平成１４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.....2
2 研究開発分野の現状.....2
3 研究開発の全体計画.....2
3-1 研究開発課題の概要.....2
3-2 研究開発目標.....3
3-2-1　最終目標.....3
3-2-2　中間目標.....3
3-3 研究開発の年度別計画.....4
3-4 研究開発体制.....5
4 研究開発の概要（平成14年度まで）.....6
4-1 研究開発実施計画.....6
4-1-1研究開発の計画内容.....6
4-1-2 研究開発課題実施計画.....9
4-2 研究開発の実施内容.....11
5 研究開発実施状況（平成14年度）.....12
5-1 デバイスシミュレーションに関わる研究開発.....12
5-1-1　　序論.....12
5-1-2　　実施結果.....12
5-1-3　　今後の課題と展望.....15
5-2 デバイス・回路試作に関わる研究開発.....15
5-2-1　　序論.....15
5-2-2　　実施結果.....15
5-2-3　　今後の課題と展望.....17
5-3 乱数評価に関わる研究開発.....18
5-3-1　　序論.....18
5-3-2　　実施結果.....18
5-3-3　　今後の課題と展望.....19
5-4 総括.....19

参考資料、参考文献.....21

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17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15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）

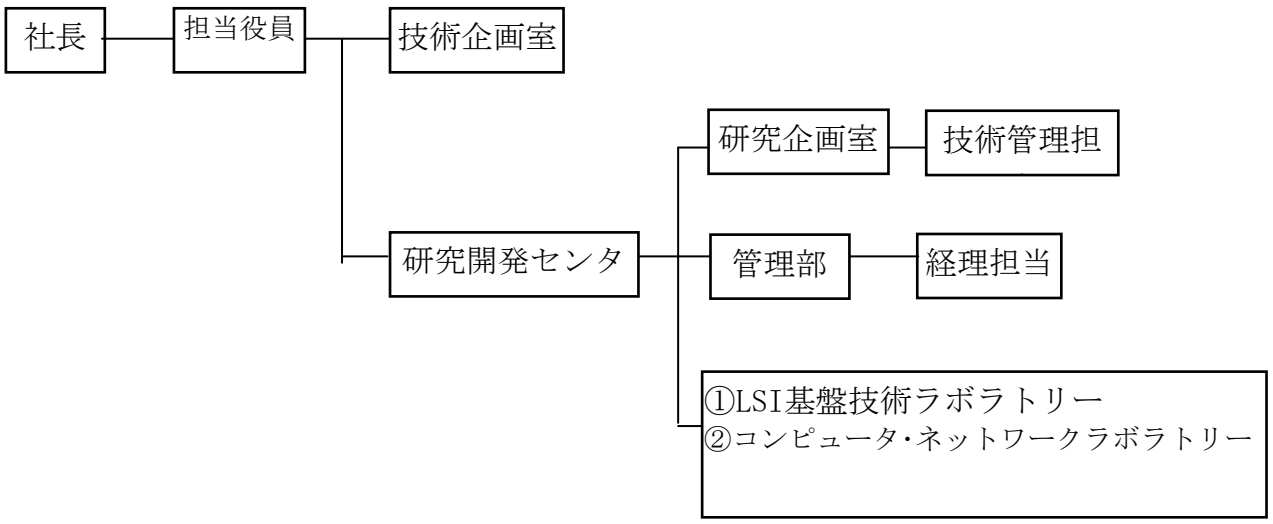
研究開発項目	13年度	14年度	中間評価15年度	16年度	17年度	計	備考
高度情報セキュリティに向けた真性乱数生成用集積回路の研究開発 ①デバイスシミュレーションに関わる研究開発 ②デバイス・回路試作に関わる研究開発 ③乱数評価に関わる研究開発 研究開発の方針・計画策定							
間接経費							
合　　計							

注）１　経費は研究開発項目毎に消費税を含めた額で計上。また、間接経費は直接経費の３０％を上限として計上（消費税を含む。）。

２　備考欄に再委託先機関名を記載。

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
　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

