管理番号＃１３－０３

平成１６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１７年５月

情報通信研究機構

平成１６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

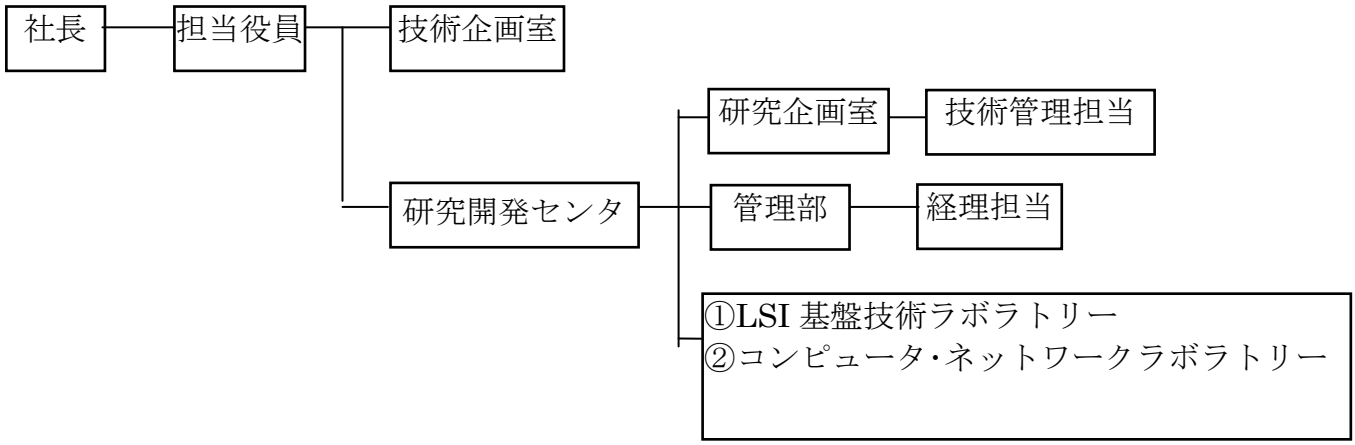
（金額は非公表）

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
藤田忍
主任研究員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）①

（２）デバイス・回路試作担当
大場　竜二　研究主務（主担当）①
内田　健　　研究員①
安田　心一　研究員①

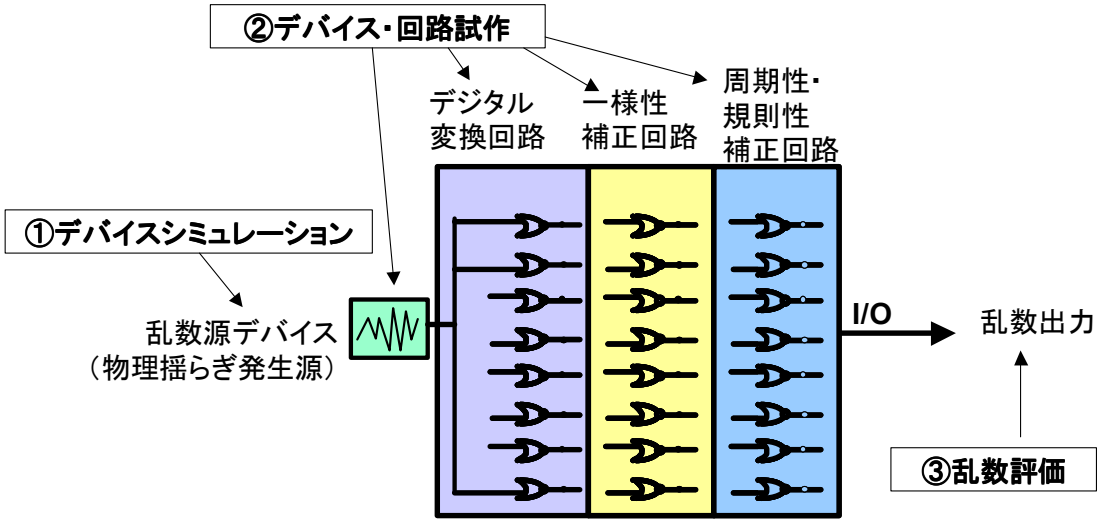
（３）乱数評価担当
藤田　忍　　主任研究員（主担当、研究代表者兼務）
棚本　哲史　研究主務①
野崎　華恵　研究主務②

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

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、これまで通り継続して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。



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 16 年度は、①のデバイスシミュレーションと、②のデバイス・回路試作、特に乱数源デバイスの開発に重点をおきながら研究を進めるが、②のデバイスでは平成 15 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、これまで設計してきた乱数化回路部をさらに改良を加える。③の乱数の評価については、平成 15 年度までに行ってきた回路を実際に暗号のアプリケーションに盛り込んだ際のセキュリティ

強度の評価を具体化する。

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、具体的な計画を以下に記す。

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

平成 15 年度までは、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を元に、デバイス物理のシミュレーションを行ってきた。トラップ準位(量子ドット)が電流に及ぼす影響について、スレーブボソン法を用いて計算した。また、より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複雑な非平衡 Green 関数の表式を導出することに成功した。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。今年度はこの 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。

