Vol.2018-MBL-88 No.14
Vol.2018-CDS-23 No.14
2018/8/31

検定を用いた PUF に対するサイドチャネル解析の安全性評価手法

野崎佑典[†1]　吉川雅弥[†1]

概要：IoT のセキュリティ基盤技術として Physical Unclonable Function (PUF) が注目されている．一方で，PUF 動作時の消費電力等の物理情報を利用したサイドチャネル解析の脅威が報告されており，対策手法の研究も行われている．また PUF の安全性評価では，多くの消費電力波形を利用したモデリング攻撃を実際に行う必要がある．そのため，安全性評価には解析のための時間や，専門知識が必要となる．本研究では，新たに統計的検定を用いた PUF の安全性評価手法を提案する．提案手法では，取得した消費電力波形データから PUF の内部処理に依存したサイドチャネル情報が漏えいしているかどうかを評価する．提案手法では，実際にモデリング攻撃を実施する必要がないため，安全性評価を容易に行うことができる．FPGA を用いた実験では，提案手法を用いることで，実装した PUF が脆弱であるかどうかを簡易的に評価できることを確認した．

キーワード：PUF，サイドチャネル解析，統計的検定，ハードウェアセキュリティ，耐タンパ性

Security Evaluation Method using Statistical Test against Side-Channel Analysis for PUF

YUSUKE NOZAKI[†1]　MASAYA YOSHIKAWA[†1]

Abstract: Physical unclonable functions (PUFs) have been attracted attention as security core technologies for internet of things. On the other hand, the threat of side-channel analysis using physical information such as power consumption has been reported. Hence, countermeasures against side-channel analysis for PUFs have been studied. For security evaluation of PUFs, actual modeling attacks using many power consumption waveforms must be performed; therefore, processing time for analysis and expertise are required. This study proposes a new security evaluation method using a statistical test for PUFs. The proposed method evaluates side-channel leakage dependent on operations of PUFs from the measured power consumption waveforms. Thus, the proposed method can easily perform the security evaluation of PUFs. In experiments using an FPGA, the proposed method could easily evaluate the vulnerability of PUFs was confirmed.

Keywords: PUF, Side-channel analysis, Statistical test, Hardware security, Tamper resistance

1. はじめに

IoT のセキュリティを支える技術として，半導体の製造ばらつきをデバイスの真贋判定に用いる Physical Unclonable Function（PUF）が注目されている [1]–[4]．しかし，PUF は回路動作時の消費電力などの物理情報（サイドチャネル情報）を利用した解析（サイドチャネル解析）に対して脆弱であることが知られている [5]–[10]．サイドチャネル解析では，サイドチャネル情報を利用したモデリング攻撃を行うことで，対象とする PUF 回路を複製する．そこで我々は，これまでに PUF のサイドチャネル解析に対する対策回路の実装評価を行い，その安全性について検証してきた [11]．一方で，対策を施した PUF が安全であるかを評価するためには，多くのサイドチャネル情報を利用したモデリング攻撃を実際に適用する必要があり，安全性評価のための専門知識や時間が必要となる．評価者の立場において，対象の PUF がサイドチャネル解析に対して耐性を有しているかを簡易的に検証できることは非常に重要である．

そこで本研究では，新たに統計的検定を用いた PUF の安全性評価手法を提案する．提案手法では，取得した波形データから PUF の内部処理に起因したサイドチャネル情報が漏えいしているかを検定により評価する．検定を用いた評価により，実際にモデリング攻撃を行う必要がないため，安全性評価を容易に行うことができる．また，Field Programmable Gate Array（FPGA）を用いた評価実験により提案手法の有効性について検証する．

2. 準備

2.1 PUF とモデリング攻撃

これまでに多くの PUF が提案されており，中でも製造ばらつきにより生じる信号の伝搬時間の差を利用するアービターPUF [1]は代表的な PUF の 1 つである．一方で，アー