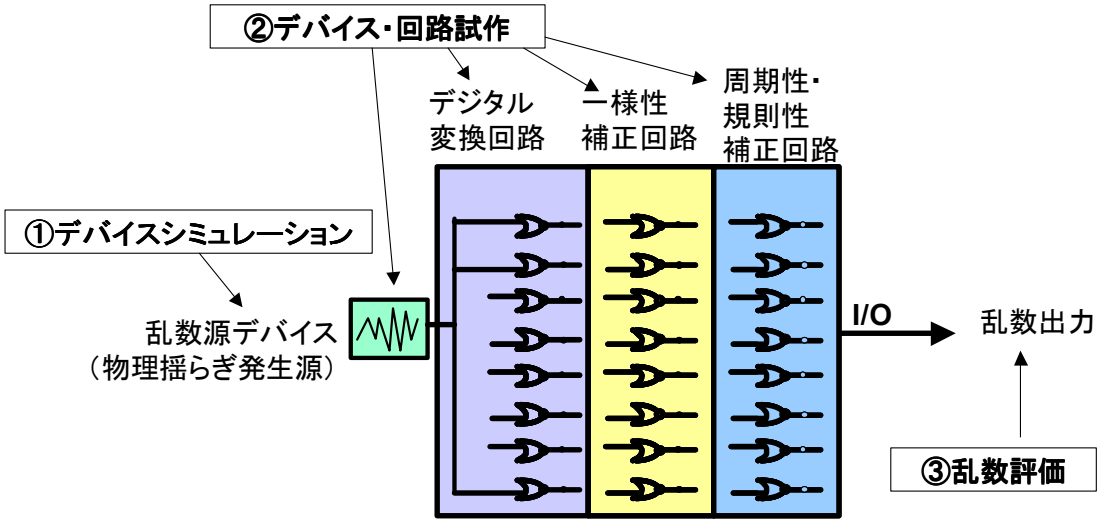
4　研究開発の概要（平成14年度まで）

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。



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。

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						

4-2　研究開発の実施内容

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。

５　研究開発実施状況（平成14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

ナノスケールで起きる物理現象を乱数源として利用するためには、乱数源のデバイス内で起きている物理現象をシミュレーションで予測し、有望な乱数源を探索することが大変重要となる。初めから実験だけで検証することは、原理的に不可能だからである。

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。今年度は、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。

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。

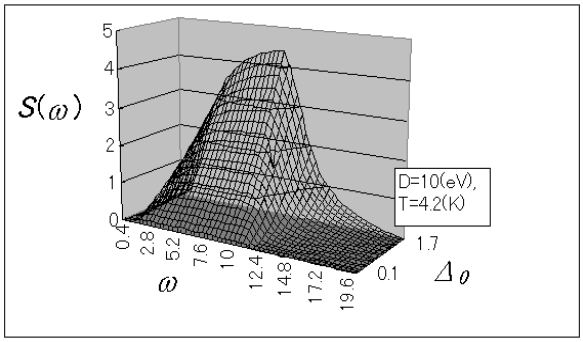
シリコンの量子ドット（量子効果を示す微結晶）を内包するシリコンデバイスは、乱数源デバイスの有力候補である。また、シリコンデバイスのチャネル近辺の電気的不純物準位は通常のデバイスとっては有害な雑音の原因の一つと考えられている。今回、伝導チャネルのそばに位置し、伝導チャネルと電子がトンネリングで行き来できるトラップ準位を一つ設けたモデルと多数設けたモデルを考え、そのノイズ特性をノイズパワースペクトラムから計算することにより調べた。この際、準位は量子ドットとしても不純物準位としてもみなすことができるものと考えられる。トラップ準位には上向きスピンと下向きスピンの両方が入ることができるが、電子間にはクー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場合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：

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

ここでH_{band}がチャネル電流：　$H_{\mathrm{band}} = \sum_{km} E_k c_{km}^{+} c_{km}$ 、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1である。



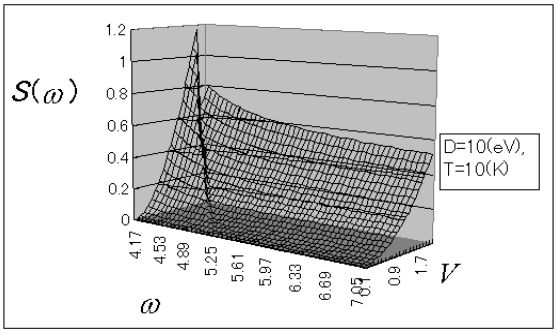


図1　　図2

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2に示した計算結果はこの傾向を示している。図ではバンド構造の影響が低周波部分に見られる。

