様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

令和　元 年　 ６ 月　 ６ 日現在

機関番号：８２６２６
研究種目：基盤研究(B)（一般）
研究期間：2016～2018
課題番号：１６Ｈ０２８３３

研究課題名（和文）超低消費電力トランジスタSOTBにおけるICチップ偽造防止技術PUFの有効性検証

研究課題名（英文）Feasibility study of the SOTB implementation of the anti-counterfeit technology PUF

研究代表者

堀　洋平（Hori, Yohei）

国立研究開発法人産業技術総合研究所・エレクトロニクス・製造領域・主任研究員

研究者番号：６０５３０３６８

交付決定額（研究期間全体）：（直接経費）　　12,900,000円

研究成果の概要（和文）：本研究では、65nm SOTBプロセス製造されたArbiter PUFおよびPseudo Linear-Feedback Resister PUF (PL-PUF) の評価を通じ、これまで明らかでなかった超低電圧デバイスSOTBよるPUFの実現可能性を明らかにした。本成果は、省電力とセキュリティが重要なIoTにおいて、超低消費電力デバイスSOTBの有効性を世界で初めて示したものである。また、本研究はSOTBデバイスの特徴である基板バイアスを調整することで、PUFを用いた認証のエラー率を低減できることを示した。

研究成果の学術的意義や社会的意義
超低電圧デバイスSOTBを用いてセキュリティプリミティブであるPUFを実装可能であることを世界で初めて明らかにした。これは、省電力やセキュリティが重要なIoTにおいて、SOTB PUFが有効であることを示したものである。また、SOTBの特徴の1つである基板バイアス制御によってPUFの特性を改善可能であることを初めて見出した。これは、製造前の性能予測が困難なPUFにおいて、基板バイアス制御によって出荷後にもPUFの特性を調整可能であることを示唆しており、社会実装に向けて極めて有用な知見が得られたということができる。

研究成果の概要（英文）：We demonstrated for the first time the feasibility of the Silicon-On-Thin-Buried-oxide (SOTB) transistor implementation of Physically Unclonable Functions (PUFs) through the evaluation of the 65nm SOTB PUF chips. The implemented Arbiter PUF shows high reproducibility and enough uniqueness for the use of identification and authentication. The results indicate that the SOTB can be practically used in the Internet of Things (IoT) where the low-power consumption and security are of great importance. In addition, we found that, by controlling the back bias of the SOTB device, the uniqueness of the PUF can be improved and the authentication error can be significantly decreased.

研究分野：ハードウェアセキュリティ

キーワード：PUF　SOTB　ハードウェアセキュリティ

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９、ＣＫ－１９（共通）

１．研究開始当初の背景

数兆個を超えるセンサや機器がネットワークで接続される IoT により、利便性が高くエネルギー効率の良いスマート社会が近い将来実現すると期待されている。IoT エッジデバイス（＝IoT に接続されるセンサや機器等）は、例えばボタン電池 1 個で 10 年稼働することが求められており、そのためには消費電力の低いトランジスタが必要不可欠である。ゆえに、0.4V 以下の超低電圧でも駆動可能な超低消費電力トランジスタ SOTB は、省電力な IoT エッジデバイスを実現するキーデバイスであると言える。

一方で、IoT を構成する数兆個ものエッジデバイスは、情報を盗んだりニセの情報を流したりする不正品や信頼性の低い粗悪品であってはならない。ところが、2011 年には 20 兆円分もの模倣半導体製品が見つかり[1]、米国国防総省内でも 1800 点の兵器に 100 万個を超える模倣電子部品が搭載されていた例[2]からもわかるように、IoT にニセモノが混入することを防ぐのは非常に難しい。そこで、不正機器の排除や機器認証のために PUF が有効である。PUF はデバイスのばらつき（トランジスタのサイズ、不純物濃度、しきい値電圧等のわずかな違い）を利用して、チップに固有の ID（「チップの指紋」とも呼ばれる）を生成する回路である。ばらつきは製造過程でどうしても生じてしまい、しかも同じばらつきを意図的に再現することはできないので、同じ入出力特性を持つ PUF は 2 つと存在しない。ゆえに、PUF を用いて IC チップの真贋判定ができる。

しかし、超低電圧デバイス SOTB において PUF が正しく機能するかはまだ検証されていない。PUF は「ばらつき」という不確定な要素を利用しているうえ、ノイズの影響も受けやすいため、上記の性質が必ず満たされるとは限らない。また、SOTB はばらつきが小さいことが特長であるが、それゆえ PUF のユニーク性が得られるかどうかは未知である。ゆえに本研究において、SOTB-PUF の実現可能性と性能を明らかにする。

[1] “Top 5 most counterfeited parts represent a $169 billion potential challenge for global semiconductor market,” iSuppli (現、IHS Technology), 2012.
[2] “Inquiry into counterfeit electronic parts in the department of defense supply chain”, Committee on Armed Services, United States Senate, 2012.

