度)

SiN 乱数素子シミュレーション

平成 17 年度は SiN 乱数素子のシミュレーションを行った。使用したシミュレータは drift-diffusion 模型をベースに、モンテカルロ計算を行った。短い時間間隔の間にチャネルを流れる電子が SiN 膜中のトラップに捕獲、放出される確率を割り当て、乱数を振っ

て実際に捕獲または放出が起こるかを決定する。フォノンや不純物及び界面散乱についても取り込まれている。電子数の変化は再結合項にフィードバックされ、また電子密度は電流の連続の式にフィードバックされるようになっている。

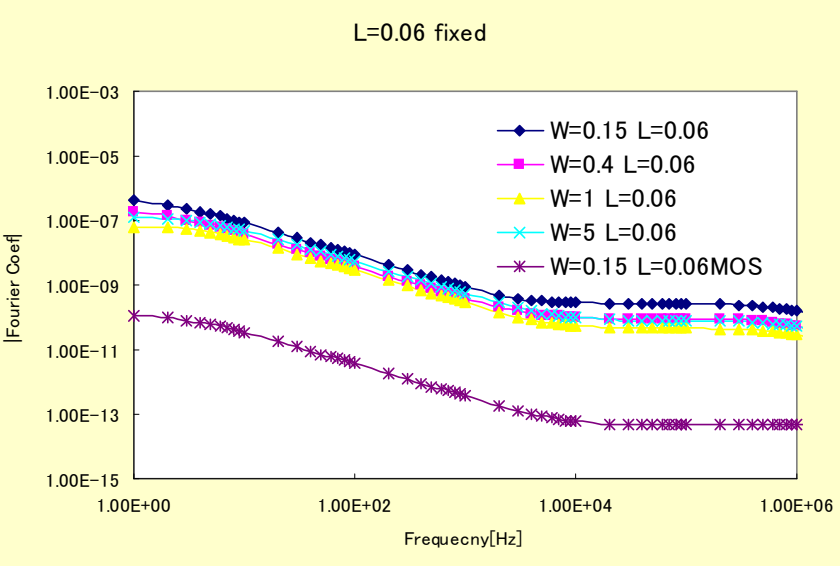


図 4-1-D-1：ゲート長を固定したときの SiN 乱数素子のノイズの大きさを示す計算例

計算結果を図に示す。基板濃度は 10^{18} 個/cm^3, ゲート電圧は５Ｖ、ドレイン電圧は４Ｖ、トラップ準位はバンドギャップの中心から±１Ｖのバンドの中に存在し、トラップの濃度は 10^{18} 個/cm^3 付近を計算した。トンネル時間は 0.1psec を仮定している。

図 4-1-D-1 ではゲート長を 0.06μm に固定し、ゲート幅を 0.15μm から５μm まで変えた場合の電流ノイズのフーリエ変換した場合の周波数依存性を示す。また参考にトラップのない MOSFET のノイズも記入してある。まず、通常の MOSFET に比べて SiN 中にトラップがあるものはノイズレベルが 1000 倍以上であることがわかる。そしてゲートの幅が狭くなるほどノイズが大きくなることがわかる。

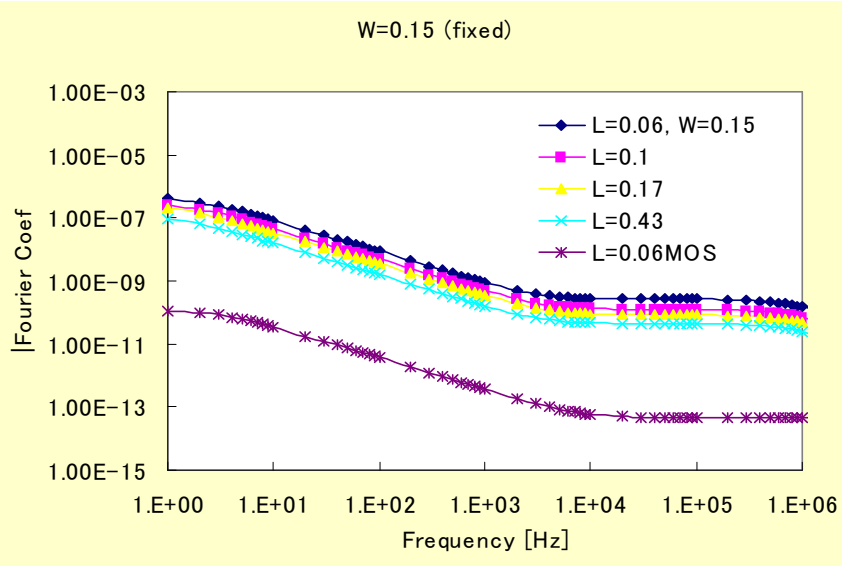


図 4-1-D-2:ゲート幅を固定したときの SiN 乱数素子のノイズの大きさを示す計算例

図 4-1-D-2 はゲート幅を 0.15μm に固定したときのノイズの大きさをフーリエ変換した場合の周波数依存性を示す。ゲート長は 0.06μm から 0.43μm まで変化させてある。図を見てわかるようにゲート長が短くなるほど、ノイズが大きくなることがわかる。

以上のようにゲート幅、もしくはゲート長を小さくすればするほどノイズが大きくなるのは、チャネル電流に対する一つ一つのトラップからの電子の捕獲と放出がより見えやすくなっているからであると考えられる。ゲート長、ゲート幅が大きいときはトラップ準位による局所的な電荷の移動が起こっても、チャネル内電子の再配置あるいはスクリーニング効果があるため、ドレイン電流に出てくる効果が小さくなると予想される。

４－１－３　まとめ

(平成 13,14 年度)

一番基本となる乱数の源として、近接した複数のシリコンの量子ドット（量子効果を示す微結晶）を内包するシリコンデバイスを考えた。この状態がデバイスの電気的特性に揺らぎをもたらすことが予想し、平成 13,14 年度は、単一の量子ドットと量子ドットから数 nm 距離に設けた電子の通過するチャネル層を考えて、チャネル層から電子が量子ドットにトンネル現象で行き来する状態のシミュレーションを行った。

(平成 15 年度)

二つの FG を縦型及び横型に結合したときのデバイス特性についてフローティングゲート型素子のシミュレータを用いて計算した。そして二つの構造ともメモリ保持特性の改善が期待されることを示した。また、二つの FG 構造の間に SiO_2 とは別の誘電率をもつ絶縁体を挿入した場合のデバイス特性についても調べ、この絶縁体が high-k 材料であればされにメモリ特性が改善されることが期待できることも示した。以上の結果は、トラップの数が少ない場合には、そのデバイス特性がトラップの数、構造により様々な影響を受けることを示している。

(平成 16 年度)

実際のデバイスに近いものとするため、電極まで入れて、電圧を加えた状態での非平衡電流について計算を行い、トラップ準位がある場合の電気伝導度について、導出した複雑な非平衡Green関数の表式を導出することに成功した。16年度はこのGreen関数を用いて、電気伝導度を解析すると同時に数値計算をすることにより、トラップ準位のある場合の効果を調べた。本研究の特徴は電極の効果まできちんと取り入れたところにある。これらにより、デバイスの揺らぎ特性と、量子ドットのエネルギー準位と、ゲート酸化膜内に多数の量子ドットを含んだ乱数生成素子の実験との比較することが概ねできるようになった。

(平成 17 年度)

社内で使用されている汎用デバイスシミュレータを用いて、SiN 膜中トラップに起因するノイズのシミュレーションを行った結果、下記に述べる実験結果と同様の傾向を計算することができた。これによりデバイスシミュレータを用いて最適なデバイスパラメータの抽出が可能となった。

４－２　デバイス・回路試作に関わる研究開発

４－２－１　序論

乱数生成回路は、デバイスの物理的な物理揺らぎ信号を用い、それを増幅し、デジタル化して乱数とするものであり、これを数百ミクロン角内に収まる回路とすることが大きな目標である。デバイス・回路の開発は、本研究開発の中核をなす、最重要テーマである。

まず**平成 13, 14 年度**は、マルチバイブレータと呼ばれるデジタル化処理部分の回路を開発した。また、特殊な絶縁膜のゲート電極から発生する物理揺らぎ信号を用いて、マルチバイブレータで、乱数を発生させるデモンストレーションも行った。また、以前に試作した量子ドットを内蔵したトランジスタ(単一電子トランジスタ)を使い、電気的特性の揺らぎを直接的に観測することも試みた。さらに、量子ドットを内蔵したランダム信号発生源のトランジスタを試作開始した。

平成 15 年度は乱数源デバイスの基礎的検討に注力した。まず、物理揺らぎの信号としての候補を選び、乱数源として適用可能かどうか実験で検討する。考えた候補は、

1)ゲート酸化膜に捕獲された電子数の変化によって生じるトランジスタのチャネル抵抗の揺らぎ
2)トランジスタチャネル抵抗が２つの抵抗値を行き来する Random Telegraph Signal(RTS)と呼ばれる現象
3)数十 nm 以下のゲート長を持つ MOS トランジスタに大きな出力として現れる 1/f 揺らぎ
4)擬似的絶縁破壊（ソフトブレークダウン）させたゲート電極に見られるリーク電流の揺らぎ

等である。1), 2)については、以前に当社で独自に試作した量子ドットを内蔵したトランジスタを使い、電気的特性の揺らぎを直接的に観測することを試みた。これらを通して、揺らぎ信号源を絞り込んで行った。また、1)～4)等から取り出した信号をデジタル変換するための回路は、揺らぎ信号の強度や、周波数特性等で変わってくる。従って、それぞれの揺らぎ信号に対して、揺らぎ信号の特性によって変わってくる。これも揺らぎ信号源の絞込みを行いつつ、回路構成を検討した。

以上の研究により、乱数源デバイスとして、ゲート酸化膜中のトラップまたは量子ドットに捕獲された電子数の変化によって生じるトランジスタのチャネル抵抗の揺らぎに変換する型が、乱数の生成速度の高速性という観点から最も有力であることがわかった。

平成 16 年度はモバイル機器のシステムクロックが MHz オーダーであることから MHz オーダーの乱数生成速度に近づくように、デバイス構造の改良を進めた。例えば、シリコン酸化膜中ではトンネリングは速度が遅いことからシリコン酸化膜よりもバンドギャップが小さい材料でトンネル絶縁膜を置き換えるなど検討した。

また、前年度までに開発した乱数換変換回路は、CR 型発振回路を利用していたため、回路の性質上、50kHz 程度が動作限界であった。これを改善するためフィルタと差動増幅器を組み合わせた回路設計を新規に行った。

平成 17 年度は乱数源デバイスの乱数生成速度の向上と、半導体事業部への将来的な移管を考えて、前年度まで使用していた Si ドット部分を Si-rich SiN 膜に変更した。これで素電荷の捕獲／放出に係わるトラップの数が格段に多くなることを期待した。また数 M bits/sec 程度の高速乱数生成を目的に試作した、フィルタと差動増幅器を組み合わせた乱数生成回路の評価を行った。

４－２－２　研究の実施状況

（平成 13, 14 年度）

委託業務実施計画書に記載した３種類の方式、すなわち、擬似的絶縁破壊（ソフトブレークダウン）させたゲート電極のリーク電流揺らぎの利用、単一電子トランジスタにおいてトランジスタチャネル抵抗が２つの抵抗値を行き来する Random Telegraph Signal(RTS)現象の利用、ゲート酸化膜に捕獲された電子数の変化によって生じるトランジスタのチャネル抵抗揺らぎを利用した Si 量子ドットデバイスについての検討を計画通り実施した。以下に実施した内容を述べる。

（１）ソフトブレークダウンさせたゲート電極の電流揺らぎの利用

回路規模の小さい乱数回路を作成するためには、乱数源には CMOS 回路に実装可能でかつ揺らぎ強度の大きなものが求められる。現状の半導体のショット雑音を乱数源とした回路は、その信号強度が約 10^{-5}%と小さいためにアナログ増幅せざるをえず、回路が大きくなってしまう。

シリコン上の薄い酸化膜に電気的なストレスを印加すると、完全な絶縁破壊の前に擬似的な破壊が起こり、その後の電気伝導特性が乱雑になることが知られている。図 4-2-A-1 は面積４μm^2、酸化膜厚 4.9nm の MOS キャパシタに-7Ｖの一低電圧を印加したときの、擬似破壊の様子とその後の電流揺らぎの様子である。擬似破壊後は電流が大きく揺らいでいることがわかる。図 4-2-A-1 は１秒ごとにサンプリングしたものであるが、この試料の場合、約 10%を越える揺らぎの大きさを示している。ショット雑音と比べ、酸化膜擬似破壊後の電流揺らぎが非常に大きなものであることがわかる。

しかし、ショット雑音と酸化膜擬似破壊後の雑音は、その周波数特性が大きく違う。ショット雑音はパワースペクトル密度が周波数に依存しない、いわゆるホワイトノイズであるが、酸化膜擬似破壊後の雑音は周波数の増加とともにパワーが減少していく、いわゆる 1/f 的特性を示す。これは二つの意味で問題である。

一つは、周波数の高い領域の揺らぎ強度が小さくなってしまうことである。上で 10%の揺らぎと述べたが、これは１Hz の周波数での値であり、現状のスペックである数 MHz の領域ではショット雑音と同等になってしまう。このため、基本的な揺らぎ強度をもう少し大きくする必要があるが、この点については現在調査中である。

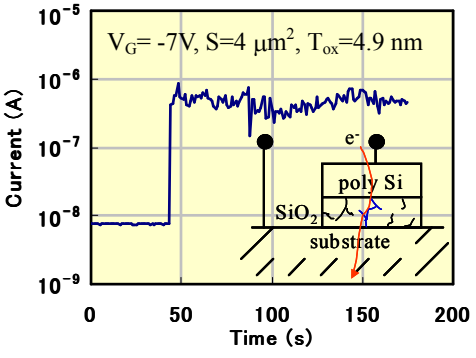


図 4-2-A-１：面積 4μm、酸化膜厚 4.9nm の MOS キャパシタに一定電圧-7V 印加したときの擬似破壊の様子。

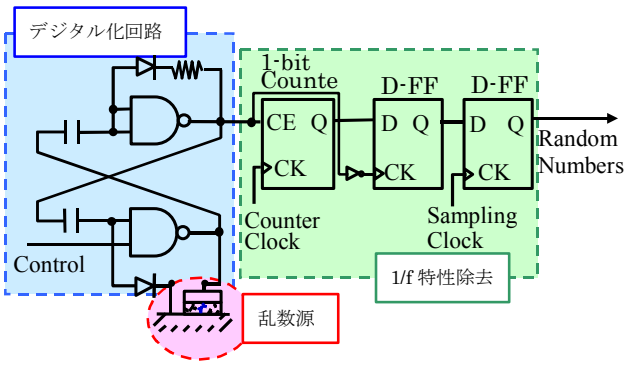


図 4-2-A-2：乱数生成回路全体の回路図。乱数源、デジタル化、1/f 特性除去の３つの部分からなる。

もう一つは、1/f 的特性が、得られる乱数の「0」と「1」の出現頻度に偏りをもたらす、ということである。この点について我々は、A/D 変換後の信号を、出現頻度を平坦化するようなデジタル回路に通すことで改善した。図 4-2-A-2 は全体の回路図である。回路は大

まかに、乱数源、デジタル化、1/f 特性除去の３つの部分からなる。

第一段階として、数十 kHz 程度の速度で乱数回路を作成し、シリコン酸化膜擬似破壊後の電流揺らぎが小型乱数回路における乱数源として有効であることを実証した。結果として、最大 50kHz の動作速度で、非常に高度な乱数を得ることに成功した。