†1 名城大学
Meijo University

ⓒ 2018 Information Processing Society of Japan

Vol.2018-MBL-88 No.14
Vol.2018-CDS-23 No.14
2018/8/31

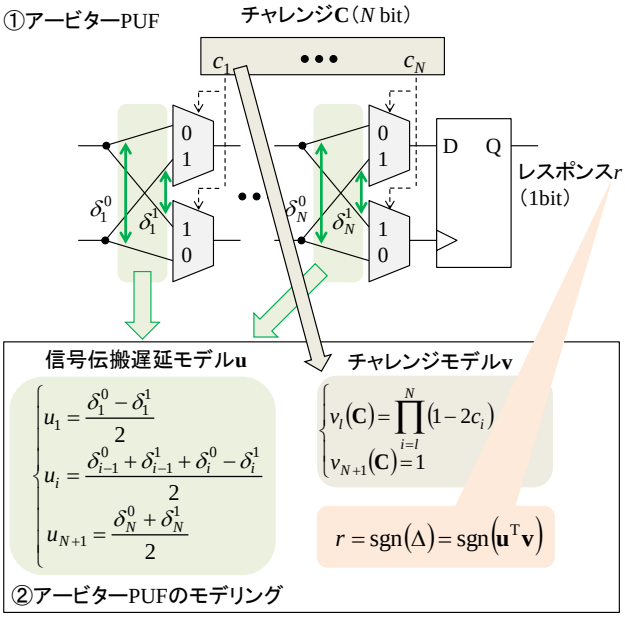

図 1　アービターPUF とモデリング

Figure 1　Arbiter PUF and its modeling method.

ビターPUF はモデリング攻撃に対して脆弱であり，一定のチャレンジとレスポンスのペア（Challenge and Response Pairs : CRPs）を利用することで，PUF 回路の複製が可能であると報告されている [12][13]．アービターPUF とアービターPUF のモデリングの概要を図 1 に示す．図 1 の①に示すように，アービターPUF は 2 本の等長配線と 2N 個のセレクタ，アービター回路で構成する．そして，外部から Nbit のチャレンジ（c_1, …, c_N）を入力し，信号の伝搬経路を選択する．このとき，チャレンジが 0 のとき，信号は直進する経路を，チャレンジが 1 のとき信号は交差する経路を選択する．そして，アービター回路では上側と下側のどちらの信号が早く到着したかを判定し，1bit のレスポンスを生成する．図 1 の例では，アービター回路に DFF を使用しており，上側の信号の方が早い場合レスポンスは 1 に，そうでない場合レスポンスは 0 となる．

アービターPUF に対するモデリング攻撃では，アービターPUF の構造を線形モデルで表現する [12][13]．モデリングの概要を図 1 の②に示す．具体的には，チャレンジモデル $\mathbf{v}$ と信号伝搬遅延モデル $\mathbf{u}$ を用いて，アービターPUF のレスポンス r は式(1)で表される．

$$r = \mathrm{sgn}(\Delta) = \mathrm{sgn}\left(\mathbf{u}^{\mathrm{T}}\mathbf{v}\right) \tag{1}$$

ここで，Δはアービター回路における信号の伝搬時間差，$\mathbf{u}$ は信号伝搬遅延モデル，$\mathbf{v}$ はチャレンジモデルであり，$\mathbf{u}$ (= u_1, …, u_{N+1})，$\mathbf{v}$ (= v_1, …, v_{N+1})はそれぞれ式(2)(3)で表される．

$$\begin{cases} u_1 = \dfrac{\delta_1^0 - \delta_1^1}{2} \\ u_i = \dfrac{\delta_{i-1}^0 + \delta_{i-1}^1 + \delta_i^0 - \delta_i^1}{2} \\ u_{N+1} = \dfrac{\delta_N^0 + \delta_N^1}{2} \end{cases} \tag{2}$$

$$\begin{cases} v_l(\mathbf{C}) = \displaystyle\prod_{i=l}^{N}(1-2c_i) \\ v_{N+1}(\mathbf{C}) = 1 \end{cases} \tag{3}$$

