平成１５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

（添付資料）

1　研究発表、講演、文献等一覧

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　研究開発分野の現状

スマートカード（セキュリティ機能付ICカード）を中心にセキュリティ機能を強化する傾向があり、ドイツのインフィニオン社等、乱数回路開発の動きがある。しかし、これは従来のデジタルLSIで作られた擬似乱数回路の改良型であり、本研究のように量子現象を取り入れた本格的な真性乱数生成回路を開発する動きは、他では未だ見えていない。

また、要素技術について本件と共通性が多い量子計算機用固体素子の基礎研究が進んでいる。その調査のために、米国物理学会定例会議に参加して調査した。量子計算機の実用化は最低でも10年は要すると思われる。当研究開発については、量子計算機の技術を参考にしながら、量子計算機の実用化よりも早期に実現することを目指している。

3　研究開発の全体計画

3-1　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。）

3-2　研究開発目標

3-2-1　最終目標（平成18年度末）

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。

3-2-2　中間目標（平成16年度末）

（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）

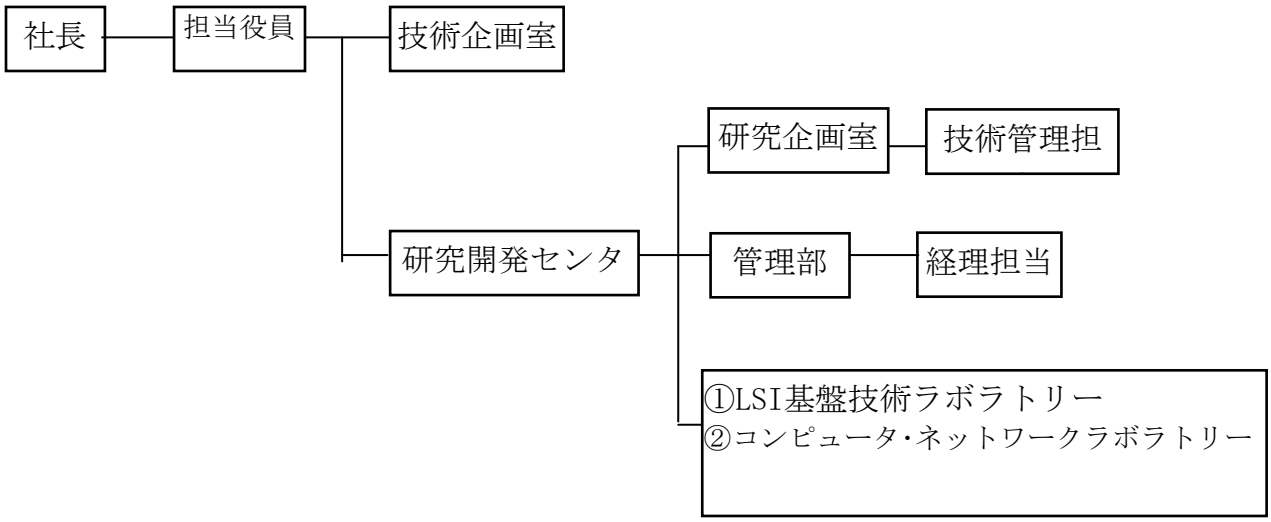
3-3　研究開発の年度別計画

（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							

3-4　研究開発体制

○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（平成15年6月末まで）
安田　心一　研究員①
安部　恵子　研究員①（平成15年7月から）

（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

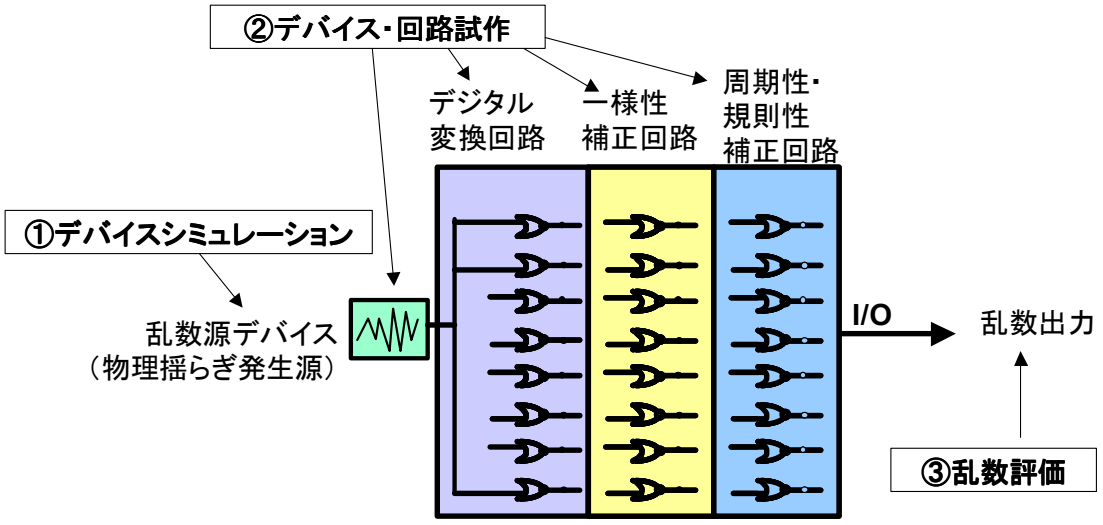
4　研究開発の概要（平成15年度まで）
4-1　研究開発実施計画

4-1-1　研究開発の計画内容

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（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、単純にはこれ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。

以下、研究開発の具体的計画内容を平成13、14、15年度ごとに記載する。尚、初年度の平成13年度は2ヶ月半のみであるで、平成14年度と一緒に記載した。



〈平成13、14年度の計画内容〉

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）からこの選定を開始している。今年度は、ひき続き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。並行して、③の乱数の評価についても、統計的手法を使った一般的なところから着手し、独自の評価手法を模索していく。

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。

①デバイスシミュレーションに関わる研究開発

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。電子は量子ドット内で波動として振る舞い、量子ドットが近接していれば、量子ドット間で波動の干渉性を保ちながら相互作用を行う。この状態がデバイスの電気的特性に理想的な揺らぎをもたらすことが予想される。基本的なデバイスの構成要素は、量子ドットと電子が伝導するチャネルの２つになる。量子ドットに電子が捕獲されているか否かで、チャネル中を伝導する電子の散乱の度合いが決まり、それが電気抵抗の変化に相当する。電気抵抗の変化の速さは、量子ドットとチャネルの間の電子トンネリング確率で決まる。これをシミュレーションしていく。まずは、平成13年度からの継続として、量子ドットと電子伝導を扱うためのモデルを解析的に計算し、デバイスシミュレーションの基盤を構築する。次に、これを②での実験データと相互比較しながら、シミュレーションモデルを現実に沿うように改良して行く。

