様　式　Ｃ－１９、Ｆ－１９、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

平成 ２７ 年　 ５ 月　 ８ 日現在

機関番号：１２６０１
研究種目：若手研究(B)
研究期間：2012～2014
課題番号：２４７０００４２

研究課題名（和文）微細トランジスタの経年劣化効果を有効活用したＰＵＦによるチップＩＤ識別システム

研究課題名（英文）Chip Identification System based on Physically Unclonable Function Utilizing Aging Effect on Nano-Scale Transistors

研究代表者
飯塚　哲也（Iizuka, Tetsuya）

東京大学・工学（系）研究科（研究院）・准教授

研究者番号：１０５５２１７７

交付決定額（研究期間全体）：（直接経費）　　3,500,000円

研究成果の概要（和文）：集積回路の製造ばらつきを固有の物理的特徴とみてIDとして利用するシリコンPUFと呼ばれる技術が注目されている。本研究では、集積回路上の微少な性能差の正確な検出のため、トランジスタの経年劣化効果の物理現象をモデル化し劣化シミュレーションの高速化を達成した。また、チップ上のランダムな性能ばらつきによって生じる微少な遅延差を検出・記憶し、その遅延差をデジタル信号に変換する新規回路を提案し、設計および実測による評価を行いその有効性を示した。さらに、外部に漏洩する磁界を高感度磁界プローブにより検出し、磁界マップから内部の回路動作の差異を推定し真贋判定のためのIDとして用いる方法についても検討を行った。

研究成果の概要（英文）：Silicon physically unclonable function (PUF) based on pefromance fluctuation caused by fabrication processes, which is utilized as an ID of a chip, has been attracting a lot of attention, mainly from the viewpoint of security purposes. For the purpose of detecting a tiny on-chip performance difference, this research first proposes a high-speed estimation method for FET performance variation due to aging effect. A fine time-resolution time-to-digital conversion circuit, which includes a novel time-difference hold-and-replication circuit is also proposed to detect a tiny on-chip delay difference. This research also investigates the possibility of a chip ID based on magnetic field emitted from the chip utilizing a high-sensitivity magnetic probe.

研究分野：電気電子工学

キーワード：電子デバイス・機器　集積回路　経年劣化　NBTI　PUF ID　時間-デジタル変換

１．研究開始当初の背景

近年の半導体製造技術の向上により、システムLSIは様々なデジタル情報家電に広く利用され、生活のあらゆる場面に溶け込んでいる。これらの情報家電を通して我々は多くの秘密情報を取り扱っており、製造過程でLSIの内部にトラップ回路が挿入されたり、偽のLSIが製品に混入されたりすることで、システムLSIの内部情報が外部から不正に取得され、秘密情報が盗み出される危険性が近年指摘されている。

これらの偽造LSIを検出し不正混入を防ぐため、物理的複製困難関数(PUF; Physically Unclonable Function)と呼ばれる複製困難な物理的特徴を用いて、人間における指紋のように、デバイス固有の情報を生成する技術が注目されている[1]。半導体集積回路において製造時の特性ばらつきを利用してLSI固有のIDとするシリコンPUFと呼ばれる技術では、製造ばらつきによって生じる経路の遅延差を利用するアービターPUF と呼ばれる方式や、メモリセルの閾値ばらつきを利用する方式などが提案されている。しかしながら、製造ばらつきによって生じるデバイス間の微小な性能差によって出力を決定するため、その値は動作時の温度・電源電圧・雑音などに強く依存し、ID出力のランダム性・再現性がそれら環境要因に強く依存することが実用化に対する一つの制約となっている。温度やプロセス状態のセンサをチップ上に実装し、PUF の安定化を図る研究も報告があるが[2]、チップ面積を消費する点に加えオンチップセンサ側への攻撃を通してチップ ID を解読される可能性も考えられる。

[参考文献]

[1] R. Pappu et al.,``Physical One-Way Functions," *Science*, vol. 297, pp. 2026 – 2030, 2002.

