修士論文

組込み自己テスト回路を用いた物理複製困難関数回路のチャレンジレスポンス対の収集効率化および機械学習攻撃耐性の向上

三野 智貴
奈良先端科学技術大学院大学
先端科学技術研究科
知能社会創成科学プログラム

主指導教員: 井上 美智子 教授
ディペンダブルシステム学 研究室（情報科学領域）

令和 2 年 3 月 13 日提出

本論文は奈良先端科学技術大学院大学先端科学技術研究科に
修士 (工学) 授与の要件として提出した修士論文である。

三野 智貴

審査委員：

井上 美智子 教授　（主指導教員，情報科学領域）
浦岡 行治 教授　（副指導教員，物質創生科学領域）
大下 福仁 准教授　（副指導教員，情報科学領域）
新谷 道広 助教　（副指導教員，情報科学領域）

組込み自己テスト回路を用いた物理複製困難関数回路のチャレンジレスポンス対の収集効率化および機械学習攻撃耐性の向上*

三野 智貴

内容梗概

物理複製困難関数（Physically unclonable function, PUF）回路のチャレンジレスポンス対（Challenge-response pair, CRP）を用いたデバイス認証方法は，偽造集積回路（Integrated circuit, IC）チップの対策の 1 つとして注目されている．セキュアなデバイス認証の実現には，チップの出荷前に製造者が大量の CRP を収集しておく必要があるため，計測コストが増加する．また，PUF 回路の中には，機械学習を用いた攻撃に脆弱であるものも存在する．

本研究では，論理組込み自己テスト（Logic built-in self-test, LBIST）回路を用いて，量産テスト時において効率的に CRP を収集する手法を提案する．提案手法では，追加の回路オーバーヘッドがわずかで実現できる．さらに LBIST 回路を介することでチャレンジとレスポンスの関係が複雑になり，機械学習攻撃耐性が向上する．評価実験では，提案回路を Field-programmable gate array（FPGA）上に実装し，LBIST 回路が生成したテストパターンにより PUF の性能評価を行えることを示した．さらに，サポートベクターマシン（Support vector machine, SVM），およびランダムフォレスト（Random forests, RF）を用いた機械学習攻撃による PUF 回路の脆弱性が，チャレンジおよびレスポンスを外部から直接入出力する場合と比較して，2 倍以上小さくなることを示した．

*奈良先端科学技術大学院大学 先端科学技術研究科 修士論文, 令和 2 年 3 月 13 日.

キーワード

物理複製困難関数回路，デバイス認証，論理組込み自己テスト，チャレンジレスポンス対，偽造チップ，機械学習攻撃

Efficient Challenge-Response Pairs Collection and Machine-Learning Attacks Tolerance Improvement for PUF Circuit Using a BIST Circuit*

Tomoki Mino

Abstract

Device identification using challenge-response pairs (CRPs), in which the response is obtained from a physically unclonable function (PUF), is one of promising countermeasures for the counterfeit of integrated circuits (ICs). To achieve secure device identification, a large number of CRPs are collected by the manufacturer before shipping, therefore, a large measurement cost is required. In addition, there are existing PUFs which are vulnerable to machine learning attacks.

This work proposes a novel scheme, which employs a logic built-in self-test (LBIST) circuit, to efficiently collect CRPs during production tests. As a result, additional measurements are realized with very small circuit overhead. In addition, the proposed technology is able to counter machine-learning (ML) attacks thanks to the complicated relationship between challenge and response through the LBIST circuit. In the experimental evaluation, in which a field-programmable gate array (FPGA) was used it was shown that the PUF performance can be evaluated by test patterns generated by the LBIST circuit. Furthermore, the vulnerability of PUF circuit due to ML attacks using support vector machine (SVM) and random forest (RF) was also shown to be reduced by more than half, compared with the case where challenges and responses are directly applied and observed from the outside of IC chips.

*Master's Thesis, Graduate School of Science and Technology, Nara Institute of Science and Technology, March 13, 2020.

Keywords:

Physically unclonable function circuit, Device authentication, Logic buint-in self-test, Challenge-response pairs, Counterfeit chip, Machine-learning attack

目 次

図 目 次

表 目 次

1. はじめに

近年，半導体製品のサプライチェーンにおいて，偽造集積回路（Integrated circuit, IC）チップ流通の増加が問題視されている [1–4]．偽造チップの存在は，経済的損失やブランドイメージへの悪影響をもたらすのみでなく，動作不良による事故の原因となる危険性がある．特に，自動車，航空機，医療機器等のミッションクリティカルな製品は人命に直結するため，これらの製品に使用される部品への偽造チップの混入は未然に防がれなければならない．

この対策の 1 つとして，物理複製困難関数（Physically unclonable function, PUF）回路によるデバイス認証が提案されている [5–7]．PUF は複製困難な物理的特徴を利用してチップに固有の ID を与える関数であり，固有 ID を用いた認証によって偽造チップを検出する．PUF 回路は，同じ入力（チャレンジ）に対しチップごとに異なる出力（レスポンス）を返す関数の機能を持つ回路である．その入出力特性であるチャレンジレスポンス対（Challenge-response pair, CRP）はチップの製造ばらつきに依存し複製が困難であるため，CRP を ID として用いることでチップ認証を実現できる．

PUF 回路はチップの物理的特徴を利用して製造されるため，実装されるデバイスや回路構成により入出力特性が変化する．セキュアなデバイス認証の実現には，PUF 回路を実装するデバイスに対して，どの PUF 回路が適しているか判別するために，PUF 回路の性能を定量的に評価することが重要である．そのため，PUF 回路の製造後に製造された PUF 回路の性能を評価する必要がある．文献 [8] では，実装された PUF 回路をランダム性，安定性，正確性，拡散性，およびユニーク性の５つの指標で評価する手法が提案されている．

セキュアなデバイス認証の実現に向けて，文献 [5] では，製造者が製品の出荷前に PUF 回路にチャレンジを与えてレスポンスを得ることで，CRP データベースを構築する手法を提案している．デバイスの購入者は，そのデバイスが正規品か否かを問い合わせる際に製造者からチャレンジを受け取る．そのチャレンジを元にレスポンスを得て，製造者が有する CRP データベースに照合し，一致した場合にそのデバイスが正規品であるとみなす．

しかし，文献 [5] の手法で安全な認証を行うためには，デバイス毎に大量の

CRP を取得してデータベースを構築する必要がある．これまでに，様々な PUF 回路が提案されているが，いずれにおいても CRP の取得には高価な自動試験装置（Automatic test equipment, ATE）が必要となり，データベースの構築コストが大きくなる．また，PUF の性能評価にも CRP を取得する必要があるため，追加のコストが必要になる．さらに，PUF の安全性を脅かす要因として，一部の CRP から機械学習によって全 CRP を推定する機械学習攻撃が報告されている [9–11]. 以上のように，PUF 回路を用いたデバイス認証を実用化のためにはいくつかの解決すべき課題がある．

本研究では，テスト容易化設計手法の 1 つとして広く採用されている組込み自己テスト（Built-in self-test, BIST）回路を用いて，CRP を取得する手法を提案する．ここでは，論理回路向けの BIST 回路である論理 BIST（Logic BIST, LBIST）を対象としており，LBIST-PUF と呼称する．LBIST-PUF では，LBIST 回路で生成されるテストパターンをチャレンジとして使用することで，量産テストを行うと同時に CRP を取得する．これにより，CRP 取得のための測定コストが追加されることなく，効率的に CRP を取得することができる．また，CRP 取得のための回路オーバーヘッドも生じない．さらに LBIST-PUF では，同じチャレンジセットを複数回与えることで，PUF 回路の性能評価を行える．評価には，論理回路のテストに必要なテストパターン以上のチャレンジが用いられるため，性能評価と同時に量産テストが行える．BIST 回路を利用した既存手法として，文献 [12] で提案された BIST-PUF が存在するが，BIST-PUF は真性乱数生成器の使用を想定しており，量産テストのために使用する BIST を考慮したものではないため，別途，設計コストを要する．また，LBIST 回路を用いて PUF 回路へのチャレンジを生成するため，外部から CRP 取得の手続きの秘匿性が向上する．その結果，機械学習アルゴリズムなどを用いた PUF 回路のモデル化が難しくなるため，PUF 回路の機械学習攻撃耐性も向上する．

本研究の主な貢献は以下のものである．

- 計測コストや回路の面積オーバーヘッドの追加をほぼなしで CRP 取得を実現するために，LBIST 回路を用いて量産テストと同時に CRP 計測を行う．
- 提案回路の実現性を市販の Field-programmable gate array（FPGA）上への実

装により証明する．

- LBIST-PUF が，文献 [8] の評価指標を用いた実装した PUF の性能評価中に，論理回路をテストできることを示す．
- LBIST-PUF の機械学習攻撃耐性が高いことを，従来の PUF の使用方法との比較により実証する．

本章では，本研究の背景，課題，および目的について述べた．本論文の構成は次のようになっている．2 章にて，チップの製造後に行われる量産テスト，テスト効率の向上のための LBIST 技術，アービター PUF を例とした PUF 回路の動作原理，CRP を用いたデバイス認証方法とその課題，および PUF の性能の評価指標について述べる．3 章では，明らかとした課題を解決する LBIST-PUF を提案する．4 章で，提案回路の FPGA 上での実装および動作について述べる，5 章で，回路オーバーヘッドを生じることなく十分な CRP と故障検出率を同時に得られることを示す．また，5 章では，LBIST-PUF により，従来手法と比較して，機械学習攻撃の耐性が向上することも示す．最後に，6 章にて本論文をまとめる．