②デバイス・回路試作に関わる研究開発

平成13年度は、前の図に示したデジタル変換回路部分を主に検討してきたが、今年度は乱数源デバイスの基礎的検討に注力する。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。現在考えられる候補は、

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る。これらを通して、揺らぎ信号源を絞り込んで行く。1)2)については、①のシミュレーションと比較して進める。

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、各々について回路構成を考える。また、変換されたデジタル信号の特性（一様性、非規則性）についても、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、回路構成を設計する。

③乱数評価に関わる研究開発

平成13年度では、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てきた。これを土台として、まずは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る。並行して、②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い、揺らぎ信号源の絞込みの判定基準として活用する。また、乱数の本質である予測困難性についても、指標化の方法を検討する。

<平成15年度の計画内容>

平成15年度も、ひき続き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14年度の研究成果を元に、候補となるデバイスを２つに分類して進める。③の乱数の評価については、平成14年度までに行ってきた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と言う観点から乱数を評価することを検討していく。

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。

①デバイスシミュレーションに関わる研究開発

平成14 年度に行った、スレーブ・ボソン法を用いたトラップ準位(量子ドット)が電流に及ぼす影響についての計算を発展させ、トラップ準位の影響そのものを見るためと、手法の限界から、電流には電圧がかかっていない平衡状態について調べた。本年度は、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う。具体的には、非平衡グリーン関数を用いたより一般的な手法で解くことを考える。これにより、乱数生成の高速化のための、デバイス構造設計指針につなげることを目指す。

また、本年度は新たに量子ドットが二つ結合した結合量子ドットを用いた場合の計
算を行う。電子が基板からトラップされる場所として結合量子ドットを使えば、トラップ保持時間を増やすことができるなど、素子特性が改善される。結合量子ドットの場合は結合量子ドットを構成する二つの量子ドット間のトンネリング時間が、新たな物理量として入ってくるので、現象を解析するためにはより詳細な理論検討が必要とされる。最終的に本計算は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を目指す。

②デバイス・回路試作に関わる研究開発

物理揺らぎの信号としての以下の候補が考えられる。

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
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

平成13、14年度の研究開発により、2) 4) 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。3)については直接実験していないが、4) と同様の原理である。

しかしながら、揺らぎ信号の平均的な時間が長く、乱数を生成する速度がkHオーダーで遅いという問題がある。本研究開発課題が目指すのはモバイル機器への搭載であり、これら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が望まれる。従って、2)～4）を使う場合には、擬似乱数のシードとして用いることが適当である。シードが真性乱数で得られる場合、擬似乱数回路でも真性乱数に近い特性が得られる。但し、その場合に、擬似乱数回路自体を乱数源デバイスの特性に応じて最適化する必要がある。または、2)～4）を用いた”遅い”乱数生成回路に、別の回路を設けて擬似的に高速化させる方法もありうる。2)～4）を利用したこれらの回路の検討を平成15年度に行う。

1)については電子のトンネル現象が揺らぎの源であり、2)～4)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。酸化膜の厚さを1nm程度にしてもMHｚオーダーに届くかどうか微妙なところである。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する必要がある。もしくは、トンネル現象を起こす際に、積極的に電界をかけることで、電子を加速させ、同時にトンネル絶縁膜を実効的に薄くすることで、トンネルの速度を上げる方法もある。この操作はメモリの書き込み、消去動作に近いので、デバイス構造としてはメモリに近いものとなる。この2面について、1)を使った乱数回路の検討を平成15年度に行う。

③乱数評価に関わる研究開発

情報セキュリティのハードウエアの専門分野で、乱数評価についての議論が盛んになりつつある。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。端的な例が、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である。FIPS140-2で代表されるような乱数の検定では、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14年度までに行ってきた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拓していく。

4-1-2　研究開発課題実施計画

平成13年度　　（金額は非公表）

研究開発項目	第１四半期	第２四半期	第３四半期	第４四半期	計	備　考
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 研究開発全体の管理費						
間接経費						
合　　計						

平成14年度　　（金額は非公表）

研究開発項目	第１四半期	第２四半期	第３四半期	第４四半期	計	備　考
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						

平成15年度　　（金額は非公表）

研究開発項目	第１四半期	第２四半期	第３四半期	第４四半期	計	備　考
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						

4-2　研究開発の実施内容

平成13、14、15年度ごとに記載する。尚、初年度の平成13年度は2ヶ月半のみであるで、平成14年度と一緒に記載した。

＜平成13、14年度の研究開発実施内容＞

①デバイスシミュレーションに関わる研究開発

乱数の源として、シリコンの量子ドット（量子効果を示す微結晶）を近接して複数配置した構造を内包するシリコンデバイスを考えている。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される。平成13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をシミュレーションした。平成14年度は、この系において、チャネル中を流れる電流の揺らぎの周波数依存性を計算した。さらに、複数の量子ドットと電子チャネルの間をトンネルする系で、チャネル中を流れる電流の揺らぎの周波数依存性を計算した。

②デバイス・回路試作に関わる研究開発

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。

平成13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を行った。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14年度は、マルチバイブレータで発生させた乱数が、そのままでは真性乱数に近い高度な乱数にならないことから、乱数の質を高めるためのデジタル回路を開発した。また、単一電子トランジスタの揺らぎ信号を巨大化する条件を探り、信号をデジタル乱数化するための方策を考案した。

③乱数評価に関わる研究開発

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、②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14年度は、改良されたマルチバイブレータ型乱数回路や単一電子素子型乱数生成回路をはじめは比較的単純な統計的な検定で評価し、徐々に高度な統計的評価を試み、乱数生成回路へのフィードバックを行った。また、乱数の質とセキュリティ強度の関係を明確にするための方策を探った。

＜平成15年度の研究開発実施内容＞

①デバイスシミュレーションに関わる研究開発

平成14年度に続いて、乱数の源として、シリコンの量子ドットを近接して複数配置した構造を内包するシリコンデバイスの揺らぎ特性を計算した。より実際のデバイスに近いものにするために、電子チャネルに電圧勾配をもたせた構造で解析的に計算を行った。また、これらの基礎的な計算結果を実際のデバイス特性に反映させるため、フラッシュメモリ等、実デバイスのシミュレータを使って、量子ドットデバイスの特性をシミュレーションしてみることも試みた。

②デバイス・回路試作に関わる研究開発

平成15年度は、ソフトブレークダウンを必要としないデバイスを開発することに努めた。具体的には、最初からソフトブレークダウンした構造に近い「Siナノクリスタル二端子デバイス」を使って揺らぎ信号を発生させることを試みた。