[2] S. Stanzione et al.,``CMOS Silicon Physical Unclonable Functions Based on Intrinsic Process Variability," *IEEE Journal of Solid-State Circuits*, vol. 46, no 6, pp. 1456 – 1462, 2011.

２．研究の目的

本研究では微細 CMOS 技術において一つの重要な問題となっている経年劣化やばらつきの効果を有効に活用した新規なシリコンPUF技術を提案することを目的とし、必要な要素技術の検討・開発を通じてLSIの動作環境に対して安定な ID 認証を実現することを目指す。提案技術では、発生する経年劣化効果を正確に見積もり、製造ばらつきおよび劣化によりチップ上に生じる性能差を高精度に検出することによる安定したランダム性と再現性の両立を目指す。必要な要素技術として、チップ上の微少な遅延等の性能差をIDに使用できるデジタル信号として正確に検出するための回路手法を提案する。また、研究開始当初ではその実現可能性を十分に考慮できていなかった、LSIから外部に漏洩する磁界を基に ID を得る方法についても、高感度・高空間分解能の磁界検出に基づいて実現が可能と考え検討を行う。

３．研究の方法

本研究では目的達成に向けて下記の３課題を設定し、各項目の研究・開発を行う。

(1)　NBTI効果によるトランジスタ性能劣化のモデル化

集積回路上のトランジスタの微細化が進むにつれて顕著な問題となっているトランジスタの劣化効果の一つである NBTI 効果のモデル化を行う。NBTI は主に PMOS トランジスタに負バイアスを印加することで発生するが、電圧ストレスを除去することで回復する性質を持ち、劣化量の正確な推定が難しい。本課題ではトランジスタの劣化の過渡解析を高速に行うための新たなモデルを構築し、トランジスタのストレス状態に依存する性能変動を正確かつ高速に見積もる手法を提案する。

(2)　微少な時間差を検出するためのオンチップ時間差記憶素子および時間デジタル変換器の設計

チップ上のランダムな性能ばらつきおよび性能劣化によって生じる微細な遅延差を検出し、ID として使用するためにその遅延差を高い分解能でデジタル信号に変換する回路が必要となる。本課題ではチップ上において入力される時間差を記憶し、任意回数再生可能とする新規回路を提案し、記憶された時間差信号を複数回の時間-デジタル変換によって高精細にデジタル信号に変換する構成を持つ変換器を提案・実証する。

(3)　LSI から外部に漏洩する磁界を高い空間分解能で検出するプローブ回路の実現

ばらつきによって生じる遅延等の時間以外の物理現象も PUF ID として使用可能である。本課題ではLSIから外部に漏洩する磁界情報を回路固有の ID として使用できる可能性について検討するため高感度・高空間分解能の磁界プローブ回路を実証し、それを用いて検出した磁界情報を基に真贋判定を行う方法を検討する。

４．研究成果

前述の研究方法に沿ってそれぞれの項目毎に研究を実施し、以下の成果を得た。

(1)　NBTI劣化過渡解析の高速化手法

反応・拡散モデルを用いた NBTI シミュレーションにおいて，論理シミュレーション結果にもとづいて各トランジスタにおけるゲート酸化膜中の水素分布を計算することにより，高精度な NBTI 劣化過渡解析を実現した。本シミュレーション解析では、反応・拡散モ

デルにおける反応・拡散の数式表現による連立方程式を、C 言語を用いた数値計算によって解くことにより, PMOS トランジスタの酸化膜・ポリシリコン電極中の H 分布を計算する。

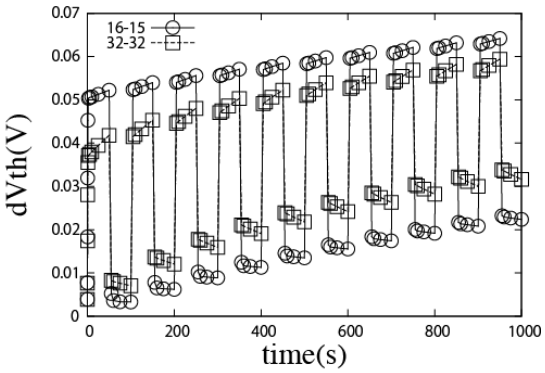

図 1 負荷周波数 0.01Hz における劣化シミュレーション結果

図 1 にストレス・回復状態が入れ替わる周波数を 0.01Hz とした遅いストレスを印加した場合の結果を示す。縦軸はストレス印加および回復現象による閾値の変化を示しており、横軸は時間である。トランジスタゲート酸化膜およびポリシリコンを格子に分割する分割数により結果の精度に違いが生じていることが分かる。

