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　２ 年　 ６ 月 ２３ 日現在

機関番号：８２６２６
研究種目：若手研究(B)
研究期間：2016～2019
課題番号：１６Ｋ１６０３１

研究課題名（和文）真贋判定技術 PUF のチップ出荷前の効率的な認証情報取得技術

研究課題名（英文）Effective Acquisition of Authentication Information before Shipping for Verification of Authenticity using PUF Technology

研究代表者

小笠原　泰弘（Ogasahara, Yasuhiro）

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：３０６３５２９８

交付決定額（研究期間全体）：（直接経費）　　3,000,000円

研究成果の概要（和文）：本研究では半導体チップの偽造品の流通を防止するための技術である、真贋判定技術PUFの実用化のための課題について取り組んだ。PUF技術は出荷前に真贋判定の際に用いる認証情報を、製造した半導体チップから取り出す必要がある。さらに、出荷後には特定のシーケンスでのみ認証できるようにして、認証情報そのものにはアクセスできないようにする必要がある。
本研究ではPUF回路の認証時の入力と応答のペアを出荷前に多数取得するための回路を埋め込み、さらに出荷時の検査後にこの回路を破壊することで、出荷後に悪意あるものが認証情報を取得することを防ぐ仕組みを提案し、回路のシミュレーションにおいて動作、性能を実証した。

研究成果の学術的意義や社会的意義
半導体チップの偽造品はすでに多数流通しており、専門的な報告のみならず、一般市民の目に触れる技術ニュース等でも取り上げられている。本研究成果は単にPUF技術の回路を提案する他の研究とは異なり、PUF技術を実際に実装し、製品に搭載して真贋判定の認証システムを運用する上で重要な役割を果たす。
本研究成果により正規の事業者が十分な量の認証情報の取得し、悪意あるものが認証情報を取得することを防ぐことの両方が同時に実現される。さらに、本手法により十分な量の認証情報を取得することにより、最新の攻撃技術である機械攻撃によるPUFへの攻撃に対しても十分な耐性を得ることが可能となる。

研究成果の概要（英文）：In this work, we worked on the authentication data collection before shipping of the authentication technology, PUF(Physical Unclonable Function). PUF technology needs to acquire the authentication data from the fabricated LSIs before shipping the products. In addition, PUFs needed to be protected from the attack to extract the authentication data after shipping.
The feature of this work is adopting BIST(Built-In Self Test) technology, and preventing from exploiting the BIST circuits for the attack after shipping by destroying the BIST circuit after the test before shipping. We proposed the circuit structures of BIST circuit with disabling structure. The PUF circuit including the proposed BIST circuit was implemented on the circuit simulation and operation of the whole PUF circuit was validated on the circuit simulation.

研究分野：回路設計

キーワード：PUF　真贋判定　回路設計　BIST　真正乱数

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９（共通）

１．研究開始当初の背景

近年の半導体チップの製造技術の進歩は目覚ましく、将来的には、社会インフラの至る所に半導体チップを応用し、自動車の自動運転、自然エネルギーを含む電力網の制御、より高度な医療機器、行政サービスの利便性の向上等が期待されている。一方で社会インフラに組み込まれる半導体チップは高い信頼性が求められる。特に、粗悪な偽造品の混入は、大規模停電や医療事故等、社会への重大な損害を引き起こす恐れがあり、偽造品の排除は重要な課題である。

２．研究の目的

本研究課題では真贋判定技術 PUF において、攻撃に耐えうる十分な量の認証情報をチップ出荷前に安全かつ高速に取得する技術を開発する。PUF 方式のうち、PUF 回路自体が製造ばらつきを利用して入力ビット列から応答ビット列を生成する方式は、回路の内部状態の読み取りが困難であり、応答を模倣する攻撃に強い。その反面、防御側も十分な量の応答の情報（認証情報）を事前に取得する必要があるという課題を持つ。本研究では擬似・真性乱数を利用したランダムで高速かつ小規模な回路で実装可能な入力の生成技術を開発し、チップに混載した上で出荷前に破壊して攻撃者による悪用を防ぐ技術を開発し、この問題を解決する。