また、多数の量子ドットを内蔵したトランジスタを新たに開発し、これまでのデバイスで問題となっていた信号発生速度の高速化を行った。

また、上記の乱数源デバイスから発生させる信号をデジタル信号に変換するための回路については、これまでは独自に開発した無安定マルチバイブレータ回路を使ってきたが、この回路も乱数生成速度を律速する要因となっていた。平成15年度から、デジタル信号変換回路（ADC）の改良を開始した。まずは、1/ｆ特性を除去することも同時に求められるため、アナログフィルター回路を使って、1/ｆ特性を白色化することを試みた。

③乱数評価に関わる研究開発

乱数検定に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を参照し、独自に検定項目を選択しながら、平成14年度まで乱数評価を行ってきた。しかしながら、これらの検定は、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年度から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。

５　研究開発実施状況（平成15年度）

5-1　　デバイスシミュレーションに関わる研究開発

5-1-1　序論

従来のデバイスシミュレーションにおいてはトラップ、散乱体などの効果は多数の統計平均をとってから取り入れられる。つまり従来のデバイスシミュレーションではトラップ、散乱体が多数存在することが仮定されている。ところが、デバイスサイズが小さくなるにつれてトラップ、または散乱体の数は少なくなり、通常のシミュレータが使えなくなることも考えられる。つまり本プロジェクトのように乱数発生という観点からは従来のデバイスシミュレータのそのままの使用は困難であると考えられる。この観点から我々は新しい理論的評価方法を開発している。

5-1-2　実施結果

デバイスシミュレーションに関わる研究開発ついては計画通りに実施した。以下に実施した内容を述べる。

昨年度はトラップ準位の引き起こすノイズに、1個の場合、2個の場合、多数の場合についてスレーブ・ボソン法を用いて調べた。その際、トラップ準位に近接した一元伝導体に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ている。今期は、特にその基礎となる計算をいくつか行った。系が非平衡状態にあるとき、前回のような厳密な対角化はできない。今回、この問題を扱う方法はGreen関数法が適当と考えた。なぜならGreen関数を求めれば、電流はそのGreen関数を用いて

$$I = \frac{4e\gamma}{h}\int d\varepsilon \sum_k \left[f_L(\varepsilon) - f_R(\varepsilon)\right]\left(-\mathrm{Im}\, G_k^r(\varepsilon + i\delta)\right) \qquad (1)$$

と表すことができるからである(ここで・=(・$_L$+・$_R$)/2、・$_{L,}$・$_R$はそれぞれソース、ドレインからトラップのある伝導領域へのトンネル確率をしめす)。トラップが一つでソース・ドレインのない場合の極限は先期に行った状況に帰着し、Kondo効果としても扱うことができる。この場合、Green関数は比較的簡単な形をしている。しかし、トラップ準位が二つ以上、そして散乱がある場合、Green関数もかなり複雑になっていく。図1に今回考えた状況を示す。

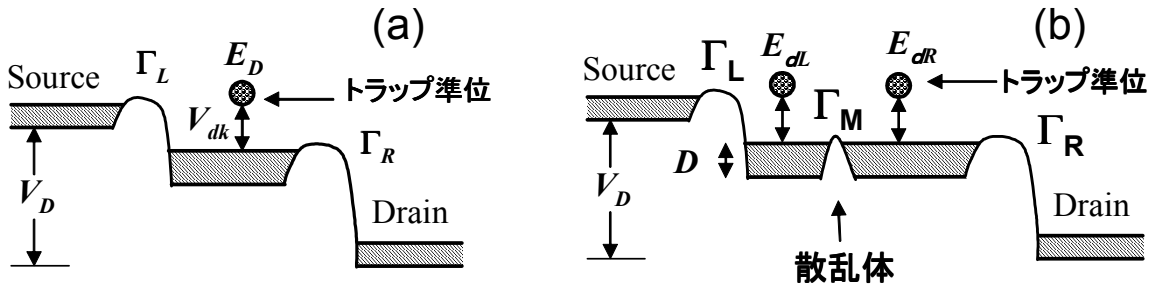


図5-1-1トラップ準位が存在する場合のバンド構造図

まず、トラップ準位が一つにソースとドレインのついた図1(a)の場合のGreen関数は

$$G^r_{kk}(\omega+i\delta)=\frac{1}{\omega-\varepsilon_k+i\gamma-\dfrac{|V_{dk}|^2}{\omega-E_D-\sum_{k_1}\dfrac{|V_{dk_1}|^2}{\omega-\varepsilon_{k_1}+i\gamma}+\dfrac{|V_{dk}|^2}{\omega-\varepsilon_k+i\gamma}}} \qquad (2)$$

となる。ここでV_{dk}がトラップへの伝導電子のトンネリングする割合である。・が小さい場合には通常のKondo効果のGreen関するに帰着する。これと比べて散乱体が中間にある場合のGreen関数(図1(b))はかなり複雑になる。ここでは電流の計算に必要な虚数部分のGreen関数を示す：

$$-\mathrm{Im}\,G^L_{kk}(\omega+i\delta)=\frac{\gamma_L}{(\omega-\varepsilon_{kL})^2+\gamma_L^2}+\frac{-C_2[(\omega-\varepsilon_{kL})^2-\gamma_L^2]+2\gamma_L(\omega-\varepsilon_{kL})C_1}{[(\omega-\varepsilon_{kL})^2+\gamma_L^2]^2(B_R^2+B_L^2)} \qquad (3)$$

ただし

$$\begin{cases}C_1=C_RB_R+C_IB_I\\ C_2=C_IB_R-C_RB_I\end{cases}$$

$$\begin{cases}C_R=|V_L|^2(\omega-E_{dR})+\gamma_M(\omega-E_{dR})(\omega-E_{dL})\\ C_I=|V_L|^2\Delta_R\end{cases}\quad\begin{cases}B_R=(\omega-E_{dL})(\omega-E_{dR})(1-\gamma_M)-\Delta_{dR}\Delta_{dL}\\ B_I=\Delta_R(\omega-E_{dL})+\Delta_R(\omega-E_{dL})\end{cases}$$

ここで・$_M$=・$_M$/2は散乱体を透過するトンネル確率、また・$_L$=・$_L$/2・・$_R$=・$_R$/2, ・$_L$∝V_L^2・・$_R$∝V_R^2である。

図２にトラップが一つの場合(図1(a))の電流電圧特性(式(1))の計算結果を示す。横軸はトラップ準位との結合定数の強さ(・$_0$∝V_{dk}^2)である。図をみてわかるようにトラップ準位との結合が強くなれば電流が著しく減少していくことがわかる。