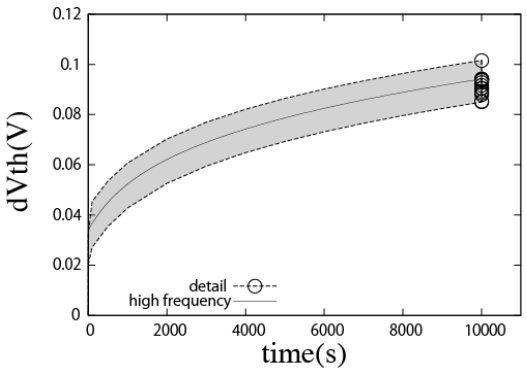

図 2 1Hz 負荷時の詳細劣化シミュレーションとデューティー比を用いた高速シミュレーションとの比較

前述のシミュレーション結果では非常に遅いストレス信号周波数を仮定したが、ある程度の高い周波数においては、劣化の進行が周波数に依存せず、ほぼ信号のデューティー比に依存することを明らかにした。この性質を利用することで周期負荷に対する劣化シミュレーションの高速化が可能となる。図 2 に本高速化手法を適用した劣化シミュレーション結果を示す。灰色の、幅を持ったグラフが周期ストレスを与えた場合の詳細なストレスの変化を示している。詳細なシミュレーションにおいてはこの幅の間をストレス・回復現象に応じて往復しながら大局的には閾値の劣化が発生する。中央を通るグラフがデューティー比を用いた高速シミュレーションによる結果である。高速シミュレーションでは詳細な劣化・回復の往復を無視しているが、長時間にわたるストレスによる大局的な閾値の変化を正確に見積もることができていることが分かる。本シミュレーションモデルにより長時間にわたるトランジスタ劣化シミュレーションの高速化を達成した。

(2) オンチップ時間差記憶素子および時間デジタル変換器

上記のモデルで見積もられる閾値劣化を受けたトランジスタによってオンチップで生成される性能に応じた時間差は非常に僅かなものであり、高い分解能でデジタル信号に変換するための時間-デジタル変換器 (Time-to-Digital Converter; TDC)が必要となる。オンチップの時間差記憶再生回路およびそれを備えた時間-デジタル変換器を提案し、試作・測定により実証を行った。

図 3 に、実証した時間差記憶再生回路のブロック図を示す。入力された時間差は、二つのパルスの立ち上がりタイミングの差に変換され、それらのパルスは互いの時間差を維持したまま、Dual Pulse Ring Oscillator (DPRO) と呼ぶ回路内を、リセット信号が外部から与えられるまで周回し続ける。二つのパルス信号は全く同じ経路を常に周回し続けるため、二つのパルス信号の時間差がばらつき等の影響で変化してしまうことはない。そのため入力された微少な時間差を安定して保持することができる。