また、トラップ準位が二つの場合のノイズパワーに与える効果について調べた。実際の実験系ではトラップ間の位置がランダムであるため、トラップ準位同士が相互作用をしている場合のノイズパワーの特性を調べて置く必要があるからである。図１のように、±R/2の場所に同じ種類のトラップ準位があると仮定する。二つのトラップ準位が同一であるため、対応するボソンの平均場も同じであると考えられ、ラグランジェ未定乗数・$^{(2)}$、またボソン場b$^{(2)}$はそれぞれ、・$^{(2)}\equiv$・(R/2)=・・(-R/2)、b$^{(2)}\equiv|$b(R/2)$|=|$b(-R/2)$|$と置くことができる。そして、この場合の平均場のハミルトニアンは互いに独立な部分の和として下記のように書き換えられる:

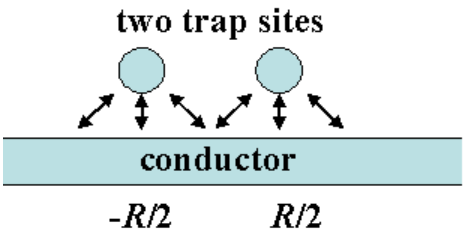


図1

$$H = H_{band} + \varepsilon_f^{(2)}(n_{f1} + n_{f2}) + \sum_{km} b^{(2)}V(k)[c_{km}^{+}(f_{1m}e^{ikR/2} + f_{2m}e^{-ikR/2}) + \text{H.c.}]$$
$$= \sum_{P=\pm}\{E(k)c_{km}^{P+}c_{km}^{P} + \varepsilon_f^{(2)}n_f^{P} + \sum_{km} b^{(2)}V^{P}(k)(c_{km}^{P+}f_m^{P} + \text{H.c.})\}$$

ここでf_{1m}とf_{2m}はそれぞれ、左(-R/2)と右(R/2)のトラップ準位の消滅演算子であり、また・$_f^{(2)}$=E_D+・$^{(2)}$である。 そしてn_f^P=n_{f1}+Pn_{f2} (n_{fi}=$f_{im}^{+}f_{im}$)， f_m^P=(f_{1m}+Pf_{2m})，$V^P(k)$=V(k)[$2N_P(k)$]$^{1/2}$の変換が使われている。ここで$N_P(k)$≡(1+P sin(k_FR)/k_FR)/2 (P=±)であり、また

$$c_{km}^{(+)} = \frac{1}{N^{+}(k)}\int \frac{d\Omega_k}{4\pi}\cos\left(\vec{k}\cdot\vec{R}/2\right)c_{km},$$
$$c_{km}^{(-)} = \frac{1}{N^{-}(k)}\int \frac{d\Omega_k}{4\pi}\sin\left(\vec{k}\cdot\vec{R}/2\right)c_{km}$$

が新しい演算子として使われている。以上により電流も同じように二つの独立部分の和として

$$I = -ei\sum_{P=\pm}\sum_{km} b^{(2)}V^{P}(k)[c_{km}^{P+}f_m^{P} - f_m^{P+}c_{km}^{P}]$$

と表されることがわかった。ノイズパワースペクトルに関してもP=+ 部分とP=-部分の和となることが明らかになった。数値計算の結果、このノイズパワーはトラップ準位が一つの場合と同様に単一のピーク構造をもつ。二つのトラップ準位が十分離れている場合、つまりk_F R ≫ ・のとき(ここでk_Fはフェルミ運動量)、パワースペクトルはトラップ準位が一つの場合の単純のちょうど二倍の振る舞いを示す。 これはk_F R →∞でN_+～ N-となるためである。トラップ準位が一つのときとの違いは二つのトラップ準位が近くなる場合(k_F R ＜ ・)に現れ、ノイズパワースペクトルがエンハンスされる。図２はノイズパワーのピーク値を二つのトラップ準位間の距離の関数として表したものである。二つのトラップ準位が近づくにつれ、また、トラップ準位と電流チャネルの結合が強くなるにつれ、ノイズパワーが大きくなるのがわかる。