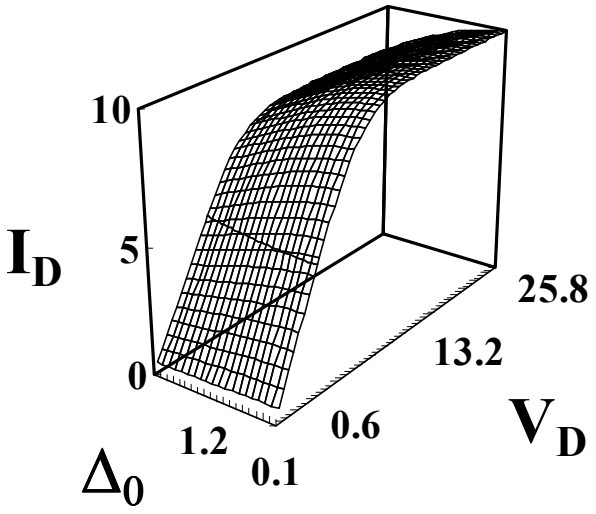


図5-1-2：トラップ準位が一つある場合(図5-1-1(a))の電流電圧特性

我々は通常のデバイスシミュレータでは予測することのできない微小デバイス領域のトラップ準位等の電流に与える影響を解析的な計算により調べている。これらの解析結果を生かすことを念頭に、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。

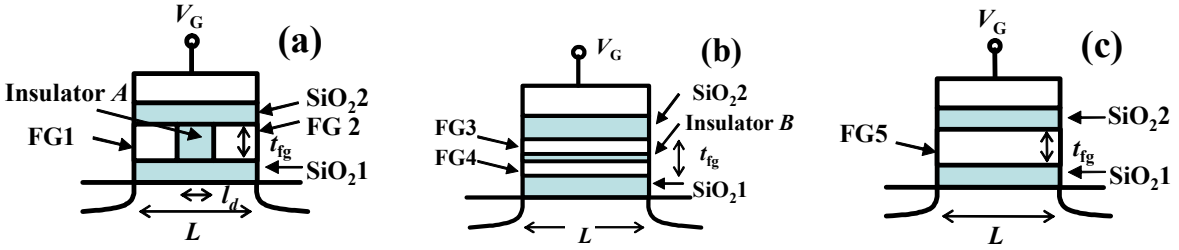


図5-1-3. (a)：横型フローティングゲート(floating gate：FG)構造。FG1とFG2はポリシリコンを仮定。(b)：縦型FG構造。(c)：(a)(b)と比較するための通常のFG構造。絶縁物A, B はSiO_2を含め、high-k材料を視野に入れ、誘電率を変化させる。

ゲート長は（L=0.2μm)，SiO_2 膜厚($SiO_2$1:9e-3 μm，$SiO_2$2:6e-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5e+17cm^{-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１．1.5V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2と3はそれぞれ、横型FG構造(図5-1-3(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(図5-1-4) 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(図5-1-5)、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5-1-3 (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5-1-6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。

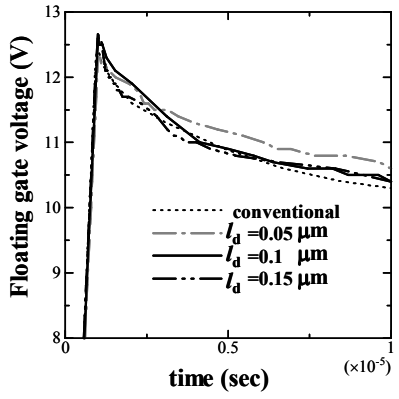


図5-1-4 横型FG構造(図 1(a))の書き込みデバイス特性。

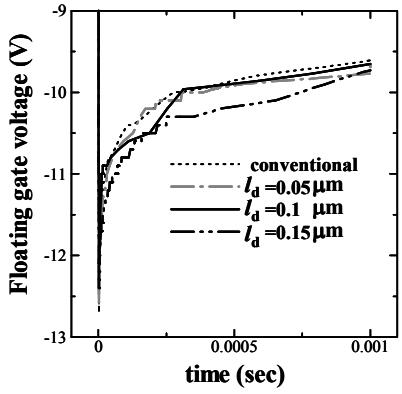


図5-1-5横型FG構造(図 1(a))の消去特性。

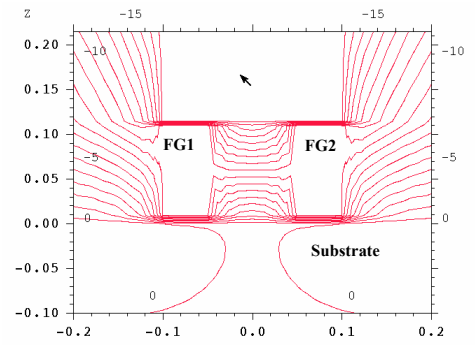


図5-1-6
横型FG構造の電位ポテンシャル分布。 l_d=0.1umの素子。

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]。もし二つの縦型FG構造を、単なるキャパシターの直列接合とみなした場合、このFG構造に余計に印加しなくてはならない電圧を大雑把に見積もることができる。もし二つのFGに同じ電荷Q がゲート電圧V_{G0}(=Q(1/C_1+1/C_2))で蓄積できたとすると、C_1 と C_2 をそれぞれSiO_2 1とSiO_2 2のキャパシタンスとして

$$V_G - V_{G0} = \frac{C_1 C_B}{C_B(C_1 + C_2)} = \frac{\varepsilon_1}{\varepsilon_B}\frac{d_B}{(d_1 + d_2)} \qquad (1)$$

が必要となる余分な電圧であることがわかる。ここでC_B は絶縁体B ($C_i \propto \varepsilon_i / d_i$, ε_i:誘電率, d_i :絶縁体の厚さ)のキャパシタンスである。 このように必要とされる電圧の大きさは絶縁体Bの誘電率のおおきさに半比例することがわかる。図5と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。

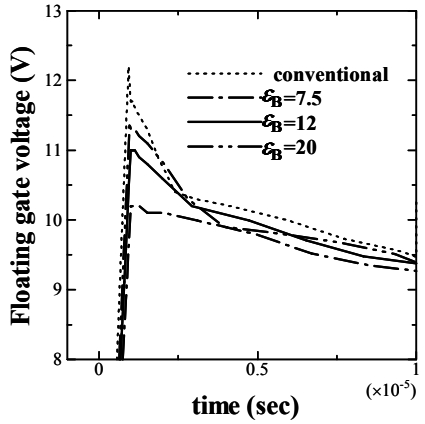


図5-1-7 縦型FG構造(図 1(a))の書き込みデバイス特性。

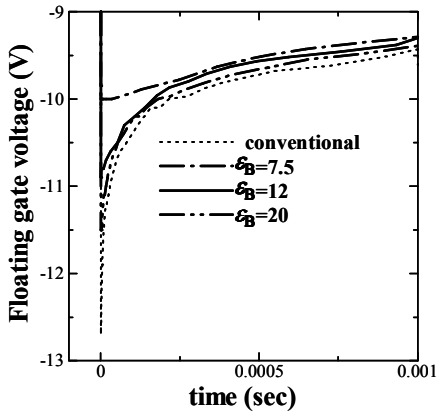


図5-1-8縦型FG構造(図 1(a))の消去特性。

以上のように、我々は二つの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。

5-1-3　今後の課題と展望

以上、トラップ準位のデバイス特性に与える影響を正確に求めることは、単純なデバイスシュミレータを使っただけでは不可能である。来年度は、以上の結果を踏まえ、従来のデバイスシミュレータの拡張と、ミクロな理論モデルを上手く融合させることにより、トラップ準位の影響を調べていく予定である。