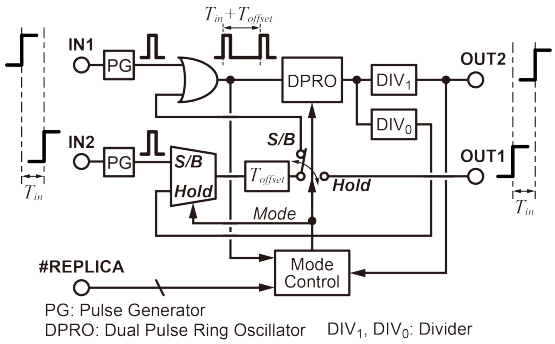

図 3 時間差記憶再生回路のブロック図

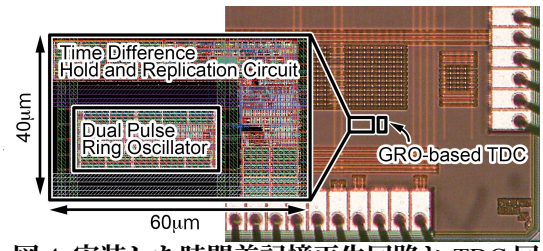

図 4 実装した時間差記憶再生回路と TDC 回路のチップ写真とレイアウト図

本回路を Gated-Oscillator 型 TDC 回路と組み合わせて使用することで TDC の時間分解能を向上させることが可能となる。時間差記憶回路と TDC を実装したチップの写真を図 4 に示し、時間差記憶回路の実測による測定波形を図 5 に示す。図 5 から、入力信号 IN1 と

IN2 の時間差 T_{in} が、OUT1 と OUT2 の二つの信号の立ち上がりタイミングの差として保持され、繰り返し再生されていることが分かる。この再生された時間差を利用して TDC の時間分解能を向上させた例を図 6 に示す。記憶再生素子により複製された時間差を TDC 回路へ入力する回数を増加させることで、実効的な TDC の解像度が向上していることが分かる。これによりオンチップで微少な時間差を高い分解能でデジタル信号に変換することが可能となる。さらに、得られたパルスをデジタル信号に変換せずに LC 型のオシレータに繰り返し導入することで発振周波数の変化として検出し、それを用いて ID として用いる方式についても検討を行った。生成されたパルスを入力することで LC オシレータ回路の発信周波数を微細に制御できることを示した。

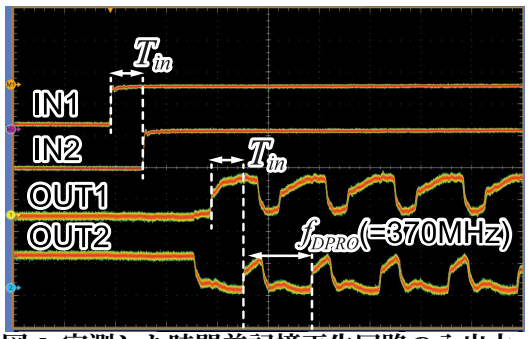

図 5 実測した時間差記憶再生回路の入出力波形

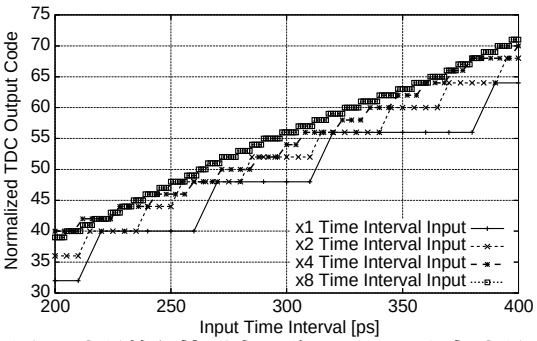

図 6 時間差記憶再生回路を用いて入力時間差を複数回 TDC 回路に導入した場合の時間分解能の向上の様子

(3)　高感度磁界プローブの実現

集積回路のばらつき等による内部の性能差を非破壊で検出し ID として用いるために、主に回路遅延に着目し上記のような結論を得たが、より直接的に回路内部の電流を外部から検出することでも真贋判定が可能である。通常の回路動作を妨げることなく外部から真贋判定を行う方法として、集積回路から外部に漏洩する磁界を検出する方法が挙げられる。二つのチップの磁界マップを取得し、これらの磁界マップの差異を検出することで集積回路の真贋判定が可能であり、高精細な磁界マップの取得を実現することで、それをチップ ID として使用できる可能性がある。真贋判定のためには極微少な磁界の差異を検出する必要があり、より高感度・高空間分解能の磁界プローブが必要となる。本研究課題においては磁界プローブの高感度化を目指し、集積化された磁界プローブの最適化を行い、漏洩磁界の測定を行った。図 7 に、本課題で実証した磁界プローブを用いて対象となる配線の上部をスキャンした際の出力電圧変化の測定結果を示す。提案プローブの場合にはプローブの位置に対して出力電圧が高感度に変化しており、対象となる配線を検出するための空間分解能が向上していることが示された。