2. 研究背景

本章では，チップの製造後に行われる量産テスト，およびそれに関連する BIST 技術について述べる．また，デバイス認証を実現するための関連研究として PUF 回路，PUF 回路を用いたデバイス認証方法，PUF 回路への機械学習攻撃，および PUF の性能の評価指標について述べる．

2.1 IC チップのテスト

2.1.1 量産テスト

IC チップの製造時には，不良品が混入することは避けられないために製造されたチップが良品か不良品かを判別するためのテストが必要となる．チップの製造時には，製造工程におけるばらつきや欠陥の混入により，チップごとに個体差が発生する．この製造時に発生するチップごとのばらつきを製造ばらつきと呼ぶ．製造されたチップが要求性能を満たしているかを診断するために，チップの製造後に検査が行われる．これを量産テストと呼ぶ．チップは微細加工技術で製造されているため，製造されたチップに不良品が発生することは避けられない．そのような不良チップを市場に流出させないために，品質の高い量産テストを行うことで不良チップを取り除く必要がある．以上のことから，量産テストは製造されたチップの高信頼性を保証するために必須の工程である．

量産テストは，ATE を用いてテストパターンと呼ばれる 0 と 1 の値の組合せをテスト対象回路（Circuit under test, CUT）に対して印加して行う．CUT から出力される値と期待値を比較することにより，故障の有無が判別できる．テストパターンは，対象とする故障に対して自動テストパターン生成器（Automatic test pattern generator, ATPG）を用いることで生成できる．故障には，回路上の配線の断線や短絡などの物理的欠陥を抽象化した故障モデルが用いられる．故障モデルは，現在までに様々なものが提案されている [13]．生成した全てのテストパターンを用いて故障シミュレーションを行うことで，故障検出率を算出することができる．故障検出率は，印加するテストパターンによって，想定する故障をどれだけ検出できるかを表すテストの評価指標である．故障検出率が高いほど，品質の

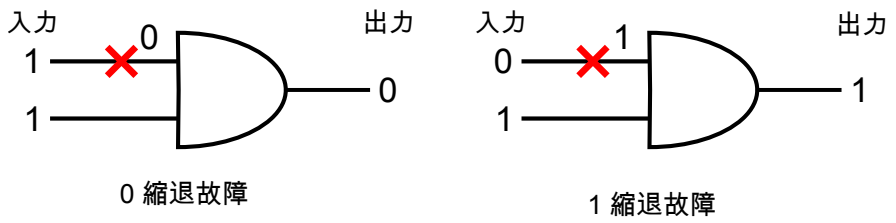

図 1 縮退故障モデル

高いテストができることを示し，用いたテストパターンが多くの故障を検出できる．故障検出率は，以下の式で算出できる．

$$\text{故障検出率} = \frac{\text{検出できる故障数}}{\text{想定した全故障数}} \times 100[\%] \tag{1}$$

回路に発生する故障モデルの例として，もっとも広く用いられる縮退故障を図 1 に示す．縮退故障は，回路上の配線が物理的欠陥により短絡や開放され，0 または 1 に固定されてしまう故障モデルである [13]．その結果，信号が正しく伝達されなくなり，回路が正しく動作しなくなる．図 1 の 0 縮退故障の場合，テストパターンとして 11 を 2 入力の AND ゲートに印加し，出力値の 0 と期待値の 1 を比較することで 0 縮退故障が検出できる．

2.1.2 論理組込み自己テスト

近年のチップの高集積化技術の発展に伴い，回路規模が巨大化している．チップへのテストを ATE のみで行う場合，大量のテストパターンと期待値を ATE が保持しておく必要がある．そのため高品質なテストを行うには，高価な ATE と膨大なテスト時間が必要になる．この課題を解決する技術の 1 つとして，BIST 回路が広く用いられている [13]．BIST 回路はテスト容易化設計技術の 1 つであり，ATE の一部の機能をチップ内に組込んだ回路である．BIST 回路により高価な ATE が不要になり，1 つの ATE で，並列にテストできるチップ数が増加するため，テストコストの削減が可能になる．BIST には，メモリを検査するメモリ BIST，論理回路を検査するための LBIST があるが [13]，ここでは，LBIST 回路について述べる．

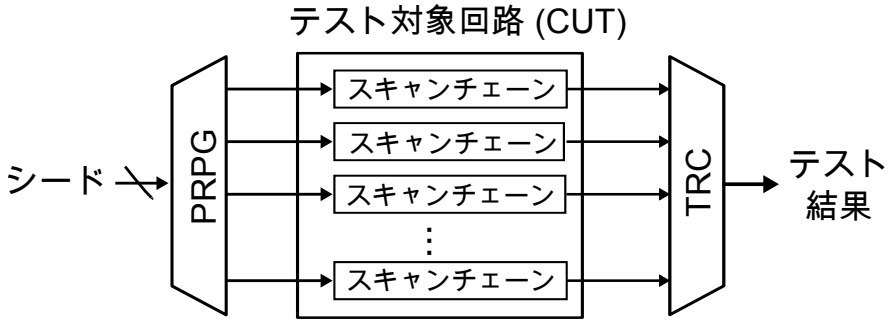

図 2 LBIST 回路の構成

図 2 に LBIST 回路の構成を示す．LBIST 回路は，CUT をテストするためにテストパターンを生成する疑似乱数パターン生成回路（Pseudo random pattern generator, PRPG），スキャンチェーン，および CUT により出力されたテスト応答のデータを圧縮するテスト応答圧縮回路（Test response compactor, TRC）で構成される．一般的に PRPG としては，線形帰還シフトレジスタ（Linear feedback shift register, LFSR），およびフェーズシフタが用いられ [14]，TRC は多入力シグネチャレジスタ（Multiple-input signature resister, MISR）が用いられる．LFSR はシードと呼ばれる初期値を入力することで，テストを行うための疑似乱数テストパターンを発生させる．フェーズシフタは LFSR からの出力系を指定したクロック数分ずらすことができ，テスト効率の向上ために使用される．生成されたテストパターンはスキャンチェーンを介して CUT に入力される．スキャンチェーンは，回路内部に存在するフリップフロップ（Flip flop, FF）同士を繋げたチェーンであり，テストを行う際のテストデータの観測性や制御性の向上に用いられる．MISR は CUT から出力されたテスト応答をシグネチャと呼ばれるデータに圧縮する．たとえば，m（m: MISR の入力数）ビットの MISR を用いた場合，テスト応答を m ビットのシグネチャに圧縮できる．

LBIST 回路を用いたテストでは，MISR より出力される CUT のシグネチャと期待値として，予め LBIST が保持しているシグネチャを比較することで故障の有無の判断が可能である．これにより，テストに必要なデータを大幅に削減することができる．

また，LBIST 回路では，テスト効率化のためにリシーディング手法が用いられ

る．リシーディングは，LBIST 回路に搭載される LFSR が出力する擬似乱数テストパターンのシードを入れ替える技術である [15,16]．BIST 方式によるテストでは，擬似乱数テストパターンが用いられるため，ATPG で生成した決定論的なテストパターンによるテストに比べて，故障検出率が低いという問題がある．故障検出率を上げるには，多くの疑似乱数テストパターンをテストに用いる必要がある．この問題の解決方法として，テスト中に LFSR のシードを入れ替えるリシード方式がある．リシードを行うことで，故障検出に寄与しないテストパターンを削減でき，BIST 方式のテストを効率化できる．

2.2 物理複製困難関数回路

PUF 回路は，複製困難な物理的特徴を利用して，チップ毎に異なる入出力特性を持つ関数として機能する回路である．PUF 回路はチップの製造時において，他回路と一緒に組込まれ，製造ばらつきにより複製困難な関数 $f(\cdot)$ として機能する．PUF 回路にチャレンジ $\boldsymbol{c} = (c_1, c_2, \cdots, c_n)$（$n$:PUF 回路の入力数）が与えられるとレスポンス $\boldsymbol{r} = (r_1, r_2, \cdots, r_n)$ を返す．つまり，PUF は関数 $\boldsymbol{r} = f(\boldsymbol{c})$ の関係が成り立つ．このとき，関数 f をチップの製造ばらつき α に依存するように設計すると，たとえ同じ関数回路 f を異なるチップに実装した場合であっても，チップ A の関数 $f_{\alpha_A}(\cdot)$ とチップ B $f_{\alpha_B}(\cdot)$ の関数では．異なるレスポンスが得られる．したがって，得られる各 CRP$(\boldsymbol{c}, \boldsymbol{r})$ はチップ毎に固有のものとなる．これまでに，様々なタイプの PUF が提案されており，電源投入時のメモリの初期値を利用する SRAM PUF [17], 発振回路の配置による発振周波数の違いを利用するリングオシレータ PUF [5]，２信号の遅延差を利用するアービター PUF [18,19] がある．

一般的に，PUF 回路はストロング PUF とウィーク PUF に分類される [10,20]．ストロング PUF は，1 つの PUF 回路に大量の CRP が存在する． ウィーク PUF は 1 つの PUF 回路に少量の CRP しか存在しない．ウィーク PUF の 1 種である SRAM PUF と異なり，1 つの回路から 2^n 個の CRP を得ることができるため，図 3 に示すアービター PUF はストロング PUF に分類され，高いセキュリティが要求される場合に有効である．

