物理特性を用いたLSIの真贋判定法

堀　洋平[†1]　片下敏宏[†1]
姜　玄浩[†1]　佐藤証[†1]

暗号回路をベースとした発振器の物理情報を利用し，LSI の真贋判定を行う手法を開発した．本手法は，疑似 LFSR 発振回路の出力を AES 回路で暗号化する際のサイドチャネル情報とデジタル出力値を用いて個々のデバイスを識別する．疑似 LFSR 発振回路によって抽出されたデバイスのばらつきを AES 回路で増幅することで，通常は個体差の出づらいサイドチャネル情報からデバイスを識別することを可能とする．デジタル出力値のみを用いる従来の Physical Unclonable Function (PUF) では，機械学習によって入出力関係が導出可能であることが報告されているが，本手法ではアナログデータであるサイドチャネル情報を用いるため，安全性の高い真贋判定器を実現できる．FPGA 上に提案回路を実装し，サイドチャネル情報の一つである消費電力を用いて本手法を実施し，特定のデバイスが正しく識別可能であることを確認した．

Counterfeit LSI Detection Based on Physical Property

Yohei HORI,[†1] Toshihiro KATASHITA,[†1]
Hyunho KANG[†1] and Akashi SATOH[†1]

This paper presents the counterfeit LSI detection method utilizing physical properties of cryptographic modules. Our counterfeit detector is developed based on a pseudo-LFSR oscillator and AES encryption circuit, and the side-channel information of these modules are used for distinguishing the genuine LSI from the counterfeits. The pseudo-LFSR oscillator extracts the device variation and its device-specific outputs are mixed up by the AES circuit so that more side-channel information is generated. Since our method utilizes analog side-channel data, it can realize more accurate counterfeit detection than usual PUFs using only digital outputs. We implemented the proposed counterfeit detector on an FPGA to demonstrate the feasibility of our method. The experimental results show that the proposed detector can distinguish a specific device from others.

1. はじめに

Physical Unclonable Function (PUF)[1] は，複製困難な物理的特徴を利用してデバイス固有の値を出力する．LSI 上の PUF (Silicon PUF) は，デバイスのばらつきを利用して LSI チップ固有の値を出力する回路であり，2 信号の遅延の差を利用する Arbiter PUF[2] や，発振回路の配置による発振周波数の違いを利用する Ring Oscillator PUF[3]，電源投入後のメモリの初期値を利用する SRAM PUF[4]，クロス接続されたフリップフロップを利用した Buttefly PUF[5] 等がある．Arbiter PUF や RingOscillator PUF は，数十から数百ビットのチャレンジ入力によって信号の経路や発振器の位置を選択し，最終的に 1 ビット〜数ビットのレスポンス値を出力する回路である．しかし，本来は複製困難なデバイスのばらつきを高々数ビットのデジタル値に変換してしまうため，異なるデバイス間の出力値のユニーク性が低く，また機械学習によって Challenge-Response Pairs (CRPs) を予測しやすいという致命的な問題[6] があることが知られている．そこで本研究では，デジタル出力値だけでなく，回路が生じる物理情報の一つである電力波形を利用することで LSI の真贋判定を行う．アナログの電力波形を模倣できる回路の作成は極めて困難と思われるため，より安全なデバイス認証の実現が期待できる．

広範なばらつきを効率よく抽出する真贋判定器を構築するためには，比較的規模が大きく複雑な回路を利用するのが良いと考えられる．本研究では疑似 LFSR 発振回路 (第 2 章参照) と AES 暗号化回路を組み合わせて真贋判定器を構築した．疑似 LFSR 回路発振器は，通常はシフトレジスタによって構成する LFSR 回路において，レジスタの代わりにインバータを使用したものである．このような構成にすることで，発振部は遅延の大きな組み合わせ回路となり，デバイスのばらつきによる信号伝播速度の差を効率よく抽出することができる．疑似 LFSR 発振器によって抽出されたばらつきは，AES 暗号化回路によって増幅される．AES 回路は平文データを撹拌する複雑な機構を有するため，電力情報が大きくなると期待されるだけでなく，鍵を変えることで様々な電力パターンを発生させることが可能である．

提案方式の有効性を確認するため，複数の SASEBO-GII 上の Xilinx FPGA に真贋判定器を実装し，それぞれのデバイスを識別可能であるか実験を行った．実験対象としたデバイスは，Virtex-5 LX30 のスピードグレード 1 と 2 がそれぞれ 2 枚ずつ，LX50 のスピード

†1 (独) 産業技術総合研究所
National Institute of Advanced Industrial Science and Technology (AIST)