３．研究の方法

本研究課題では真贋判定技術 PUF のための識別情報の取得を高速に行う技術を開発する。チップ上に混載したテスト回路について下記に示す計画で課題を解決する。

(1) 予測困難な入力を生成するための各種乱数生成手法の回路規模の推定

(2) 識別情報取得に必要とされる予測困難性の検討と乱数生成手法の改良と実装する回路の小面積化

(3) 入力を生成するテスト回路にのみ高電圧を付加して破壊する回路の設計

(4) 識別情報を高速に取得する回路の実装とシミュレーションによる動作の実証

４．研究成果

(1) 予測困難な入力を生成するための回路機構の検討と小規模化

予測困難な入力を生成する回路として乱数発生回路の検討を行った。ハードウェアで乱数を生成する場合、擬似乱数と真正乱数に分かれる。擬似乱数は数学的計算法により乱数を生成する方式であり、ソフトウェアで乱数を生成する場合は一般的にこちらが用いられる。しかし、調査の結果、メルセンヌ・ツイスタ法に代表されるソフトウェアで良質な乱数を生成するアルゴリズムの大多数は大きなメモリ空間を消費し、ハードウェア実装の場合大規模なフリップ・フロップ回路を必要とするため今回の用途には適さない。他のハードウェアテスト手法等でも用いられている疑似乱数生成手法として、線形帰還シフトレジスタを用いた方式が存在する。しかし、乱数の質が悪いため、セキュリティ強度が必要な本方式には適さないと判断した。一方、真正乱数生成器 (TRNG: True Random Number Generator)は物理現象を利用して回路から乱数を取り出す方式である。ハードウェアでの実装コストは比較的小さいものの、物理現象を利用するため実際に実チップ上で良好なランダム性を得るために物理現象への十分な理解等、回路設計の難易度が高い。これは、実用上はチップを作った際に良好な乱数が良好な歩留まりで得られるまで何度も作り直しが必要となり、開発コストの高騰と開発期間の長期化の問題につながる。研究代表者は真正乱数生成方式の調査の結果、Torii 氏らによる多数のラッチ回路を使用する方式の乱数生成回路[1]は回路パラメータの調整は難しくないことを見出した。さらに、研究代表者は自らの過去の研究[2]から、乱数生成にのみ用いるのであればラッチから書き込み機構を除去したバスキーパーと呼ばれる回路を用いることで、回路規模を削減することが可能であることを見出した。さらに、シミュレーションした結果、128bit のバスキーパーを用いることで、高い歩留まりで良好なランダム性を持つ回路が実現できることを確認した。この回路の回路規模は 801 ゲート相当であり、ハードウェア実装として十分小さい規模を実現した。なお、チップでの検証も試行したが、予算額の範囲内で試行した有機デバイスを用いた回路では残念ながら有機トランジスタの特性が悪く、乱数生成器としての特性を検証できなかった。[3]

[1] N. Torii, et al., “ASIC implementation of random number generators using SR latches and its evaluation.” EURASIP J. on Info. Security, Vol. 10, 2016.
[2] Y. Ogasahara et al., “Standard cell implementation of buskeeper PUF with symmetric inverters and neighboring cells for passing randomness tests,” In Proc. IEEE Global Conference on Consumer Electronics (GCCE), pp. 550-551, 2015.
[3] Yasuhiro Ogasahara, et al., "Feasibility of a low-power, low-voltage complementary organic thin film transistor buskeeper physical unclonable function," Japanese Journal of Applied Physics (JJAP), Vol. 58, No. SB, p. SBBG03, 2019.