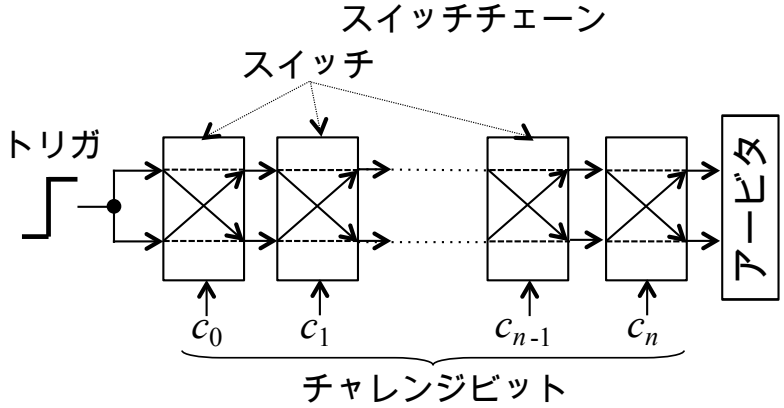

図 3 アービター PUF

2.2.1 アービター物理複製困難関数の動作

PUF 回路の動作を説明するため，ここでは，もっとも原始的な PUF 回路であるアービター PUF の動作について，図 3 を用いて説明する．アービター PUF では，等負荷，等配線長となるように設計，レイアウトされるスイッチチェーンとアービタで構成される．一般的に，スイッチチェーンにはセレクタが用いられ，アービタには FF が用いられる．スイッチチェーンは，チャレンジ（$c_0, c_1, \cdots, c_n$）に応じて，入力からアービタまでの 2 つの経路を選択し，アービタでは，選択された 2 経路間の内どちらのトリガ信号が先に到達したかを判別して，1 もしくは 0 をレスポンス r として返す．スイッチチェーンを等負荷，等配線長に設計した場合であっても，製造ばらつきによりスイッチや配線ごとに信号の伝達速度に差が発生する．その差により 2 つの経路を通る，どちらかの信号が先にアービターに到着する．アービター PUF では，例えば n ビットのチャレンジビットがある場合，CRP 数は 2^n となる．アービター PUF の場合，生成されるレスポンスは 1 ビットであるため，CRP は CRP($\boldsymbol{c}, r$) と表現できる．

2.2.2 デバイス認証

PUF の CRP をチップの ID とすることで，チップを対象とした認証系を構築することが可能となる．ここでは，文献 [5] で提案されている PUF 回路を用いたデ

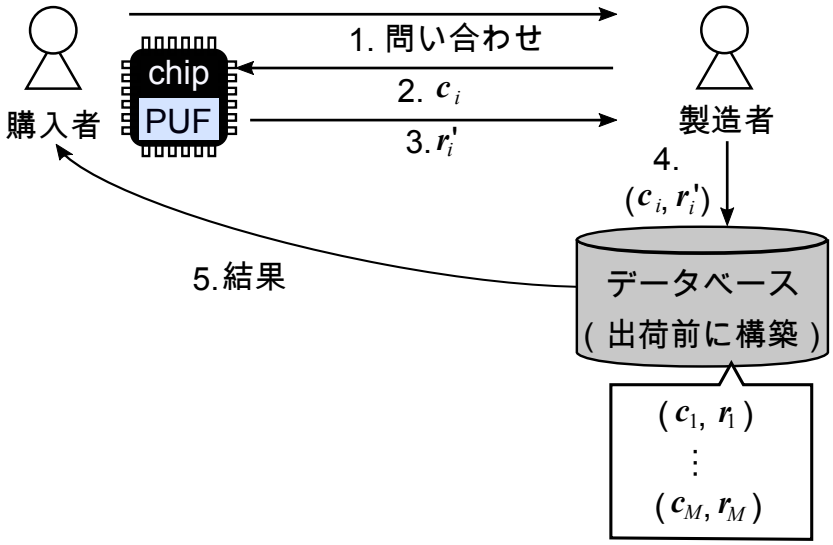

図 4 PUF 回路を用いたデバイス認証 [5]

バイス認証の方式を述べる．

文献 [5] では，ストロング PUF を用いたデバイス認証方式が提案されている．その手順を，図 4 に示す．本手順の前に，チップ製造者は M 通りのチャレンジを選定し，これに対応する PUF の CRP を取得する．取得した CRP は，データベース $\{(\boldsymbol{c}_1, \boldsymbol{r}_1), (\boldsymbol{c}_2, \boldsymbol{r}_2), \cdots, (\boldsymbol{c}_M, \boldsymbol{r}_M)\}$ として構築される．

1. 製品の購入者は，使用に先立って，購入した製品が正規品であるか否かを製造者に検査の要請をする．

2. 製造者は，問い合わせのあった製品に組込まれた PUF に対する CRP データベースから選択した i 番目のチャレンジ $\boldsymbol{c}_i$ を返信する．

3. 購入者は，$\boldsymbol{c}_i$ を PUF に入力し，得られたレスポンス $\boldsymbol{r}_i' = f_\alpha(\boldsymbol{c}_i)$ を製造者に送信する．

4. $\boldsymbol{r}_i' = f_\alpha(\boldsymbol{c}_i)$ を受け取った製造者は，CRP$(\boldsymbol{c}_i, \boldsymbol{r}_i')$ とデータベース内の CRP$(\boldsymbol{c}_i, \boldsymbol{r}_i)$ を比較する．

5. 比較結果を購入者に返す．ここで，CRP$(\boldsymbol{c}_i, \boldsymbol{r}_i')$ と CRP$(\boldsymbol{c}_i, \boldsymbol{r}_i)$ が一致していれば購入者の製品は正規品となる．

なお，アービター PUF などのレスポンスが 1 ビットである PUF の場合は，1 回の検査時に製造者は購入者から既定数の CRP($\boldsymbol{c}_i, r_i'$) を受け取り，データベースの複数の CRP($\boldsymbol{c}_i, r_i$) と比較することで認証が行われる．

ここで注目したいのは，デバイス認証を行うために製造者側で PUF データベースを事前に構築する点である．上述のように，高セキュアなデバイス認証を行うためには 1 デバイスあたり複数の CRP を取得する必要がある．すなわち CRP 数 M は大きいことが望まれる．高性能な PUF に関する研究は様々行われているが，CRP の取得に関する研究は非常に限られている．一般的に，チップ上に設計された PUF 回路の CRP を取得することは容易ではなく，量産テスト同様に ATE を用いる必要がある．したがって，高いセキュリティを確保するためには，取得コストが別途加算され，製造コストの増加に繋がる．以上から，PUF 回路を用いたデバイス認証を実現するためには，効率的な CRP 取得方法の確立が不可欠である．

2.2.3 機械学習攻撃耐性

近年，PUF 回路をデバイス認証に使用する際の課題として，機械学習攻撃に対する脆弱性が報告されている [9–11]．従来の PUF の回路方式の多くは，回路遅延の大小が直接レスポンスを決定づける仕組みであるため，CRP が線形分離可能な集合を成す．これにより，サポートベクターマシン（Support vector machine, SVM）[21] などの線形分離器を用いた PUF の関数 f のモデリングが可能となり，機械学習攻撃への脆弱性となる．

ある CRP の集合が学習データとして与えられた時，レスポンスが 1 ビットである PUF は，テストデータのチャレンジを 0 と 1 に分類する 2 クラス分類問題に定式化できる．PUF 回路が機械学習攻撃に脆弱である原因 1 つは，提案されているデバイス認証時の PUF 回路の CRP の取得方法にあるといえる．認証時において，レスポンス生成に必要な任意のチャレンジを外部から入力し，対応するレスポンスを外部へ出力する．攻撃者は，購入者と製造者の間で行われる CRP の受け渡しを傍受し，蓄積する．この蓄積したデータを機械学習に用いることにより，機械学習攻撃を可能とする．そのため，PUF 回路を用いたデバイス認証を実現するには，PUF が機械学習攻撃に耐性があることも不可欠である．したがって，推定

困難な CRP 生成機構を持つ PUF を実現することが強く求められている．

2.2.4 物理複製困難関数の性能指標

PUF 回路はチップの物理的特徴を利用して製造されるため，実装されるデバイスや回路構成により入出力特性が変化する．製造された PUF 回路の性能を保証するために，製造後に性能を評価する必要がある．PUF の性能を評価するための評価指標としては，主に一意性，および再現性の 2 つ指標が用いられる．一意性は，異なる PUF に対して同じチャレンジを入力した場合に異なるレスポンスを出力するかという性質を表す指標である．再現性は，ある PUF に対して同じチャレンジを何度も入力した場合に同じ値のレスポンスを常に出力するかという性質を表す指標である．一意性が満たされない場合，デバイス認証時に偽造チップが認証を通過する危険性が生じる．一方，再現性が満たされない場合，正規のチップが認証を通過しない可能性が生じる．以上のことから，セキュアに PUF 回路を用いたデバイス認証を行うには，これらの 2 つの指標が十分に高いことが重要である．

文献 [8] では，PUF 回路を実装するデバイスに対して，どの PUF 回路が適しているか判別するための PUF 回路の性能を定量的に評価する手法が提案されている．上述した指標を一意性はランダム性，拡散性，およびユニーク性の 3 つの指標で評価し，再現性は安定性，および正確性の 2 つの指標で評価する．本項では，文献 [8] で提案された指標について述べる．ここでは，先に評価に用いられる定数のについて述べる．K は生成する ID の数であり，W は生成する ID の長さであり，T は同じ ID を繰り返し生成する回数であり，V は評価に使用する PUF 回路の台数である．