（２）単一電子トランジスタにおけるＲＴＳ現象の利用

東芝では２０００年度までに、極薄膜ＳＯＩの表面に表面起伏を意図的に形成することで、室温で動作可能な単一電子トランジスタを作製し、この単一電子トランジスタは、ゲートバイアス条件を適当に選ぶことで、不揮発性メモリ素子としても機能することを確認していた。このような不揮発性メモリ機能の起源は、表面起伏によって導入したポテンシャル揺らぎにおける、ポテンシャル極小点（以下、メモリノード）への電子の注入／放出である。

また、東芝では２００１年度までに、上述の構造の単一電子トランジスタにおいて、表面起伏の形成条件と、SOI 膜厚を最適化することで、あるゲートバイアス条件下では、メモリノードへの一電子の注入／放出が確率的に頻繁に起こることで、単一電子トランジスタの出力電流がデジタルに変化することを見出し（Random Telegraphic Signal：RTS)、その確率的な注入／放出現象を１桁の電流比という非常に高い感度で検知することに成功している（図 4-2-A-3)。このような一電子の注入／放出現象を高感度で検知することが可能になったのは、単一電子トランジスタの電荷変化に対する高い感度を利用することが可能であったためと考えられる。このような素子では、出力信号がはじめからデジタルの信号列であり、アナログーデジタルの信号変換を行う必要がない。また、高感度検知のために、出力信号がはじめからデジタル信号と同程度になっており、大規模な電圧増幅器も必要としない。そのため、乱数生成器の回路規模を大幅に簡素化することが可能となる。

平成 14 年度上期は、上述の RTS 信号を、暗号用乱数源として評価することを行った。その結果、我々の単一電子素子型の乱数生成器（Random Number Generator: RNG）において、電子の注入／放出現象がポアソン過程に従うことを確認。また、一連の乱数検定を行い、すべての検定に合格することを確認した。

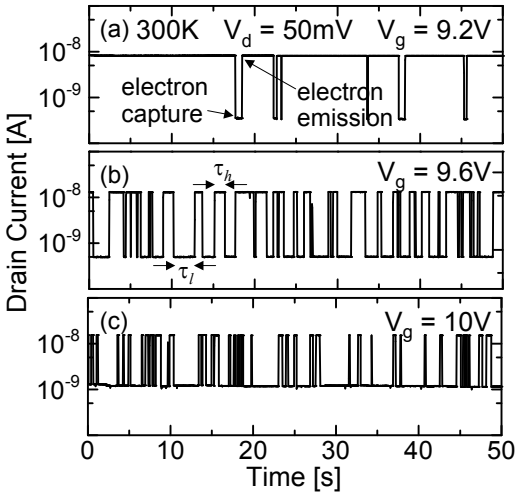


図 4-2-A-3：単一電子乱数生成器からの出力信号。

（３）ゲート酸化膜に捕獲された電子数の変化によって生じるトランジスタのチャネル抵抗の揺らぎ（Ｓｉ量子ドットデバイス）の利用

Ｓｉドット MOSFET において、Ｓｉドットへの電荷の出入りに起因するドレイン電流のゆらぎを観察した。ゲート絶縁膜はトンネル酸化膜２nm と上部酸化膜 12nm から成り、浮遊ゲート部のＳｉドットは粒径８nm、面密度 $2x10^{11}cm^{-2}$ である。狭チャネル部Ｌ／Ｗ＝１／0.2μmのＳｉドット素子に対しての経時変化を図 4-2-A-4 に示す。Ｗの太いもの、Ｌの短いもの、Ｓｉドットの無い Reference MOSFET についても参考に示す。振幅比 10%、時定数 10～100ms で揺らぎがでている。Ｒｅｆ，ＭＯＳＦＥＴとの比較から、この揺らぎはＳｉドットへの注入放出によるものであることがわかる。

よい乱数源の条件の１つは振幅（Ｓ／Ｎ）比が大きいことである。現状の振幅比 10%は、チャネル幅 0.2μm がＳｉドットの電荷による遮蔽の影響が及ぶ範囲（デバイ長、10nm 程度）より大きいのが主要因である。現にＷ＝１μm となると揺らぎは非常に小さい。これはデバイ長 10nm にかからない領域が増えるためと考えられる。よって振幅比を得るにはチャネル幅を 10nm に近づけることである。もう一つ、Ｌ＝0.5μm では振幅が減っていることに気づくが、これは揺らぎ源であるＳｉドット数が半分に減ったためと思われる。多ドットである程、揺らぎの重ね合わせの影響により振幅が増えると考えられる。実際デバイ長の二十倍のＷ＝0.2μm で、単一素電荷の影響のみで 10%も変動するのはちょっと疑問であり、多ドットの効果を既に予想させるものである。振幅比を得るにはチャネル幅を狭める他、揺らぎ源のドットを多くすることが有効と考えられる。

よい乱数源の条件のもう１つは周波数１MHz 以上ということである。現状 10～100ms の変動をあと４～5 桁早くするには、トンネル酸化膜をもっと薄膜化する必要がある。他にも図 4-2-A-1 でＬ＝0.5μm の方が、時定数が長いように見えることは、多ドットの周波数に対する有利性を伺わせる。実際トンネルバイアス１Ｖ程度の時の注入放出に要する時間は 10ms 程度であるのに対し（図 4-2-A-5)、トンネルバイアス 10ｍＶ（熱揺らぎ）のオーダーである揺らぎにおいて 10～100ms の変動が見られるのは、揺らぎ源が多数あることによる重ね合わせの効果で周波数が増大することを示している。振幅のみならず、時定数でも多ドット化が有効であると考えられる。

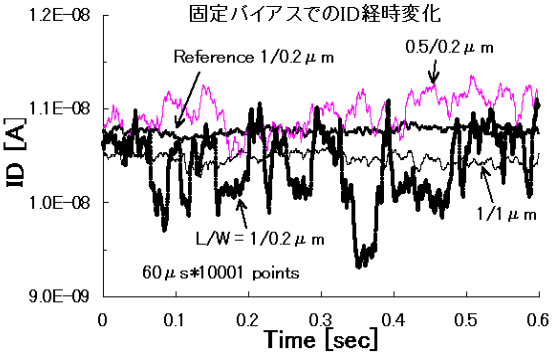


図4-2-A-4：L/W = 1/0.2μm のSiドット素子のドレイン電流経時特性。Siドットの無いRef. MOSFETとの比較、及びL,Wの各依存性を示す。

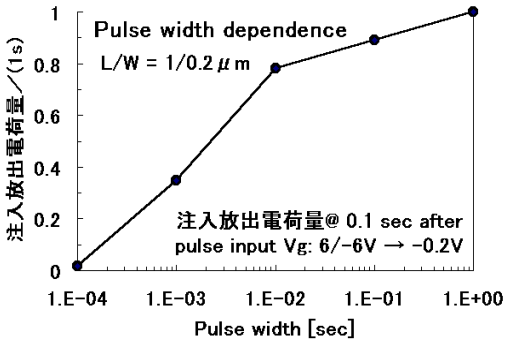


図4-2-A-5：L/W = 1/0.2μm Siドット素子における蓄積電荷量の注入・放出時間依存。トンネルバイアス1V程度では注入放出に10msかかることがわかる。

図 4-2-A-6 に電流揺らぎのフーリエ分解を示す。通常の Reference MOSFET では周波数ｆのべき乗則であるのに対し、Ｓｉドット素子では上に凸の特性で、特徴的時間に相当するｆ＝30Hz 辺りを境に低周波側と高周波側で異なるべき乗則を示す。またこのｆ依存は、揺らぎが単一ドットから起因する台形型のｆ依存（図 4-2-A-6 中に典型的な形を示す）とも明らかに異なる。この結果は多ドットの効果による揺らぎ特性への影響を明示しており、特に先に予想した振幅と周波数の改善効果を裏付ける点で重要である。量産という意味でも現実的なチャネル幅 0.1μｍでも、トンネル酸化膜を極力薄くした上でＳｉドット数をぎりぎりまで増やして多ドット効果を可能なかぎり利用すれば、十分な振幅比と十分な早い

振動数が出る可能性がある。

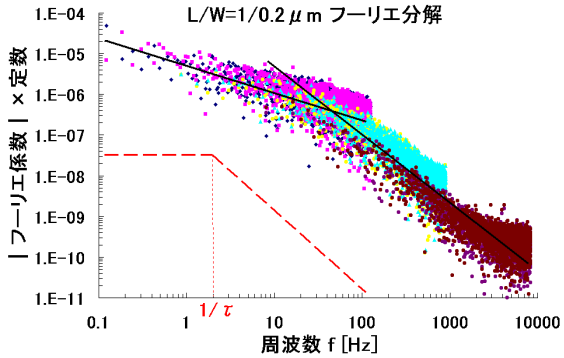


図 4-2-A-6：Ｓｉドット素子電流揺らぎのフーリエ分解。３０Hz 付近を境に低周波側と高周波側でべき乗が異なる。赤で示すのは単一ドット（典型的時間τ）の時の周波数分布。

（平成 15 年度）

（1）Siナノクリスタル二端子デバイスの電流揺らぎの利用

擬似破壊した酸化膜を利用した乱数源デバイスは、擬似破壊させるために、成膜後に電気的なストレスを加えなければならないという短所があった。

そこで、デバイス作製後に電気的ストレスを加えることなく、大きな揺らぎ特性を得られる素子を開発した。膜構造は、薄い酸化膜中に Si ナノクリスタルを埋め込んだ構造をしており、電流は膜厚方向にトンネル電流の形で流す。大部分の電子はナノクリスタルを経由して流れるが、その大きさはナノクリスタルに捕獲されている電子の影響を受ける。酸化膜が薄いためにナノクリスタルでの電子の捕獲／放出が頻繁に起こり、その結果、大きく揺らいだ電流が観察されると考えられる。

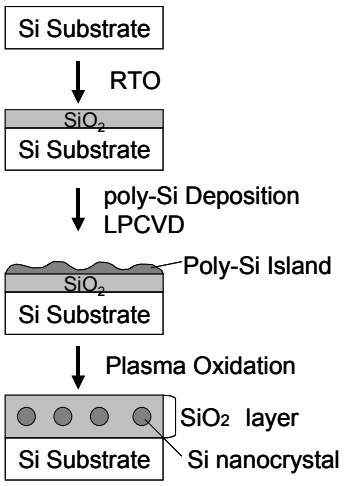


図 4-2-B-1：Si ナノクリスタルの作製手順

素子の作製手順を図 4-2-B-1 に示す。まず、基板を RTO により酸化し、薄い酸化膜を形成する。次に LPCVD により、ポリシリコンを堆積する。この際、ポリシリコンの堆積量を少なくすると平坦な膜ではなく凹凸を持ったアイランド状のポリシリコン膜が出来上がる。このアイランド状ポリシリコン膜を酸化することにより、アイランドの島の部分がナノクリスタルとして酸化膜中に残る。最後に上部電極として N+のポリシリコンを堆積した。素子サイズは 100μm×100μm である。

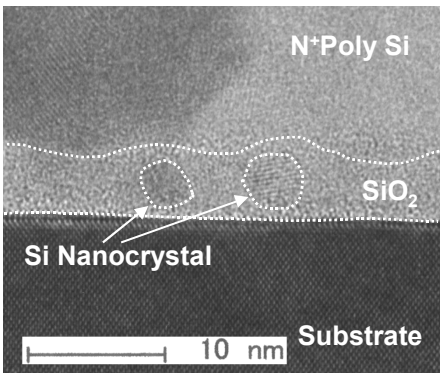


図 4-2-B-2：ノイズ発生素子の断面 TEM 写真。

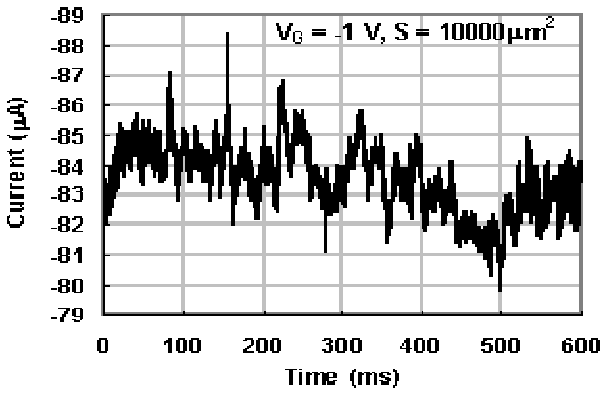


図 4-2-B-3:一定電圧-1 V での電流特性。

次に、作製した素子の断面 TEM 写真を図 4-2-B-2 に示す。Si 基板と上部電極の間に膜厚約 5～6nm の SiO2 層があり、その SiO2 層の中央に直径約 3nm のシリコンナノクリスタルが存在する。SiO2 層と上部電極の界面は平坦ではなく、作製途中のアイランド状ポリシリコンの表面形状の名残であると考えられる。

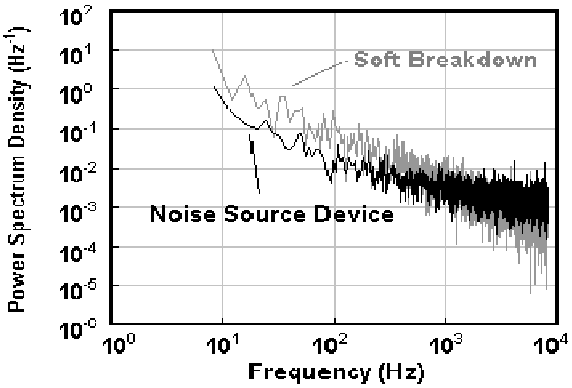


図 4-2-B-4:平均電流からの揺らぎの大きさをフーリエ変換して求めたパワースペクトル密度。

図 4-2-B-3 は P 型基板上に作製したデバイスに、N^+ポリシリコン電極に－1V の電圧を加えたときの電流揺らぎの様子である。サンプリング間隔は 60μs である。
電流の平均値に対して、おおよそ 10%程度の揺らぎ電流が得られている。また、平均の電流値が 1 V に対して 80 μA と、擬似破壊酸化膜が数 nA～数 100nA であったのと比べて大きい。無安定マルチバイブレータのような、RC 発振型の回路を利用して乱数化する場合には、素子の抵抗値は直接乱数生成速度につながるので、低抵抗であることは高速乱数生成が行える可能性を与える。

図 4-2-B-4 は、平均電流からの揺らぎの大きさをフーリエ変換して求めた、規格化したパワースペクトル密度である。ノイズ発生素子と擬似破壊した酸化膜について同時に示している。これに見られるように、測定した周波数全域に於いて、ノイズパワーは両者でほぼ同じとなっており、図 4-2-B-3 の電流特性で得た予測と矛盾しない。ただし、ノイズスペクトルはやはり 1/f 的で、周波数の増加に対してノイズパワーが減少する傾向が見える。乱数回路を高速で動作させる場合には、その分ノイズパワーが小さい領域で動作させることになるので、抵抗が低いだけで高速乱数生成が行えるとは、必ずしも言えないことがわかる。