グレード 1 と 2 がそれぞれ 2 枚ずつの合計 8 個である．

本稿において，提案真贋判定器を用いたデバイス識別の手法，およびその実証実験の方法と結果を述べる．本稿は以下のように構成されている．第 2 章では，提案する真贋判定器の構成とそれを用いたデバイス識別手法について説明する．第 3 章では，提案する真贋判定器の実装環境と実装結果について述べる．第 4 省では，提案手法の有効性の実証実験の方法と結果について述べ，最後に第 5 章で本研究についてまとめる．

2. 疑似 LFSR-AES 真贋判定器

本研究では，疑似 LFSR 発振器と AES 暗号化回路を組み合わせて真贋判定器を構成する．AES のブロックサイズは 128 ビット，鍵長は 128 ビットである．LFSR のステージ数は，AES に合わせて 128 とする．以下では，真贋判定器の構成について説明したのち，デバイスの真贋判定の方法について述べる．

2.1 真贋判定器の構成

通常の 128 ビット LFSR 回路の構成を図 1 に示す．128 ビット LFSR において最長 LFSR となる帰還多項式として

$$x^{128} + x^{126} + x^{101} + x^{99} + 1 \tag{1}$$

を用いた[7]．図中の LFSR_core は，通常の LFSR ではレジスタで実装される．本研究では，LFSR_core は図 2 に示すようにインバータとマルチプレクサを用いて実装した．インバータを用いるのは，ゲート遅延が生じデバイスのばらつきを効果的に利用できるためである．D_{init} は LFSR_core の初期出力値であり，D_{in} は前ステージの D_{out} である．初期状態では固定値の D_{init} が出力されているが，これを SEL 信号によって D_{in} に切替えることで LFSR_core チェイン全体が発振する．このような構成により図 1 は遅延の大きな組み合わせ回路となり，デバイスのばらつきが信号遅延に大きく影響するようになる．本稿では，このように構成された LFSR ベースの発振回路を疑似 LFSR 発振器 (あるいは単に LFSR 発振器) と呼ぶ．

本研究が提案する真贋判定器の構成を図 3 に示す．LFSR 発振器の出力は AES 暗号化回路に入力される．LFSR 発振器の出力にはデバイスのばらつきが反映されるが，デバイス間の出力値の差はそれほど大きくない可能性がある．一方，AES 回路では入力の差がわずかであっても出力値は大きく異なるため，LFSR 発振器の出力を AES 回路に入力することでサイドチャネル情報の差は大きくなると期待される．

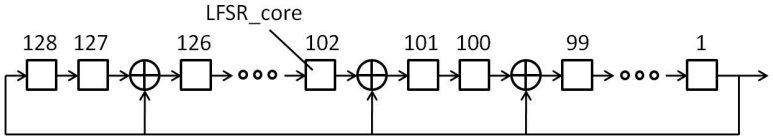

図 1 128 ビット LFSR の構成.
Fig. 1 The structure of the 128-bit LFSR circuit.

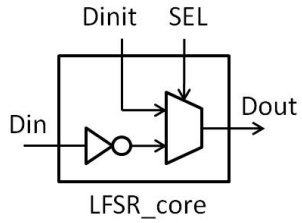

図 2 LFSR_core の構成.
Fig. 2 The structure of LFSR_core.

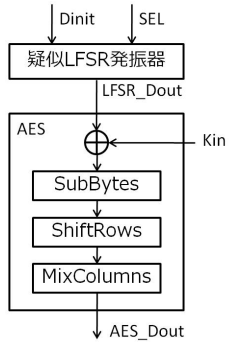

図 3 提案する真贋判定器の構成.
Fig. 3 The structure of the proposed counterfeit detector.

2.2 デバイス識別手法

本研究では，サイドチャネル情報としてデバイスのコア電圧波形を利用する．電圧波形の測定にはデジタルオシロスコープを用いる．各デバイスごとにコア電圧波形の**テンプレート**を作成し，同時に AES 回路のデジタル出力の期待値である**デバイス ID** も取得する．判定対象デバイスでは，テンプレート作成時と同一の条件下で**クエリ波形**と**クエリ ID** を作成する．このようにして，デジタル出力である ID の比較だけでなく，アナログデータであるテンプレートとクエリ波形の類似度に基づいてデバイスを識別する．

テンプレートはデバイスベンダやシステム提供者 (プロバイダ) が作成するもので，十分に大きな測定回数の下で作成される．クエリ波形はユーザ (検証者) が短時間に作成する必要があり，数回〜数十回程度の測定から作成される．テンプレートはプロバイダのサーバ等に置かれ，検証者からのクエリに応じてマッチングを行う．提案回路を用いた真贋判定の手

順を以下に示す.