ランダム性は，単一 PUF のレスポンスの 0 と 1 の偏り度合いを表す．理想的には，PUF が生成する全レスポンスの 0 と 1 の出現確率 [%] は 50:50 であることが好ましい．どちらか一方の値に出現確率が大きく偏ってしまうと，ID の予測が容易になりデバイス認証の安全性が低くなる．以下の式で，1 デバイスあたりのランダム性 H_v は表現される [8].

$$H_v = -\log_2 \max(p_v, 1 - p_v) \tag{2}$$

ここで，p_v は v 台目の PUF で生成される全てのレスポンスの中で，レスポンスビットが 1 であるものの相対頻度を表す．相対頻度は 1 つの PUF で生成された全てのレスポンスビットの 1 の割合と定義する．

安定性は，単一 PUF において，同じチャレンジで生成される ID が，どれほど安定しているかの度合いを表している．理想的には同じ PUF に対して，同じチャレンジを用いて T 回 ID を生成した場合，同じ値を出力することが好ましい．デバイス認証時に，あるチャレンジで生成された ID が，生成されるたびに異なる値を出力していては正しく認証が行えない．以下の式で，1 デバイスあたりの安定性 S_v は表現される [8].

$$S_v = 1 + \frac{1}{K \cdot W} \sum_{k=1}^{K} \sum_{w=1}^{W} \log_2 \max(p_{v,k,w}, 1 - p_{v,k,w}) \tag{3}$$

ここで，$p_{v,k,w}$ は v 台目の PUF において，k 個目の ID の w 番目の値を T 回生成したときの平均値である．

正確性は，単一 PUF が出力するレスポンスの正確度合いを表す．たとえ，安定性が高い場合でも，生成される ID が PUF 回路の故障等により誤った値が，毎回出力されると認証に失敗するため，正確性も評価する必要がある．以下の式で，1 デバイスあたりの正確性 C_v は表現される [8].

$$C_v = 1 - \frac{2}{K \cdot T \cdot W} \sum_{k=1}^{K} \sum_{t=1}^{T} \sum_{w=1}^{W} (b_{v,k,w} \oplus b_{v,k,t,w}) \tag{4}$$

ここで，$b_{v,k,w}$ は v 台目の PUF で生成される k 個目の ID の w 番目の正しい値であり，$p_{v,k,w}$ が 0.5 以上の場合は 1 となり，0.5 未満では 0 と定義する．$b_{v,k,t,w}$ は v 台目の PUF で生成される k 個目の ID の w 番目の t 回目に生成される値であり，$\oplus$ は排他的論理和を表している．

拡散性は，単一 PUF の異なるチャレンジ間で出力されるレスポンスのばらつき度合いを表している．異なるチャレンジで同じ ID が生成されると，ID の予測が容易になってしまうため，ID は 1 つの PUF でも異なる必要がある．以下の式で，1 デバイスあたりの拡散性 D_v は表現される [8].

$$D_v = \frac{4}{W \cdot K^2} \sum_{w=1}^{W} \sum_{y=1}^{K-1} \sum_{z=y+1}^{K} (b_{v,y,w} \oplus b_{v,z,w}) \tag{5}$$

ユニーク性は，複数の PUF において出力されるレスポンスが，PUF 間でどれほどばらついているかという度合いを表している．異なる PUF で同じ値の CRP が生成された場合，偽造チップが認証を通過する可能性がある．そのため，異なる PUF 間の CRP は異なっている必要がある．以下の式で，1 デバイスあたりのユニーク性 U_v は表現される [8].

$$U_v = \frac{4}{K \cdot W \cdot V} \sum_{k=1}^{K} \sum_{w=1}^{W} \sum_{z=1, z \neq v}^{V} (b_{v,k,w} \oplus b_{z,k,w}) \tag{6}$$

いずれの指標も 0 から 1 の範囲で値を取り，1 に近いほど性能が高いことを示している．

3. LBIST 回路を用いた PUF 回路の改良手法

本章では，PUF 回路を用いたデバイス認証に存在する課題を解決するための手法を提案する．また，提案手法におけるデータベース構築方法，およびデバイス認証方法について述べる．

3.1 概要

PUF の効率的な CRP 取得，および機械学習攻撃耐性の向上を目的に，本章では論理組込み自己テスト物理複製困難関数（LBIST-PUF）を提案する．LBIST-PUF の概念図を図 5 に示す．LBIST-PUF は，BIST および PUF で構成される．BIST の PRPG の出力を PUF にも接続することにより，PUF のレスポンス生成に必要なチャレンジが，PRPG を介して生成可能となる．本研究では BIST 回路として，LBIST 回路を利用する．ランダムロジックを検査するための LBIST 回路は，よりランダムなチャレンジ集合の生成が期待できる．また，デバイス認証時にも PUF 回路は LBIST 回路を介して動作するため，外部からの CRP 生成動作の秘匿性が向上し，ひいては機械学習攻撃耐性の向上に繋がる．

LBIST-PUF は，LBIS 回路に対して PUF 回路の制御動作を加えるものであり，PUF 回路に対しては変更を加えない．そのため，LBIST-PUF は，既存の多くのストロング PUF への適用が可能である．

3.2 データベース構築

提案する LBIST-PUF 回路の最大の特徴は，PRPG で生成されたテストパターンを用いて CUT をテストすると同時に，PUF のチャレンジ入力としても使用される点にある．2.1.1 項で述べたように，IC チップの製造後にはチップの品質を保証するために必ずテストが行われる．量産テスト時に PUF 回路の CRP を取得することにより，追加の測定オーバーヘッドが生じることなく，量産テストと同時に CRP データベースを構築可能となる．また，LBIST 回路は広く採用されている回路方式であるため，既に多くの回路に既に組込まれている．したがって，

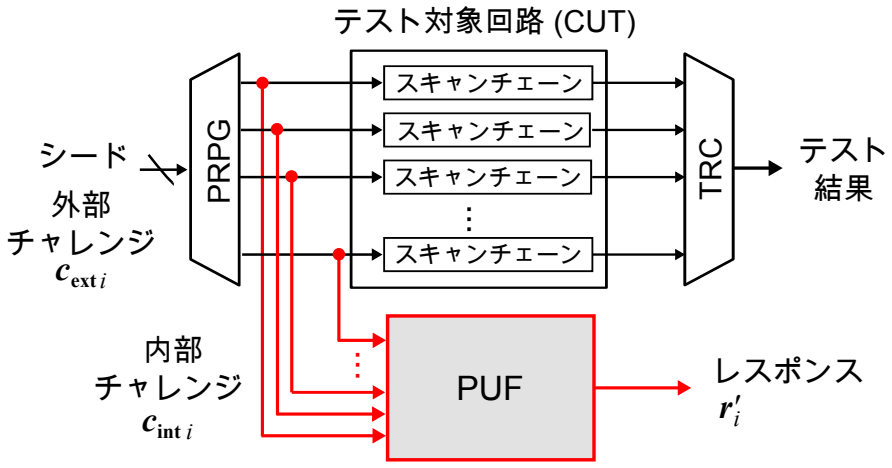

図 5 LBIST-PUF の概念図

LBIST-PUF 回路で生じる回路オーバーヘッドは，PRPG と PUF 回路間の配線オーバーヘッドと，多少のテスト制御回路の増加のみであるが，無視できる大きさである．

LBIST-PUF 回路のもう 1 つの特徴として，レスポンス生成が LFSR を介して行われる点が挙げられる．これにより，1 ビットのレスポンスを出力する PUF であっても，1 度の認証過程で外部チャレンジ $\boldsymbol{c}_{\mathbf{ext}i}$ を 1 つ与えると，内部で複数の内部チャレンジを生成し，複数ビットのレスポンス $\boldsymbol{r}_i$ を生成できる．図 6 に，LBIST-PUF 回路のレスポンス生成方法を示す．2.1.2 項でも述べたように，多くの LBIST 回路には，少ないテストパターン数で高故障検出率を達成するために，リシーディング手法が広く採用されている [15,16]．LBIST-PUF では，リシーディングにより LFSR に入力されるシードを外部チャレンジ $\boldsymbol{c}_{\mathbf{ext}i}$ と考え，外部チャレンジ入力後に PRPG が生成する規定の長さのテストパターン列を内部チャレンジ列 $\boldsymbol{c}_{\mathbf{int}i}$ と考える．ここで，$\boldsymbol{c}_{\mathbf{ext}i}$ をシードとして LFSR を $l-1$（l: 任意数）回動作させた場合，$\boldsymbol{c}_{\mathbf{int}i} = (c_{\mathrm{int}(i,1)}, \cdots, c_{\mathrm{int}(i,l)})$ となる．$g(\cdot)$ を PRPG の符号化関数とすると，外部チャレンジ $\boldsymbol{c}_{\mathbf{ext}i}$ と内部チャレンジ列 $\boldsymbol{c}_{\mathbf{int}i}$ の関係式は，$\boldsymbol{c}_{\mathbf{int}i} = g(\boldsymbol{c}_{\mathbf{ext}i})$ と表現できる．よって，LBIST-PUF では，$\boldsymbol{r}_i = f(g(\boldsymbol{c}_{\mathbf{ext}i}))$ を考えることとなる．LBIST-PUF により構築される CRP データベースは，$\{(\boldsymbol{c}_{\mathbf{ext}1}, \boldsymbol{r}_1), (\boldsymbol{c}_{\mathbf{ext}2}, \boldsymbol{r}_2), \cdots, (\boldsymbol{c}_{\mathbf{ext}M}, \boldsymbol{r}_M)\}$ と表現できる．