ただし，δ_i^0 （δ_i^1）はチャレンジが 0（1）のときの i 番目のセレクタ間の信号伝搬遅延差を表している．また，i = 1, …, N，l = 1, …, N である．

実際のモデリング攻撃では式(3)で表現されるチャレンジモデルとレスポンスを用いた機械学習を行い，学習モデルを作成する．そして，この学習モデルを用いて，未知のレスポンスの予測を行う．

2.2　Lightweight PUF [2]

そのため，モデリング攻撃に対する耐性を持つ PUF として Lightweight PUF [2]が提案されている．Lightweight PUF の概要を図 2 に示す．Lightweight PUF は，Interconnect network，Input network，k 個のアービターPUF，Output network で構成する．Lightweight PUF に入力するチャレンジは Interconnect network と Input network の 2 つの層で変換され，k 個のアービターPUF には異なるチャレンジがそれぞれ与えられる．そして，k 個のアービターPUF の出力はそれぞれ Output network で XOR 演算を用いた処理が行われ，最終的に，$m$bit のレスポンスが生成される．以上のように，Lightweight PUF では各アービターPUF の出力を XOR 演算することで，PUF の線形モデルでの表現を難しくし，モデリング攻撃への耐性を向上させている [2].

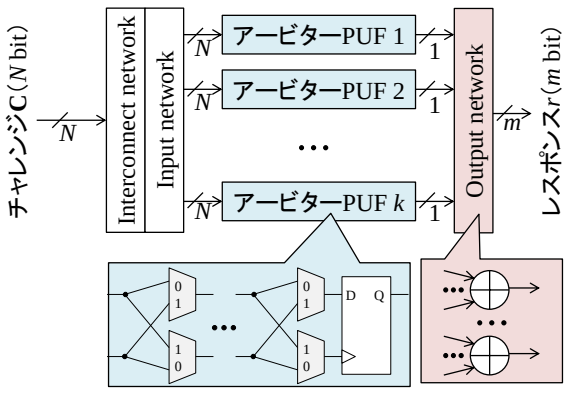

図 2　Lightweight PUF

Figure 2　Lightweight PUF.

ⓒ 2018 Information Processing Society of Japan

Vol.2018-MBL-88 No.14
Vol.2018-CDS-23 No.14
2018/8/31

2.3 サイドチャネル解析とその対策

これまでに PUF に対するサイドチャネル解析がいくつか提案されている [5]–[10]. Lightweight PUF や XOR アービターPUF を対象としたサイドチャネル解析では，アービター回路動作時の消費電力を利用する [5][6]. 具体的には，アービター回路の出力遷移時の消費電力が，出力が変化しない場合と比較して異なることを利用する．Lightweight PUF を対象としたサイドチャネル解析の概要を図 3 に示す．図 3 に示すように，この解析では Lightweight PUF を構成する各アービターPUF の出力が全て 0 または 1，すなわち，出力のハミング重み（Hamming Weight : HW）が 0 または k となるようなチャンレンジ（良いチャレンジ）のみをモデリング攻撃に利用する．そして良いチャレンジを利用し，PUF のレスポンスの予測に必要な学習モデルを生成する [5].

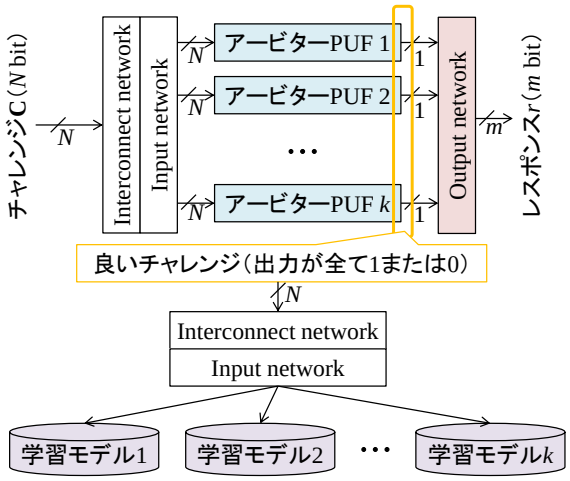

図 3　PUF に対するサイドチャネル解析
Figure 3　Side-channel analysis for PUF.