	Test	Pass Condition	Random Master ™		Pseudo-RNG (16bit-LFSR)		Soft Breakdown Based RNG		**Noise Source Based RNG**	
NIST SP 800-22 (8000 data)	chi square	> 0.05	0.314305	○	0.92873	○	0.754243	○	0.893273	○
	Run	> 0.05	0.902218	○	0.395438	○	0.140286	○	0.474149	○
	Freq. within B	> 0.05	0.718465	○	0.292868	○	0.755063	○	0.458102	○
	Freq.	> 0.05	0.782031	○	0.854326	○	0.447391	○	0.803335	○
	Serial Corr.	-0.022 - 0.022	-0.001627	○	0.009499	▲	-0.016521	▲	0.008002	▲
	Serial	> 0.05	0.058543	▲	0.902358	○	0.358361	○	0.625875	○
	Poker	> 0.05	0.804011	○	0.709127	○	0.467575	○	0.130855	○
	Coupon	> 0.05	0.967344	○	0.172219	○	0.578381	○	0.704695	○
	Gap of 0	> 0.05	0.881333	○	0.03093	✕	0.389933	○	0.181534	○
	Gap of 1	> 0.05	0.705905	○	0.368279	○	0.643145	○	0.506113	○
	Gap of 2	> 0.05	0.322428	○	0.08272	▲	0.231471	○	0.470768	○
	Gap of 3	> 0.05	0.231817	○	0.457027	○	0.66437	○	0.80663	○
	Gap of 4	> 0.05	0.690399	○	0.431837	○	0.332151	○	0.603575	○
	Gap of 5	> 0.05	0.190103	○	0.484632	○	0.370829	○	0.290221	○
	Gap of 6	> 0.05	0.183618	○	0.315686	○	0.282157	○	0.247732	○
	Gap of 7	> 0.05	0.089538	▲	0.56715	○	0.999526	○	0.654338	○
	Gap of 8	> 0.05	0.907953	○	0.673652	○	0.624145	○	0.40432	○
	Gap of 9	> 0.05	0.179379	○	0.67811	○	0.49009	○	0.326107	○
	Gap of 10	> 0.05	0.932978	○	0.496866	○	0.100871	○	0.186661	○
	Gap of 11	> 0.05	0.757808	○	0.106453	○	0.275991	○	0.510545	○
	Gap of 12	> 0.05	0.859729	○	0.372005	○	0.525807	○	0.724555	○
	Gap of 13	> 0.05	0.22462	○	0.578269	○	0.989583	○	0.264397	○
	Gap of 14	> 0.05	0.794274	○	0.77847	○	0.870752	○	0.671465	○
	Gap of 15	> 0.05	0.098699	▲	0.784983	○	0.164742	○	0.986399	○

表 4-2-B-1：一般検定による乱数の検定結果

このノイズ発生素子を、擬似破壊酸化膜の場合と同様に、無安定マルチバイブレータと

カウンタ(図 4-2-A-2)を用いて乱数化した。表 4-2-B-1 は NIST SP 800-22 に記載されている統計検定のいくつかを、我々の乱数に対して適用した結果である。熱雑音を利用した乱数発生回路であるランダムマスター™が出力した結果、擬似乱数回路であるリニアフィードバックシフトレジスタ、および擬似破壊酸化膜での結果も同時に示す。

擬似乱数回路の結果で一つ不合格を出しているが、他の乱数回路では全ての検定項目に対して合格している。また、我々の結果は、高品質な乱数回路である熱雑音を基にした乱数と同等もしくはそれ以上の結果を示している。

以上のように、ノイズ発生素子は、それを使った乱数回路が擬似破壊酸化膜と同様に高品質な乱数を生成することができ、なおかつ、擬似破壊酸化膜と違い、デバイス作製後の電圧ストレスを必要としない、乱数生成に有効な素子であることがわかる。

（2）Ｓｉドット乱数素子の開発

Ｓｉドット MOSFET においてデバイス設計による高速乱数生成への指針が得られた。Ｓｉドット MOSFET において、Ｓｉドットへの電荷の出入りに起因するドレイン電流ゆらぎのデバイスパラメータ依存を実験により解明した。揺らぎに大きな影響を与えるパラメータは、チャネル幅 W（狭いほどＳｉドットからのクーロン力の影響が大きい)、Ｓｉドット密度Ｄdot（高い程揺らぎ源が多い)、トンネル酸化膜厚 Tox（薄い程Ｓｉドットへの電荷の出入が速い）の３つである。これらのパラメータ依存より、Ｓｉドット MOSFET を乱数生成源とするためのデバイス設計が明らかとなる。

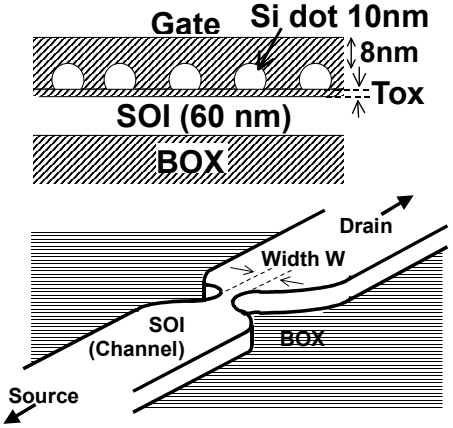


図 4-2-B-5：素子構造の断面図と鳥瞰図。

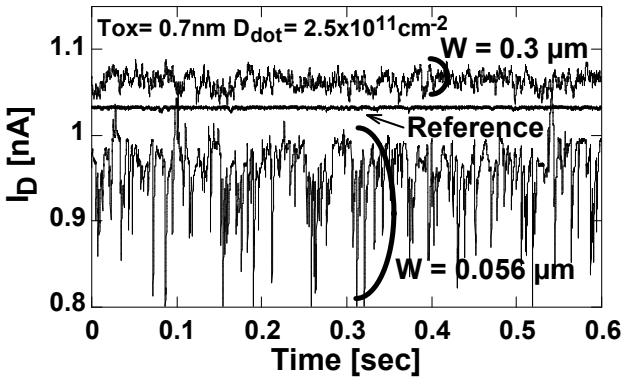


図 4-2-B-6：電流揺らぎ W 依存。

素子構造を図 4-2-B-5 に示す。SOI―MOSFET において、チャネル表面の厚さ Tox =0.8nm 程度の極薄膜トンネル酸化膜上に粒径 10nm 程度のＳｉ微結晶ドットを Ddot =2.5x10^{11}cm^{-2} の面密度で形成する。Ｓｉドット群とゲート電極の間は厚さ８nm の制御酸化膜で絶縁されている。ＳＯＩチャネル部には幅 W の細線部を形成する。

チャネル幅Wのみを変化させた時の電流揺らぎを図 4-2-B-6 に示す。Ｓｉドットを有しない Reference MOSFET においては殆ど揺らぎが無いのに対し、Ｓｉドット MOSFET においては電流に顕著な揺らぎが発生する。Ｓｉドット MOSFET においてはWが狭い程揺らぎが大きいことがわかる。これらはＳｉドット内の素電荷によるクーロン力によって電流がゆらいでいることを示す。電流揺らぎのフーリエ特性を図 4-2-B-7 に示す。Ｓｉドット MOSFET のフーリエ特性は、周波数に対し自然ノイズに特徴的なべき乗依存と、単一Ｓｉドットに特徴的なローレンツ型の中間の特性を示している。これはＳｉドット MOSFET における揺らぎは特定の単一ドットではなく多ドットに起因することを示す。図

4-2-B-8 のフーリエ係数のW依存から、１／W則に従って電流揺らぎは増大することがわかる。

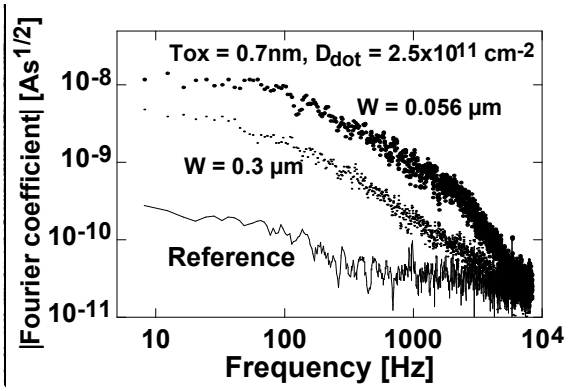


図 4-2-B-7：電流揺らぎフーリエ特性 W 依存。

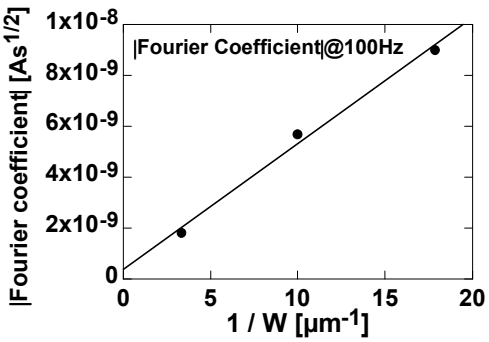


図 4-2-B-8：電流揺らぎフーリエ係数 W 依存。

Ｓｉドット密度 Ddot のみを変化させた実験からは Ddot が高い程揺らぎが大きいことが示された。これは揺らぎの重ね合わせの影響によると考えられる。また、トンネル酸化膜 Tox のみを変化させた実験から Tox の減少に対し、揺らぎは顕著に大きくなることが示された。これはチャネル～Ｓｉドット間のトンネル確率が Tox 減少に対し指数関数的に増大することによる。

良質な高速乱数源を得る為には電流揺らぎをより速く、より大きくする必要がある。以上の実験から電流揺らぎは 1／W, Ddot、$Rt^{-2/3}$ に比例して変化することがわかったが、これらの結果は高性能乱数生成素子のためのデバイス設計において重要な指針を示している。まずチャネル幅 W を細くすることと、Ｓｉドットをできるだけ最密にして Ddot を高くすることで電流揺らぎを増大させることができる。

このノイズ発生素子は、無安定マルチバイブレータとカウンタ(図 4-2-A-2)を用いて乱数化した。図 4-2-B-9 は、適当な固定電圧条件で得られた 25kHz のアウトプットパルスのオシロコープ観察結果である。25kHz アウトプットパルスにおいては、周期 t_J はＳｉドットＭＯＳＦＥＴにおいてはっきりと揺らいでいるのがわかる。一方Ｓｉドットを有さない Reference MOSFET の方では、I_D 揺らぎ(ドレイン電流 I_D) が無いのに応じて殆ど揺らぎが無いことがわかる。

この周期回路内の 1-bit Counter は、25kHz よりも高周波なクロックパルスを有している。これにより個々の周期 t_J を 1-bit の乱数（つまり"0"または"1"）にデジタル変換できる。例えば、ある周期 t_J 内に高速クロックパルスが奇数（／偶数）個存在した場合に"0"（／"1"）を対応させれば良い。こうして 25kHz の生成レートを有する乱数生成回路が増幅回路無しの簡単な構成で得られる。

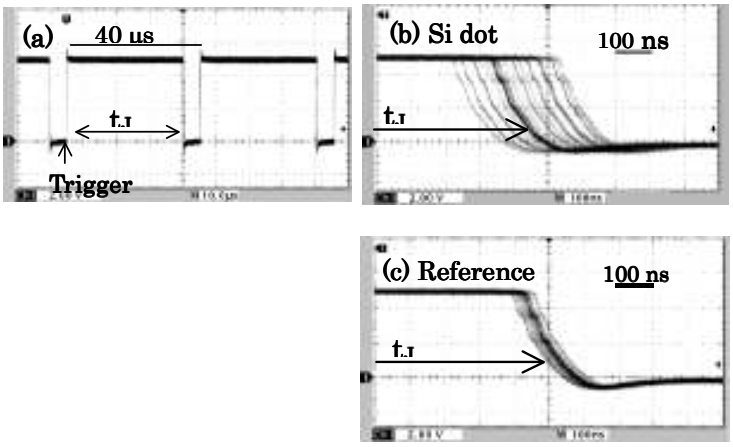


図 4-2-B-9：アウトプットパルスのオシロスコープ観察結果。

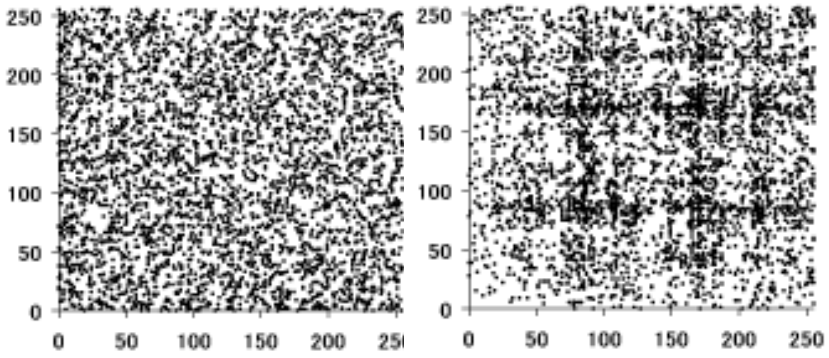
この 25kbits/s の高速乱数列の真性度を統計テストで調べたのが表 4-2-B-2 である。ＳｉドットＭＯＳＦＥＴではすべての検定にパスし、乱数真性度が優れていることがわかるのに対し、Reference MOSFET の場合はパスしないものがあり、乱数真性度が不完全であることがわかる。もう一つの乱数真性度チェックは、図 4-2-B-10 に示す相関プロット

(self-correlation plots for sequential 8-bit random numbers)である。ＳｉドットＭＯＳＦＥＴでは完全にランダムな分布図となり、真性乱数であることを示しているが、Reference MOSFET を用いた場合は、疑似周期性を示し乱数が不完全であることがわかる。

Test		Requirement	Si Dot-MOSFET		Ref. MOSFET	
monobit		9,725 – 10275	9853	Yes!	10582	No!
Poker test		2.16 – 46.17	29.3184	Yes!	662.4832	No!
Long run test	'0'	1 –26	13	Yes!	11	Yes!
	'1'		16	Yes!	15	Yes!
Length of run 1	'0'	2,315 – 2,685	2373	Yes!	3804	No!
	'1'		2393	Yes!	3523	No!
Length of run 2	'0'	1,114 – 1,386	1179	Yes!	1242	Yes!
	'1'		1204	Yes!	1225	Yes!
Length of run 3	'0'	527 – 723	633	Yes!	528	Yes!
	'1'		639	Yes!	611	Yes!
Length of run 4	'0'	240 – 384	312	Yes!	217	No!
	'1'		300	Yes!	288	Yes!
Length of run 5	'0'	103 – 209	167	Yes!	60	No!
	'1'		178	Yes!	119	Yes!
Length of run 6+	'0'	103 – 209	197	Yes!	54	No!
	'1'		147	Yes!	139	Yes!