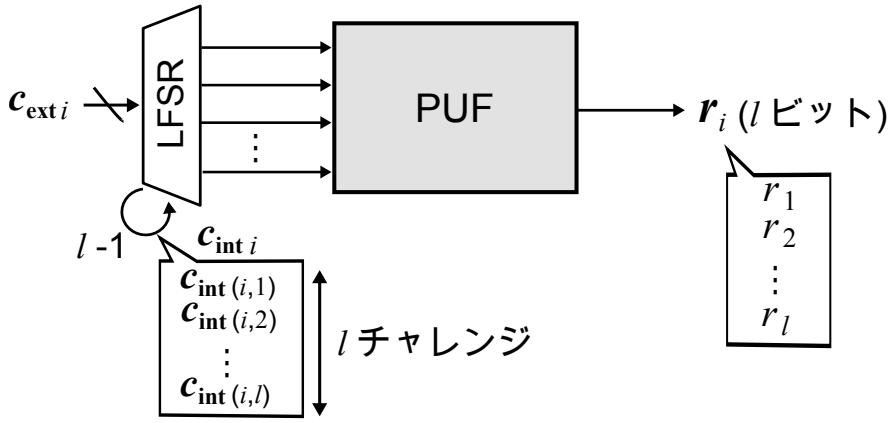

図 6 LBIST-PUF 回路のレスポンスの生成方法

3.3 デバイス認証

図 7 に LBIST-PUF 回路におけるデバイス認証の手順を示す．大まかな手順としては，文献 [5] の手法と同様の流れで認証が行われる．デバイス認証を行うタイミングで，購入者は製造者から外部チャレンジ $\boldsymbol{c}_{\mathbf{ext}i}$ を受け取り，PUF 回路はレスポンス $\boldsymbol{r}_i'$ を生成する．その後，製造者に生成した $\boldsymbol{r}_i'$ を返信し，得られた CRP($\boldsymbol{c}_{\mathbf{ext}i}, \boldsymbol{r}_i'$) と CRP データベースに存在する CRP($\boldsymbol{c}_{\mathbf{ext}i}, \boldsymbol{r}_i$) を比較することで認証が行われる．

従来の PUF 回路を用いたデバイス認証方法との違いは，レスポンスの生成方法にある．デバイス認証時において，従来手法では与えられた 1 つのチャレンジに対して 1 つのレスポンスを生成する．一方，LBIST-PUF 回路では，外部チャレンジ $\boldsymbol{c}_{\mathbf{ext}i}$ が製造者より与えられるが，レスポンス $\boldsymbol{r}_i'$ の生成は LFSR が生成する内部チャレンジ列 $\boldsymbol{c}_{\mathbf{ext}i}$ で行われる．そのため，$\boldsymbol{c}_{\mathbf{ext}i}$ は複雑なシーケンスを持つこととなり，チャレンジとレスポンスの間の線形性が失われる．したがって，従来の単純なチャレンジによるデバイス認証に比べて，機械学習攻撃耐性が向上する．なお，LBIST-PUF 回路においても，$l = 1$ とすることで従来のデバイス認証方法としても使用可能である．

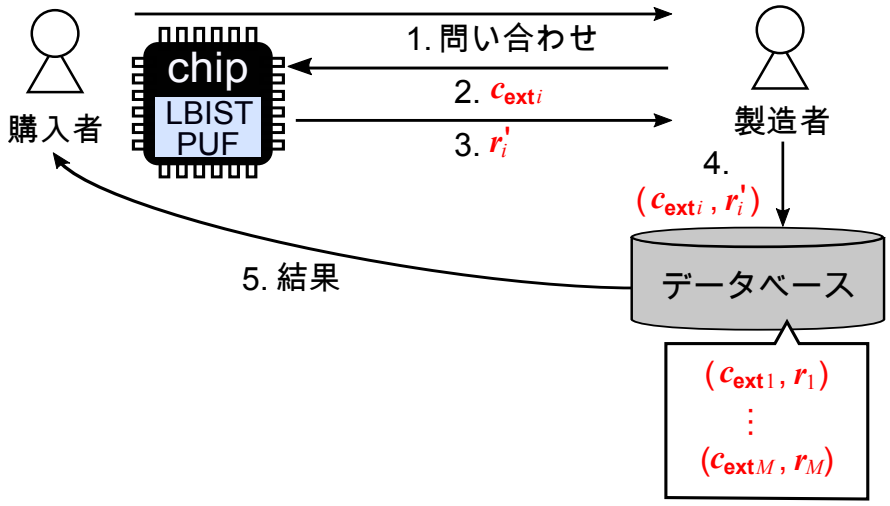

図 7 LBIST-PUF 回路を用いたデバイス認証

4. 実装

提案回路の実現性を検討するために，市販の FPGA を用いて LBIST-PUF 回路の実装を行った．FPGA は，Xilinx 社製の Artix-7 を用いた [22]．図 8，9 に実装した LBIST-PUF 回路のブロック図と FPGA 上でのレイアウト図をそれぞれ示す．

実装回路は，CUT，PUF 回路，LBIST 回路，およびテストコントローラ回路で構成される．CUT として，ISCAS'89 ベンチマーク回路の s38584 を選定した [23]. s38584 は，D フリップフロップ（DFF），および論理ゲートで構成される順序回路である．スキャンチェーン数は 16 本，1 本あたりのスキャンチェーンの DFF の接続数は 85 段で構成する．PUF 回路はとして，16 ビットのチャレンジ入力を有するアービター PUF の実装を行った．LBIST 回路の PRPG としては，16 ビットの LFSR を設計した．LFSR の出力は，CUT に接続するのとともに，アービター PUF のチャレンジ入力にも接続した．本実装では設計の簡易化のため，フェーズシフタは実装していない．また，本来であれば，CUT のテスト応答を圧縮する MISR が接続されるが，本実装では提案回路の評価の簡易化のために MISR の実装は行わず，スキャン出力を外部出力に接続している．また，PUF 回路のレスポンス出力も外部出力に接続させているため，直接観測を可能としている．テストコントローラ回路は，LFSR の動作を含むスキャンテストの動作の制御を行う．なお，スキャンチェーン化された CUT は，市販の Computer-aided design（CAD）ツール [24, 25] で設計し，Xilinx 社の CAD ツール（Vivado）で論理合成を行うことで，FPGA 上に実装した [26]．以下では，実装した回路の詳細について述べる．

4.1 アービター物理複製困難関数

本実装では，16 ビットのチャレンジ入力を有するアービター PUF の設計を行った．入力が 16 ビットであるため，実装したアービター PUF は 65536（$= 2^{16}$）の CRP が生成できる． 2.2 節で述べたように，アービター PUF ではスイッチチェーンを等負荷，等配線長となるように設計する必要があるため，自動で回路の配置配線を行う CAD ツールを使って，理想的な PUF 回路を設計する際には設計上の注意が必要となる．本実装では，Vivado ツールのハードマクロ機能を利用して

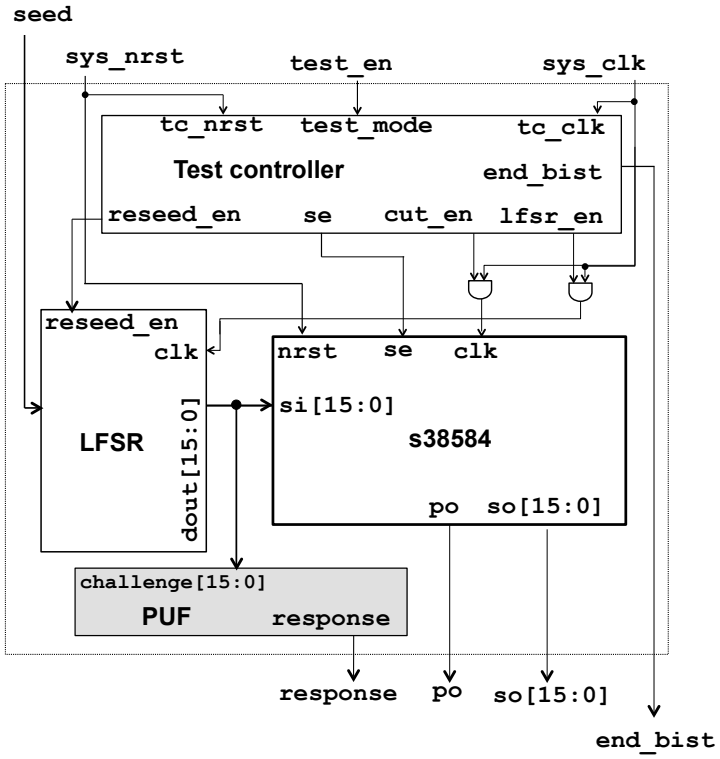

図 8 実装した LBIST-PUF 回路のブロック図

図 3 のアービター PUF のスキャンチェーン部分をハードマクロ化することで，等負荷，等配線長になるように設計した．

図 10 に実装したアービター PUF のレイアウトを示す．アービター PUF のスイッチとして，FPGA に搭載されるセレクタを利用した．PUF 回路に入力するトリガ信号は，トリガ FF から出力され，2 つのセレクタチェーンを水平になるように配置した [27]．FPGA には，ハードマクロとして DFF が搭載されるが，意図的にクロック入力を遅延させるための制御が行われているため [27, 28]，アービター PUF のアービタとしての使用には適していない．ここでは，アービターとして NAND ゲートを 2 つ用いた SR ラッチを実装した．上段のセレクタチェーンの出力を SR ラッチの入力 S へ，下段セレクタチェーンを出力 R へ，それぞれ接続した．