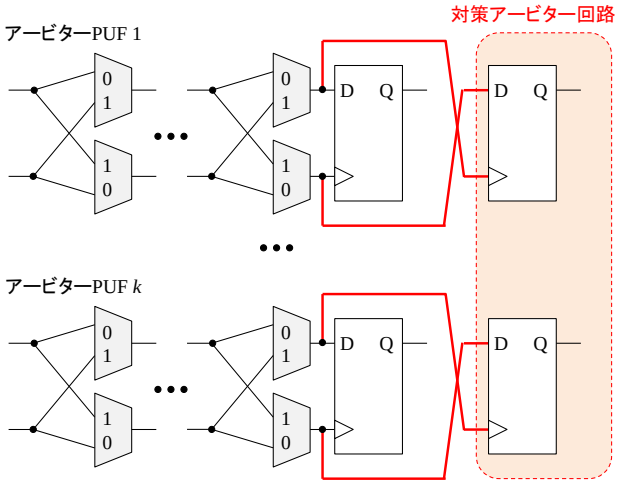

図 4　PUF のサイドチャネル解析対策回路
Figure 4　Countermeasure circuit against side-channel analysis for PUF.

そのため，サイドチャネル解析に対する対策手法が提案されており，FPGA による実装評価も行われている [11]. 対策回路の概要を図 4 に示す．図 4 に示すように対策回路では，対策用アービター回路を k 個追加実装する．この対策用アービター回路には通常のアービター回路に入力させる 2 つの信号を交差させて入力する．信号を交差させることで，対策用アービター回路の出力は通常のアービター回路の出力と比較して反転する．したがって，対策用アービター回路を追加実装することにより，各アービター回路の遷移回数は，出力に依らず常に一定になる．すなわち，常にサイドチャネル情報は一定となるため，サイドチャネル解析への耐性が向上する．

2.4 関連する研究

検定を用いた安全性評価手法について，これまでに暗号回路に対するサイドチャネル解析に関するものが提案されている [14]. これらの評価では，安全性評価に秘密鍵の解析を行うのではなく，秘密鍵や平文が既知という条件で，測定した消費電力波形からサイドチャネル情報が漏えいしているかを評価する．また，近年ではこれらの検定を用いた安全性評価手法が，ISO/IEC 17825 で標準化されている [15]. さらに，ISO/IEC 17825 の有効性に関していくつかの研究が行われている [16][17].

一方で，PUF を対象に検定を用いたサイドチャネル解析の安全性評価手法の研究は筆者らの知る限り報告されていない．

3. 提案手法

本研究では，PUF のサイドチャネル解析に対する安全性評価手法を提案する．提案手法では，PUF 動作時の消費電力波形に対して，統計的検定を適用することで PUF の内部処理に依存したサイドチャネル情報が漏えいしているかどうかを評価する．提案手法の概要を図 5 に示す．

図 5 に示すように提案手法では，ある選択関数に従い消費電力波形を 2 つのグループへと振り分ける．このとき提案手法では，評価者にとって各アービターPUF の出力値は既知であるものとする．また選択関数に関して，良いチャレンジのみについて評価を行う場合では，Lightweight PUF を構成するアービターPUF の出力の HW が 0 または k を選択関数に用いる．すなわち，HW が 0 の場合はグループ 1 に，HW が k のときはグループ 2 へと消費電力波形を振り分ける．