表 4-2-B-2：25 kbits/s の乱数列の真性度統計テスト結果。

今回の 25kHz という生成レートは、I_D 揺らぎを上述のWの細線化やＤdot の稠密化や、トンネル抵抗を低くするといった手立てで十分に強化してやれば、まだまだ高速化が可能である。よって以上の結果は、ＳｉドットＭＯＳＦＥＴは非常に優れた小型化可能な高速真性乱数生成源であることを示すものである。



(a) Si-dot-MOSFET　(b) Reference MOSFET

図 4-2-B-10：25kbits/s 高速生成乱数列の相関プロット。

（３）乱数生成用 A/C コンバータの検討

小型な乱数生成を実現するためには、乱数源となる素子が小さいことに加えて、デジタル化する ADC も小さくなければならない。これまで検討してきた、無安定マルチバイブレータを用いた AD 変換方式は、非常に小型な回路で実現できるという特徴がある。しかし、ノイズ素子をマルチバイブレータの抵抗に用いているため、出力速度がノイズ素子の抵抗値に依存するという課題があった。この課題はノイズ素子の改良により克服を目指すが、一方で、新たな乱数読み出し方式も合わせて検討を開始した。

まずは、従来型の乱数読み出し方法を、SPICE を使った回路シミュレーションにより検討した。入力のノイズ信号をアナログ回路のハイパスフィルタにいれ DC 成分をカットし、同時にフィルタが持つ逆 1/ｆ特性を使って、乱数源デバイスが持つ 1/ｆ特性をキャンセルすることを考案した。適当な参照電圧を用いて、コンパレータにて２値化する手法を試みた。ノイズ信号がある程度大きければ、この方法でデジタル乱数が得られることが確認できた。

（平成 16 年度）

（1）Si ドット乱数源素子の改良

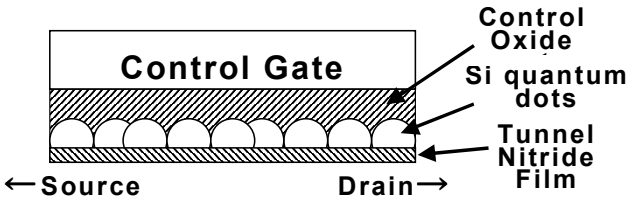


図 4-2-C-1：素子断面構造図。

図 4-2-C-2：断面ＴＥM像。

ＳｉドットメモリはＳｉドットへの素電荷の確率過程によるランダムな出入を、そのまま信号であるドレイン電流で読めるため、乱数生成に好都合な構造である。良い乱数源の条件はＳ／Ｎ比が大きいことと、周波数が速いことである。Ｓ／Ｎ比を大きくするにはＳｉドットメモリのチャネル幅を狭くすることであり、Ｓｉドットへの出入を速くするにはトンネル膜の抵抗を極力低くすることである。

平成 16 年度は細線チャネル幅 0.15μm の、熱窒化による薄膜トンネルＳｉＮ膜と、高密度なＳｉドット郡を有するバルク構造の短チャネルＳｉドットＭＯＳＦＥＴ素子を作製、前回の２００倍の電流揺らぎが得られた。内訳は、バルク構造としたことで約１０倍、SiN 膜の低トンネル抵抗により約２倍、高密度なＳｉドットにより約２倍、ゲート長をスケーリングすることで約５倍、で併せて２００倍の改善を成している。前回 25kHz だったものから２００倍の改善ということで、増幅回路無しの数 MHz 真性乱数生成回路へとても近づいたと言える。トンネル抵抗の低下と、素子サイズ微小化にまだ余地があることから見て、さらに強力なノイズ源への改良も十分可能である。

乱数生成用ＳｉドットＭＯＳＦＥＴの素子構造は、バルク基板上のＳＴＩトレンチ素子分離により、狭チャネル幅Ｗ＝0.15μm とした。さらにトンネル絶縁膜は低トンネル抵抗の熱窒化膜である。ゲート長は最短 0.04μm まで形成する。Ｓｉドット径はおよそ 10nm で、面密度は $1x10^{12}cm^{-2}$ である。断面構造を図 4-2-C-1、図 4-2-C-2 示す。高密度なためＳｉドット同士の接触の機会があるが、乱数減の性能への影響はない。

まず従来のＳＯＩ構造と比較して、バルク構造にしたことによる改善を報告する。図 4-2-C-3 は 25kHz で良質な乱数生成ができたＳＯＩ細線ＳｉドットＭＯＳＦＥＴの電流揺らぎフーリエ特性と、全く同一条件でバルク基板上に作成したものとの比較である。トンネル絶縁膜の酸化膜、Ｓｉドット密度 $2.5x10^{11}cm^{-2}$、素子サイズはＬ／Ｗ＝0.4／0.15μm はすべて同一である。バルク構造では約１０倍の改善があることがわかる。埋め込み酸化膜が無いことで、基板からのキャリア供給があることで、Ｓｉドットへの注入・放出効率が上がるためと考えられる。

次にこのバルク構造において、Ｓｉドット密度を増やした場合の改善を見てみる。先と同じＳｉドット密度 $2.5x10^{11}cm^{-2}$ と、その 2 倍の $5x10^{11}cm^{-2}$ の場合、ランダムノイズはおよそ $2^{1/2}$＝１．４倍程度増えている。

次にトンネル絶縁膜を酸化膜から、よりトンネル抵抗の低い薄膜窒化膜とし、Ｓｉドット密度を $1x10^{12}cm^{-2}$ でまで増やした場合を見てみる。図 4-2-C-4 には、トンネル酸化膜でＳｉドット密度 $2.5x10^{11}cm^{-2}$ の場合の電流ノイズフーリエ特性と、トンネル窒化膜で密度 $1x10^{12}cm^{-2}$ の場合のフーリエ特性を示す。トンネル抵抗低下と密度の増加により４倍の改善である。先の統計学の定理に従いドット密度による増加が $4^{1/2}$＝２倍で、トンネル抵抗低下によるものが２倍と考えられる。

最後にゲート長Ｌのスケーリングによるさらなる改善について報告する。図に歯示さないがトンネル窒化膜で密度1x10^{12}cm^{-2}の場合、Ｌ＝0.4μmに対し、ゲート長の短いＬ＝0.04μmでのフーリエ特性は５倍の改善を示す。

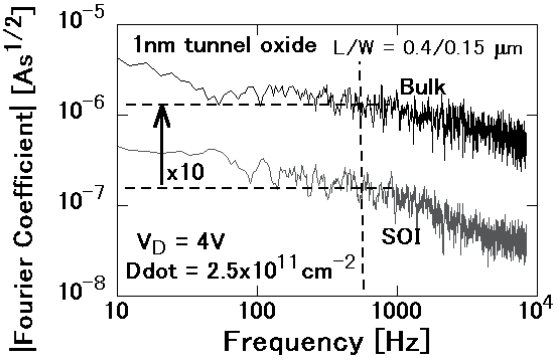


図 4-2-C-3：電流ランダムノイズフーリエ特性。ＳＯＩ構造とバルク構造。

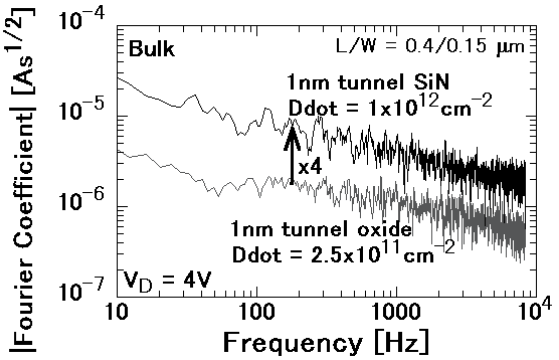


図 4-2-C-4：電流ランダムノイズフーリエ特性。トンネル膜とＳｉドット密度による改善。

このようなゲート長スケーリングによる改善の理由はスクリーニング効果の減少によると考えられる。観察ではゲート電圧を上げて反転層キャリア電子密度を上げると、キャリア電子自身によるスクリーニング効果により、ドレイン電流値（∝反転層キャリア電子密度）にほぼ反比例してランダムノイズのＳ／Ｎ比は小さくなる。ゲート長 40nm になったことでチャネル抵抗も１／１０になるので、同じ電流値（例えば 10μA）では 0.4μm より少ない反転層キャリア電子密度になっており、キャリア電子自身によるクーロンスクリーニング効果の減少により、結果として同じ電流値で見てノイズがより大きくなるものと考えられる。

以上の内容をまとめると図 4-2-C-5 のようになる。昨年増幅回路無しで 25kbit/s で真性乱数生成した時と比較して、２００倍のノイズが各種素子設計により得られたことがわかった。トンネル抵抗低下と素子サイズ微小化はまだ可能なので、ノイズ源素子としての能力向上はまだ可能である。ここでは乱数源素子のみの改善を述べたが、これと組み合わせる乱数変換回路の改良も可能であることを考慮すると、増幅回路無しの数ＭＨｚ真性乱数生成回路は十分な期待ができる。

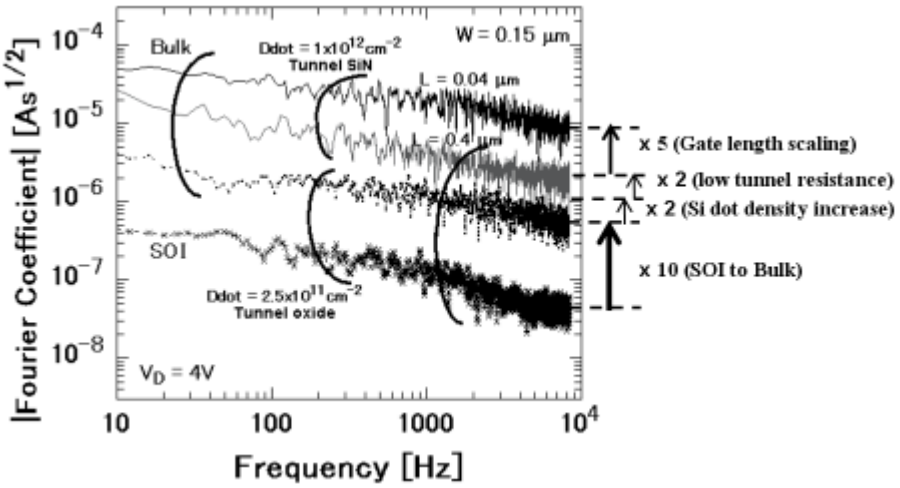


図 4-2-C-5：各種素子設計による電流ランダムノイズ特性改善。２５ｋｂｉｔ／ｓで真性乱数生成したもの（一番下）から、２００倍の改善をなす。

また、高速乱数生成デバイスの検討の一環として、トンネル絶縁膜のトンネル速さに関する検討も行った。高速に乱数を得るためには乱数生成デバイスの電流揺らぎをより

速くする必要がある。電流揺らぎはデバイスの幅 W、ドット密度の他、トンネル絶縁膜のトンネル抵抗にも依存する。トンネル抵抗は膜厚にも依存するがトンネル障壁高にも依存する。そこで(1)SiO2 と SiO2 よりトンネル障壁の低い(2)SiN の 2 つの絶縁膜のトンネル特性を比較することにより、トンネル速さの違いを明らかにした。まず、SiO2 と SiN の電流―電圧静特性を測定した（図 4-2-C-6 及び図 4-2-C-7)。サンプルはどちらも MIS キャパシタ構造、面積は 100μmx100μm、基板は SiO2 は n、SiN は p である。SiN 膜は直接窒化 2nm の後 CVD（ジクロロシランガス）で 4nm 積んで狙い膜厚 6nm に作製した。SiN のうち片方はアニールを施した。SiN の 0 から-1V にかけて見られるピークは、測定前に膜中に含まれていた電荷によるものである。SiN は低電界からリーク電流が大きいことが分かる。この結果は、前述したデバイスのトンネル膜を SiO2 から SiN 膜に変えることで、トンネル速度が格段に向上し、その結果、ノイズスペクトルの高周波成分が急増したことと、定性的に一致している。しかも、SiN のトラップ現象による負性抵抗ピークの存在は、ドットに電子が蓄積されることに加え、SiN のトラップに電子が蓄積される可能性も示唆しており、よりノイズ強度を高める効果が期待される。

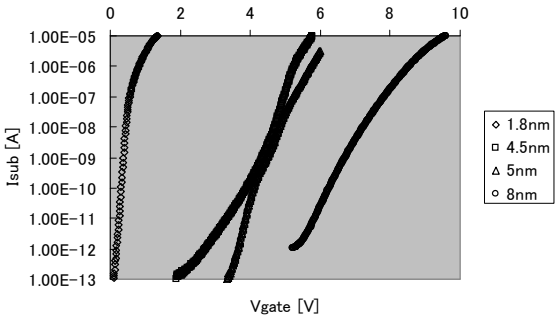


図4-2-C-6:SiO2膜の電流－電圧特性。

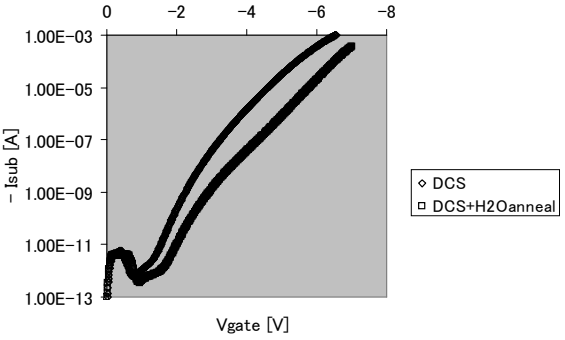


図4-2-C-7:SiN膜の電流－電圧特性。

（２）乱数変換回路の改良

小型物理乱数生成回路のテスト回路作製の設計を行った。この試作の主な目的は、これまで検討してきた乱数生成回路の集積化、ノイズ源となるソフトブレークダウン（SBD）させるキャパシタと通常の回路との混載の試み、フィルタと差動増幅を利用した高速乱数生成回路の設計、である。レイアウト設計は TSMC の 0.25μm mixed signal のプロセスを想定して行った。

作製する回路は大まかには３種類であり、１）マルチバイブレータ型、２）ローパスフィルタ（LPF）＋差増増幅型、３）ハイパスフィルタ（HPF）＋差動増幅型、である。

マルチバイブレータ型は、これまでにディスクリート素子の組み合わせにより動作を確認している。この回路方式では、通常高抵抗のノイズ源を抵抗として組み込むという本質的な問題もあるが、集積化によって生成速度がある程度改善することも考えられる。今回の試作では、ノイズ源との混載とともに、集積化の効果を確かめたい。レイアウト作製は基本となるマルチバイブレータと、ノイズ源に SBD を使用するのかノイズ信号を外から入れるのか、および、周波数特性補正用のカウンタとフリップフロップ（FF）の有無のそれぞれの組み合わせについて行った。

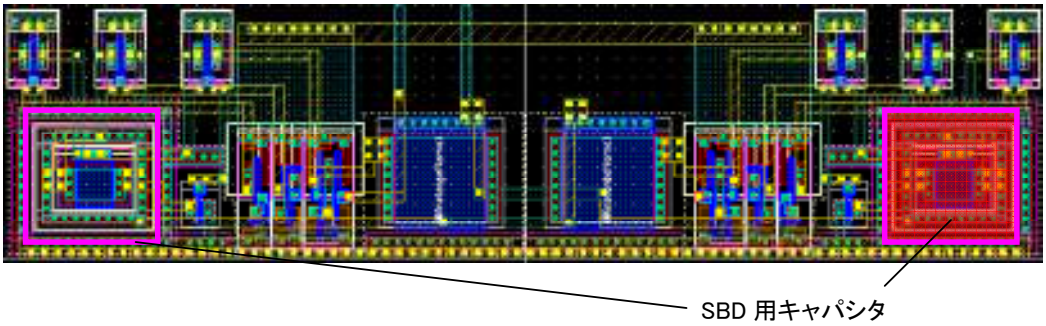


図 4-2-C-8：SBD 用キャパシタ付きマルチバイブレータ乱数生成回路のレイアウト。

図 4-2-C-8 は SBD 用のキャパシタを備えた、マルチバイブレータ方式の乱数生成回路レイアウトである。レイアウト面積は約 56.58 μmx 13.64μm であったが、その面積の多くは、SBD をノイズ源として使うことに費やされている。ノイズ源を外から入れる場合には、SBD 用キャパシタ、およびそれに付随する PMOS、NMOS のスイッチ、プルダウン、プルアップ用の抵抗（トランジスタ）をはずす。1/f 特性除去用のカウンタとフリップフロップ（FF）は、この出力の後ろに、まず一度 FF で値をラッチした後、その出力につなぐ形で作製した。すなわち、マルチバイブレータ、FF、カウンタ、FF というならびになる。SBD 用キャパシタを備えた、マルチバイブレータ方式の乱数生成回路にカウンタと FF を使用した回路のレイアウトは、約 116.34μm x 14.24μm というサイズである。