5-2　　デバイス・回路試作に関わる研究開発

5-2-1　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、全体としてできるだけ小型な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。

平成13、14年度は、ソフトブレークダウンさせた絶縁膜から発生する物理揺らぎ信号を用いて、揺らぎ信号の1／f特性を除去する回路を使って、乱数発生を確認した。しかしソフトブレークダウンを起こすことは、実際の回路の中では容易でない。そこで、平成15年度は、ソフトブレークダウンを必要としないデバイスを開発することに努めた。具体的には、最初からソフトブレークダウンした構造に近い「Siナノクリスタル二端子デバイス」を使って揺らぎ信号を発生させることを試みた。

また、平成13、14年度は、単一の量子ドットを内蔵したトランジスタが巨大なデジタルランダム信号を出力することを見出し、質の高い乱数を得る方法を開拓した。しかし、このトランジスタの信号発生速度が平均で２秒に一回以下と、極端に遅いため、平成15年度は多数の量子ドットを内蔵したトランジスタを新たに開発し、信号発生速度の高速化を行った。

また、上記の乱数源デバイスから発生させる信号をデジタル信号に変換するための回路については、これまでは独自に開発した無安定マルチバイブレータ回路を使ってきたが、この回路は高速動作に向いていないことが分かってきた。この回路はCR発振回路の一種であり、我々が開発している乱数源デバイスは、基本的にナノスケール幅の電子チャネルを微小電流が流れるデバイスであり、デバイス抵抗Rが本質的に高い。抵抗Rはギガ Ω 程度になる。容量CはfF程度が下限であるから、CR時定数は μ 秒オーダーとなり、発振周波数は１MHｚ程度でしかなく、あまり高く出来ない。（理想的には発振周波数が数十MHｚ以上となることが望ましい。）平成15年度から、デジタル信号変換回路（ADC）の改良を開始した。まずは、1/ｆ特性を除去することも同時に求められるため、アナログフィルター回路を使って、1/ｆ特性を白色化することを試みた。

5-2-2　実施結果

デバイス・回路試作に関わる研究開発についての検討を計画通り実施した。具体的には、実施計画に記した、乱数源デバイスの高速動作に関して、デバイスの試作検討を行った。以下に実施した内容を述べる。

（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

これまで我々は、擬似破壊した酸化膜が大きな揺らぎ特性を示すことを利用して、無安定マルチバイブレータと組み合わせることで、周期性の無い高品質な乱数を得ることに成功している。しかし、このデバイスは、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。

素子の作製手順を図5-2-1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100um×100umである。

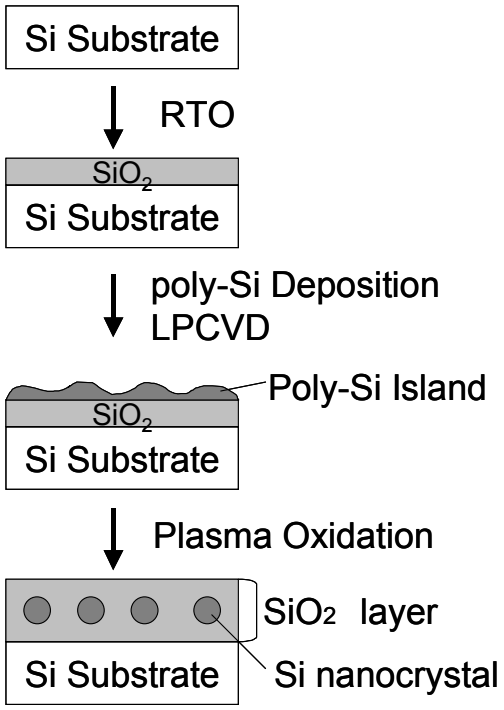


図5-2-1　Siナノクリスタルの作製

次に、作製した素子の断面TEM写真を図5-2-2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。

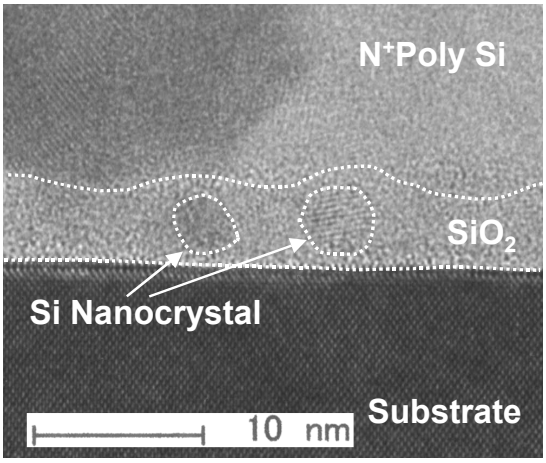


図5-2-2　ノイズ発生素子の断面TEM写真

図5-2-3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60・sである。

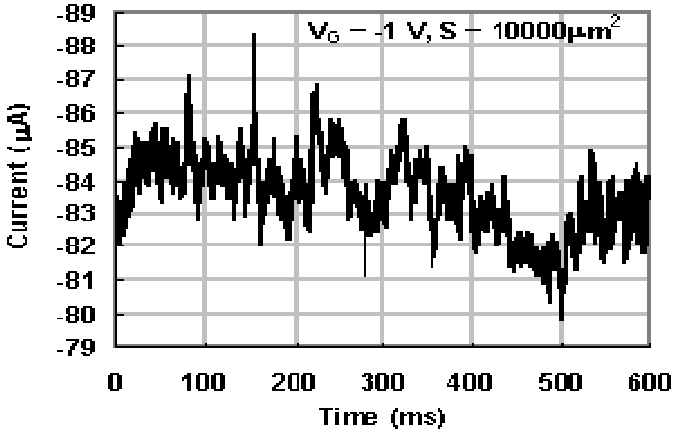


図5-2-3一定電圧-1 Vでの電流特性

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 ・A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。