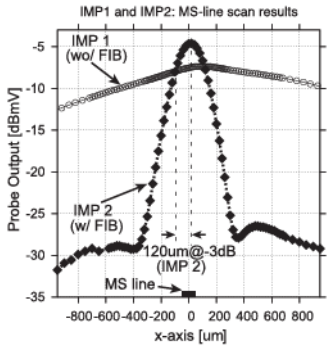

図 7 マイクロストリップライン上をスキャンした場合の磁界プローブ出力

5．主な発表論文等

（研究代表者、研究分担者及び連携研究者には下線）

〔雑誌論文〕（計２件）

[1] Nguyen Ngoc Mai-Khanh, Tetsuya Iizuka, Shigeru Nakajima, and Kunihiro Asada, ``Spacial Resolution Enhancement for Integrated Magnetic Probe by Two-Step Removal of Si-Substrate Beneath the Coil," *IEEE Transactions on Magnetics,* vol. 51, no. 1, article no. 6500404, Jan. 2015.

[2] Kazutoshi Kodama, Tetsuya Iizuka, Toru Nakura, and Kunihiro Asada, ``Frequency Resolution Enhancement for Digitally-Controlled Oscillator based on a Single-Period Switching Scheme," *IEICE Transactions on Electronics*, vol. E95-C, no. 12, pp. 1857 - 1863, Dec. 2012.

〔学会発表〕（計６件）

[1] 森 一倫, 名倉 徹, 飯塚哲也, 浅田邦博, ``NBTI の周波数依存性を利用した劣化過渡解析の高速化手法," 電子情報通信学会 総合大会論文集, 2015 年 3 月.

[2] 森 一倫, 名倉 徹, 飯塚哲也, 浅田邦博, ``論理シミュレーションにもとづいた NBTI 劣化過渡解析の高速化手法,"電子情報通信学会研究報告会集積回路研究会(ICD2014), 2014 年 12 月.

[3] Nguyen Ngoc Mai-Khanh, Tetsuya Iizuka, Shigeru Nakajima, and Kunihiro Asada, ``Spacial Resolution Enhancement for

Integrated Magnetic Probe by Two-Step Removal of Si-Substrate Beneath the Coil," in *Proceedings of IEEE 10th European Conference on Magnetic Sensors and Actuators (EMSA)*, Jul. 2014

[4] Tetsuya Iizuka, Teruki Someya, Toru Nakura, and Kunihiro Asada, ``An All-Digital Time Difference Hold-and-Replication Circuit utilizing a Dual Pulse Ring Oscillator," *in Proceedings of IEEE Custom Integrated Circuits Conference (CICC)*, Sep. 2013.

[5] **中村 陽二, 飯塚 哲也, 浅田 邦博, ``LSIセキュリティ対策のための集積回路の表面磁界分布からの動作状態推定," 情報処理学会 DA シンポジウム 2013 論文集, pp. 151 - 156, 2013年8月.**

[6] **児玉 和俊, 飯塚 哲也, 名倉 徹, 浅田 邦博, ``制御信号の周期内切替によるデジタル制御発振器の高解像度化," 電子情報通信学会 LSI とシステムのワークショップ 2012, 2012年5月.**

〔図書〕（計０件）

〔産業財産権〕
○出願状況（計０件）

○取得状況（計０件）

〔その他〕
なし

６．研究組織
(1)研究代表者
飯塚 哲也（IIZUKA TETSUYA）
東京大学・工学系研究科電気系工学専攻・准教授
研究者番号：10552177

(2)研究分担者
なし

(3)連携研究者
なし

(4)研究協力者
Nguyen Ngoc Mai-Khanh
東京大学・大規模集積システム設計教育研究センター・助教