(1) 各デバイスのテンプレートの作成.

(a) LFSR 発振回路の初期値 D_{init} および AES 暗号化回路の秘密鍵 K_{in} を設定する．また，オシロスコープのパラメータ (時間・電圧解像度，オフセット，サンプリング周波数等) を設定する.

(b) L クロックサイクルだけ LFSR 発振回路と AES 回路をアクティブにし，その際の電力波形 W とデジタル出力 C を取得する．同一の D_{init}，K_{in}，L および測定条件の下，各デバイスでこれを N ずつ回繰り返す.

(c) 取得された電圧波形の N 回の平均を，各デバイスのテンプレートとする．また，デジタル出力値の期待値であるデバイス ID を決定する．デバイス ID は，あるビットの”1” の出現率が 50%より大きければそのビットは”1”，それ以外は”0” とすることで決定される.

(2) 判定対象デバイスのクエリ作成と，テンプレートとのマッチング

(a) 判定対象デバイスにおいてテンプレート作成時と同一の条件で，L クロックサイクルだけ LFSR 発振回路と AES 回路をアクティブにし，その際の電力波形 $\hat{W}$ とデジタル出力 $\hat{C}$ を取得する．これを M 回繰り返す.

(b) 取得された電圧波形の M 回の平均を，そのデバイスのクエリ波形とする．また，M 個のデジタル出力値をクエリ ID とする.

(c) 各デバイスのテンプレート波形と対象デバイスのクエリ波形の相関係数を算出する．最大の相関係数の得られるテンプレートを与えるデバイスが，対象デバイスの候補となる.

(d) 各デバイス ID と M 個のクエリ ID のハミング距離を算出し，デバイスごとのハミング距離の分布 P_H を得る．最も小さい P_H の平均値を与えるデバイスが，対象デバイスの候補となる.

(e) (2c)(2d) の候補が一致していれば，対象デバイスは候補デバイスであると判定される.

3. 実　　装

提案する真贋判定器を，SASEBO-GII (Side-channel Attack Standard Evaluation Board)[8] 上の Xilinx Virtex-5 FPGA[9] に実装した．SASEBO-GII は電源ラインに直列にシャント抵抗が実装されており，FPGA コアに流れる電流の時間変化を観測することができる．今回実験対象としたデバイスは 8 個で，Virtex-5 LX30 と LX50 の 2 種類に対してスピードグレード 1 と 2 をそれぞれ 2 個ずつ用意した．パッケージはすべて FF324 である．8 個の実験対象デバイスを表 1 に示す.

表 1 実験対象デバイス
Table 1 The target devices.

No.	Device family	Sub-family	Speed grade
1	Virtex-5	LX30	1
2	Virtex-5	LX30	1
3	Virtex-5	LX30	2
4	Virtex-5	LX30	2
5	Virtex-5	LX50	1
6	Virtex-5	LX50	1
7	Virtex-5	LX50	2
8	Virtex-5	LX50	2

表 2 真贋判定器のハードウェアリソース使用量
Table 2 Hardware resource utilization of the counterfeit detector.

リソース	使用量	使用率 (%)
Slice	789	16
LUT	185	9
FF	1124	5
Block RAM	1	3
I/O Block	26	11

真贋判定回路の AES 部分は，東北大学 Cryptographic Hardware Project[10] の AES-Comp を利用した．回路の開発環境は Xilinx ISE 13.1i である．真贋判定器は FPGA 上の SliceX0Y2 と SliceX7Y65 を対角線とする長方形領域に配置された．真贋判定器および制御回路等をすべて含むシステムのハードウェアリソース使用量を表 2 に示す.

4. 実　　験

FPGA に実装された真贋判定器を用いて，提案手法の有効性の実証実験を行う．本章では実験環境・実験方法を説明した後，実験結果を示す.

4.1 実験方法

今回の実験では，真贋判定器の動作直後の電圧波形をサイドチャネル情報として利用する．動作直後の電圧波形は，真贋判定器のアクティブ時間 L を 2 クロックサイクルとし，アクティブ時間が終了する時刻付近の 50 ns の範囲の波形である (図 4)．コア電圧の変化は，

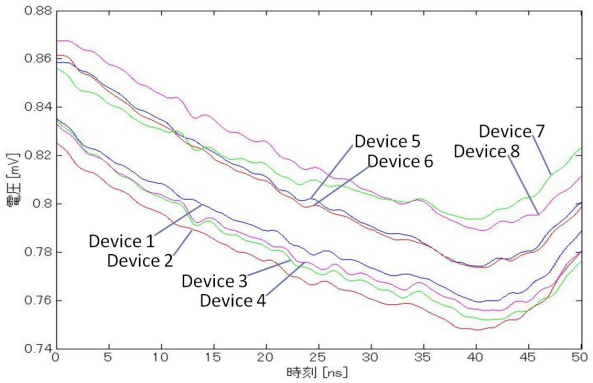

図 4 真贋判定器動作時の 2 サイクル目の拡大電圧波形
Fig. 4 The wave traces of the counterfeit detector near the 2nd clock cycles.