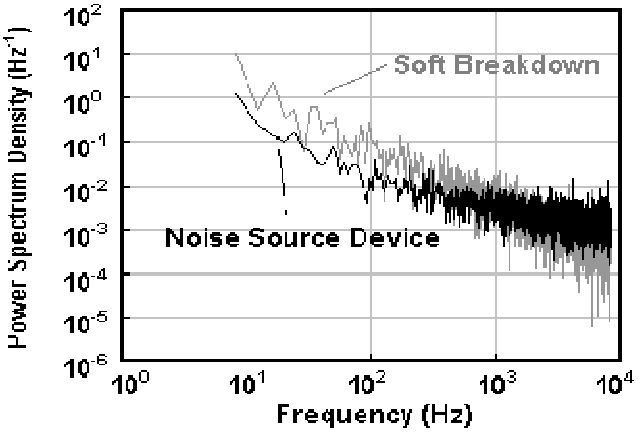


図 5-2-4　平均電流からの揺らぎの大きさをフーリエ変換して求めたパワースペクト

図5-2-4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。

なお、ノイズパワーの周波数依存性が擬似破壊酸化膜とノイズ発生素子で違っているが、これは擬似破壊の原因である酸化膜中のトラップと、ナノクリスタルの空間分布や状態密度などの違いからくるものと考えられる。ノイズ発生素子は周波数に対するノイズパワーの減少がゆるく、高速動作に好ましい特性を示しているが、これが本当に高速動作につながるかどうかは、今後慎重に検討していく必要がある。

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を用いて乱数化した。表5-2-１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。

	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 5-2-1　統計検定の結果

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MOSFETの電流揺らぎの利用

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。

素子構造を図5-2-5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 =２．５×１０^{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。

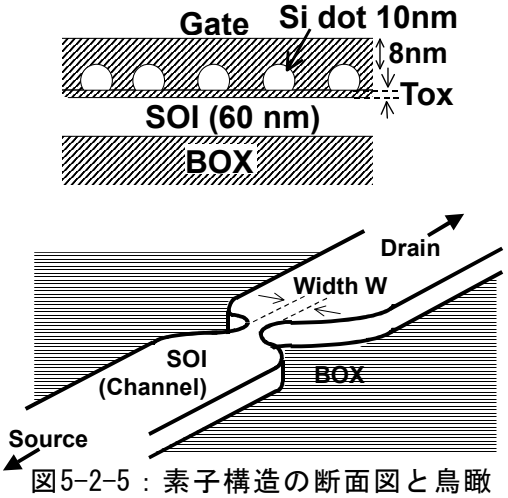


図5-2-5：素子構造の断面図と鳥瞰

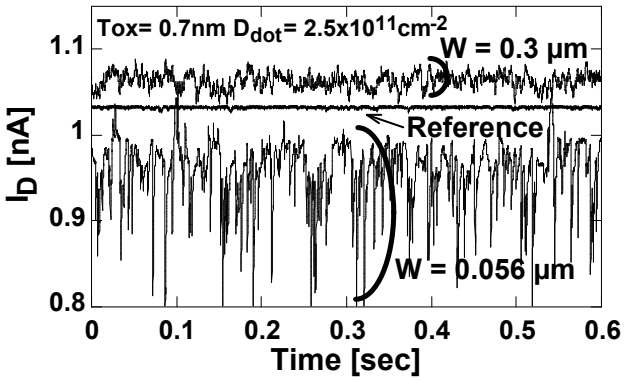


図5-2-6：電流揺らぎW依存

チャネル幅Wのみを変化させた時の電流揺らぎを図5-2-6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5-2-7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5-2-8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。

Ｓｉドット密度Ddotのみを変化させた時の電流揺らぎフーリエ特性を図5-2-9に示す。Ddotが高い程揺らぎが大きい。これは揺らぎの重ね合わせの影響によると考えられる。図5-2-10のフーリエ係数のDdot依存から、Ddotに比例して電流揺らぎは増大することがわかる。

トンネル酸化膜Toxのみを変化させた時のの電流揺らぎフーリエ特性を図5-2-11に示す。Toxの減少に対し、揺らぎは顕著に大きくなる。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。図5-2-12のフーリエ係数のTox依存から、電流揺らぎはTox減少に対し$10^{-Tox/0.37nm}$に従って指数関数的に増大していることがわかる。一方チャネル～Ｓｉドット間のトンネル抵抗Rtは、直接トンネルでの電子の実効質量を静止質量の０．３倍として、$Rt \propto 10^{Tox/0.24nm}$となることから、電流揺らぎはトンネル抵抗Rtに対し$Rt^{-2/3}$則に従って変化することがわかる。

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。

高速乱数生成のために、とりわけ重要なのはRt依存である。Rtはトンネル膜厚にも指数関数的に依存するが、トンネル障壁高の２乗根にも指数関数的に依存する。即ちトンネル膜厚０．８ｎｍ迄薄膜化することで、指数関数的に電流揺らぎの向上を実現させたが、さらにトンネル障壁高の低い絶縁体をトンネル膜に用いることにより、さらなる指数関数的電流揺らぎの高速化が可能である。つまり現状のSiO2（障壁高３．１ｅＶ）に対し、ＳｉＮ（２ｅＶ）、Hf02（１．５ｅＶ）、ＣｅＯ２（０．１ｅＶ）等の低トンネル障壁絶縁体を用いれば、飛躍的に電流揺らぎが高速化できることを意味しており、Ｓｉドット MOSFETは高速乱数源として極めて有望であることを示すものである。