ローパスフィルタ、もしくは、ハイパスフィルタと差動増幅器を使った乱数生成回路は、ノイズ源と乱数変換回路を並列に使用することにより、マルチバイブレータ方式よりも高速な乱数生成を目的としている。ノイズ信号のようなアナログ信号を 1 ビットデジタル信号にするには、適当な参照電圧とレベルコンパレータで可能である。しかし、ノイズ発生素子から出力されるノイズ信号は、典型的には 1/f 的特性を示すため、コンパレータでそのままデジタル化しただけでは、変換後のデジタル信号に、1/f 的特性を反映した長周期の規則性が現れてしまう。よって、何らかの方法で長周期成分を除去する必要がある。長周期成分の除去に LPF を使うか HPF を使うかで 2 通りの構成が可能である(図 4-2-C-9)。

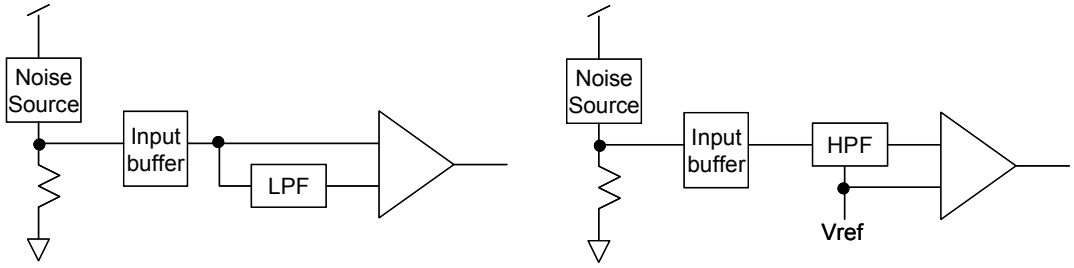


図 4-2-C-9：フィルタと差動増幅を使った乱数生成方式。

LPF では、元の信号とフィルタリングされた信号を比較することで、フィルタで除去された高周波成分の信号を反映した値が出力される。HPF では、フィルタリングされた信号と参照電圧を比較するので、フィルタを通過した高周波成分を反映した値が出力される。どちらも高周波成分、すなわち短周期の成分が残ってしまう可能性があるが、もし問題が残ったとしても、マルチバイブレータ式で用いたようなデジタル回路を少し加えるだけで修正できる。

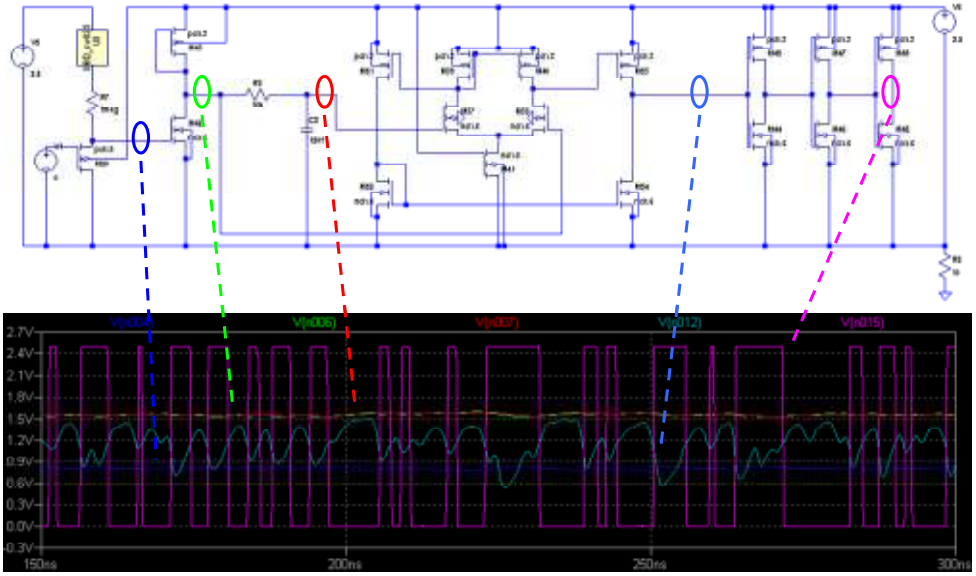


図 4-2-C-10:LPF を使った方式の回路図とシミュレーション結果。

図 4-2-C-10 は LPF を使った構成を具体的に実現する回路図の一例と、SPICE シミュレーション結果である。トランジスタモデルは、TSMC 0.25μm のものを用いた。ノイズ素子に関しては、ランダムな信号を正確にシミュレーションすることはできないので、rand()関数で作った電圧信号をトランジスタのゲートに入力することで、擬似的に抵抗のランダム変化を表現している。LPF は抵抗とキャパシタで構成している。差動増幅器は、目標としている動作速度が数 Mbits/s～数十 Mbits/s であるので、動作速度よりも出力振幅を重視して二段オペアンプの構成を採用した。出力はデジタル値であるので、差動増幅器の出力を数個のインバータで整形し、最終出力としている。カットオフ周波数は、抵抗にポリ抵抗、キャパシタに MOS キャパシタを想定し、なるべく面積を小さくすることを考慮したため、100MHz と目標よりも１～２桁大きい値になっている。

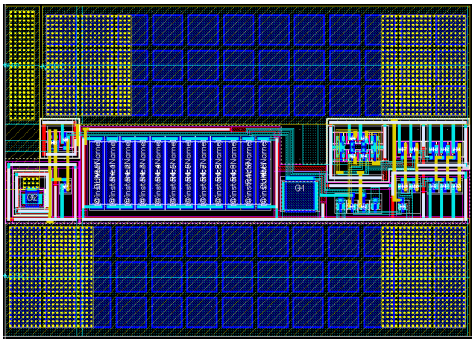


図 4-2-C-11：LPF と差動増幅器を使った乱数生成回路のレイアウト。

HPF を使った構成についても、抵抗とキャパシタによるフィルタの構成が若干違うのみで、基本的にはほぼ同様の形で構成できる。

図 4-2-C-11 は LPF と差動増幅器を使った乱数生成回路のレイアウト図である。先に述べたように、抵抗はポリ抵抗、キャパシタは MOS キャパシタを使用している。この他に、マルチバイブレータ方式と同様にカウンタと FF を作製したもの、SBD 用のキャパシタをはずしてノイズ信号を外から入力できるようにしたもの、差動増幅器の電流源にしているトランジスタのゲート入力を外から入力できるようにして増幅器の安定動作を試みたもの、を同時に作製した。

(平成 17 年度)

(1)　SiN 乱数素子の開発

Si ドットメモリは、Si ドットへの素電荷の確率仮定によるランダムな出入りをそのまま信号であるドレイン電流で読めるため、乱数生成に好都合な構造である。平成 17 年度は、浮遊ゲート部分を今まで用いていたＳｉドットにかわり、Ｓｉリッチ SiN 膜を用いたメモリと同じ構造の素子を用いることにより、Ｓｉドットを用いたときよりも高品質な乱数の

生成が可能であることを示した。

□Si ナノ微結晶を用いた乱数生成素子と Si-rich SiN 膜を用いた乱数生成素子の比較

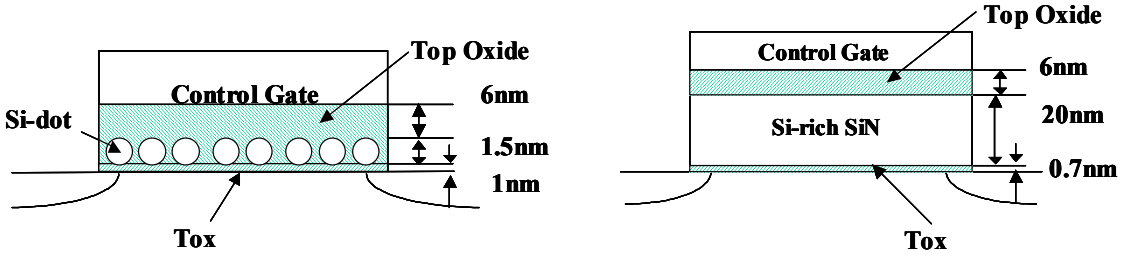


図4-2-D-1：(a)乱数生成用SiドットMOSFETの素子構造，(b)乱数生成用SiリッチSiN乱数素子。

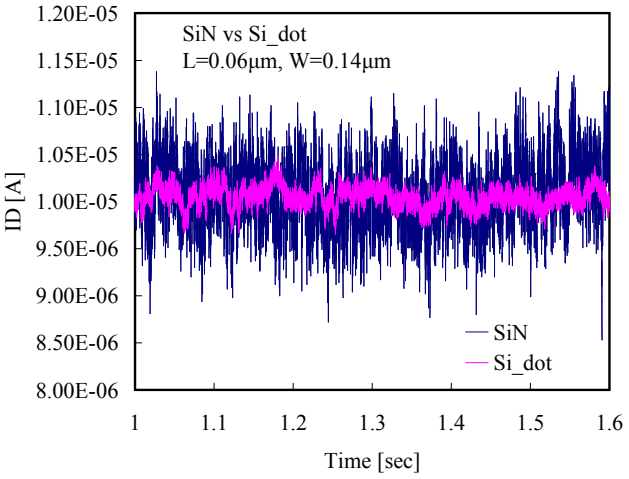


図 4-2-D-2：Si ドットデバイスと SiN デバイスのＩＶ特性の比較。Ｌ/Ｗ＝0.06/0.14μm。

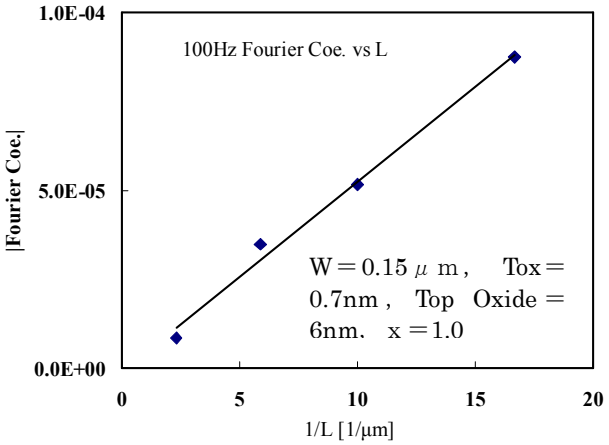


図 4-2-D-3：100Ｈｚでのフーリエ係数のＬ依存性

乱数生成用 SiN 乱数素子の構造は、Si/N 原子数比 x = 1 のＳｉリッチ SiN 膜を浮遊ゲートとするメモリと同様である。これと比較するのは、これまでで最高性能を示した乱数生成用 Si ドット MOSFET で、その素子構造は、粒径 10nm、面密度 $10^{12}cm^{-2}$ の Si ドットを浮遊ゲートとし、トンネル酸化膜を SiN 膜としたメモリと同様である。Si ドット乱数素子，Si リッチ SiN 乱数素子の素子構造の略図はそれぞれ図 4-2-D-1 (a)，(b)である。浮遊ゲート部分を Si ドットから Si リッチ SiN 膜に変更することによりトラップ数が格段に多くなり、S/N 比の増大につながることが狙いの一つである。

乱数生成における質を両者で比較するため、同じ大きさの素子を用い、電圧固定で I_D＝10μA 付近での電流揺らぎの経時変化を測定した。その結果が図 4-2-D-2 である。これより、Si ドット乱数素子では 10μA で 3%程度の揺らぎ成分であることに対し、SiN 乱数素子では 10%もの揺らぎ成分を確認することができ、SiN 乱数素子のほうが S/N 比が大幅に大きいことがわかる。

□SiN 乱数素子の設計指針

Si リッチ SiN 乱数素子が、乱数生成において、より良いランダムノイズを得るための条件を決定する基本パラメータとして、ゲート長 (L)、ゲート幅 (W)、トンネル酸化膜厚 (Tox)、Si/N 比（ｘ）が挙げられる。これらがランダムノイズに与える影響について調べた結果について以下に順に示す。

○L 依存性

まず電流揺らぎのゲート長依存性について示す。フーリエ係数は L に対して単調に減少し、キャリア電子密度が少なくても良い短チャネルほど、大きなランダムノイズを発生さ

せる。また、フーリエ係数は周波数に対し、どの L においてもほぼ周波数の-1/2 乗で表すことができる。周波数 100Hz 付近におけるフーリエ係数を 1/L でプロットしたものが図 4-2-D-3 である。青のプロットは各 L の 100Hz におけるフーリエ係数、直線は近似直線であり、ある周波数におけるフーリエ係数は 1/L に比例する。

○W 依存性

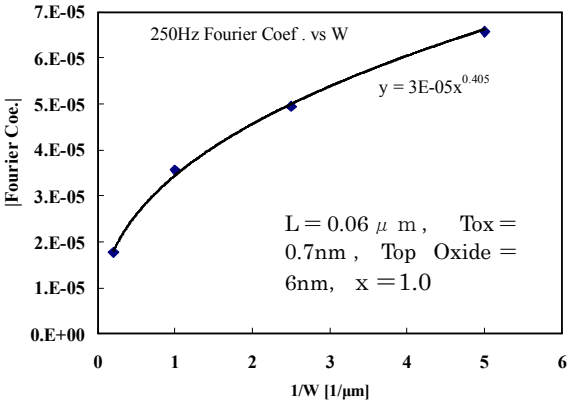


図 4-2-D-4：250Ｈｚでのフーリエ係数のＷ依存性。

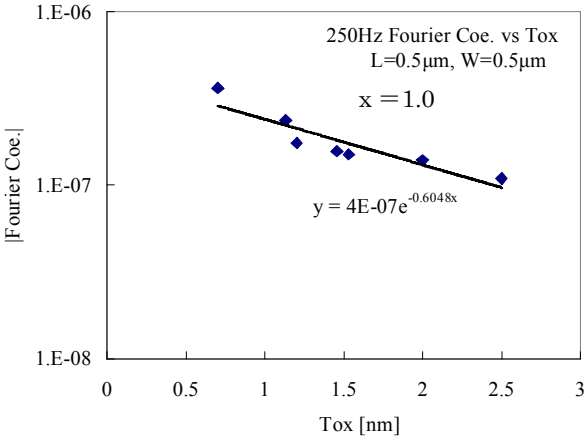


図 4-2-D-5:250Ｈｚでのフーリエ係数の Tox 依存性。

次に、ゲート幅（W）依存性について示す。フーリエ係数は W に対して単調に減少し、局所トラップ電子の影響が大きくなる狭い W ほど大きなランダムノイズを発生させることがわかる。また、どの W においても周波数の-3/5 乗にほぼ比例する。周波数 250Hz 付近におけるフーリエ係数を 1/W でプロットしたものが図 4-2-D-4 である。この累乗近似により 1/W の 0.4 乗でよく近似できることがわかる。

○Tox 依存性

続いてトンネル酸化膜厚 Tox 依存性について示す。Tox が厚くなるにしたがって、トンネル抵抗が増加し、これにより、フーリエ係数は Tox が厚くなるとともに減少する。さらに、Tox が 2nm より厚くなると Tox がこれ以上厚くなってもその振る舞いに与える影響が小さくなってくる。周波数 250Hz 付近における各 Tox におけるフーリエ係数の振る舞いは図 4-2-D-5 のようになる。これより、Tox に対しフーリエ係数は指数関数的に減少することがわかる。