(2) 入力を生成するテスト回路にのみ高電圧を付加して破壊する回路の設計

入力を多数生成して応答を取得するテスト回路は悪意あるものが使用した場合、搭載した PUF から多数の入力と応答のペアを取得する攻撃に利用することが可能である。本研究では出荷前

の識別情報の取得の後、乱数生成回路を破壊して攻撃者が使用できないようにする方式について、当初の研究計画の方式に加えさらに 2 種の方式を提案し、実証を行った。

1 つ目の方式は乱数生成回路全体に高電圧を付加し、乱数生成回路を破壊する方式である。この方式では、乱数生成回路の電源線を他の回路と分離し、破壊の際に分離したテスト回路用の電源線に高い電圧(2～5V)を付加して破壊する。乱数生成回路は乱数回路を制御する部分と生成した乱数をテスト回路に伝える部分で他の回路と接続されており、付加した高電圧がこの部分から周囲の回路を破壊する可能性がある。本方式ではこの部分に高耐圧トランジスタを使用したトランスミッションゲートを配置して電圧が伝搬するのを抑制し、さらにトランスミッションゲートの微小な漏れ電流を逃がすために小さいトランジスタを介してグラウンドと接続する。グラウンドとの接続は、小さいトランジスタを介することにより、通常の信号伝搬に影響を及ぼさない。2 つ目の方式は乱数生成回路からテスト回路への乱数の値の伝搬経路を切断し、無効化する方法である。乱数生成回路の出力に一方の入力をヒューズを使用した回路に繋いだ AND ゲートを挟む。この回路はヒューズを切る前は 1、ヒューズを切った後は 0 を常に出力する。この構造により、ヒューズを切った後は AND ゲートの出力は常に 0 となり、テスト回路が乱数を使用することができない。この方式の利点は、乱数生成回路自体を破壊しないため、乱数生成回路を別の用途に転用することが可能である点と、LSI 製品の出荷前にヒューズを切り設定等を書き込む手法自体はすでに広く使用されている実績のある方法であり、実用化が容易な点である。3 つ目の方式(図 1)は今回設計したラッチを使用した乱数生成方式独自の物である。ラッチを使用した乱数生成の場合、パワーゲートによりラッチの電源をオン・オフすることにより乱数を生成する。この電源のオン・オフを行うパワーゲートの制御信号を 2 つ目の方式と同様の AND ゲートとヒューズを用いて固定することにより、乱数生成回路を使用できないようにする。この方式の利点はヒューズを用いる実績のある方法を用いつつ、乱数生成回路自体は使用できないようになっているため、万が一回路にセキュリティホールがあった場合でも乱数生成器を悪用される可能性を排除できる点である。これらの方式について、回路を設計し、シミュレーションを行って動作の実証を行った。1 つ目の高電圧の付加においては、乱数生成回路に高電圧を付加した場合でも、周辺の回路に高電圧がかからないことを確認した。2 つ目、3 つ目の方法では、ヒューズを切ることにより、生成した乱数の伝搬、または乱数生成回路の動作が停止されることを確認した。

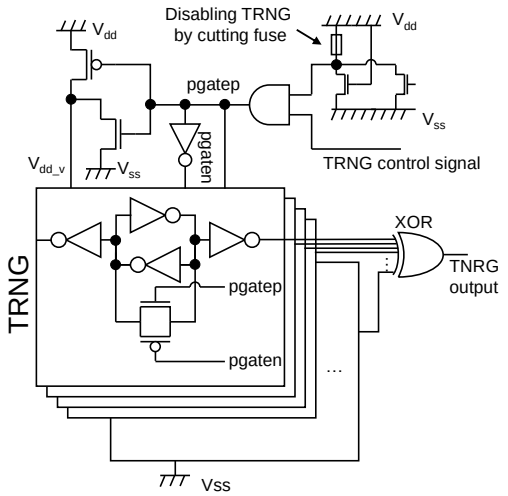

図 1 真正乱数生成回路(TRNG)と出荷後に使用できないようにするためのヒューズを用いた回路

(3) 識別情報を高速に取得する回路の実装とシミュレーションによる動作の実証

本研究で開発した出荷前テスト用回路とその無効化の機構を用いて、入力から応答を直接生成する方式の PUF の中から、PL-PUF と呼ばれる PUF 回路をシミュレーション上で実装し、動作の検証に成功した。回路規模は全体で 3,328 論理ゲートであり、小規模な実装が可能である。