表 3 オシロスコープのパラメータ
Table 3 The parameters of the oscilloscope.

パラメータ	設定値
時間解像度	5 ns
時間オフセット	110 ns
電圧解像度	5 mV
電圧オフセット	785〜835 mV (デバイスによる)

シャント抵抗の電源側の電位を Agilent DSO8014A で測定することで取得する．真贋判定回路がアクティブになる際にトリガが出力され，測定が開始される．オシロスコープのパラメータは表 3 のように設定した．

8 個のデバイス上の真贋判定器のコア電圧変化を 1000 回ずつ測定し ($N = 1000$)，テンプレート波形を作成する．同時に，デジタル出力値からデバイス ID を決定する．LFSR 発振器の初期値および AES 回路の秘密鍵は以下の通りである．

$$D_{init} = 0x001122...FF$$
$$K_{in} = 0x000102...0F$$

次に，テンプレート作成時と同一の条件で 8 個のデバイスそれぞれで 10 回ずつコア電圧波形を測定し，クエリ波形およびクエリ ID を生成する．テンプレート波形とクエリ波形の

表 4 実験で得られたデバイス ID
Table 4 The device IDs obtained in the experiments

Device No.	Device ID obtained
1	0x21DAD5AABEF8A06A1B6AEB9C3BD24981
2	0x6991EC70C872423A3D76197FBBCF3C3D
3	0x9B8278ACEE4A1AF9C5307F8058DC9BB1
4	0x40517035CBDB72A16E2F689DE89862DC
5	0xC1024272275202A0D967080760E78459
6	0x03102C0231BD4BB07B238A9E9E6831C2
7	0xEB020AC0EBF01439AC918D49E31CD1E1
8	0x441A0703A94049BB3C0DB4921D5161E3

表 5 デバイス ID とクエリ ID の平均ハミング距離
Table 5 The average Hamming distance among the device IDs and query IDs.

Device No. \Query ID	1	2	3	4	5	6	7	8
1	**44.9**	65.5	67.5	64.7	63.3	67.3	67.1	64.3
2	63.5	**38.1**	64.3	63.3	60.7	63.5	62.3	66.3
3	63.6	67.4	**34.0**	65.2	66.6	72.8	61.4	69.8
4	64.9	65.5	66.5	**42.1**	64.3	61.7	70.7	63.7
5	64.7	64.3	66.3	62.3	**38.1**	69.5	62.9	66.3
6	67.0	65.2	65.2	64.4	66.0	**44.0**	65.4	64.0
7	65.7	64.3	61.3	67.7	67.9	71.3	**43.1**	64.3
8	64.8	65.8	64.6	70.8	70.2	64.2	58.2	**44.8**

相関係数を算出して類似度を判定する．また，デバイス ID とクエリ ID の平均ハミング距離を算出し，デバイスを判別する．

4.2 実験結果

8 個のデバイスのデジタル出力値から得られた ID を表 4 に示す．また，これらデバイス ID とクエリ ID との平均ハミング距離を表 5 に示す．表 5 中の太字は，各行における最小値を示す．8 個のデバイスすべてにおいて，最小値を与えるクエリ ID の番号とデバイス番号は等しく，正しいデバイスが判定されていることがわかる．

表 6 は，各デバイスのサイドチャネル情報のテンプレート波形とクエリ波形の相関係数を示している．表中の太字は，各行の最大値を示す．表より，8 個のデバイスすべてにおいて，最大値を与えるクエリ波形の番号とデバイス番号は等しく，正しいデバイスが判定されていることがわかる．

以上より，真贋判定器のデジタル出力であるデバイス ID を用いた場合と，アナログ情報であるサイドチャネル情報のテンプレートを用いた場合のどちらでもデバイスを正しく判定

表 6 テンプレートと参照波形の相関係数.
Table 6 The similarity of the device temprates.