２．研究の目的

本研究の目的は以下の 3 つにまとめられる。

(1) SOTB-PUF が、PUF として正しく機能することを示す。すなわち、高い再現性やユニーク性を有することを定量的に評価する。通常使用時だけでなく、温度や電圧を変化させても性能が維持されるか明らかにし、実用上問題ないことを示す。また、SOTB ならではの「基板バイアス」に応じた SOTB-PUF の動作電圧範囲を明らかにすることで、どこまで省電力化・高速化できるかを評価する。

(2) SOTB-PUF の安全性を評価する。具体的には、機械学習攻撃への耐性を評価する。機械学習攻撃は、大量の入出力データから PUF 回路の遅延を機械学習し、入力に対する出力を予測するものである。出力が予測可能な PUF は「数学的にクローンされた」に等しく、セキュリティ用途には使えない。

(3) 提案方式の PUF の動作を理論的に説明する。これまでは、「ばらつきがあるから」という理由と実験データの統計解析から定性的に説明することしかできなかったが、PUF 回路の信号遅延やばらつきのモデルを作ることで、異なる ID が出ることの理論を明らかにする。PUF の理論を構築することで、「作ってみなければわからない」状況から脱し、製造前の性能予測や、より優れた PUF 方式を理論から導くことを可能とする。

３．研究の方法

交付金で製造され平成 28 年 6 月に納品される 65nm STOB-PUF チップを、様々な電圧・温度・タイミングの下でデータ収集し、これを解析することで SOTB-PUF の実現可能性と性能を評価する。研究期間は平成 28～30 年の 3 年間である。平成 28 年度：SOTB-PUF チップの評価環境を構築し、動作確認を兼ねて典型的な（＝通常使用時の）電圧・温度・タイミングパラメータの下でデータ収集と解析を行う。平成 29 年度以降：典型値から外れた様々なパラメータ下でのデータ収集と解析を行う。また、SOTB-PUF の機械学習攻撃に対する安全性評価を実施する。さらに、PUF 回路のモデルを検討し、PUF 動作の理論的説明を試みる。研究体制として、研究代表者、研究分担者 1 名、補助プログラマ 1 名、実験補助員 1 名の、合計 4 名で実施する。

４．研究成果

(1) 成果の概要

本研究では、65nm SOTB プロセス製造された Arbiter PUF および Pseudo Linear-Feedback Resister PUF (PL-PUF) の評価を通じ、これまで明らかでなかった超低電圧デバイス SOTB よる PUF の実現可能性を明らかにした。本成果は、省電力とセキュリティが重要な IoT において、

超低消費電力デバイス SOTB の有効性を世界で初めて示したものである。また、本研究は SOTB デバイスの特徴である基板バイアスを調整することで、PUF を用いた認証のエラー率を低減できることを示した。これは、製造前の性能評価が困難な PUF において、基板バイアスの調整により PUF の特性を調整できることを示唆しており、SOTB を用いた PUF の実用化に向けて重要な知見が得られたといえる。本成果は国際会議 IEEE SOI-3D-Subthreshold Microelectronics Technology Unified Conference (S3S) で発表された。

(2) 環境構築

評価対象の Test Element Group (TEG) チップはは本研究の開始前に研究代表者及び研究分担者が製造したものであり、Arbiter PUF, PL-PUF 及び Ring Oscillator PUF 等が 65nm SOTB を用いて実装されている (図 1)。SOTB PUF では従来と動作電圧が異なり、基板電圧の制御も必要であるため、既存基板を改変して評価基板を開発した。また、SOTB PUF 用のデータ収集及びデータ解析を自動化するプログラムをそれぞれ C#を用いて開発した。

温度変動評価では、Espec 社製の恒温槽 SH-241 を用いた。TEG チップを搭載した評価ボードを恒温槽に入れ、外部のノート PC からチップの制御及びデータ取得を行った。