４－１－２　研究の実施状況

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。

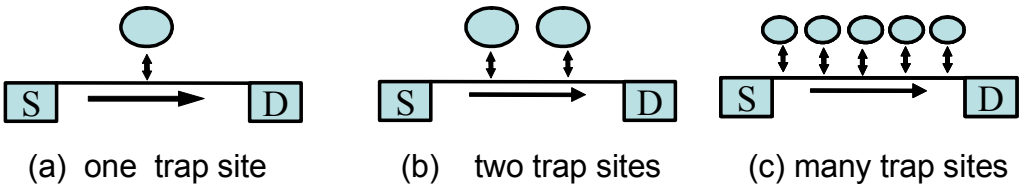


図１：電気伝導を計算した３つのトラップの配置

電気伝導度については一般化された Landauer 公式(Y. Meir and N. S. Wingreen and P. A. Lee, Phys. Rev. Lett.Vol.66, p3048 (1991))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。まずトラップ準位が一つの場合の Green 関数は

$$G^r_{kk}(\omega+i\delta)=\frac{1}{\omega-\varepsilon_k+i\gamma}+\frac{1}{(\omega-\varepsilon_k+i\gamma)^2\left[\omega-\varepsilon_f-\dfrac{|V_k|^2}{\omega-E_F+i(D+\gamma)}\right]} \qquad (2)$$

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：

$$G=\frac{4e^2}{h}\frac{\Gamma_L\Gamma_R}{(\Gamma_L+\Gamma_R)(D+\gamma)}\frac{(\varepsilon_f-E_F)^2}{(\varepsilon_f-E_F)^2+\Delta_1^2} \qquad (3)$$

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

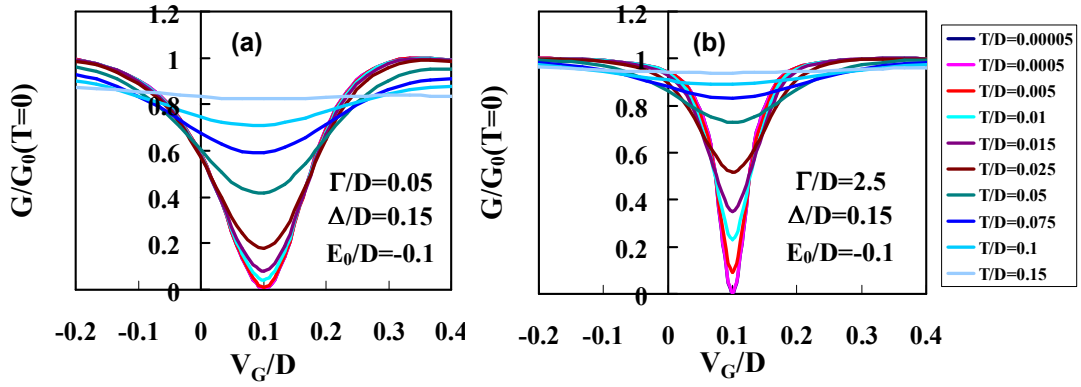


図２トラップが一つの場合のゲートバイアス依存性。(a) $\gamma<D$。(b) $\gamma>D$

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、昨年ノイズを計算したときと同様に Hamiltonian を二つの独立な部分に分離することができる。その結果、電気伝導度はその独立部分に対する式(3)と同様な式の和で表されることがわかった。