そして，2 つの集団（グループ 1 とグループ 2）の，母平均の差についての検定，すなわちウェルチの t 検定を行う．ここで，サイドチャネル対策が想定通りに機能していれば，各グループの消費電力は一定となるため，2 つの母平均の差の検定では，有意な差は表われない．一方で，サイドチャネル対策が上手く機能しない場合や，対策が施さ

ⓒ 2018 Information Processing Society of Japan

Vol.2018-MBL-88 No.14
Vol.2018-CDS-23 No.14
2018/8/31

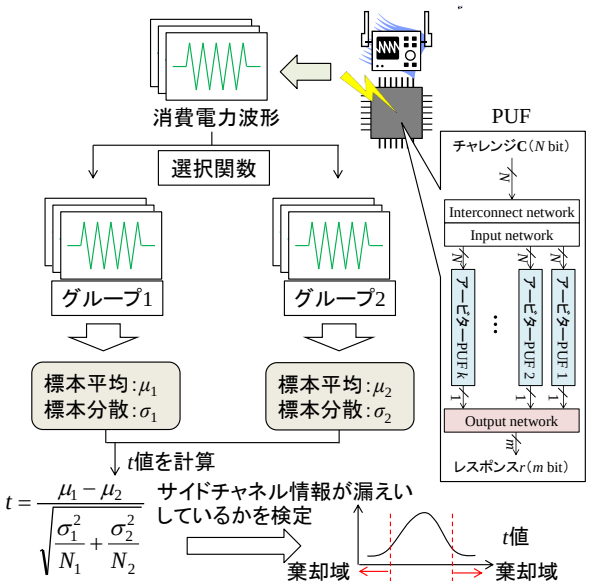

図 5　提案手法の概要

Figure 5　Outline of the proposed method.

れていない場合，消費電力は一定とならず，検定において 2 つの母平均には有意な差が表れる．

具体的には，2 つのグループのサンプル数を N_1，N_2，標本平均を μ_1，μ_2，標本分散 σ_1，σ_2 をとすると，統計量 t 値は，式(4)で計算できる．

$$t = \frac{\mu_1 - \mu_2}{\sqrt{\frac{\sigma_1^2}{N_1} + \frac{\sigma_2^2}{N_2}}} \tag{4}$$

このとき，提案手法で用いる帰無仮説 h0 と対立仮説 h1 は以下の通りである．式(5)に示すように，帰無仮説 h0 は「2 つの母平均に有意な差が表れない」であり，対立仮説 h1 は「2 つの母平均には有意な差が表れる」である．

$$\begin{cases} \text{h0}: \mu_1 = \mu_2 \\ \text{h1}: \mu_1 \neq \mu_2 \end{cases} \tag{5}$$

次に, 以下の式(6)より自由度 f を計算する [18]. そして，求めた自由度 f の t 分布から，有意水準 α の棄却域を計算する．このとき，式(4)より計算した t 値が棄却域に入る場合，式(5)の帰無仮説 h0 は棄却されるため，有意な差があり，サイドチャネル情報が漏えいしていると考えられる．一方で，t 値が棄却域に入らない場合，帰無仮説 h0 は採択され，有意な差は見られず，サイドチャネル情報は漏洩していないと考えられる．

$$f = \frac{\left(\frac{\sigma_1^2}{N_1} + \frac{\sigma_2^2}{N_2}\right)^2}{\frac{\sigma_1^4}{N_1^2(N_1 - 1)} + \frac{\sigma_2^4}{N_2^2(N_2 - 1)}} \tag{6}$$

このように，提案手法を用いることで実際にサイドチャネル解析を行う必要がなく，簡易的に安全性評価を行うことができる．

4. 評価実験

4.1 実験環境

実験環境とその詳細を図 6 と表 1 に示す．実験では，FPGA ボードにサイドチャネル対策を施した Lightweight PUF と，無対策の Lightweight PUF を実装した．実装に関して，本研究では $N = 64$，$k = 2$ の Lightweight PUF を実装