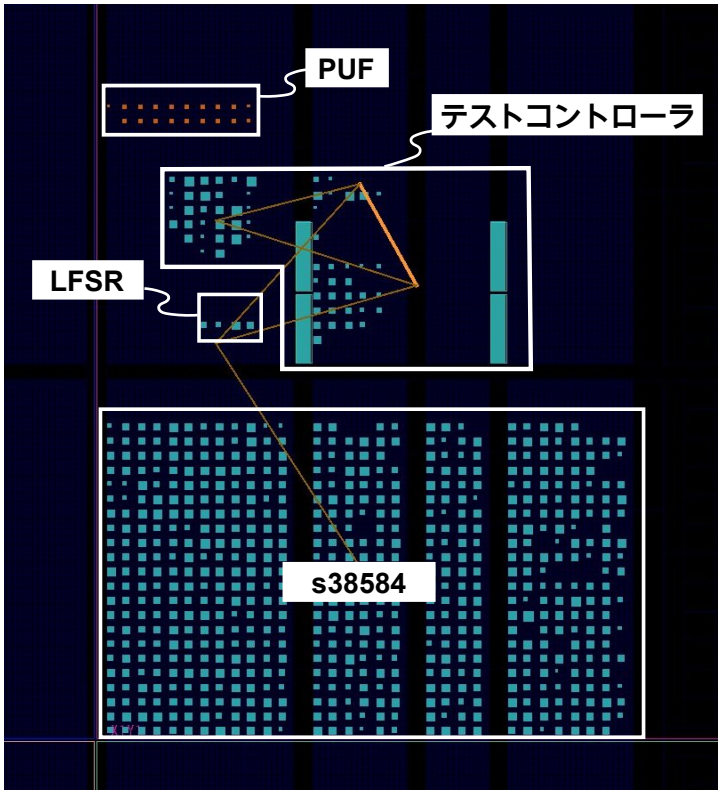

図 9 実装した LBIST-PUF 回路のレイアウト

4.2 論理自己組込みテスト回路

LFSR は，XOR ゲートとシフトレジスタで構成され，帰還多項式により回路構成が表現できる．以下に，用いた LFSR の帰還多項式 $G(x)$ を示す．

$$G(x) = x^{16} + x^{14} + x^{13} + x^{11} + 1. \tag{7}$$

本実装では，16 ビットのガロア LFSR を実装し，上記の帰還多項式の用いることで全ての出力が 0 以外の 65535（$= 2^{16} - 1$）のチャレンジの生成ができる．

4.3 テスト制御回路と全体の動作波形

テストコントローラ回路により，LFSR と CUT 内のスキャンチェーンを制御する．図 11 に CRP 取得時の動作波形を示す．信号 `sys_clock` および `sys_nrst`

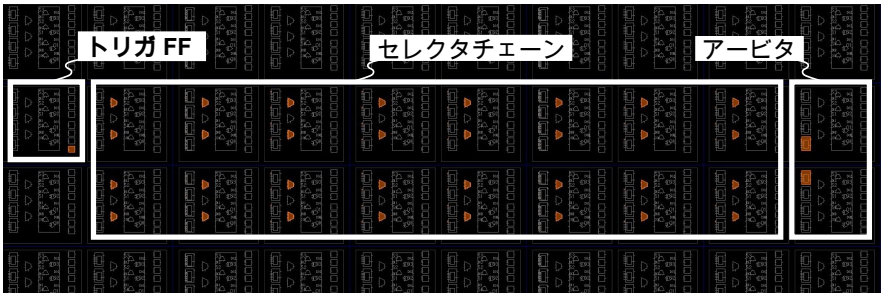

図 10 実装したアービター PUF のレイアウト

は，システムクロックおよびリセットを行う．test_en がイネーブルになった時，CUT のクロック clk が供給され，se も制御可能となる．テストコントローラ回路により生成される信号 reseed_en により，リシーディングを行うか LFSR の巡回動作を行うかを決定し，リシーディングを行う場合は，seed から得た値を LFSR 内に取り込む．また，LFSR へのクロック供給も lfsr_en により可能となる．se は内部のレジスタでスキャン段数をカウントして制御される．si[15:0] と so[15:0] は，それぞれスキャンイン信号とスキャンアウト信号である．LFSR の出力 dout[15:0] は，CUT のスキャンイン信号 si[15:0] と PUF 回路のチャレンジ入力信号 challenge[15:0] に接続される．したがって，スキャンインの値は全てチャレンジ信号となる．したがって，スキャンイン動作がはじまると同時に，PUF によりレスポンスも変化する．LFSR からの全ての信号を出力し終えた後，end_bist 信号がイネーブルとなり，LBIST によるテスト（CRP 取得）を終える．ただし，動作時の電力問題から，デバイス認証時には LFSR は動作させるが CUT への信号伝達は行わないよう設計した．ここでは，テストコントローラ回路で生成した cut_en 信号により CUT へのクロック供給を止めている．

本実装のテストコントローラ回路にはシリアル通信を行うために，Universal synchronous receiver/transmitter（UART）回路が含まれている．これにより，PUF の CRP の取得後に取得したレスポンスを PC へ送信を行う．

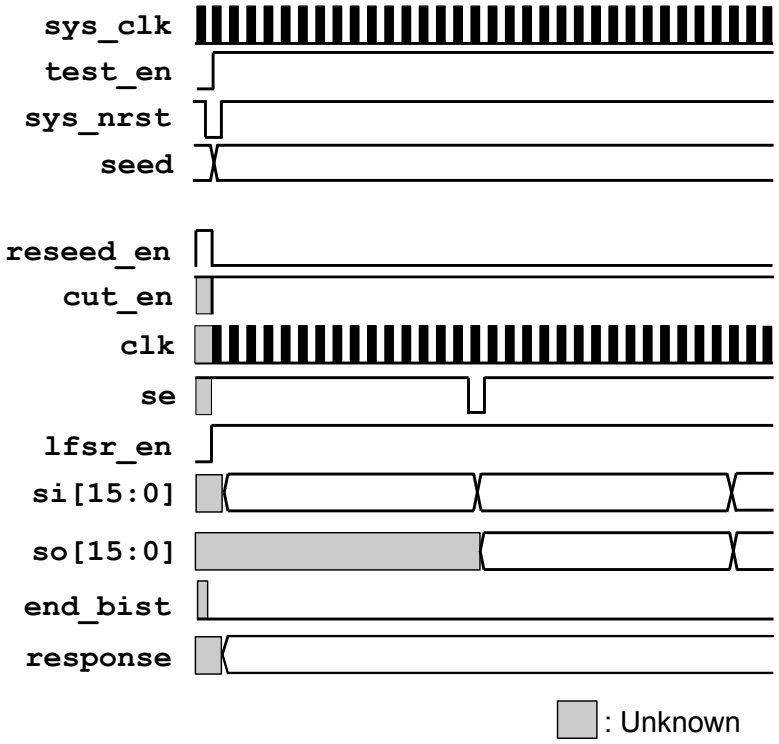

図 11 データベース構築時の提案回路の動作波形

表 1 回路面積

	LBIST-PUF		Conv.	
	LUT 数	FF 数	LUT 数	FF 数
s38584 (CUT)	2401	1354	2401	1354
テストコントローラ	108	148	96	143
LFSR	2	16	2	16
アービター PUF	2	1	2	1

5. 評価

本章では，4 章で実装した提案回路に対して，行った評価実験について述べる．以下に，面積評価，量産テスト評価，PUF 回路の性能評価，および機械学習攻撃の耐性評価について述べる．

5.1 面積評価

実装した LBIST-PUF 回路の回路面積の評価を行った．表 1 に LBIST-PUF 回路を実装した場合と，Conv. の欄に LBIST-PUF 回路は実装せず，PUF 回路の従来の使用方法と同様に PUF 回路および LBIST 回路を個別に実装した場合の各回路の回路面積をそれぞれ示す．FPGA に対して実装を行っているため，ここでは，実装に使用されたルックアップテーブル（Lockup table, LUT）数，および FF 数を回路面積としている．また，表の結果は Vivado ツールより得た．表の結果より，LBIST-PUF 回路の量産テスト時における CRP 生成に必要な追加の面積オーバーヘッドは，従来の量産テスト向けのテストコントローラ，LFSR，およびアービター PUF と比較して，ほぼないといえる．

5.2 量産テストおよび CRP 取得の評価

実装した LBIST-PUF 回路を用いて，提案回路の実現性の評価を行った．CUT のテストを行うと同時に，実装したアービター PUF のレスポンスが取得可能か確認

するために，LFSR で生成された擬似乱数テストパターンを用いて，CUT のスキャンテストおよび CRP 計測を行った．FPGA-1，FPAG-2，FPGA-3，および FPGA-4 の 4 台の FPGA に対して，LBIST-PUF 回路の実装を行った．図 12 に，CUT の故障検出率とテストに使用したチャレンジセットを，4 台の FPGA に実装したアービター PUF 回路に 10 回適用した場合に得られたレスポンスのランダム性の評価結果を示す．本実験では，ランダム性の評価を行うために，65535 チャレンジを 10 回適用した．使用した CUT のスキャンチェーン数は 85 段であるため，図の横軸は適用された 1 回分のテストパターン数（771 パターン）の 85 倍の値で表している．

ランダム性は，2.2.4 項で述べた PUF の性能の評価指標の 1 つである．検出する故障として，2.1.1 項で述べた縮退故障モデルを対象としている．縮退故障の故障検出率の算出には，市販のテストツールを用いた [29]．また，ここでは，評価を簡単化するためにリシーディングは行わずに，特定のシードを用いて故障検出率を算出している．