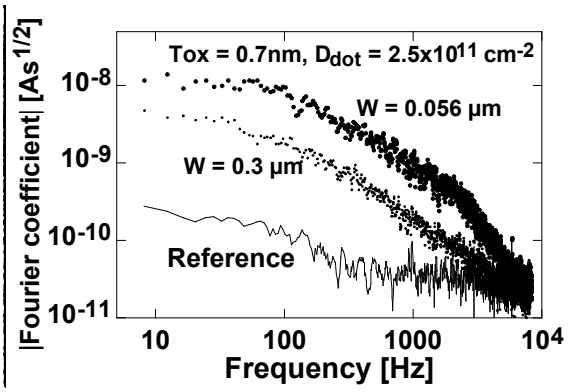


図5-2-7：電流揺らぎフーリエ特性W依存

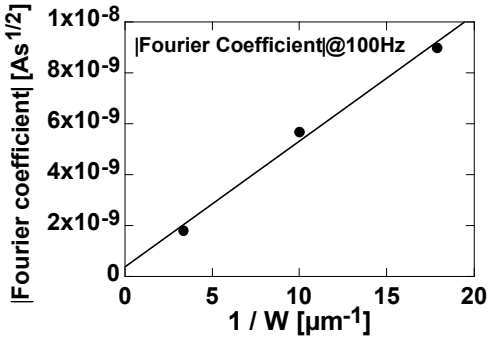


図5-2-8：電流揺らぎフーリエ係数W依存

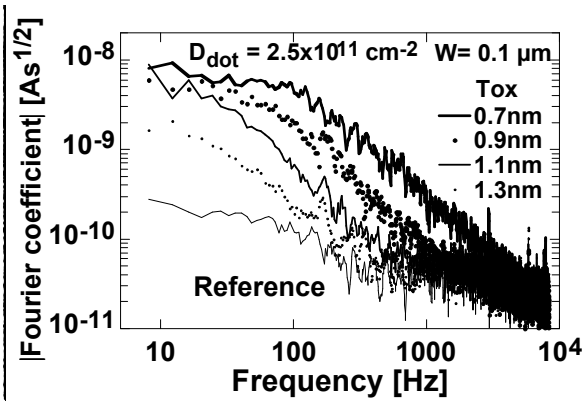


図5-2-9：電流揺らぎフーリエ特性Ddot依

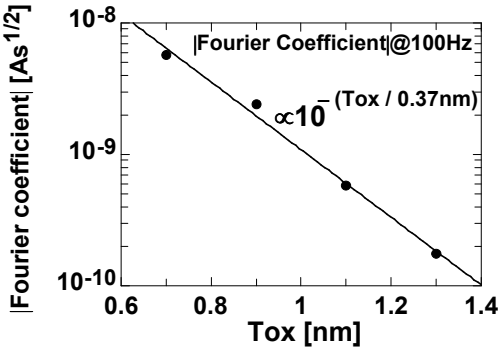


図5-2-10：電流揺らぎフーリエ係数Ddot依存

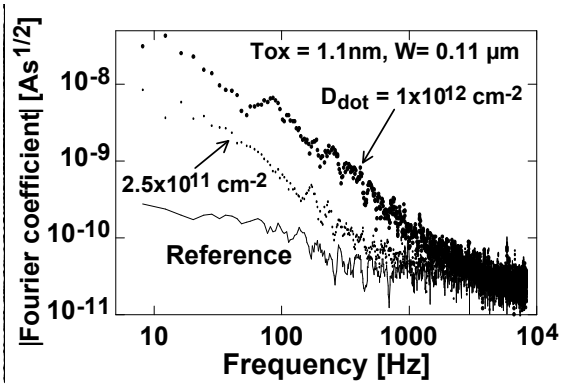


図5-2-11：電流揺らぎフーリエ特性Tox依存

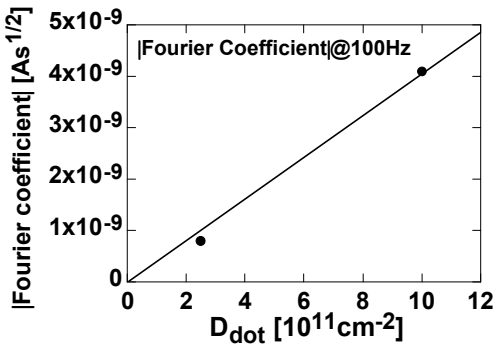


図5-2-12：電流揺らぎフーリエ係数Tox依存

上述のＳｉドットＭＯＳＦＥＴ ＲＮＧによって、増幅回路無しで高速乱数生成が可能である。例えば、図９のようなマルチバイブレータと1-bitカウンターを組み合わせた回路を用いればよい。用いた乱数源素子は T_{OX} = 0.7nm、W = 0.1μm、D_{dot} = $2.5x10^{11}cm^{-2}$ のものである。この時のアウトプットパルスの周期 t_J は、回路内のR_B×C_Bに相当するため、ＳｉドットＭＯＳＦＥＴに印加する電圧値によりその平均値を調整でき、さらに個々の周期 t_J は、上述のＳｉドットＭＯＳＦＥＴの顕著なID 揺らぎに応じて揺らぐことになる。

図5-2-13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ドットを有さないレファレンスＭＯＳＦＥＴの方では、ID揺らぎ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。

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１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、レファレンス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１１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、レファレンス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。

今回の２５ｋＨｚという生成レートは、ＩＤ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。

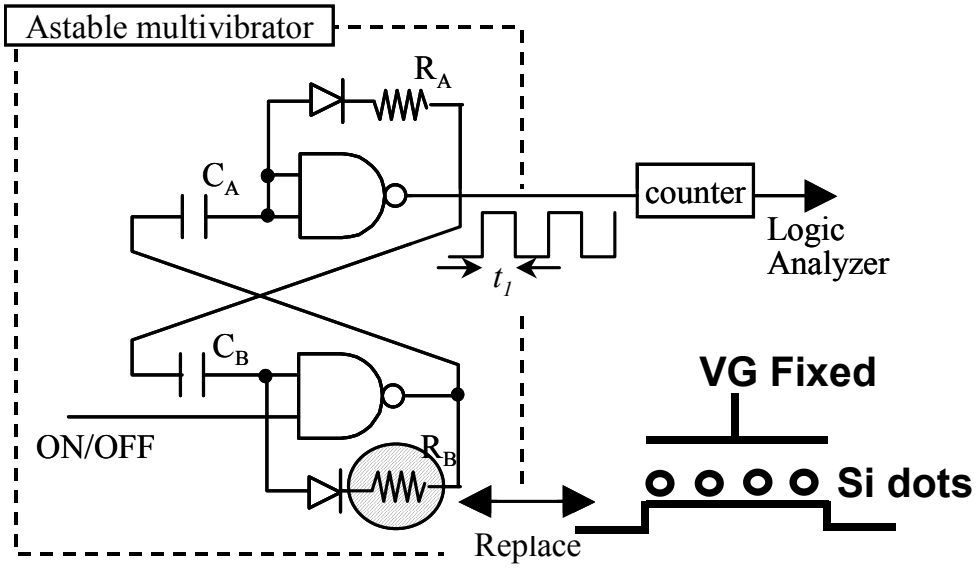
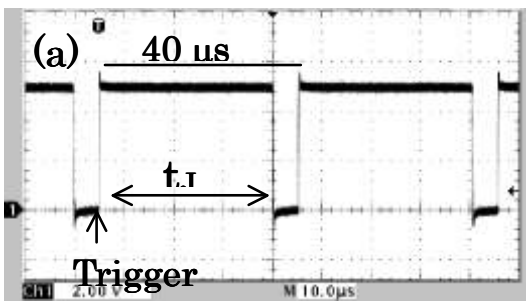