また、本研究期間中に PUF に対する機械学習攻撃が提唱されたため、本研究でも実装した PL-PUF に対して機械学習攻撃の検証を行った。その結果、PL-PUF を用いた真贋判定には 128bit の入力･応答ペアを 8 組用いて 1,024bit の長さの入力・応答ペアを用いることで十分な機械学習攻撃態勢が得られることが判明した。本研究の出荷前テスト回路を用いることにより多数の入力･応答ペアを取得することにより、1,024bit を用いる認証は容易に対応可能であり、PUF 技術のセキュリティ強度の向上の面で、本研究の有用性が新たに明らかになった。これらの成果は論文誌として掲載された[4]。

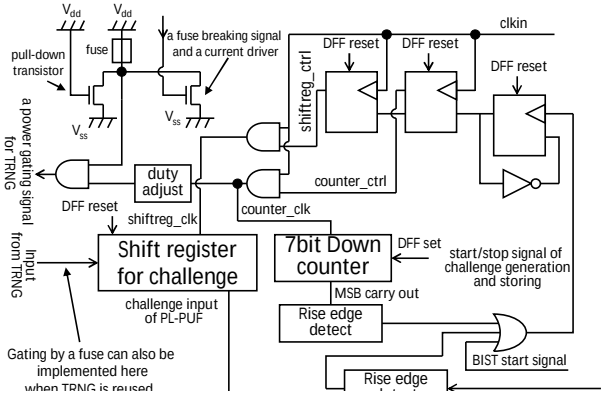

図 2 PUF 回路と乱数を用いたテスト回路の制御回路

[4] Yasuhiro Ogasahara, et al., “Implementation of pseudo-linear feedback shift register-based physical unclonable functions on silicon and sufficient Challenge-Response pair acquisition using Built-In Self-Test before shipping,” Elsevier, Integration, the VLSI Journal, Vol. 71, pp. 144-153, 2020.

５．主な発表論文等

〔雑誌論文〕　計2件（うち査読付論文　2件／うち国際共著　0件／うちオープンアクセス　1件）

１．著者名 Ogasahara Yasuhiro、Kuribara Kazunori、Shintani Michihiro、Sato Takashi	４．巻 58
２．論文標題 Feasibility of a low-power, low-voltage complementary organic thin film transistor buskeeper physical unclonable function	５．発行年 2019年
３．雑誌名 Japanese Journal of Applied Physics	６．最初と最後の頁 SBBG03～SBBG03
掲載論文のDOI（デジタルオブジェクト識別子） https://doi.org/10.7567/1347-4065/aaf7fd	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

１．著者名 Ogasahara Yasuhiro、Hori Yohei、Katashita Toshihiro、Iizuka Tomoki、Awano Hiromitsu、Ikeda Makoto、Koike Hanpei	４．巻 71
２．論文標題 Implementation of pseudo-linear feedback shift register-based physical unclonable functions on silicon and sufficient Challenge?Response pair acquisition using Built-In Self-Test before shipping	５．発行年 2020年
３．雑誌名 Integration	６．最初と最後の頁 144～153
掲載論文のDOI（デジタルオブジェクト識別子） https://doi.org/10.1016/j.vlsi.2019.12.002	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

〔学会発表〕　計1件（うち招待講演　0件／うち国際学会　1件）

１．発表者名 Yasuhiro Ogasahara
２．発表標題 Feasibility of Low-Power Organic Buskeeper PUF using Low-Voltage-Operation Complementary Organic TFT
３．学会等名 The 2018 International Conference on Solid State Devices and Materials（国際学会）
４．発表年 2018年

〔図書〕　計0件

〔出願〕　計1件

産業財産権の名称 半導体デバイスのセキュリティ機能の検査装置	発明者 小笠原泰弘、堀洋平	権利者 国立研究開発法人産業技術総合研究所
産業財産権の種類、番号 特許、特願2019-122969	出願年 2019年	国内・外国の別 国内

〔取得〕　計0件

〔その他〕

―

６．研究組織

	氏名 （ローマ字氏名） （研究者番号）	所属研究機関・部局・職 （機関番号）	備考