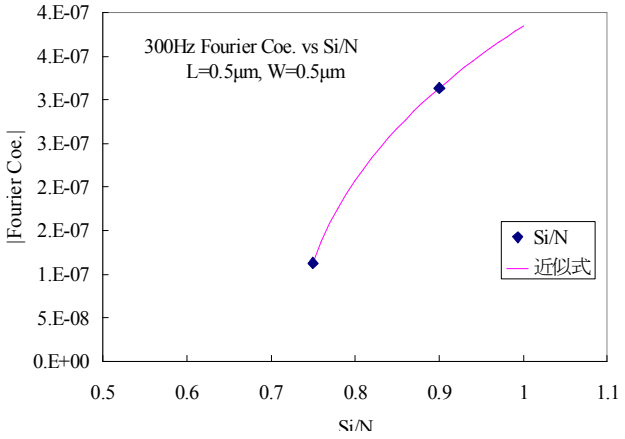


図 4-2-D-6：300Ｈｚでのフーリエ係数の Si/N 比依存性。

○Si/N 比（原子数比率）依存性

最後に Si/N 比依存性ついて示す。これより、ｘが１に近づくほど、すなわち、Si リッチであるほど、フーリエ係数は大きくなり、乱数デバイスとしては優位であることを示している。図 4-2-D-6 はフーリエ特性図から、周波数３００Ｈｚにおけるフーリエ係数を横軸に Si/N 比ｘとして示したものである。青のプロットは各ｘにおけるフーリエ係数、曲線は近似式として、$|F|=\sqrt{A^2N+A^2C\cdot\frac{x-0.75}{1+x}}$ をひいた。ここで A, C は定数、N はｘ＝0.75（Si と N の原子比率の安定箇所）におけるトラップ密度である。まず、前提として、ここで言

うトラップ数とは、1 原子あたりの過剰 Si 原子数に比例する値としており、フーリエ係数は統計的にトラップ密度の 1/2 乗に比例するという考えのもと上記のような近似式をおいている。

□SiN 乱数素子のまとめ

今回の結果から、Si リッチ SiN 膜 MOSFET は、従来の熱窒化膜をトンネル絶縁膜として用いた Si ドット MOSFET と比べ、より高品質な乱数の生成が可能であることがわかった。さらに、Si リッチ SiN 乱数素子の基本パラメータであるゲート長 L，ゲート幅 W，トンネル酸化膜厚 Tox，Si/N 比 x について上記のような依存性から設計指針が得られ、これらの各パラメータの依存性には Si-dodt 乱数素子のときと異なる依存性が見られた。ここでそれぞれの乱数素子の基本パラメータの依存性について挙げると、以下のようになる。

	Si リッチ SiN	Si-dot
ゲート長（L）	L^{-1}	$L^{-0.5}$
ゲート幅（W）	$W^{-0.4}$	W^{-1}
トンネル絶縁膜厚（Tox）	exp(-0.6048*Tox)	exp(-6*Tox)
Si/N 比（ｘ）	$(A-x^{-1/2})1/2$ （A:定数）	
Si-dot 密度（D_{dot}）		D_{dot}

表 4-2-D-1：SiN 乱数素子と Si ドット素子の比較。

各基本パラメータの依存性は両乱数素子で異なることが上の表より明らかとなったが、両者ともに乱数の質を上げるためには微細化が必要となる。ただし、微細なＬよりも微細なWの方が加工が煩雑なので、W依存性の小さい Si リッチ SiN 乱数素子のほうが有利と考えられる。また、同サイズの素子における S/N 比の差などから、Si リッチ SiN 乱数素子のほうが優位であると思われる。

また、課題として、Si リッチ SiN 乱数素子は、トラップ密度が多い分、電流揺らぎは大きいが抵抗が大きく I_D を大きくとれず、現在用いているマルチバイブレータを用いた乱数生成法では高速乱数の生成が難しい、という点が挙げられる。よって今後は乱数生成方法についても見直しが必要であり、新たに差動増幅器を使った乱数生成回路を用いて、乱数生成を試みる予定である。また、今後製品化に向けて、望ましい基本パラメータの範囲の規定のみではなく、Si リッチ SiN 乱数素子を用いた際の乱数生成に必要な乱数特性に対応する必要な微細化の程度の見積もりについても検討する必要があると考えている。

（２）乱数変換回路の改良

数 Mbits/sec 程度の高速乱数生成を目的に試作した、フィルタと差動増幅器を組み合わせた乱数生成回路の評価を行った。評価した回路の回路図は図 4-2-D-7 の通りである。ノイズ源は擬似破壊した酸化膜を用いた。

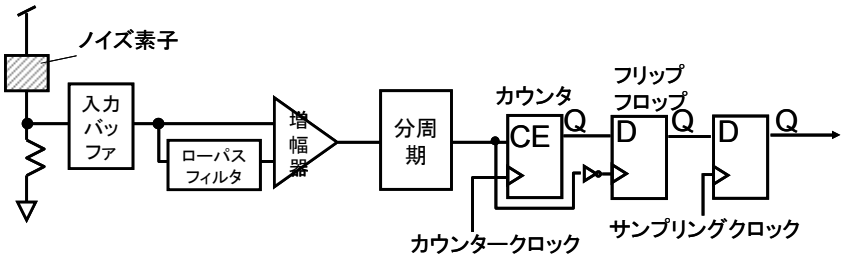


図 4-2-D-7：乱数生成回路図。

ノイズ素子から出力される電流揺らぎは、ノイズ素子と抵抗とで分圧されて、入力バッ

ファを通して電圧の揺らぎに変換される。揺らぎ信号は、ローパスフィルタを通った信号と比較され、高周波成分に依存した信号が増幅器から出力される。出力信号は周波数分周期で所望の周波数に変換するとともに、波形を整形して、ポストプロセス回路に受け渡される。ポストプロセス回路では、波形の時間揺らぎをカウンタで計測して 1 ビットデータとしてフリップフロップで保存する。波形の時間情報を 1 ビット化することで、信号のもつ 1/f 的な周波数成分を実効的に除去することが可能になる。生成速度は、揺らぎ信号に応じて非同期に出力されるデータをラッチするサンプリングクロックの周波数で決定され、どの程度の速さのサンプリングクロックまで乱数を得られるかで最大生成速度が決まる。

テスト項目	合格条件	検定結果	
x^2 test	>0.05	0.270	Pass
Run test	>0.05	0.274	Pass
Frequency test within Block	>0.05	0.886	Pass
Frequency test	>0.05	0.120	Pass
Serial Correlation test	-0.0141 ~ 0.0140	-0.00786	Pass
Serial test	>0.05	0.062	Pass
Poker test	>0.05	0.546	Pass
Gap test	>0.05	0.058 ~ 0.997	Pass

表 4-2-D-１：サンプリングクロック周波数 1MHz での
20000 ビットデータに対する統計検定の結果。

表 4-2-D-1 は、サンプリングクロック周波数を１MHz にしたときの 20000 ビットデータに対して、標準的な統計検定を行ったときの結果である。検定の棄却率は５％としている。表にあるように、これらのデータで統計検定に合格した。このことからすなわち、この回路仕様で乱数生成速度 1M bits/sec を得ることに成功したといえる。

課題としては、大きく分けて信頼性、低消費電力化、高速生成の３つを挙げることができる。自己検査機能をつけることや、回路動作を最適化し無駄な電力を省くこと、シリコンドット FET のような高周波領域での信号が大きい素子との一体化、などを検討していく必要がある。

４－２－３　まとめ

(平成 13,14 年度)

マルチバイブレータと呼ばれるデジタル化処理部分の回路を開発した。また、特殊な絶縁膜のゲート電極から発生する物理揺らぎ信号を用いて、マルチバイブレータで、乱数を発生させるデモンストレーションも行った。

また、以前に試作した量子ドットを内蔵したトランジスタ(単一電子トランジスタ)を使い、電気的特性の揺らぎを直接的に観測することも試みた。さらに、量子ドットを内蔵したランダム信号発生源のトランジスタを試作開始した。

(平成 15 年度)

Si ドット MOSFET 型の乱数源デバイスとマルチバイブレータ型の ADC の組み合わせで、25Kbit/s での高質乱数な生成が可能になった。しかし、先に述べたように ADC が高速性の律速となっており、これの改良化によって高速性が見込まれる。

(平成 16 年度)

乱数源素子の構想駆動さ性能を大幅に改善することに成功した。また、小型集積化による乱数生成速度の高速化、ノイズ素子と CMOS 回路の混載化、差動増幅型乱数回路のテスト、を目的としていくつかの乱数回路を設計した。

(平成 17 年度)

引き続き乱数源素子の構想駆動さ性能を大幅に改善することに成功した。回路とあわせて、以前作製した SOI 型の乱数素子に比べて 200 倍のノイズ強度を達成、乱数の生成レートは 0.12Mbit/s を達成した。今後は、回路と素子の整合性を検討し、また事業部に移管できるプロセス技術、デバイスの改良を行い、生産ベースに適合できる素子を目指す。

４－３　乱数評価に関わる研究開発

４－３－１　序論

平成 13 年度は、既存の乱数サンプルについて、カイ２乗検定、ギャップ検定など統計的な観点から検定を使って評価することを試み、第一次的な乱数の評価を行った。

平成 14 年度はこれを土台として、世の中で知られている乱数生成手法（擬似乱数や白色雑音増幅など）で作られた乱数を検定で評価して、相対評価の指標とすることを試みた。並行して、マルチバイブレータ回路の実験から得られたアナログデータを計算機処理(デジタル変換、一様性補正、周期性・規則性補正)してデジタル乱数を作り、実際に統計検定し、目標である白色雑音のレベルに到達できるか否かの大まかな判断を行った。これらの評価は米国商務省の研究所である NIST が提唱した標準的な統計検定プログラムである FIPS140-2 とその他の推奨されている一般の検定方法 NIST800-22 に基づくものである。

上記の通常の検定方法は一回だけのサンプリング結果を元に、ある危険率を想定して判断するというものであり、評価としては十分でない。そこで、平成 15 年度はある程度以上の乱雑度をもった乱数間の比較を行うべく、多数回サンプリングデータをもとにしたより多量なデータを使って、より高度な検定方法について検討することにした。また、乱数をセキュリティ技術に応用した場合を考えて、セキュリティ強度への乱数の質が与える影響を検討した。この場合、質の差の影響が最も顕著に出るのは、ストリームデータとしての時系列乱数列ではなく、同じタイミングで多数回発生させた乱数のデータのほうであることが、明確になってきた。セキュリティシステムで用いられるのは、主に後者であるためである。この観点からの検討も合わせて行った。

平成 15 年度までに情報セキュリティという観点から乱数の質を検討することも行ってきた。しかし、サイドチャネル攻撃に代表されるような攻撃に対する耐性という観点から考えると、むしろ従来の統計的な手法はかなりオーバースペックを要求していることになる。逆に、どのくらい乱数の質を落としていくと情報漏洩のリスクが生じるのかを見出すことのほうが重要で、その最低レベルと試作した乱数回路のレベルの差が、セキュリティの強固さを示すものになると予測しており、**平成 16 年度**はこの定量化を試みた。

端的な例として、時系列でサンプリングした乱数と、システム起動後の同一クロックでサンプリングした乱数との違いがあげられる。乱数の統計検定では、時系列でサンプリングした乱数が使われる。多少なりとも工夫された擬似乱数回路であれば、この検定は通ってしまう。しかし、同一クロックでサンプリングした乱数の場合には、擬似乱数のアルゴリズムが如何に高度であっても、乱数の質はシードのランダムネスにのみ依存するので、簡単な検定ですら通らないことになる。暗号を実装した機器で暗号鍵への攻撃に対処するために乱数を使ったスクランブリングが用いられるが、この場合、時系列サンプリングした乱数と同一クロックでサンプリングした乱数と両方について乱数の質が高くなければならない。

これらの背景から、平成 16 年度は上記の統計的手法を使った一般的な検定に加えて、回路を実際に暗号のアプリケーションに盛り込んだことを想定して、セキュリティの強度、つまり攻撃に対する耐性と言う観点からも、乱数を評価する方法を開発した。

平成 17 年度は前年度に引き続き暗号チップに対する攻撃の対策として用いる乱数の強度評価を行った。特に DEMA (Differential Electromagnetic Analysis)攻撃に対する外注評価を行った。

４－３－２　研究の実施状況

(平成 13、14 年度)

乱数検定のプログラム作成

平成 13 年度に作成した NIST の標準的な統計検定プログラムを拡張して、検定項目の数を増やした。これに基づいて、擬似乱数、熱雑音乱数、フリップフロップなどを用いた乱数等を検定した。表 4-3-A-1 は二つの擬似乱数回路で作った 8000 個の乱数データを評価したものである(棄却率は 5%)。

また、高精度な擬似乱数として知られている PANAMA と MT (Mersenne Twister)法を統計テストによる相対評価の指標として利用するため、これら二手法の調査とシミュレーション環境の構築を行った。

それと同時に乱数評価に関する動向調査を進め、国際会議 CHES (Workshop on Cryptographic Hardware and Embedded Systems)2002 において、暗号応用の乱数評価に関する米国や欧州標準の改定が進みつつある情報を得た。これを受け、乱数評価の方針を現在の世界的動向により沿って検討を開始した。最後に乱数解読の攻撃方法についての調査を始めた。

	data1		data2	
<x2 test>	0.210498	○	0.283131	○
<Run test>	0.327465	○	0.090995	○
<Frequency test within a block>	0.030662	X	0.128083	○
<Frequency test>	0.368364	○	0.363174	○
<Serial correlation test>	0.010806	X	0.018868	X
<Serial test>	0.31792	○	0.349596	○
<Poker test>	0.324884	○	0.775234	○
<Gap of `0'>	0.202245	○	0.056932	○
<Gap of `1'>	0.124494	○	0.183581	○
<Gap of `2'>	0.40666	○	0.000268	○
<Gap of `3'>	0.69734	○	0.186805	○
<Gap of `4'>	0.167518	○	0.007362	○
<Gap of `5'>	0.912858	○	0.490363	○
<Gap of `6'>	0.097639	○	0.00026	X
<Gap of `7'>	0.481867	○	0.282324	○
<Gap of `8'>	0.985871	○	0.281062	○
<Gap of `9'>	0.841877	○	0.003898	X
<Gap of `10'>	0.595494	○	0.057672	○
<Gap of `11'>	0.766111	○	0.034413	X
<Gap of `12'>	0.305195	○	0.549064	○
<Gap of `13'>	0.636195	○	0.189829	○
<Gap of `14'>	0.884666	○	0.000073	X
<Gap of `15'>	0.235323	○	0.000546	X

表 4-3-A-1:一般検定による擬似乱数回路の乱数評価。データ数 8000 個。

(平成 15 年度)

（１）多数回サンプリングデータを元にした統計評価の検討

まず､検定方法のうち０と１のバランスを図る最も基本的な検定がχ^2(カイ二乗)検定をベースに検定ソフトを作成した。これは上記の FIPS140-2 や NIST800-22 などが多数のデータを統計分布として扱ったとき、どの程度数学的理想曲線からずれているかを評価すべきところを、簡便さのため棄却率という値を決めて、数値一点で乱数度を検定していることからくる反省でもある。上記のような一般検定、頻度検定、ポーカーテスト、系列検定、間隔検定などは検定の最後に必ず、カイ二乗曲線や、誤差関数が現れる。今回これらを分布として扱い、その理想数学曲線からのずれを乱数度と考えることにした。今回、考察したのは(1)カイ二乗検定　(2)頻度検定　(3)間隔検定　(4)ポーカー検定　(5)系列検定の５項目で、比較したのは我々が開発したソフトブレークダウン素子(SBD と表記)と Intel

社製の熱雑音乱数生成器である。注目するところは理想数学曲線からのずれの小さい方が乱数度が高い、という点である。調べたデータ数は1M ビット、統計量を出す単位は 1000 ビットである。

この結果をより数値的に表すため、数学曲線値とデータ値の標準偏差を計算すると Intel 熱雑音乱数が 0.029357、ソフトブレークダウン乱数素子が 0.022308 となり、我々の開発した乱数素子の方が理想的な乱数の統計分布に近いことが示された。