Template\Query	1	2	3	4	5	6	7	8
1	**1.0000**	0.9981	0.9968	0.9975	0.9961	0.9968	0.9936	0.9872
2	0.9986	**0.9999**	0.9942	0.9955	0.9933	0.9940	0.9890	0.9930
3	0.9972	0.9937	**0.9999**	0.9997	0.9954	0.9976	0.9949	0.9827
4	0.9976	0.9947	0.9996	**1.0000**	0.9950	0.9969	0.9939	0.9852
5	0.9959	0.9922	0.9954	0.9950	**1.0000**	0.9992	0.9988	0.9784
6	0.9969	0.9931	0.9974	0.9969	0.9994	**1.0000**	0.9987	0.9797
7	0.9937	0.9880	0.9957	0.9948	0.9985	0.9987	**0.9999**	0.9721
8	0.9873	0.9943	0.9819	0.9848	0.9795	0.9805	0.9728	**0.9999**

できていることがわかる．ただし，デバイス ID のみを用いる方法はオシロスコープ等の測定機器を必要とせず簡便である一方，真贋判定器のデジタル出力は機械学習によって模倣される可能性がある．要求されるセキュリティレベルに応じて，通常はデバイス ID のみを用いてデバイスの識別を行い，異なる場所から同一デバイス ID にマッチするクエリがあった場合や，特定のデバイス ID のマッチ回数が異様に増加した場合等にサイドチャネル情報を利用した調査を行う等の方法が考えられる．

本研究では 8 個のデバイスを用いて判定を行ったが，より多くのデバイスを用いた場合に正しい判定が得られるかを調べる必要がある．また，テンプレートを用いた場合は相関係数の最大値を用いることでデバイスを正しく判定できているものの，他のデバイスとの相関係数の差が小さい．デバイスの誤判定を防ぐため，より個体差を抽出しやすい測定方法や評価方法の開発が必要である．

5. おわりに

LSI の物理的特徴 (サイドチャネル情報) を用いてチップの真贋判定を行う回路を開発し，FPGA 上に実装して有効性を実験により確認した．真贋判定器は，疑似 LFSR 発振回路と AES 暗号化回路から構成されている．LFSR 発振回路は遅延の大きな組み合わせ回路であり，デバイスのばらつきを信号遅延として抽出する働きを持ち，その出力差は AES 回路によって増幅される．

今回，真贋判定器のコア電圧をテンプレートとして利用することで，デバイスを正しく判定することができた．従来の PUF と同様にデジタル出力値を用いても正しい判定が可能であるが，この方法は測定機器が不要で簡便である半面，機械学習によって出力値が模倣される危険性がある．要求されるセキュリティレベルに応じて，デジタル出力とサイドチャネル情報の双方を利用した真贋判定を行うことが有効と考えられる．

今後，より多くのデバイスを用いて提案手法の有効性の実証実験を行ってゆく．また，デバイスの真贋判定をより正確に行うための優れた測定方法・評価方法の開発を行ってゆく．

参 考 文 献

1) Pappu, S.R.: Physical One-Way Functions, PhD Thesis, MIT (2001).
2) Lim, D., Lee, J.W., Gassend, B., Suh, G.E., van Dijk, M. and Devadas, S.: Extracting Secret Keys From Integrated Circuits, *IEEE Trans. VLSI Syst.*, Vol.13, No.10, pp.1200–1205 (2005).
3) Suh, G.E. and Devadas, S.: Physical Physical Unclonable Functions for Device Authentication and Secret Key Generation, *DAC'07*, pp.9–14 (2007).
4) Guajardo, J., Kumar, S.S., Schrijen, G.-J. and Tuyls, P.: FPGA Intrinsic PUFs and Their Use for IP Protection, *CHES'07*, pp.63–80 (2007).
5) Kumar, S.S., Guajardo, J., Maesyz, R., Schrijen, G.-J. and Tuyls, P.: The Butterfly PUF, *HOST'08*, pp.67–70 (2008).
6) Rührmair, U., Sehnke, F., Sölter, J., Dror, G., Devadas, S. and Schmidhuber, J.: Modeling Attacks on Physical Unclonable Functions, *CCS'10*, pp.237–249 (2010).
7) Alfke, P.: Efficient Shift Registers, LFSR Counters, and Long Pseudo-Random Sequence Generators (1996).
8) 佐藤　証，片下敏宏，坂根広史：暗号モジュールの安全な実装を目指して–サイドチャネル攻撃の標準評価環境の構築–，*Synthesiology*, Vol.3, No.1, pp.56–65 (2010).
9) Xilinx, Inc.: *Virtex-5 Family Overview* (2009).
10) : Cryptographic Hardware Project, http://www.aoki.ecei.tohoku.ac.jp/crypto/. Aoki Lab., Tohoku University.