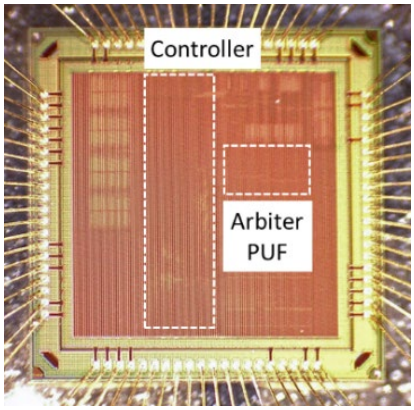

図 1 SOTB PUF チップ

(3) PUF の特性試験

構築・開発した実験環境および解析プログラムを用いて、Arbiter PUF および PL-PUF の動作確認を行った。図 2 は 128 段 Arbiter PUF の PUF 内ハミング距離 (Intra-HD。再現性の指標となる)及び PUF 間ハミング距離 (Inter-HD。ユニーク性の指標となる)を示している。評価した Arbiter PUF 回路は 64 個であり、1 個の PUF 回路から 128 ビットの ID を 1024 種類取得した。再現性の評価のため、ID は 1 個当たり 128 回ずつ繰り返して取得された。図 2 が示すように、Arbiter PUF の平均 Intra-HD は 0.0347 であり、ID の再現性は高いことが示された。一方、Inter-HD は 0.331 と理想の 0.5 よりやや小さい。しかし、Intra-HD と Inter-HD は十分に離れて分しており、この Arbiter PUF を用いて個体識別が可能であることが示された。

なお、PL-PUF の解析結果については未発表であるため、割愛する。

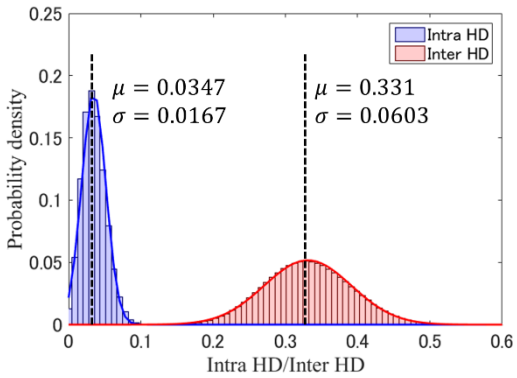

図 2 SOTB Arbiter PUF の再現性及びユニーク性

(4) 電圧変動試験

コア電圧を 0.4 から 0.8V まで 0.1V ずつ変化させて取得した Arbiter PUF のレスポンスの解析結果を図 3 に示す。データ取得時の雰囲気温度は室温である。図 3 が示すように、0.4V では Intra-HD と Inter-HD の平均値が十分に離れていたが、コア電圧が上がるにつれて Inter-HD の平均値は減少する結果が得られた。これにより、当該 PUF を用いた認証のエラー率は 0.6V の約 3%から上昇し、0.8V では約 37%に達した。ゆえに、室温で基板バイアスの制御を行わなかった場合、当該 PUF を認証に使えるのは 0.4 から 0.6V 程度までであることが示された。

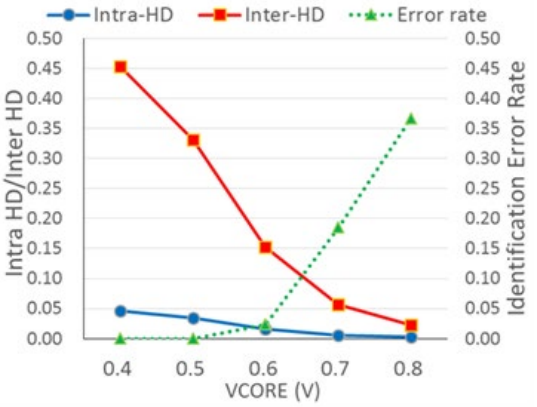

図 3 電圧変動時の SOTB Arbiter PUF の特性変化

(5)基板バイアス制御による PUF 特性の改善

基板バイアス電圧を−0.5 から 0.5V まで 0.1V ずつ変化させながら PUF のレスポンスを取得して解析した際の、Intra-HD および Inter-HD の平均値を図 4 に、認証エラー率を図 5 に示す。コア電圧は、0.4, 0.5 及び 0.6V とした。データ取得時の雰囲気温度は室温である。

図４が示すように、基板バイアスを上げると、Intra-HD はほとんど変化しなかったが、Inter-HD が改善された。これにより、図５が示すように、認証エラー率を大幅に低減することができた。これは、基板バイアスによってデバイスの速度が遅くなった結果、信号遅延に対するデバイスのばらつきの影響が相対的に大きくなり、異なるチップ間で信号遅延に差が出やすくなりユニーク性が向上したためと推察される。

PUF はデバイスのばらつきを利用するため、製造前に特性を予測するのが困難であるが、SOTB を用いれば基板バイアス制御によって出荷後にも PUF の特性を調整できることが示された。