図 12 の結果より，LBIST-PUF は PUF 回路の性能評価中に，量産テストを行うことができる．また，この結果は，65535 チャレンジを 1 回のみ適用した場合を想定すると量産テスト時の CRP 取得により，CRP データベース構築が可能であると言える．実装した LBIST-PUF 回路では，最終的に縮退故障に対して，90%の故障検出率を達成している．一方，各 FPGA のランダム性は，0 から始まり早期の段階で，チャレンジ数によらず特定の値に収束している．また，FPGA-1，FPGA-2，および FPGA-4 のランダム性の値は，0.8 以上に収束しているが，FPGA-3 の値は 0.3 付近で収束している．この原因としては，文献 [30] で報告されている，固有の製造ばらつきが FPGA-3 に発生したためである．

5.3 アービター物理複製困難関数回路の性能評価

LBIST-PUF 回路によって取得できた CRP を用いて実装したアービター PUF の性能評価を行った．表 2 に，4 台の FPGA に実装したアービター PUF の評価結果の平均値を示す．評価には，2.2.4 項で述べた文献 [8] のランダム性，安定性，正確性，拡散性，およびユニーク性の 5 つの指標を用いた．5 つの指標は 0 から 1

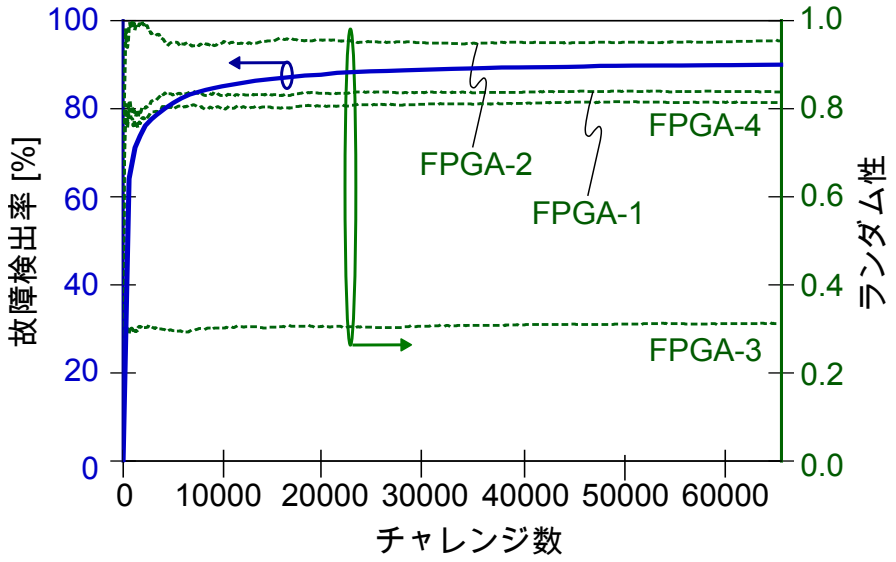

図 12 故障シミュレーション結果および 4 つの PUF のランダム性

の値を取り，1 に近いほど高性能であることを表す．本実験では，PUF の ID 数 K を 65535，ID の長さ W を 1，同じ ID の生成回数 T を 10，および使用する PUF の台数 V を 4 として評価を行った．そのため，上述の評価実験と同様に 1 つのチャレンジを 10 回，PUF 回路に対して与えている．評価結果より，ランダム性，安定性，正確性，および拡散性は，十分に高い性能を示している．しかし，ユニーク性は低いため，PUF の実運用を行う場合には改善を行う必要がある．図 12 に示すように，全ての指標の評価時に IC チップの量産テストが行える．なお，本実験では ID の長さ W を 1 として評価を行っているが，評価指標の定義より，ID の長さ W が 2 以上の場合であっても同様の結果が得られる．

5.4 機械学習攻撃耐性の評価

実装した LBIST-PUF 回路に対して，機械学習攻撃耐性の評価を行った．図 13 に機械学習に使用する学習データ量を変化させた場合のレスポンスの予測不可能性の変化を示す．予測不可能性は，機械学習アルゴリズムが予測した全レスポンスと，その中で予測が出来なかったレスポンスとの比率で定義し，確率が高いほ

表 2 設計したアービター PUF の性能評価結果

指標	説明	スコア
ランダム性 H	単一の PUF のレスポンスの均一度	0.730
安定性 S	単一の PUF のレスポンスの安定度	0.896
正確性 C	単一の PUF のレスポンスの正確度	0.990
拡散性 D	単一の PUF のレスポンス間のばらつき度	0.991
ユニーク性 U	複数の PUF 間のレスポンスのばらつき度	0.490

どレスポンス予測が難しいことを表す．学習データは，取得した 65535 個の CRP の中から選択し，残りの学習データを予測に用いた．械学学習アルゴリズムとして，SVM，およびランダムフォレスト (Random forest, RF) [31] の 2 つのアルゴリズムを用い，実装は Python の Scikit-learn ライブラリ [32] を用いて行った．高精度な予測結果を得るために 2 つの学習手法に必要なハイパーパラメータは，グリッドサーチ法にて決定した [33]．学習データは，外部チャレンジ，およびそれに対応する内部チャレンジによって生成された l ビットのレスポンスのデータセットからランダムに選択し，学習させた．残りの外部チャレンジとレスポンスのデータセットの予測を行った．図 13 の実線の結果は，SVM の予測不可能性を表し，破線の結果は RF の予測不可能性を表す．1 ビットの場合の結果は，従来の PUF 回路の使用方法でのレスポンスの予測結果であり，その他の結果は，LBIST-PUF 回路が出力するレスポンス長 l を 2，4，および 8 に変化させた場合の予測結果である．

どの結果においても，学習データ数が増加するほど予測不可能性は低くなっている．これは，攻撃者によって傍受される CRP 数が増えるほど，機械学習を用いた PUF 回路のモデル化の精度が上がるためである．また，RF の予測精度は，8 ビットの場合を除いて SVM の予測精度より高い．l が大きくなるに連れて予測精度が低なっており，特に 8 ビットの場合では，従来の PUF 回路の使用方法である 1 ビットの場合と比較してレスポンス予測が難しいため，安全性が向上している．以上より，LBIST-PUF 回路を用いて l の大きさを増やすことにより， 予測精度の改善が確認できる．具体的には，学習データが 10%（6553 チャレンジ）時

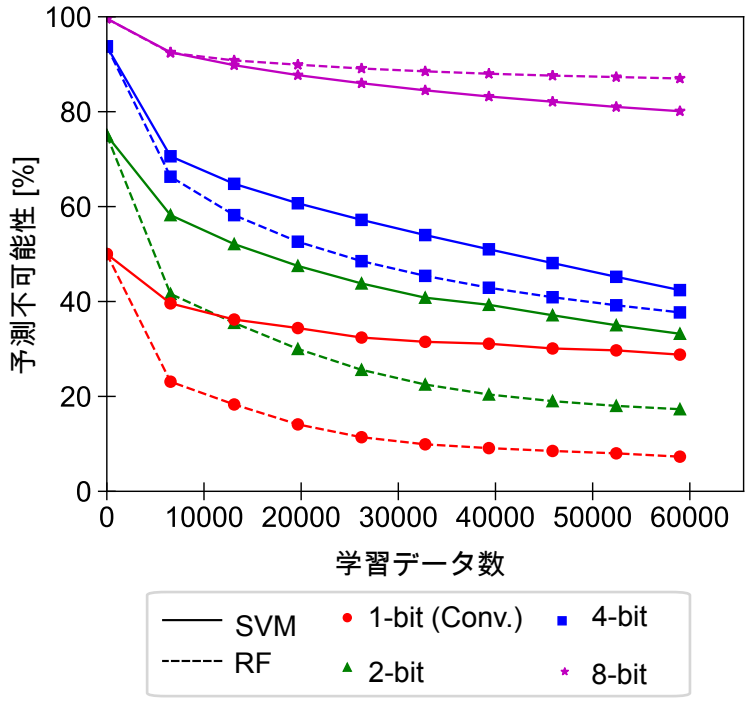

図 13 機械学習の学習データを変化させた時のレスポンス予測精度

における従来手法の RF の予測不可性は，23.1%であるのに対し，$l = 2, 4, 8$ の場合では，それぞれ 41.6%，66.3%，および 92.4%に改善されている．したがって，LBIST-PUF 回路は従来手法と比較して，少なくとも 2 倍以上の予測不可能性の改善を達成している．以上より，LBIST-PUF は，LBIST 回路によって PUF 回路のチャレンジとレスポンスの関係性が複雑化するため，機械学習攻撃耐性を向上できる．

6. まとめ

本論文では，高セキュアなPUF回路のCRPを利用したデバイス認証に必要となるデータベース構築を効率的に行うことを目的として，量産テストで使用されているLBIST回路を用いるLBIST-PUFを提案した．提案手法では，LBIST回路で生成されるテストパターンをPUF回路のチャレンジとしても用いるため，量産テストを行いつつ，PUF回路のCRPを取得することができる．したがって，CRPデータベースの構築に，回路および測定のオーバーヘッドが生じない．また，デバイス認証においてもLBIST回路を介してレスポンスを生成するため，CRP生成の手続きが複雑化し，PUF回路のレスポンスに対する機械学習攻撃耐性が向上する．提案手法の市販FPGAへの実装を通して，追加の回路面積が小さく，CUTのテスト時において同時にアービターPUFのCRP取得が行えることを実験的に確認した．さらに，同じチャレンジを複数回適用することで，アービターPUFの性能を評価中にCUTをテストできることも示した．また，機械学習攻撃を想定した実験において，LBIST-PUF回路の予測不可能性が従来のPUF回路の使用方法と比較して，少なくとも2倍以上高くなることを実証した．