最後に図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。

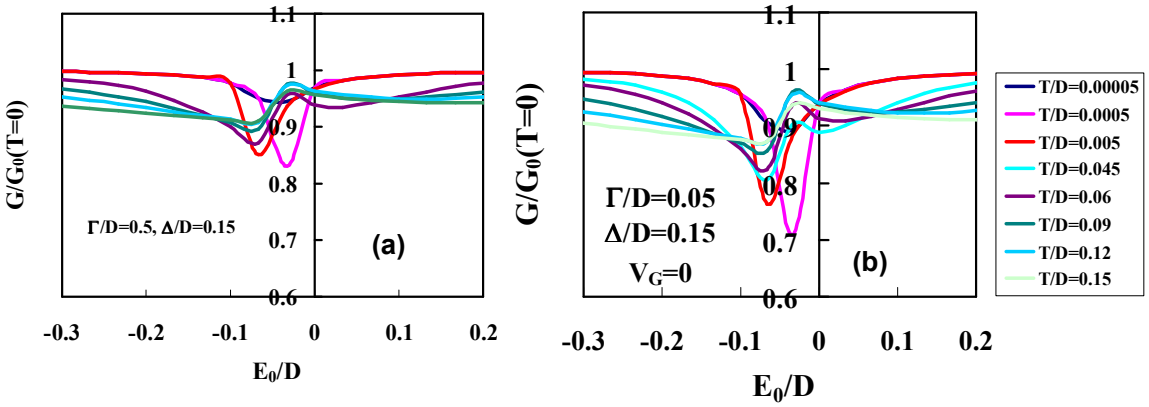


図 3 トラップが多数(図 1(c))場合のゲートバイアス依存性。(a) $\gamma < D$。(b) $\gamma > D$

H16 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 である。

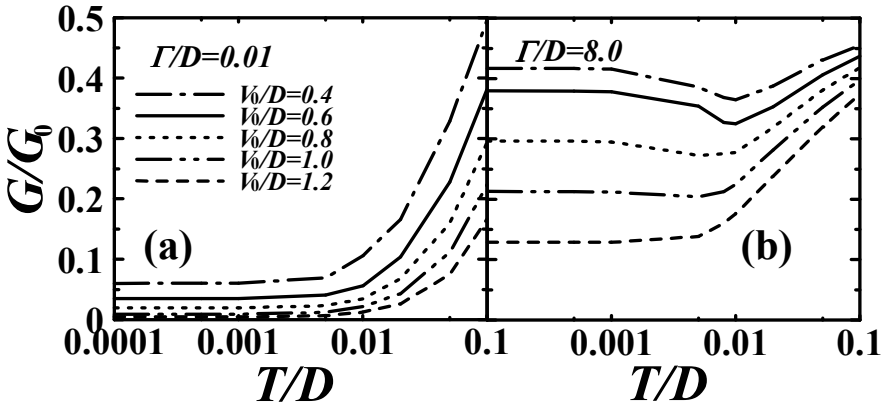


図 4 電気伝導度の温度依存性。V_0 はトラップと伝導体との結合の強さを表す($\Delta_1 = V_0^2/D$)。(a) $\gamma < D$。(b) $\gamma > D$ ($\gamma \propto \Gamma$)。

図 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 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。

４－１－３　まとめと今後の課題

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。今年度はこの 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。今後は、シミュレーションの最終段階として、これらの基礎的モデルの上にデバイス設計のモデルを構築することを目指す。

４－２　デバイス・回路試作に関わる研究開発

４－２－１　序論

1)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,または､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、または、3)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を使って、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と同等またはそれ以上の乱数が得られた｡従って､本研究開発課題の目標に到達しうる超小型真性乱数回路が早くも確認できた。

さらに 1）を中心に、モバイル機器のシステムクロックと同等である MHz オーダーの乱数生成速度となるように、デバイス構造の改良を進めてきた。このデバイスは、電子のトンネル現象が揺らぎの源であり、他と比べると、高速で揺らぐ信号強度が大きいが、MHz オーダーで乱数生成させるためには、通常のシリコン酸化膜中のトンネリングは速度が遅い。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ことを検討した。

また、高速で発生する揺らぎ信号をデジタルの 0,1 に変換する乱数変換回路もあわせて開発することが必要である。これまで開発した乱数変換変換回路は、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。これを改善する回路設計を新規に行った。

４－２－２　研究の実施状況

１）乱数源素子の開発

情報セキュリティに用いられる乱数発生源において、増幅回路無しで良質な乱数を高速に発生させる小型で低電力の素子が求められている。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。実際チャネル幅０．１μｍ程度のＳＯＩ細線ＳｉドットＭＯＳＦＥＴにおいては、トンネル酸化膜１ｎｍ程度とすることで、２５ｋＨｚの生成レートで高品質な乱数の生成が増幅回路無しで可能であることを昨年報告した。しかしながらセキュリティ上の多くの用途のためには、数 MHz の生成レートで高品質な乱数の生成が求められているので、より高周波なランダムノイズ生成源が必要である。

今回。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ので報告する。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$1\times10^{12}\mathrm{cm}^{-2}$である。断面構造を図１，２に示す。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。

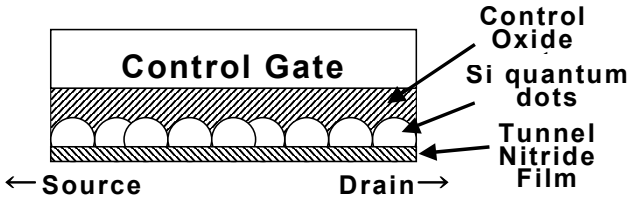


図１：素子断面構造図

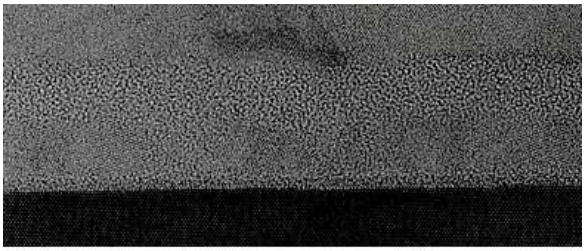


図２：断面ＴＥＭ像

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２．５×$10^{11}\mathrm{cm}^{-2}$、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。図４には、先と同じＳｉドット密度２．５×$10^{11}\mathrm{cm}^{-2}$と、その 2 倍の５×$10^{11}\mathrm{cm}^{-2}$の場合の電流ランダムノイズを示す。ランダムノイズはおよそ$2^{1/2}$＝１．４倍程度増えている。重ねあわせが頻繁になると揺らぎは重ね合わされる数の１／２乗に比例する、という統計学の定理によるものである。