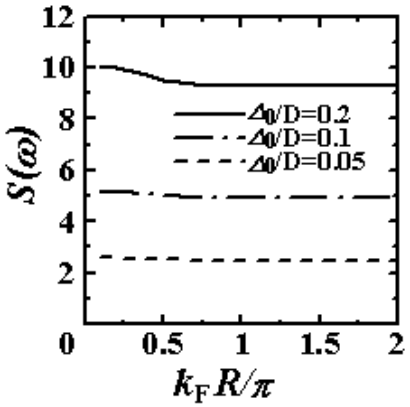


図2：二つのトラップ準位があるときのノイズパワースペクトルのピーク値を二つのトラップ準位の距離Rの関数として計算したもの。 ここでE_F=0、E_D=-0.01D、T=0.001D。

5-1-3　今後の課題と展望

今後は、ランダム信号を高速に発生するためには、量子ドットとチャネル間の構造がどうあるべきかという知見を見出すための計算を展開する。

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、先に掲げたように、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。

昨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、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、乱数発生を試みたが、質の高い乱数が得られなかった。物理揺らぎ信号が1/f特性であったためである。今年度は、さらに1/f特性を取り除く方法を開拓した。

また、昨年度は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も試みた。今年度は、このトランジスタが巨大なRTSを見出すことを利用して、質の高い乱数を得る方法を開拓した。

5-2-2　実施結果

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。(Si量子ドットデバイスについては学会発表を控えているため記載せず。)

（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。

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。

我々は第一段階として、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。

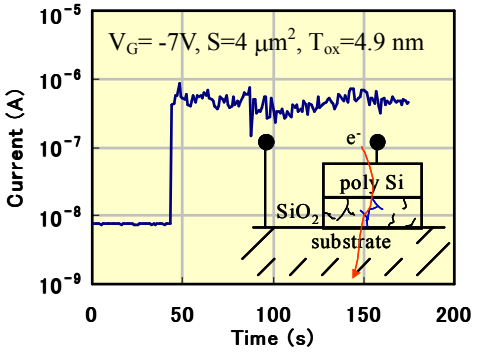


図１　面積4μm、酸化膜厚4.9nmのMOSキャパシタに一定電圧-7V印加したときの擬似破壊の様子。擬似破壊後の電流は大きく揺らいでいる。

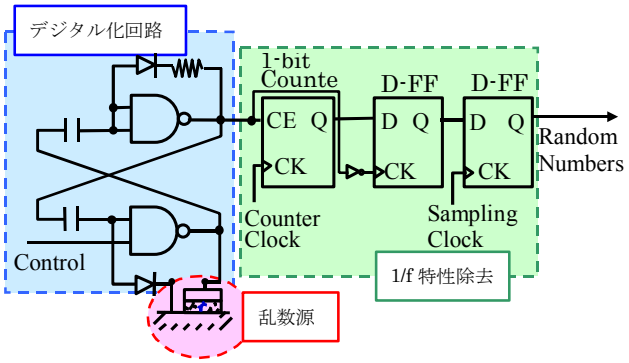


図２　乱数生成回路全体の回路図。乱数源、デジタル化、1/f特性除去の３つの部分からなる。

（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。

本年度は、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。

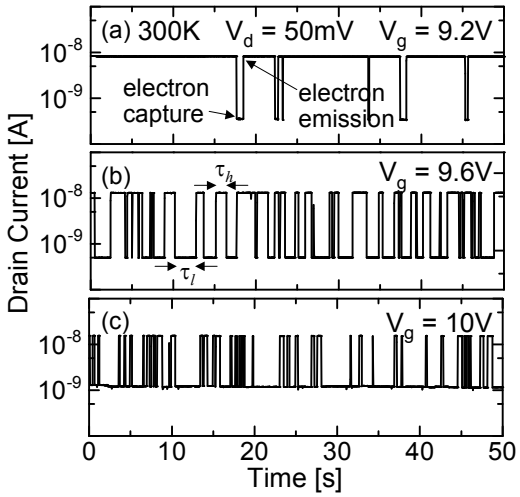


図３：単一電子乱数生成器からの出力信号。

5-2-3　今後の課題と展望

高度な乱数を生成可能な小型回路を開発できたが、現状では生成速度が数十ｋビット/ｓ程度にしかできないため、今後は生成速度を上げるための工夫を行っていく。

5-3　乱数評価に関わる研究開発

5-3-1　序論

平成13年度に続き、出発点として、数理統計的な検定の手法を用いて、乱数の評価を行った。当チームで開発した新型の小型乱数生成回路と既存の高度な物理乱数回路を検定という切り口で比較検討した。さらにセキュリティ強度の観点からどういう評価を使うのが妥当かを探索した。