今後の課題として，フェーズシフタを搭載した場合の機械学習アルゴリズムを用いた評価，リシーディング手法を適用してCRPデータベースを構築した場合のLBIST-PUFの性能評価が挙げられる．フェーズシフタを用いることでCRP生成の手続き複雑性がより増加し，さらなる機械学習攻撃耐性の向上が期待できる．

謝辞

本研究を進めるにあたり，多くの方々にご指導ご協力を賜ったことに心より感謝申し上げます．本研究を進めるにあたり，主指導教員の井上美智子教授には，様々な場面で的確なご指導ご助言をいただきました．また，研究面だけでなく，学生生活においても数多くの貴重な経験やご助言をいただき，心よりお礼申し上げます．私が選択した知能社会創生科学プログラムに際して，ご多忙にも関わらず論文審査員を引き受けていただき，他分野の視点からの研究に関するご意見，および本論文をご精読いただきました副指導教員の浦岡行治教授に心より深く感謝致します．本研究において，ご指導および貴重なご助言をいただいきました副指導教員の大下福仁准教授に厚く御礼申し上げます．本研究を通じて，熱心にご指導およびサポートをしていただいた，副指導教員の新谷道広助教に深く感謝致します．また，研究以外の面においても，大いに役に立つ貴重なご助言を頂いたことを重ねてお礼申し上げます．学生生活を様々な場面において，大変お世話になりましたディペンダブルシステム学研究室の学生並びにスタッフの皆様に感謝致します．

最後に，両親並びに 2 年間の学生生活を支えてくださった全ての方々に改めて感謝の意を表します．

参考文献

[1] U. Guin, D. DiMase, and M. Tehranipoor, "Counterfeit integrated circuits: Detection, avoidance, and the challenges ahead," *Journal of Electoronic Testing: Theory and Applications*, vol. 30, no. 1, pp. 9–23, 2014.

[2] U. Guin, K. Huang, D. DiMase, C. John M., Jr., M. Tehranipoor, and Y. Makris, "Counterfeit integrated circuits: A rising threat in the global semiconductor supply chain," *Proceedings of the IEEE*, vol. 102, no. 8, pp. 1126–1141, 2014.

[3] A. Foisal, M. Shintani, and M. Inoue, "Feature engineering for recycled FPGA detection based on WID variation modeling," in *Proceedings of IEEE European Test Symposium*, 2019, pp. 1–2.

[4] ——, "Low cost recycled FPGA detection using virtual probe technique," in *Proceedings of IEEE International Test Conference in Asia*, 2019, pp. 103–108.

[5] G. E. Suh and S. Devadas, "Physical unclonable functions for device authentication and secret key generation," in *Proceedings of IEEE/ACM Design Automation Conference*, 2007, pp. 9–14.

[6] C. Herder, M.-D. Yu, F. Koushanfar, and S. Devadas, "Physical unclonable functions and applications: A tutorial," *Proceedings of the IEEE*, vol. 102, no. 8, pp. 1126–1141, 2014.

[7] Z. Qin, M. Shintani, K. Kuribara, Y. Ogasahara, and T. Sato, "OCM-PUF: An organic current mirror PUF with enhanced resilience to device degradation," in *Proceedings of IEEE International Conference on Flexible and Printable Sensors and Systems*, 2019.

[8] Y. Hori, T. Yoshida, T. Katashita, and A. Satoh, "Quantitative and statistical performance evaluation of arbiter physical unclonable functions on FPGAs," in *Proceedings of International Conference on Reconfigurable Computing and FPGAs*, 2010, pp. 298–303.

[9] U. Rührmair, F. Sehnke, J. Sölter, G. Dror, S. Devadas, and J. Schmidhuber, "Modeling attacks on physical unclonable functions," in *Proceedings of ACM Conference on Computer and Communications Security*, 2010, pp. 237–249.

[10] U. Rührmair, J. Sölter, F. Sehnke, X. Xu, A. Mahmoud, V. Stoyanova, G. Dror, J. Schmidhuber, W. Burleson, and S. Devadas, "PUF modeling attacks on simulated and silicon data," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 11, pp. 1876–1891, 2013.

[11] R. Yashiro, T. Machida, M. Iwamoto, and K. Sakiyama, "Deep-learning-based security evaluation on authentication systems using arbiter PUF and its variants," in *Proceedings of International Workshop on Security*, 2016, pp. 267–285.

[12] S. U. Hussain, S. Yellapantula, M. Majzoobi, and F. Koushanfar, "BIST-PUF: Online, hardware-based evaluation of physically unclonable circuit identifiers," in *Proceedings of IEEE/ACM International Conference on Computer-Aided Design*, 2014, pp. 162–169.

[13] M. Bushnell and V. Agrawal, *Essentials of Electronic Testing for Digital, Memory and Mixed-Signal VLSI Circuits*. Springer, 2002.

[14] J. Rajski and J. Tyszer, "Design of phase shifters for BIST applications," in *Proceedings of IEEE VLSI Test Symposium*, 1998.

[15] C. V. Krishna and N. Touba, "Reducing test data volume using LFSR reseeding with seed compression," in *Proceedings of IEEE International Test Conference*, 2002, pp. 331–330.

[16] A. Al-Yamani, S. Mitra, and E. J. McCluskey, "BIST reseeding with very few seeds," in *Proceedings of IEEE VLSI Test Symposium*, 2003, pp. 69–74.

[17] J. Guajardo, S. S. Kumar, G.-J. Schrijen, and P. Tuyls, "FPGA intrinsic PUFs and their use for IP protection," in *Proceedings of Conference on Cryptographic Hardware and Embedded Systems*, 2007, pp. 63–80.

[18] B. Gassend, D. Clarke, M. van Dijk, and S. Devadas, "Delay-based circuit authentication and applications," in *Proceedings of ACM symposium on Applied computing*, 2003, pp. 294–301.

[19] K. Fruhashi, M. Shiozaki, A. Fukushima, T. Murayama, and T. Fujino, "The arbiter-PUF with high uniqueness utilizing novel arbiter circuit with delay-time measurement," in *Proceedings of IEEE International Symposium on Circuits and Systems*, 2011, pp. 2325–2328.

[20] M. Majzoobi, M. Rostam, F. Koushanf, D. S. Wall, and S. Devadas, "Slender PUF protocol: A lightweight, robust, and secure authentication by substring matching," in *Proceedings of IEEE Symposium on Security and Privacy Workshops*, 2012, pp. 33–44.

[21] B. Schölkopf, R. Williamson, A. Smola, J. Shawe-Taylor, and J. Platt, "Support vector method for novelty detection," in *Proceedings of International Conference on Neural Information Processing Systems*, 1999, pp. 582–588.

[22] *7 Series FPGAs Data Sheet: Overview*, Xilinx, Inc., 2018, [Online: https://www.xilinx.com/support/documentation/data_sheets/ds180_7Series_Overview.pdf].

[23] F. Brglez, D. Bryan, and K. Koiminski, "Combinational profiles of sequential benchmark circuits," in *Proceedings of IEEE International Symposium on Circuits and Systems*, 1998, pp. 1930–1934.

[24] *Design Compiler User Guide Version I-2013.06*, Synopsys, Inc., 2013.

[25] *DFT Compiler User Guide Version I-2013.06*, Synopsys, Inc., 2013.

[26] *Vivado Design Suite*, Xilinx, Inc., 2018, [Online: https://www.xilinx.com/products/design-tools/vivado.html].

[27] M. Soybali, B. Ors, and G. Saldamli, "Implementation of a PUF circuit on a FPGA," in *Proceedings of International Conference on New Technologies, Mobility and Security*, 2011, pp. 1–5.

[28] D. Lim, J. W. Lee, G. E. Suh, M. van Dijk, and S. Devadas, "Extracting secret keys from integrated circuits," in *IEEE Transactions on Very Large Scale Integration(VLSI) Systems*, 2005, pp. 1200–1205.

[29] *TetraMAX ATPG User Guide Version N-2017.09-SP4*, Synopsys, Inc., 2017.

[30] T. Tuan, A. Lesea, C. Kingsley, and S. Trimberger, "Analysis of within-die process variation in 65nm FPGAs," in *Proceedings of IEEE International Symposium on Quality Electronic Design*, 2011.

[31] L. Breiman, "Random forests," *Machine Learning*, vol. 1, no. 45, pp. 5–32, 2001.

[32] F. Pedregosa, G. Varoquaux, A. Gramfort, V. Michel, B. Thirion, O. Grisel, M. Blondel, P. Prettenhofer, R. Weiss, V. Dubourg, J. Vanderplas, A. Passos, D. Cournapeau, M. Brucher, M. Perrot, and E. Duchesnay, "Scikit-learn: Machine learning in Python," *Journal of Machine Learning Research*, vol. 12, pp. 2825–2830, 2011.

[33] Á. B. Jiménez, J. L. Lázaro, and J. R. Dorronsoro, *Finding Optimal Model Parameters by Discrete Grid Search*. Springer, 2007.

発表リスト

[1] 三野智貴，新谷道広，井上美智子，”量産検査時における組込み自己テスト回路を利用した効率的なPUF回路のチャレンジレスポンス対の生成と評価”，電子情報通信学会技術報告書（ディペンダブルコンピューティング研究会），pp25–30，2019.2.