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$1\times10^{12}\mathrm{cm}^{-2}$でまで増やした場合を見てみる。図５には、図３にも示したトンネル酸化膜でＳｉドット密度２．５×$10^{11}\mathrm{cm}^{-2}$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$1\times10^{12}\mathrm{cm}^{-2}$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６はトンネル窒化膜で密度$1\times10^{12}\mathrm{cm}^{-2}$の場合のＬによる比較を示す。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７には、この時のＬ＝０．０４μｍでの電流ランダムノイズを示す。現時点得られている最も強いランダムノイズである。

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

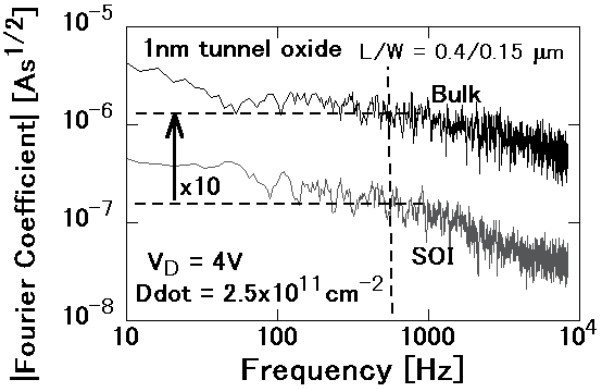


図３：電流ランダムノイズフーリエ特性。ＳＯＩ構造とバルク構造。

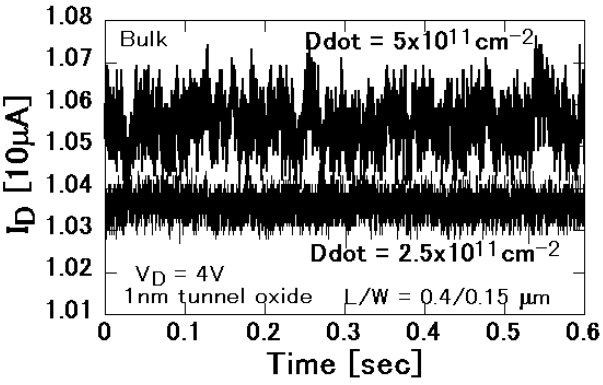


図４：電流ランダムノイズ特性。Ｓｉドット密度を変えた場合の比較。

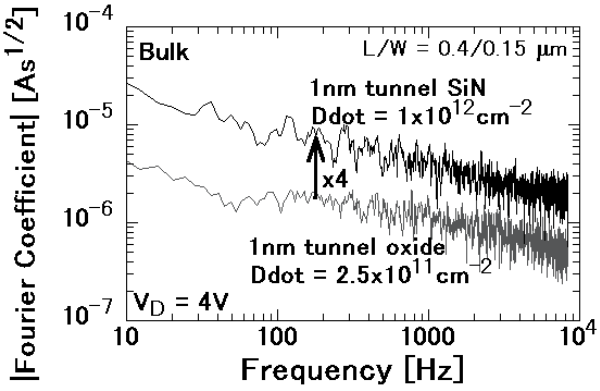


図５：電流ランダムノイズフーリエ特性。トンネル膜とＳｉドット密度による改善。

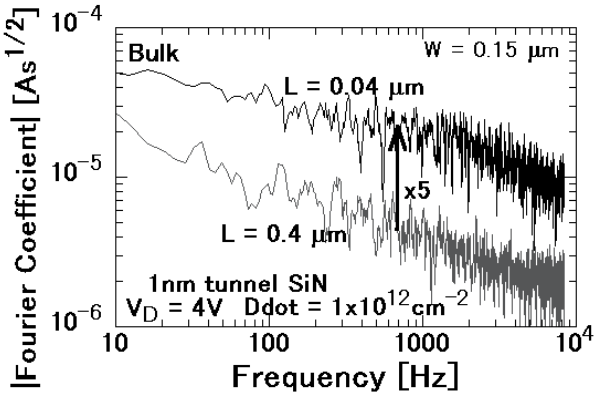


図６：電流ランダムノイズフーリエ特性。チャネル長変化による改善。

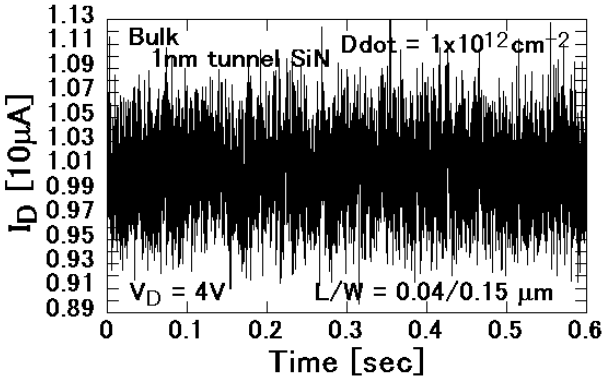


図７：現状最もおおきな電流ランダムノイズ特性。

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８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。