（2）セキュリティ応用から見た乱数評価の検討

スマートカードのような暗号モジュールに対して大きな脅威となっている電力解析攻撃は、おおまかに SPA (Simple Power Analysis)と DPA (Differential Power Analysis)とに分類される。統計的手法を利用する DPA は、暗号チップ内部の信号と消費電力とに相関がある場合に、消費電力波形と鍵との相関を計算することで秘密鍵を特定する強力な攻撃法である。そのため DPA の本質的な対策は内部信号と鍵との相関をなくすことであり、乱数を用いた隠蔽が一般的に行われている。例えば乱数と内部データとの XOR をとることで内部データが毎回ランダムに変わるため、鍵との相関を消すことができる。この対策が有効に働くには、0/1 のバイアスがないなど乱数の質が優れていることが要求される。

一方、電力解析攻撃のようなサイドチャネル解析の特徴として、攻撃対象である暗号チップが攻撃者の手中にあり、動作環境等をある程度任意に制御できるということが挙げられる。このため暗号チップの耐性評価はこの前提の下で行うことが重要であり、これらの攻撃に対するセキュリティシステムを仮想設計しながら解析を進めた結果、最も危険なものの一つとして､暗号チップに対するリセットを毎回行いながら DPA を行うという状況であることを見出した。この場合、上述した対策に用いられる乱数としては、チップがリセットされてからある一定時間が経過した後の乱数(以下、同一クロックでの乱数と呼ぶ)が用いられることになる。

例えば疑似乱数生成器の seed に偏りがある場合､その影響を受けて同一クロックの乱数にも偏りが生じることが予想されるが、これは DPA 耐性の低下に直結する。よって、暗号チップへの搭載を目的とした RNG のセキュリティ評価の一項目として、同一クロックにおける DPA の耐性評価が有効であるといえる。真性乱数は同一クロックでの DPA でも十分な耐性を示すことが期待されるため、この耐性の程度を判定することでセキュリティに関する一つの指標とすることが可能である。平成 15 年度上期は RNG のセキュリティに関する評価のために以上のような考察を行い、DPA の検討と耐性評価を実施するための思考実験とシミュレーションを行った。

(平成 16 年度)

（1） 大規模データを使った高精度の乱数統計評価方法開発

乱数検定にはこれまで幾度となく使ってきた米国商務省の研究所である NIST が提唱した標準的な統計検定プログラムである FIPS140-2 とその他の推奨されている一般の検定方法 NIST800-22 がある。通常は FIPS140-2 を用いて評価を行うが、これは検定のレベルが低いため、十分でない。(FIPS140-2 は現在セキュリティの推奨項目から削除されている。)そこで FIPS140-2 検定の棄却率を 0.1%から一気に５%に上げるとともに、これだけで評価しきれない項目を一般の検定方法 NIST800-22 から選定し､我々は乱数評価を行ってきた。

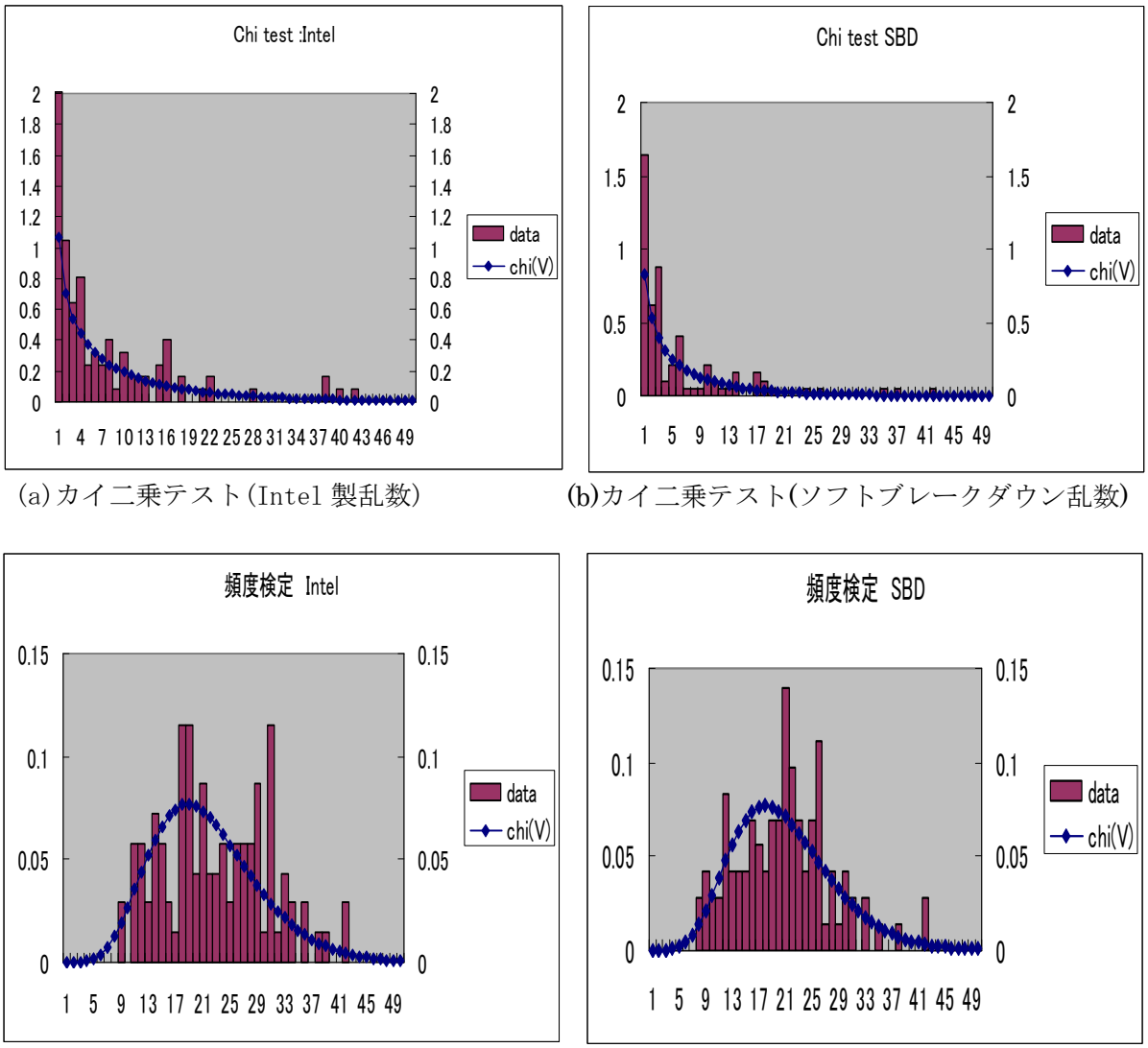
しかしながら、Intel のチップセットに入っている乱数生成期をはじめ最近の乱数はだいたい上記の二つの有名な乱数検定はパスすることがわかっている。そこで、我々はある

程度以上の乱雑度をもった乱数間の比較を行うべく、より高度な検定方法について調べている。そこで、まず原点に返り、検定方法のうち０と１のバランスを図る最も基本的な検定が χ^2 (カイ二乗)検定をベースに検定ソフトを作成した。これは上記の FIPS140-2 や NIST800-22 などが多数のデータを統計分布として扱ったとき、どの程度数学的理想曲線からずれているかを評価すべきところを、簡便さのため棄却率という値を決めて、数値一点で乱数度を検定していることからくる反省でもある。上記のような一般検定、頻度検定、ポーカーテスト、系列検定、間隔検定などは検定の最後に必ず、カイ二乗曲線や、誤差関数が現れる。今回これらを分布として扱い、その理想数学曲線からのずれを乱数度と考えることにした。

今回、グラフ化したのは

(1)カイ二乗検定　(2)頻度検定　(3)間隔検定　(4)ポーカー検定　(5)系列検定

の５項目である。ソフトは VC++を用いて作成した(図 4-3-C-1)。



(a)カイ二乗テスト(Intel 製乱数)　(b)カイ二乗テスト(ソフトブレークダウン乱数)

(c)頻度検定(Intel 製乱数)　(d) 頻度検定(ソフトブレークダウン乱数)

図 4-3-C-1：開発したソフトによる乱数検定。”chi”は数学分布曲線を表す。

今回のソフトの特徴としては(a)読み込みデータ数の制限がない(100M まで検証済み)。(b)FIPS140-2、スペクトル検定などこれまで作成してきた検定も加えた。(c)一発でグラフ化等々だれでも簡便に検定できるようにしてある。さて、今回比較したのは安田(事)のソフトブレークダウン素子(SBD と表記)と Intel 製熱雑音乱数である。ここでは(1)のカイ二乗検定と(2)の頻度検定の結果をグラフに示す。注目するところは理想数学曲線からのずれ

の小さい方が乱数度が高い、という点である。

調べたデータ数は１M ビット、統計量を出す単位は 1000 ビットである。以上の結果をより数値的に表すため、数学曲線値とデータ値の標準偏差を計算すると表 4-3-C-1 のようになる。

	Intel	SBD	LSFR13
カイ二乗検定	0.029357	0.022308	0.04086
頻度検定	0.000549	0.000378	0.000561
間隔検定	0.000172	0.000175	0.000214
ポーカー検定	0.001304	0.004735	0.002523
系列検定	0.002786	0.00178	0.003981

表 4-3-C-1：数学的曲線値とデータとの標準偏差。

より乱数度が大きいほどこの標準偏差は低くなる。表では最も低いものを緑色、最も乱数度が低いものを赤色とした。ここで、LSFR とはソフトで作成される乱数である。この結果からわかるようにソフトブレークダウン素子が必ずしも一番乱数度が高いわけではなく、検定によっては他の乱数より劣る場合が出てくる。

より高度な乱数検定を目指して、カイ二乗分布を計算できるソフトを作成し、Intel の乱数回路、ソフト的に発生する乱数、そしてソフトブレークダウン素子とマルチバイブレータの組み合わせを使った乱数を比較した。今回の検定方法によりかく乱数の持っている”個性”が浮きださせることができることがわかった。

さらに、100M ビットまで、同様の評価を行ってみたが、上記に示した表の値と大きな違いは見られなかった。すなわち、上記の方法を用いることで大規模なデータを用いることなく、高度な乱数間の差を見出すことができることが分かった。

（２） セキュリティ外注評価-1

セキュリティ応用からの乱数評価を目的として、平成 16 年度は暗号チップに対する攻撃の対策として用いる乱数の強度評価を行った。実装攻撃(サイドチャネル攻撃)と呼ばれる攻撃が 90 年代終盤に提案されて以降、暗号チップに対する大きな脅威となっている。この実装攻撃は暗号処理中の動作時間や消費電力などの漏洩情報を利用して秘密鍵を解読する非破壊型の攻撃手法で、特に金融系 IC カードでは実装攻撃に対する耐タンパー性の業界認定取得がビジネスに不可欠な要素となっている。実装攻撃の中でも大きな脅威となっているのが消費電力を利用する電力解析攻撃 DPA (Differential Power Analysis)であるが、この攻撃に対する対策では通常乱数を用いた内部信号の攪乱を必要とするため、安全性の強度は乱数の質に直結するところが大きい。このような状況を受け、DPA 耐性に着目した乱数の強度評価はセキュリティ応用から重要な課題となっており、本プロジェクトでは同時クロック DPA と呼ぶ強度評価の検討を前年度より進めてきた。

擬似乱数はシードを与えてから毎回同じタイミングでサンプリングを行った場合、シードの影響による 0/1 の偏りが発生する危険性を有する。一方、物理乱数はこのような性質を持たないため、同じタイミングでのサンプリングに着目した比較により、擬似乱数と物理乱数の特徴的な差異を捉えることが可能であると予想される。これを具体的に DPA として検証する目的で同時クロック DPA を考案した。DPA 対策では、複数の乱数系列(0/1 ビットの時系列的な並び)から、同じタイミングで 1 ビットずつサンプリングして得られた乱数列の 0/1 バランスに DPA 耐性が依存するという性質がある。よって、対策用乱数として擬似乱数または物理乱数を用いた実装に対する DPA を行うことで、上述した比較検証が可能になる。この同時クロック DPA に対する擬似乱数と物理乱数の強度評価を実施するため、外部評価機関に対する耐性評価依頼を実施した。評価依頼の概要は次の通りである。

評価機関：TNO(Netherlands Organization for Applied Scientific Research のオラン

ダ語略称)-ITSEF(Information Technology Security Evaluation Facility) --- 大手クレジットカード会社が指定する金融系カード耐タンパー機能の業界認定評価機関の一つ
評価対象：共通鍵暗号 DES に対して公知の DPA 対策を適用したソフトウエア実装 --- INSTAC(情報技術標準化研究センター)より弊社が請負受託して開発した INSTAC-8 準拠プラットフォーム[1]に、Akkar-Giraud による DPA 対策[2]に基づく DES-SW 実装を搭載
依頼内容：0/1 バランスの異なる 3 種類の乱数を対策として実装し、それぞれに対してサンプル数を 1000, 3000, 9000 の 3 パタンに変えた DPA を実施して耐性強度を比較する
依頼した評価内容の詳細と結果について以下報告する。
DPA 対策に用いる乱数はマスクと呼ばれるが、このマスクとして次の 3 種類を評価対象とした。

(a) 固定値(オールゼロ) R=0%
(b) 擬似乱数(同時クロックサンプリングによる LFSR 出力) R=約 30%
(c) 物理乱数(本プロジェクト開発の物理乱数生成器による生成) R=約 50%

各セットに対して 9000 サンプルの消費電力波形を測定し、DPA サンプル数を変えながら DPA 耐性を評価する。セット(a)は評価暗号ボードの特性を特定して DPA 実行に必要となる基礎データを取得するために用いるものであり、評価目的はセット(b)と(c)の比較にある。上記 R は 0/1 のバラツキであり、R=0%がオール 0 またはオール 1、R=50%が 0/1 のバランスが取れていることを表す。上述したように、擬似乱数は同時クロックサンプリングによるシードのバラツキを反映して 0/1 のバランスが R=約 30%に崩れたデータとなっている。
DPA は、消費電力波形と暗号処理中の内部情報との相関を統計処理で解析し、得られた相関値に基づいて秘密鍵を特定する攻撃法である。よって統計処理に要するサンプル数が多いほど DPA は困難であるといえ、DPA が成功するために要する最低サンプル数が DPA 耐性を示す一つの指標となり得る。DPA 成功に要した最低サンプル数に関するセット(a)-(c)の評価結果は次の通りとなった。

(a) 固定値　　12
(b) 擬似乱数　544
(c) 物理乱数　9000 では不可

この結果は乱数の質を反映したものであり、0/1 に偏りがある擬似乱数ではサンプル数 500 強で DPA が成功してしまうのに対し、0/1 がバランスしている物理乱数では 9000 サンプルでも DPA 耐性を示すことが分かる。今回用いたサンプル数の上限 9000 は TNO-ITSEF による標準的な DPA 耐性評価で用いられるサンプル数を上回っており、物理乱数を対策として用いた実装ではその耐性基準を満たした結果が得られた。今回の評価結果は、乱数の質に依存したセキュリティ強度を同時クロック DPA という観点から直接的に示した実例といえる。

(平成 17 年度)

セキュリティ外注評価-2

セキュリティ応用からの乱数評価を目的として、前年度に続き平成 17 年度も暗号チップに対する攻撃の対策として用いる乱数の強度評価を行った。新たに提案された電磁界解析攻撃 DEMA (Differential Electromagnetic Analysis)と呼ばれる攻撃は、消費電力の代わりに電磁界の変動を利用するDPA類似の攻撃であり、DPAよりもS/N比に優れる、暗号チップの局所的な解析が可能等の理由から、より高精度な攻撃手法となっている。このような状況を受け、DPA および DEMA 耐性に着目した乱数の強度評価はセキュリティ応用から重要な課題となっており、本プロジェクトではそのような観点からのセキュリティ評価外注を行った。評価依頼の概要は次の通りである。評価機関は平成 16 年度と同じオランダ TNO である。