図5-2-13：乱数生成回路略図



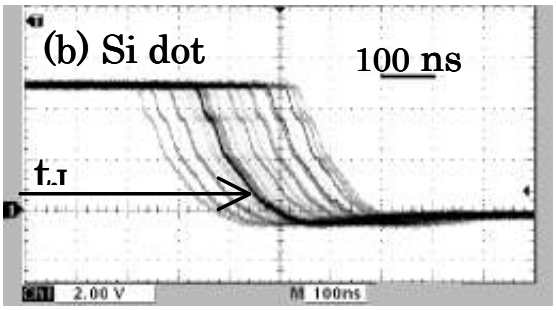
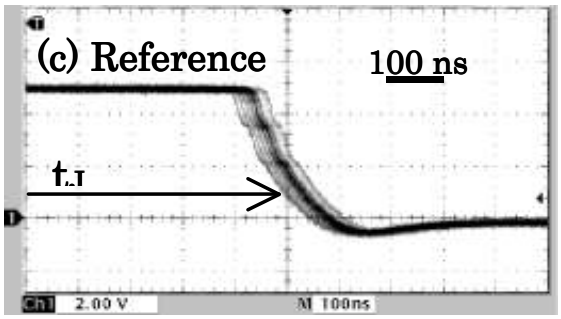


図5-2-14：アウトプットパルスの
オシロスコープ観察結果



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5-2-2：25 kbits/s の乱数列の真性度統計テスト結果

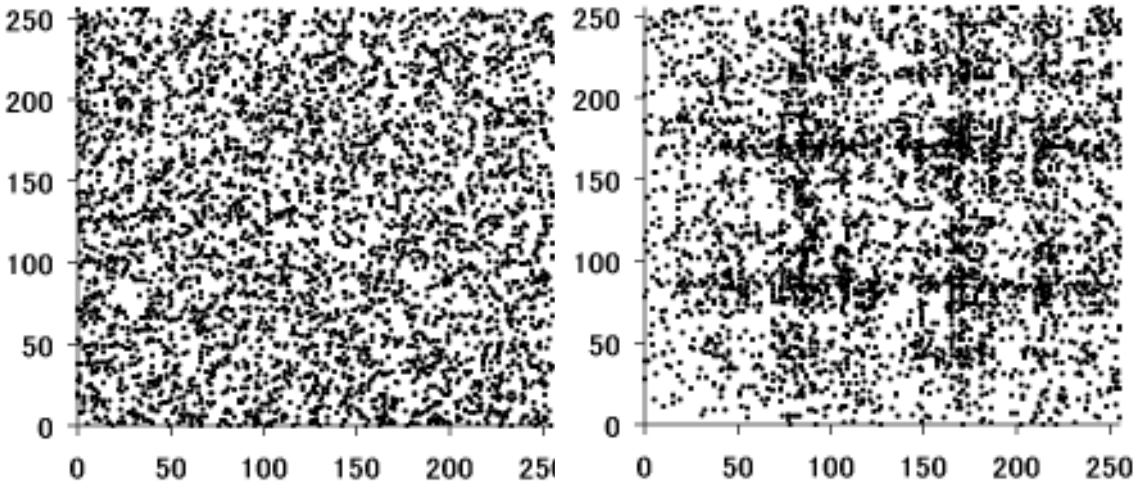


図5-2-15：25kbits/s 高速生成乱数列の相関プロット（Self-correlation plots for sequential eight bit random numbers）

（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、同時にフィルターが持つ逆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。

シミュレーションによりハイパスフィルタの抵抗値とキャパシタの値を決め、ディスクリート素子により、回路の試作を行った。これまでに検討してきたソフトブレークダウンした酸化膜をノイズ素子にして、実際に実験を行ったが、現在のところ、デジタル乱数データは得られていない。これは、ソフトブレークダウンした酸化膜ではノイズ信号がまだ小さかったことが主な原因であると考えている。よって、乱数源デバイスのノイズ信号をもっと大きくするか、ハイパスフィルタを　オペアンプを使った積分回路に置き換えて、増幅作用を持たせることが必要であることが分かった。

今後もノイズ発生素子、読み出し回路の両面から検討を続けていく。

5-2-3　今後の課題と展望

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。さらに、SiドットMOSFET型はまだ高速化改良の余地がある。これらの改良を合わせて、１Mbit/sも可能ではないかと予想している。

5-3　　乱数評価に関わる研究開発

5-3-1　序論

乱数検定に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、これらの検定は、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。我々とは別な方法で作られた乱数生成器（いずれも大型のもの）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、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。

5-3-2　実施結果

（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、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、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。以下に、例としてカイ二乗検定グラフを示す。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。

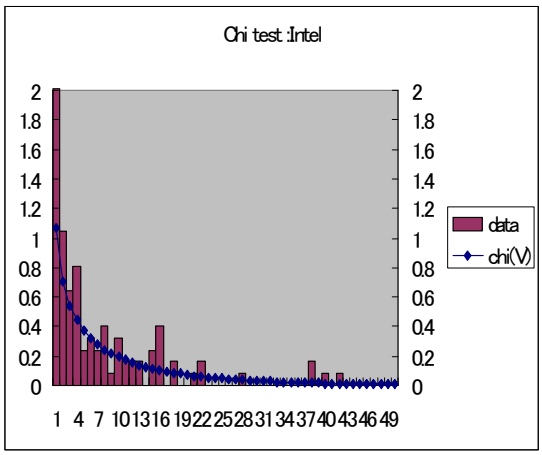


図 5-3-1：Intel 熱雑音乱数カイ二乗検定

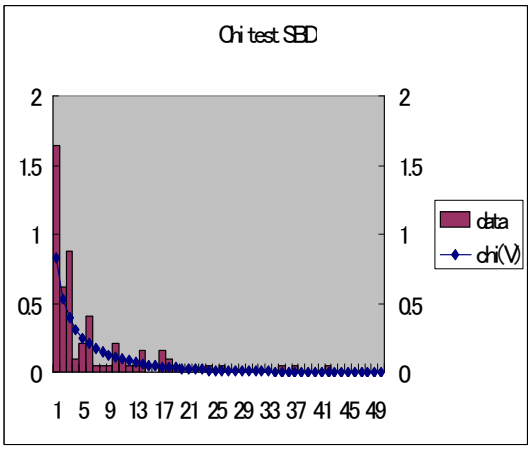


図 5-3-2：SBD 乱数素子のカイ二乗検定

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。

5-3-3　今後の課題と展望

DPA等のサイドチャネル攻撃に対するセキュリティの強度と乱数の質との関連性など、シミュレーションの精度を高めることや、実験で確かめることを検討していく。

5-4　総括

乱数源素子の開発が順調に進んでおり、この分野で世界トップレベルを走っている。全体としての計画は前倒しで進行している。乱数評価方法も従来型から脱して、独自の方法を開拓しつつある。今後は事業化を念頭に置きつつ、製品レベルに上げるための研究開発にも取り組んでいきたい。

１　研究発表、講演、文献等一覧

（◎は査読あり）

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