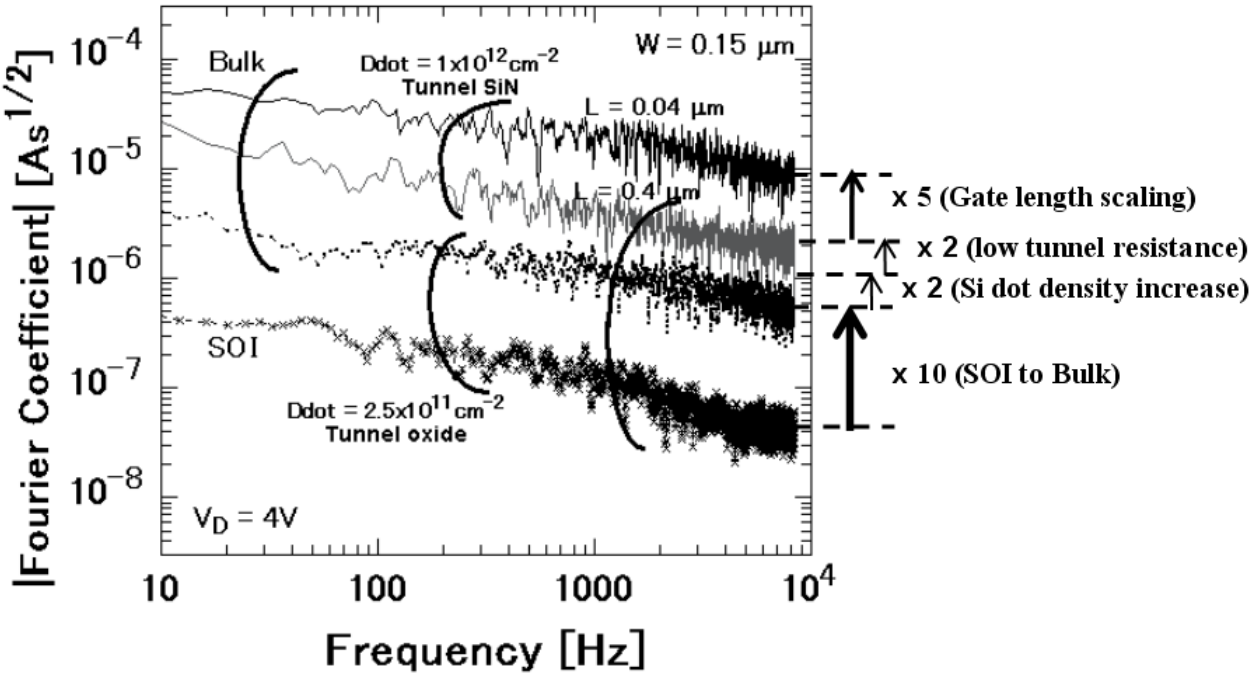


図８：各種素子設計による電流ランダムノイズ特性改善。２５ｋｂｉｔ／ｓで真性乱数生成したもの（一番下）から、２００倍の改善をなす。

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を行った。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する。まず、SiO2 と SiN の電流―電圧静特性を測定した（Fig.1、Fig.2)。サンプルはどちらも MIS キャパシタ構造、面積は 100umx100um、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。これは電子トンネリングが起こりやすいことを意味している。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。今後は動的なトンネル特性とデバイス特性の比較も行う予定。