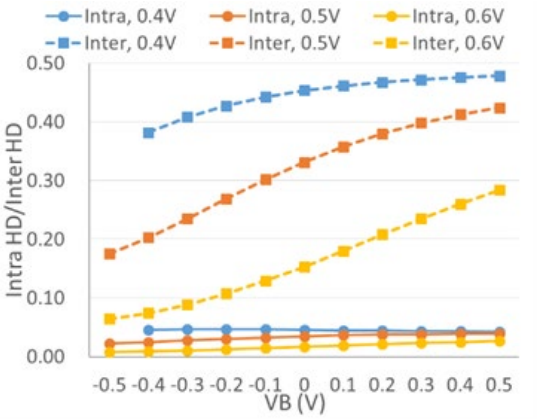

図 4　基板バイアス変動時の SOTB Arbiter PUF の特性変化

(6) 温度変動試験

PUF の特性をより詳細に解析するため、恒温槽を用いて雰囲気温度を - 40 から 125 度まで変化させ、同時にコア電圧を 0.4 から 1.0V まで 0.1V ずつ変化させて Arbiter PUF のレスポンスを収集し、再現性やユニーク性の評価を行った。その結果、あるコア電圧では、室温で動作していた PUF が低温や高温では動作しないか、PUF としての特性が失われる現象が観察された。

これについては、さらに詳細なデータを取得して解析を行い、現在論文投稿の準備を行っているところである。

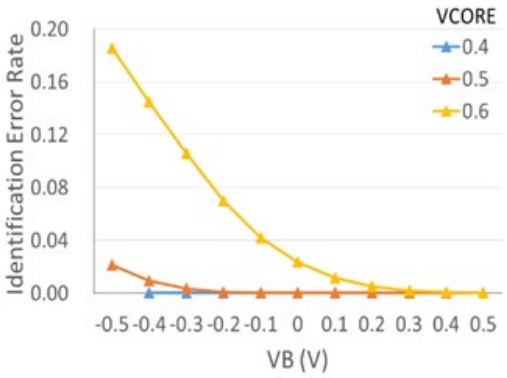

図 5　基板バイアス調整時の認証エラー率

(7) 成果のまとめ

本研究は、65nm SOTB プロセスで製造された実チップの評価を通じ、SOTB を用いた PUF が実現可能であることを初めて明らかにした。これにより、省電力及びセキュリティが重要な IoT において、SOTB の有効性が示された。

128 段の SOTB Arbiter PUF は、コア電圧の変化によって大きく特性が変化し、室温では 0.4 から 0.5V であれば認証目的に使用することができると示唆された。また、基板バイアス電圧を変化させることで SOTB Arbiter PUF のユニーク性を改善することができ、認証エラー率を大幅に低減可能であることが示された。これにより、製造前の特性の予測が困難な PUF において、出荷後に基板バイアスを制御することで PUF の特性を調整するような使用方法が可能であることが示唆された。

上記の成果のほか、恒温槽を用いた温度変動試験では、コア電圧によって低温や高温では PUF としての特性が失われる現象が観察された。これについては、さらにデータを収集し解析を行い、現在論文投稿の準備を行っているところである。また、PL-PUF については未発表であるため詳細の掲載は割愛したが、Arbiter PUF と同様に SOTB を用いた場合でも PUF としての特性が得られることが分かっている。

本研究では Arbiter PUF を主に評価したが、TEG チップに屋 Ring Oscillator PUF を含む他の PUF が搭載されており、これらの評価が課題として残っている。また、今回は TEG チップ上の PUF の単体の評価を行ったが、今後は認証や暗号の回路を含む PUF システムのとしての性能・安全性の評価が課題として挙げられる。

５．主な発表論文等

〔学会発表〕（計１件）

① Yohei Hori, Toshihiro Katashita, and Yasuhiro Ogasahara, “A 65-nm SOTB Implementation of a Physically Unclonable Function and Its Performance Improvement by Body Bias Control”, in Proc. IEEE SOI-3D-Subthreshold Microelectronics Technology Unified Conference (S3S 2017), 査読有り、pp.1-3.
DOI: 10.1109/S3S.2017.8309209

〔その他〕

研究代表者ウェブサイト

https://staff.aist.go.jp/hori.y/index_j.html

６．研究組織

(1)研究分担者

研究分担者氏名：片下　敏宏

ローマ字氏名：（KATASHITA, Toshihiro）

所属研究機関名：国立研究開発法人産業技術総合研究所

部局名：エレクトロニクス・製造領域

職名：主任研究員

研究者番号（8 桁）：90500215

研究分担者氏名：小笠原　泰弘

ローマ字氏名：（OGASAHARA, Yasuhiro）

所属研究機関名：国立研究開発法人産業技術総合研究所

部局名：エレクトロニクス・製造領域

職名：主任研究員

研究者番号（8 桁）：30635298