5-3-2　実施結果

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[1-3]。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。

	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

次にマルチバイブレータと補正回路を組み合わせた乱数生成回路で作った乱数を評価した。その際、半導体中のショットノイズを増幅した乱数と比較を行った。これは、ホワイトノイズであるショットノイズの微弱な信号を、回路ノイズを除

去しながら繰り返し増幅して乱数を得ているもので、回路規模は大きいものの現状で非常に良い乱数と言われているものである。今回は東芝製のランダムマスター™を用いた。評価方法はNISTの検定プログラムから当チームで独自に選別したものを利用した。

表１はFIPS140-2で定められていた検定と、より一般的な検定の結果である。乱数生成速度は50kHzである。表のように我々が開発した回路は全ての検定に合格していることがわかる。また、その検定結果についても熱雑音の結果と遜色ない値となっていることがわかる。

	Test (20000data)	Thermal Noise	Pass?	Our Results	Pass?
<FIPS PUB 140-2>	monobit test	9995	○	10002	○
	poker test	18.3104	○	16.9472	○
	run test 1	[0] 2510 [1] 2485	○ ○	[0] 2515 [1] 2551	○ ○
	run test 2	[0] 1219 [1] 1238	○ ○	[0] 1253 [1] 1232	○ ○
	run test 3	[0] 615 [1] 615	○ ○	[0] 662 [1] 642	○ ○
	run test 4	[0] 312 [1] 320	○ ○	[0] 312 [1] 284	○ ○
	run test 5	[0] 158 [1] 160	○ ○	[0] 157 [1] 162	○ ○
	run test 6+	[0] 165 [1] 160	○ ○	[0] 134 [1] 162	○ ○
	long run test	[0] 13 [1] 13	○ ○	[0] 16 [1] 15	○ ○
<NIST SP 800-22>	χ^2 test	0.944	○	0.977	○
	Run test	0.553	○	0.343	○
	req. Test within bloc	0.093	○	0.805	○
	Freq. Test	0.247	○	0.322	○
	erial Correlation Tes	0.004	○	-0.007	○
	Serial test	0.655	○	0.695	○
	Poker Test	0.405	○	0.596	○
	Gap test 0～15	0.20 ～ 0.94	all ○	0.12 ～ 0.96	all ○

表：　FIPS140-2とNIST800-22の検定結果。我々の結果は全ての検定に合格し

暗号応用という観点から乱数評価の方向性を探るため、DPA (Differential Power Analysis)の調査を行った。DPAは、近年、暗号モジュールに対する大きな脅威となっているサイドチャネル攻撃の中でも強力な解析法で、暗号モジュール開発では対策の組み込みが必須となっている。DPA対策では乱数を用いて秘密情報のマスクを行うため、対策の強度は乱数の質に依存して決まる。通常の(１次)DPAは0/1のバランスのみが強度に影響を与えるが、高次DPAではそれ以外の性質も対策強度に影響を与えることが予想されるため、これを利用した乱数評価の可能性の検討を開始した。

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、セキュリティの視点から評価方法を考えていく。

5-4　総括

乱数源素子の開発が順調に進んでおり、全体としての計画は前倒しで進行している。評価をセキュリティ強度という切り口で行っていくことが課題である。

参考資料、参考文献

[1] D. E. Knuth, *The Art of Computer Programming* (Addison-Wesley, Boston, ed.3, 1998), vol.2.

[2] NIST, A Statistical Test Suite for Random and Pseudorandom Number Generators for Crypto-graphic Applications (NIST SP 800-22).

[3] NIST, Security Requirements for Cryptographic Modules (FIPS PUB 104-2, 2001).

（添付資料）

１　研究発表、講演、文献等一覧
（◎は査読あり）
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。

２　出願特許一覧
乱数生成回路　特願2002-269129　平成14年9月13日　安田　心一、藤田　忍

以上