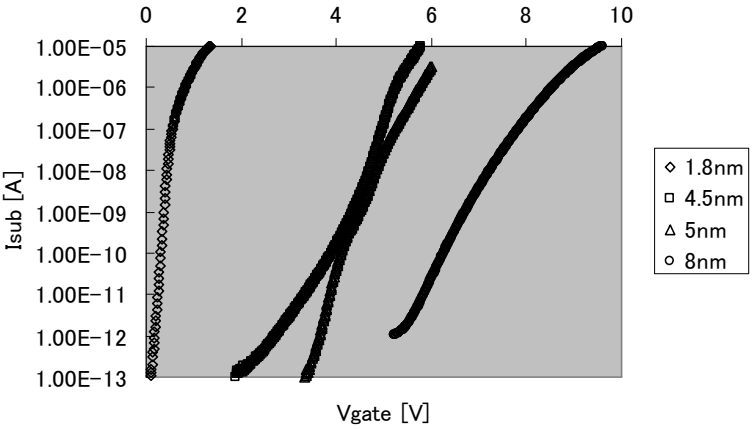


Fig.1　SiO2 膜の電流－電圧特性

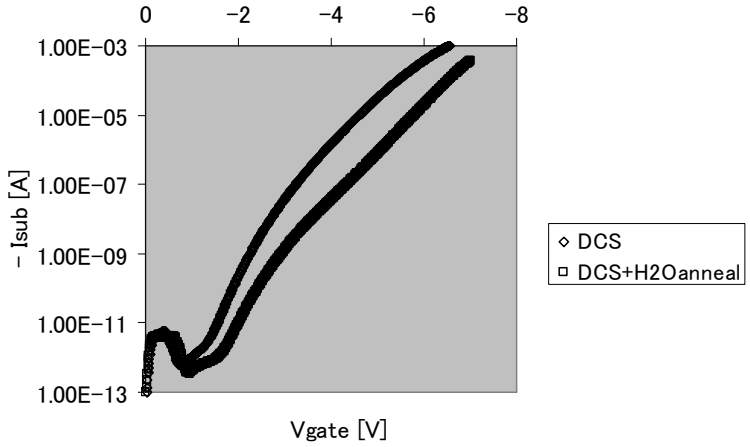


Fig.2　SiN 膜の電流－電圧特性

２）乱数変換回路の開発

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。今回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 0.25 micron 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。

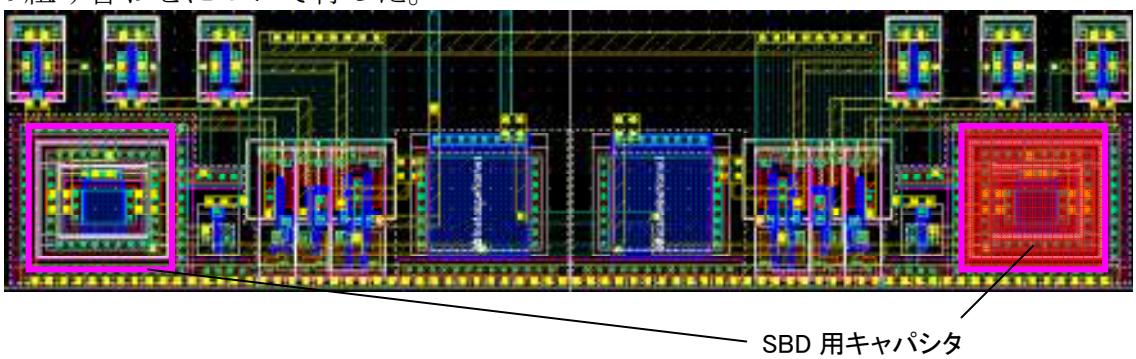


図１　SBD 用キャパシタ付きマルチバイブレータ乱数生成回路のレイアウト

図１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 micron x 13.64 micron 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 116.34 micron x 14.24 micron 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。