- 依頼期間: 平成17年10月中旬からH18年2月中旬までの約4ヶ月間

- 評価対象：共通鍵暗号DESに対して公知のDPA/DEMA対策を適用したソフトウエア実装 --- INSTAC（情報技術標準化研究センター)より弊社が請負受託して開発したINSTAC-8準拠プラットフォーム[1]に、Akkar-GiraudによるDPA対策[2]に基づくDES-SW実装を搭載
- 依頼内容：(a) 短周期擬似乱数のDPA脆弱性評価
  (b) 長周期擬似乱数のDPA脆弱性評価
  (c) 物理乱数と擬似乱数のDEMA耐性評価

依頼した評価内容の詳細と結果について以下報告する。

(a) 短周期擬似乱数の DPA 脆弱性評価

【目的】代表的な擬似乱数生成器である LFSR (Linear Feedback Shift Register)を DPA 対策用乱数として用い、その周期が短い場合に、周期の特定、および、DPA による鍵の特定が可能かを評価する。周期は $2^7-1=127$ とし、外注先での解析評価に要する日数を現実的な範囲とするため、乱数周期が 2^n-1 (n=6, 7, 8, or 9)であることは予め開示。
【評価内容】
(1) 乱数周期の決定
外注先が考案した固定平文アプローチおよびランダム平文アプローチによる解析を実施。両手法にて周期 127 が判明。
(2) DPA による周期 127 の確認
DPA に用いるサンプルを対策に用いている乱数周期に同期させてサンプリングした場合、対策無効と等価な状態になる（乱数が固定値になる）ことを利用して、DPA サンプルの取得を(1)で判明した 127 周期で行ったところ、DPA が成功し秘密鍵が判明。
【結論】短周期擬似乱数を対策に用いた場合、消費電力波形に周期的な特徴が生じ、それを足掛りとする乱数周期の特定、さらには DPA による秘密鍵の特定が可能であり、短周期擬似乱数は DPA 耐性に対する潜在的脆弱性を有する。

(b) 長周期擬似乱数の DPA 脆弱性評価

【目的】長周期 LFSR は、0/1 バランスが比較的長い周期で崩れる性質があり、この性質が DPA 耐性に与える影響を評価する。長周期 LFSR として、周期 $2^{33}-1$ および $2^{36}-1$ の乱数を評価対象とした。
【評価内容】大量のサンプル数(50,000 サンプル)による DPA を実施したところ、乱数の 0/1 バランスの僅かなずれ(バイアス 0.47)を脆弱性として DPA が成功。
【結論】長周期擬似乱数を DPA 対策に用いる場合、乱数の 0/1 バランスが長周期に渡って崩れる性質があり、かつ、DPA はサンプル数が増すほど精度の高い攻撃が可能となるため、乱数の周期と 0/1 バイアス、および、DPA サンプル数との兼ね合いによって DPA に対する脆弱性を示す危険性を有する。

(c) 物理乱数と擬似乱数の DEMA 耐性評価

【目的】委託研究にて開発した物理乱数(SiO_2 薄膜のソフトブレークダウン現象利用)と、比較対象としての擬似乱数の DEMA 耐性を評価する。擬似乱数はシードを与えてから毎回同じタイミングでサンプリングを行った場合、シードの偏りを反映して乱数列に 0/1 バイアスが生じる危険性を有するのに対し、物理乱数はそのような性質を原理的に持たない。よって、両者の本質的差異を評

価する目的で考案した“同一サンプリング評価”をDPAに対して平成16年度のセキュリティ外注にて実施した[3]。今年度はこの同一サンプリング評価をDEMAに対して行った。
【評価内容】各9,000サンプルでのDEMAを実施し、

擬似乱数(バイアス約0.3)	約1,000サンプルでDEMA成功
物理乱数(バイアス約0.5)	9,000サンプルでもDEMA不成功

との結果を得た。
【結論】同一クロックサンプリングされた擬似乱数はシードに依存した 0/1 バイアスを示し、それがDEMA に対する脆弱性になり得るのに対し、物理乱数は同様の条件下でも DEMA 耐性を有する。

以上、セキュリティ応用における擬似乱数の潜在的脆弱性、および、物理乱数の有効性を示す結果が得られた。今回の評価結果は、前年度に続き乱数の質に依存したセキュリティ強度をDPA/DEMAという観点から直接的に示した実例といえる。

参考文献:
[1] INSTAC 平成15年度調査研究報告書「耐タンパー性に関する標準化調査研究開発」http://www.jsa.or.jp/domestic/instac/committe/H15report/report-contents/01_02.PDF に記載の8ビットCPU搭載評価基板
[2] M.-L. Akkar and C. Giraud, Proceedings of Cryptographic Hardware and Embedded Systems - CHES2001, Lecture Notes in Computer Science, vol.2162, pp.309-318, Springer, 2001.
[3] 野崎, 安田, 藤崎, 新保, 藤田, “DPAマスク対策における乱数の影響について,” 電子情報通信学会技術研究報告 Vol. 105, No. 290, 2005, ISEC2005-77.

４－３－３　まとめ

(平成13、14年度)

乱数を評価する方法は、主に統計的な検定という手法が用いられるが、検定も多種多様であり、真性乱数にどれだけ近い乱数であるかを評価するための適正な手法は、必ずしも確立しているとは言えない。従って、乱数生成集積回路を開発するためには、乱数の評価手法自身も開発する必要がある。また、大規模な乱数データを高速に処理する方法も模索しなければならない。
平成14年度は、市販の熱雑音増幅型の乱数生成回路で作られた乱数(既存の乱数回路の中では最高水準の乱数)について、カイ２乗検定、ギャップ検定など統計的な検定を使って評価することを試みた。さらに、デバイス・回路の研究開発で実施したマルチバイブレータで作った乱数を評価した。

(平成15年度)

多数回サンプリングデータをもとにしたより多量なデータを使って、より高度な検定方法について検討した。
また、乱数をセキュリティ技術に応用した場合を考えて、セキュリティ強度への乱数の質が与える影響を検討した。この場合、質の差の影響が最も顕著に出るのは、ストリームデータとしての時系列乱数列ではなく、同じタイミングで多数回発生させた乱数のデータのほうであることが、明確になってきた。セキュリティシステムで用いられるのは、主に後者であるためである。この観点からの検討も合わせて行った。

(平成16年度)

大規模な乱数データを使ったより厳密な統計評価を行う方法を開発することができた。また、乱数とセキュリティ強度の相関を、DPA 耐性という切り口から明らかにすることが出来た。

(平成 17 年度)

大規模な乱数データを使ったより厳密な統計評価を行う方法を開発することができた。また、乱数とセキュリティ強度の相関を、DPA/DEMA 耐性という切り口から明らかにすることが出来た。今回の評価結果は、乱数の質に依存したセキュリティ強度を直接的に示した初めての実例といえる。

４－４　総括

今年度の研究開発により、最終目標を 100%以上達成することが出来た。
（１）乱数の質向上：乱数の質について、熱雑音（またはショット雑音）から生成された物理乱数のレベルを上回ることに成功した。まず、具体的にはソフトブレークダウン素子、単一電子素子、Si 量子ドット素子など様々な乱数素子を開発することに成功した。そしてその中でも、SiN 膜中のトラップ準位を利用した素子で MHz オーダーに迫る生成スピードを出す乱数素子の開発に成功した。(2006 年 3 月 6 日付け日刊工業新聞にて発表)。

（２）回路の小型化：標準 LSI 用の CMOS 論理ゲート換算で 1000 ゲート以下を達成した。具体的には 100 ゲート程度でマルチバイブレータを中心とした乱数デジタル回路の開発に成功した。これも当初の計画を大幅に上回る成果と考える。

（３）乱数の統計評価：大量データを評価する方法を確立した。また暗号チップとして生成された乱数を評価し、サイドチャネル攻撃(同時クロック DPA/DEMA)に対する耐性を示した。これは暗号チップという形で当計画の乱数の安全性が保障されたことを示し、当初の計画を上回る成果と考える。

５　参考資料・参考文献

５－１　研究発表・講演等一覧

（◎は査読あり）

□平成 17 年度

学会：◎Nanotechnology Conference 2005
題名：Three-Dimensional Logic Architecture by Four-terminal Electrical Switches (FES) beyond Two-dimensional CMOS Architecture
藤田　忍、安部　恵子、T.H. Lee

②学会：物理学会
題名：電荷量子ビットのデコヒーレンス・フリー状態に局所的不均一性が与える効果
棚本　哲史、藤田　忍

③学会：電子情報通信学会 情報セキュリティ研究会(ISEC)
題名：DPA マスク対策における乱数の影響について
野崎　華恵、安田　心一、藤崎　浩一、　新保　淳、　藤田　忍

④セミナー：VISA セントラル東芝デー
題名:Ultra-small Physical Random Number Generating Circuits for Information Security
藤田　忍

⑤学会：◎Electric Properties of Two-Dimensional Systems (EP2DS-16)
題名： Robustness of Decoherence-Free States for Charge Quantum bits under Local Non-uniformity
棚本　哲史、藤田　忍

⑥学会：電子情報通信学会集積回路研究会 (ICD)
題名：情報セキュリティ向け超小型物理乱数生成回路
安田　心一、棚本　哲史、大場　竜二、安部　恵子、野崎　華恵、藤田　忍

⑦学会：◎IEEE Computer Society Annual Symposium on VLSI 2006
題名：Si Nano crystal MOSFET with Silicon Nitride Tunnel Insulator for High-rate Random Number Generation
大場　竜二、安田　心一、棚本　哲史、藤田　忍

⑧学会：応用物理学会
題名：高速乱数生成を目的としたＳｉ微粒子ＭＯＳＦＥＴの特性
松本　麻里、大場　竜二, 松下　大介, 村岡　浩一, 安田　心一, 棚本　哲史, 内田　健, 藤田　忍

⑨学会：◎European Solid-State Circuits Conference (ESSCIRC 2005)
題名：Physical Random Number Generators for Cryptographic Application in Mobile Devices
安田　心一、棚本　哲史、大場　竜二、安部　恵子、野崎　華恵、藤田　忍

⑩学会：◎International Electron Device Meeting 2005
題名：35 nm Floating Gate Planar MOSFET Memory using double junction tunneling
大場　竜二、三谷　祐一郎、杉山　直治、　藤田　忍

⑪研究論文：東芝レビュー2006 年 2 月号
題名：超小型乱数発生素子
棚本　哲史、大場　竜二、藤田忍

⑫新聞発表：日刊工業新聞 2006 年 3 月 6 日
題名：Si ナノ微粒子 MOSFET による高速乱数生成
大場　竜二、安田　心一、棚本　哲史、藤田　忍

□平成 16 年度

①学会：◎Electrical Properties of Two-Dimensional Systems(EP2DS-16)
題名：Robustness of Decoherence-Free States for Charge Quantum bits under Local Non-uniformity
棚本　哲史、藤田　忍
②学会：物理学会 2004 年秋季大会
題名：量子細線脇におかれた量子ドットの伝導に与える効果
棚本　哲史、藤田　忍
③研究論文：東芝レビュー2004 年 11 月号
題名：Si ドット MOSFET を用いた情報セキュリティ用高速乱数生成
大場　竜二、安田　心一、内田　建、棚本　哲史、藤田　忍
④学会：(招待講演) 回路とシステム学会 2004
題名：Small Random Number Generator With A Novel Noise Source Device
安田　心一、野崎　華恵、棚本　哲史、大場　竜二、内田　建、藤田　忍
⑤研究論文：◎IEEE Journal of Solid State Circuits
題名：Physical Random Number Generator Based on MOS Structure After Soft-Breakdown
安田　心一、棚本　哲史、大場　竜二、内田　建、藤田　忍
⑥セミナー：(パネル講演) Summer Seminar of Systems beyond Silicon
題名：New hardware for security.
藤田　忍
⑦学会：(パネル講演) International Symposium on High-Performance Computer Architecture, Informal meeting.
題名：Issues of future security systems.
藤田　忍

□平成 15 年度
①学会：◎IEEE　NANO 2003
題名：Ultra-Small Random Number Generators Based on Si Nano-Devices for Security Systems and Comparison to Other Large Physical Random Number Generators
安田　心一、内田　建、棚本　哲史、大場　竜二、藤田　忍
②学会：◎International Conference on Solid State Devices and Materials
題名：Ultra Small Random Number Generating Circuits With A Novel Noise Source Device
安田　心一、野崎　華恵、棚本　哲史、大場　竜二、内田　建、藤田　忍
③学会：◎Fundamental Problems of Mesoscopic Physics Interactions and Decoherence（Euresco Conference）
題名：Measurement of Two-Qubit States Detected by Quantum Point Contacts
棚本　哲史
④学会：物理学会秋季大会
題名：量子ポイントコンタクトによる二量子ビットの観測理論
棚本　哲史
⑤研究論文：◎Journal of Applied Physics Vol. 94, pp.3979-3983 (2003)
題名：Noise power spectrum of a long-channel current line with electron traps: Slave-boson mean field theory
棚本　哲史、大場　竜二、内田　建、藤田　忍
⑥学会：International Symposium on Quantum Dots and Photonic Crystals 2003
題名：Small Random Number Generator With A Novel Noise Source Device
安田　心一、野崎　華恵、棚本　哲史、大場　竜二、内田　建、藤田　忍

⑦研究論文：◎IEEE Journal of Solid State Circuits
題 名 ： Physical Random Number Generator Based on MOS Structure After Soft-Breakdown
安田　心一、棚本　哲史、大場　竜二、内田　建、藤田　忍
⑧学会：◎International Electron Device Meeting 2003（IEDM2003）
題名：Narrow－channel－MOSFET having Si-dots for High-rate Rundom-number Generation
大場　竜二、安田　心一、内田　建、棚本　哲史、藤田　忍
⑨学会：◎2004 IEEE International Solid-State Circuits Conference
題名　：Novel Si nanodevices for random number generating circuits for cryptographic application
藤田　忍、内田　建、安田　心一、大場　竜二、棚本　哲史

□平成 14 年度
① 学 会 ： ◎ International Conference on Solid State Devices and Materials 2002(SSDM2002)
題名：Novel Random Number Generator Using MOS Gate After Soft-Breakdown
安田　心一、棚本　哲史、藤田　忍
②学会：◎International electron device meeting 2002
題名：Single-Electron Random-Number Generator (RNG) forHighly Secure Ubiquitous Computing Applications
内田　建、棚本　哲史、大場　竜二、　安田　心一、藤田　忍
③新聞発表：朝日新聞、読売新聞、毎日新聞、日経新聞他
題名：Si ナノデバイス（単一電子素子）を用いた乱数生成回路について
内田　建、棚本　哲史、大場　竜二、　安田　心一、藤田　忍
④学会：応用物理学会
題名：単一電子素子におけるノイズ解析
棚本　哲史、内田　建、大場　竜二、　安田　心一、藤田　忍
⑤学会：応用物理学会
題名：ソフトブレークダウンした絶縁膜を利用した高度乱数生成回路
安田　心一、棚本　哲史、内田　建、大場　竜二、　藤田　忍
⑥学会：◎Nanotech 2003
藤田　忍、内田　建、安田　心一、大場　竜二、棚本　哲史
題名：Novel Random Number Generators based on Si nanodevices for Mobile Communication Security Systems
⑦学会：米国物理学会
題名：Noise power spectrum of single electron transistor (SET) having many electron traps: slave-boson mean field theory
棚本　哲史、内田　建、大場　竜二、　安田　心一、藤田　忍

※尚、②と⑥の学会で、注目すべき論文に選ばれた。