平成１３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）

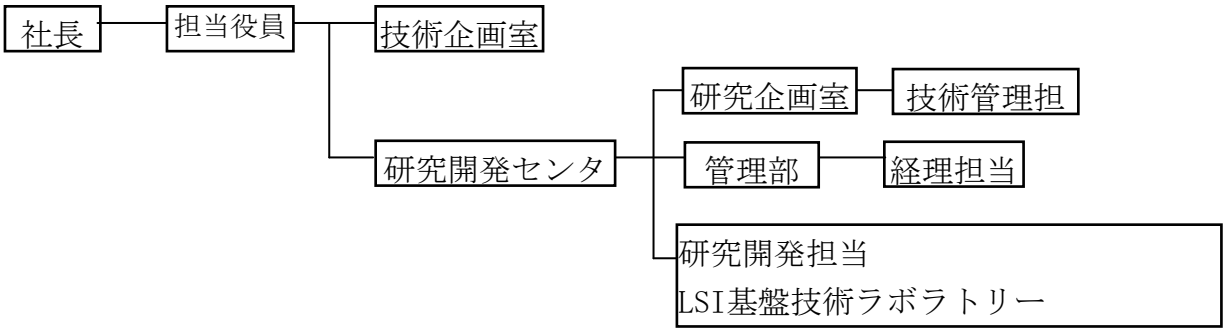
3-3　研究開発の年度別計画

（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 研究開発の全体管理							
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）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）

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

（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

4　研究開発の概要（平成13年度）

4-1　研究開発実施計画

4-1-1　研究開発の計画内容

今年度は、特にデバイスシミュレーションと乱数回路のデジタル回路部分の開発を中心に研究開発を進める。

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る。量子ドット間で電子は波動として振る舞い、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揺らぎをもたらすことが予想される。この変化をシミュレーションしていく。今年度は、基本的なデバイスシミュレーションモデルを構築する。

②デバイス・回路試作に関わる研究開発
乱数生成回路は、デバイスから発生する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。今年度は、デジタル化処理部分の回路を開発して模擬的な物理揺らぎ信号を用いて、乱数が発生できるかどうかの試験を行う。
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る。

③乱数評価に関わる研究開発
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尺度を考案する。

4-1-2　研究開発課題実施計画

（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
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 研究開発全体の管理費						
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。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。

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が、今年度は、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。

③乱数評価に関わる研究開発

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。

5　研究開発実施状況（平成13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

電子の運動量に対応する周波数と、チャネル層の抵抗変化の関係を計算するための理論式を解析的に求めた。この理論式を元にプログラムを作り、これを使ってシミュレーションを行った結果、予想通りの分散関係が得られた（図１）。このシミュレーションを行ったプログラムは、量子ドットデバイスに付随する電気的な揺らぎ現象を計算するための基本ツールになりうることが確認できた。

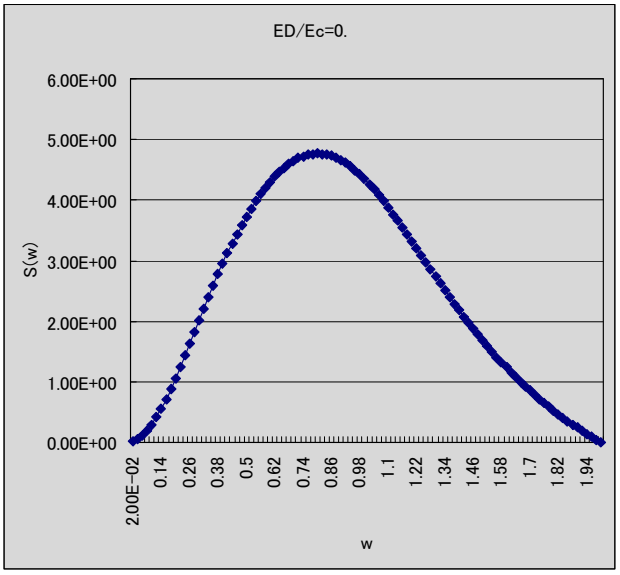


図1：電子の運動量に対応する周波数wとチャネル層の抵抗変化S(w)の関係

5-1-3　今後の課題と展望

実際にデバイスとして用いる場合には、単一の量子ドットではなく、複数の量子ドットを用いることになる。今後は、今回計算したプログラムを発展させて、複数の量子ドットが存在する場合の電流揺らぎ（チャネル層の抵抗変化）をシミュレーションしていく。また、これらの結果を実験結果と比較検討していく。

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。

今年度は、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。

5-2-2　実施結果

マルチバイブレータが、物理揺らぎ信号を乱数化させるのに有効なデジタル化処理回路であることが確認できた。

また、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)から、量子効果的な物理現象に基づく電気的特性の揺らぎをトランジスタの特性の変動として直接的に観測することもできた。

5-2-3　今後の課題と展望

マルチバイブレータだけだと、ランダムなデジタル信号は作れるが、真性乱数と呼べるレベルの乱数にはならない。今後は、乱数の定量的な評価（5-3）を進めていき、乱数の質を上げるためのデジタル回路をマルチバイブレータの後段に追加していく必要がある。

また、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)から、量子効果的な物理現象に基づく電気的特性の揺らぎを乱数源として用いて、

上記の乱数化のためのデジタル回路と合体化していく。

さらには、ナノスケールデバイスに見られる別の種類の電気的揺らぎも、乱数源の候補として探索していく。

5-3　乱数評価に関わる研究開発

5-3-1　序論

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。

今年度は、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。

5-3-2　実施結果

カイ２乗検定、ギャップ検定など従来の統計的な検定手法[参考文献：1,2,3]を使って、第一次的な乱数評価ができるようになり、乱数回路の相対比較が可能となった。これにより、先のマルチバイブレータだけで作った乱数では、熱雑音熱雑音増幅型の乱数生成回路で作られた乱数の質に到達できないことが確認された。

5-3-3　今後の課題と展望

統計的な検定手法は、乱数のデータ長、検定の棄却率等のパラメータで検定結果が大きく変わる可能性がある。これらのパラメータを同選択すべきかを明確化することが大きな課題の一つであり、来年度の最優先研究アイテムとして取り組む。これらと並行して、試作した乱数生成集積回路の乱数を相対評価し、回路改良のフィードバック情報とする。

また、検定以外の手法で乱数の質を評価する方法も探索していく。

5-4　総括

デバイス・回路試作に関わる研究者を１名追加したことで、デバイス・回路試作に関わる研究開発が当初の計画予定よりも進んだ。デバイスシミュレーションに関わる研究開発と、乱数評価に関わる人員は当初の計画どおりだが、デバイス・回路試作に関わる研究開発で、予定よりも早く具体的な実験結果が出て来たため、実験とシミュレーションの比較ができたため、また実

験で作った乱数を実際に評価できたため、目標とする乱数生成集積回路の開発が加速された。

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).

１　研究発表、講演、文献等一覧

研究開始直後のため、今年度はいずれも無し。