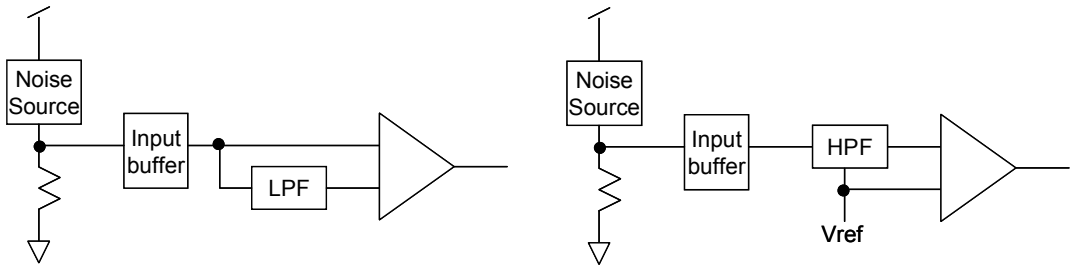


図２　フィルタと差動増幅を使った乱数生成方式

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。

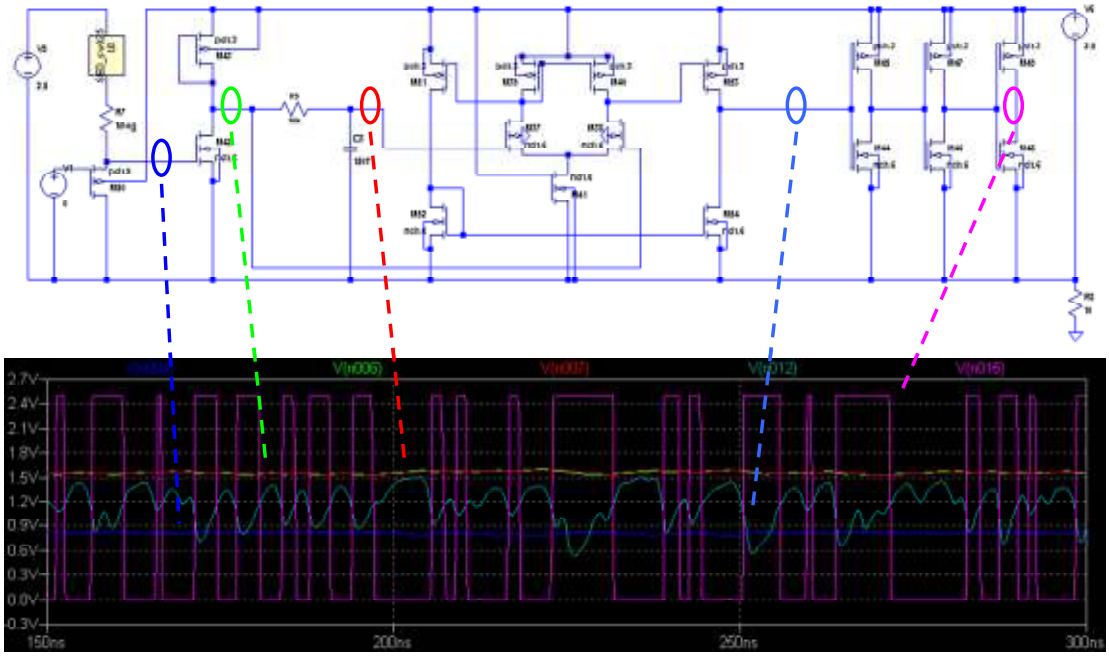


図３　LPF を使った方式の回路図とシミュレーション結果

図３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 0.25 micron 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。入力バッファは、簡便にするために、一段増幅器の構成を用いたが、増幅効果は必要ないため、むしろ SBD 後のキャパシタの抵抗値がランダムになってしまうことを考慮し、動作電圧の範囲が大きくなるように作製した。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 Mbps ~ 数十 Mbps 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。これまでの SBD 後のキャパシタのノイズ特性を考えると、これは高すぎる値であると考えられ、今後実験を通じて、面積とのトレードオフを考慮しながら、チューニングを行う。

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。

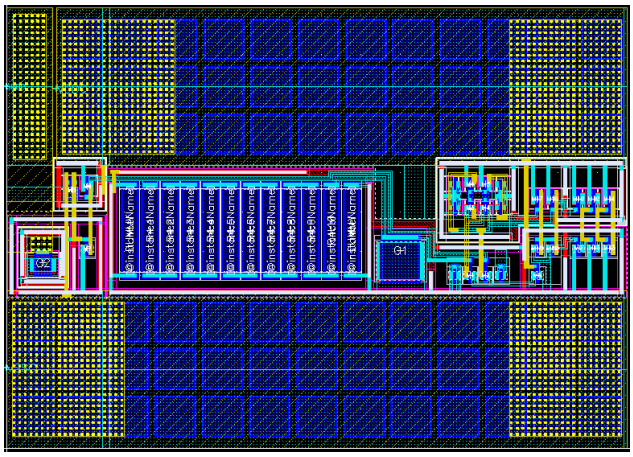


図４　LPF と差動増幅器を使った乱数生成回路のレイアウト

図４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。レイアウトは TSMC の 0.25 micron mixed signal のセットで行った。レイアウト面積は、上下の電源とグラウンドの配線を除けば、78.84 micron x 15.91 micron というサイズであった。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。

４－２－３　まとめと今後の課題

以上のように、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。今後、これらの回路の試作、測定、動作検証を行い、各素子パラメータと回路面積を考慮しながら乱数生成回路の１チップ化を目指す。

４－３　乱数評価に関わる研究開発

４－３－１　序論

H15 年度までは、統計的検定と統計検定結果自身の統計性の分析を使って、試作した乱数生成回路の評価を行ってきた。H16 年度は、これらの乱数評価データ量を上げて、評価の精度をもう一段上げることを試みた。

具体的には、大規模な乱数データを用いて、一回のみの統計検定ではなく、非常に多くの統計検定を行いる。さらに、検定で出てきた値自身が、数学的な真性乱数に対して、どのような差が見られるかを定量化するという手法である。これは、最終目標のひとつである。

また、H15 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。これは、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、これまでの一面的な統計的な検定だけでは、十分ではないという議論である。大まかな予測としては、現在の情報セキュリティで求められている乱数のレベルから、上記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、H16 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、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 H15 年度に続いて開発した。

４－３－２　研究の実施状況

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について

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。

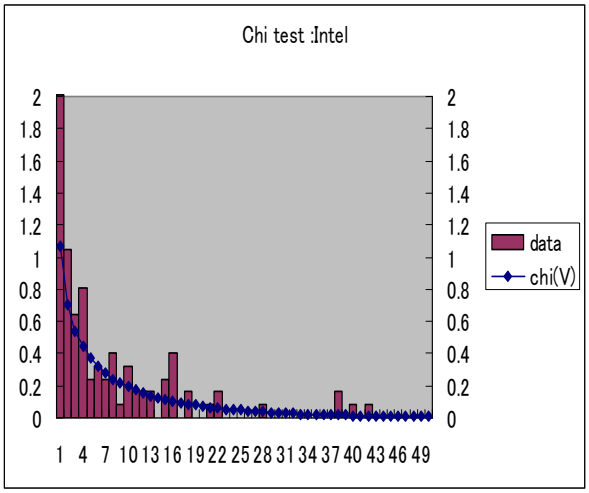
しかしながら、Intel のチップセットに入っている乱数生成期をはじめ最近の乱数はだいたい上記の二つの有名な乱数検定はパスすることがわかっている。そこで、我々はある程度以上の乱雑度をもった乱数間の比較を行うべく、より高度な検定方法について調べている。そこで、まず原点に返り、検定方法のうち０と１のバランスを図る最も基本的な検

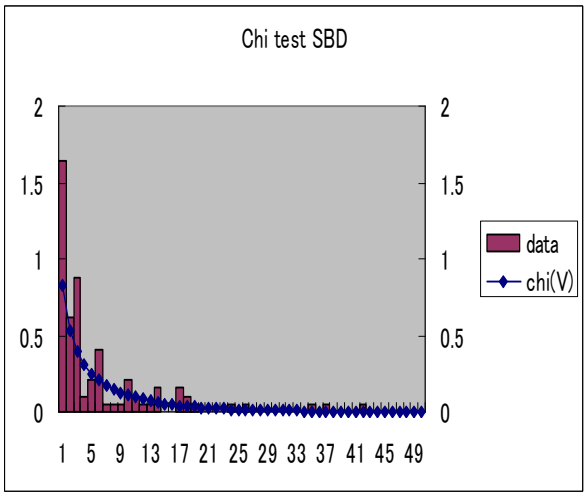
定が χ^2 (カイ二乗)検定をベースに検定ソフトを作成した。これは上記の FIPS140-2 や NIST800-22 などが多数のデータを統計分布として扱ったとき、どの程度数学的理想曲線からずれているかを評価すべきところを、簡便さのため棄却率という値を決めて、数値一点で乱数度を検定していることからくる反省でもある。上記のような一般検定、頻度検定、ポーカーテスト、系列検定、間隔検定などは検定の最後に必ず、カイ二乗曲線や、誤差関数が現れる。今回これらを分布として扱い、その理想数学曲線からのずれを乱数度と考えることにした。

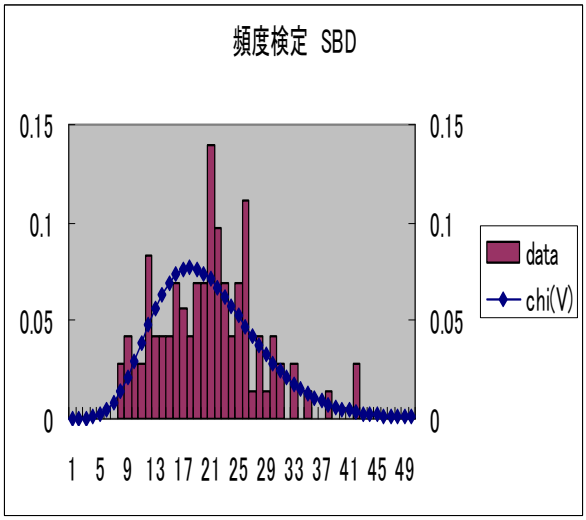
今回、グラフ化したのは

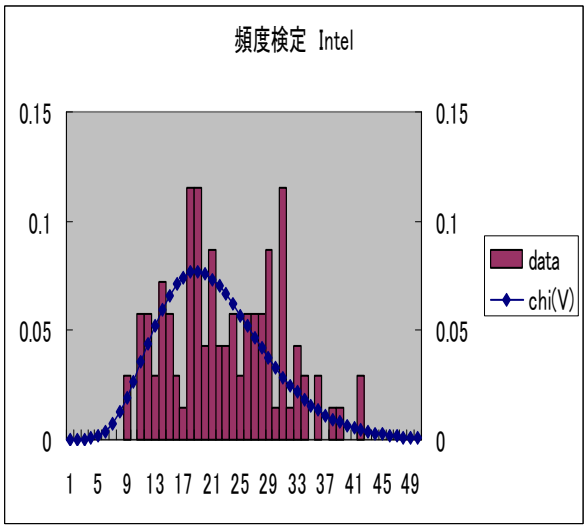
(1)カイ二乗検定　(2)頻度検定　(3)間隔検定　(4)ポーカー検定　(5)系列検定

の５項目である。ソフトは VC++を用いて作成した。









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

	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

となる。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。

セキュリティ応用からの乱数評価を目的として、H16 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ェア実装 --- 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。

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.

４－３－３　まとめと今後の課題

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。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。今後もこの延長線上で、評価を深掘りして行く。

４－４　総括

デバイスシミュレーションに関しては、基本となる素子モデルの厳密解（近似を使わない解）を得ることができた。これを土台にデバイス設計の計算に展開して行く。また、乱数源デバイスでは、MHｚオーダーで十分動作可能となるノイズスペクトルが確認できた。さらに、このような高速デバイスを前提に、ノイズを高い周波数帯でデジタル乱数に変換しうる回路を設計することができた。

一方、乱数評価のほうに関しては、最終目標のひとつである、大規模な乱数データを使った統計評価方法を開発することが出来た。さらに、同時クロック DPA 耐性という新たな評価方法に基づき、乱数とセキュリティ強度の相関を明らかにすることが出来た。

今年度の研究開発により、最終年度を待たずに、最終目標をほぼ達成することが出来た。

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）

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