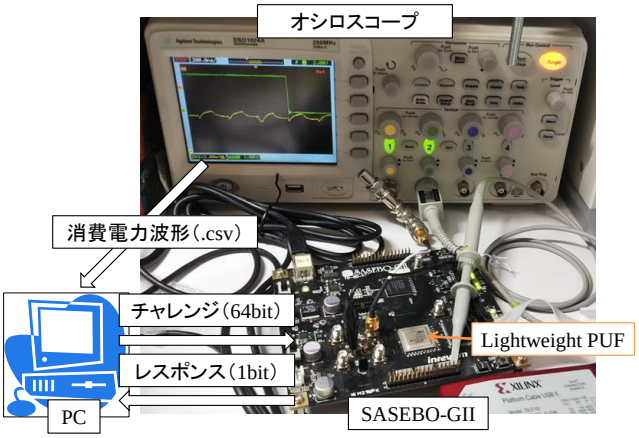

図 6　実験環境

Figure 6　Experimental environment.

表 1　実験環境の詳細

Table 1　Detail of experimental condition.

PUF	Lightweight PUF
セレクタ段数（N）	64
アービターPUF の数（k）	2
FPGA ボード	SASEBO-GII
FPGA	Xilinx Virtex-5 XC5VLX30
実装ツール	Xilinx ISE Design Suite 14.7
フロアプラン	Xilinx PlanAhead v14.7
オシロスコープ	Agilent DSO 1024A
サンプリングレート	2GSa/sec
機械学習	ロジスティック回帰
パラメータの更新	RProp
プログラミング言語	MATLAB 2013b

ⓒ 2018 Information Processing Society of Japan

表 2　提案手法で使用したパラメータ
Table 2　Parameters for the proposed method.

波形数	1,000
サンプル点数	1,999
有意水準（α）	0.05

表 3　使用した選択関数
Table 3　Selection functions for experiments.

	グループ 1	グループ 2
選択関数①	HW：0	HW：2
選択関数②	HW：0	HW：1
選択関数③	HW：1	HW：2

した. Output network に関しては, 文献 [13]と同様にして, 生成するレスポンスは 1bit とした．また，消費電力波形の測定を容易にするため，各アービター回路に対して，T 個（$T = 8$）のトグルフリップフロップを追加実装した．そして，乱数で生成したチャレンジを，実装した Lightweight PUF に入力し，このときのレスポンスを収集した．また，それぞれ PUF 動作時の消費電力を, オシロスコープを用いて測定した．消費電力波形の取得に関して，ノイズの影響を軽減するために, 同じチャレンジに対する消費電力を 10 回測定し，この平均を波形データとして取得した．

また，サイドチャネル解析に関して，機械学習にはロジスティック回帰を使用し，パラメータの更新には RProp [19]を使用した．

そして，提案手法では有意水準を 0.05 として，評価を行った．提案手法で用いたパラメータを表 2 に示す．また，選択関数に関しては表 3 に示すものを使用した．

4.2 実験結果

評価実験では，まず実際のサイドチャネル解析を行い，実装した Lightweight PUF の安全性を確認した. 実験結果を図 7 に示す．図 7 の横軸は解析に使用したデータの数を，縦軸は 10,000 個のテストデータのレスポンスの予測率を示している. 図 7 より, 無対策の Lightweight PUF では, 5,000 個のデータで 80%以上のレスポンスの予測に成功しており, サイドチャネル解析に対して脆弱であることが確認できる. 一方で, 対策 Lightweight PUF では，レスポンスの予測率は約 50%であり，サイドチャネル解析に対して耐性があることが確認できる.

次に，取得した消費電力波形に対して提案手法を適用し，サイドチャネル解析に対する安全性を簡易的に評価する. 無対策 Lightweight PUF と対策 Lightweight PUF に対する実験結果をそれぞれ図 8 から図 10 に示す. 図 8 は選択関数①を，図 9 は選択関数②を，図 10 は選択関数③を用いた場合の結果である．また，図の横軸は時間を，縦軸は提案手法により算出した t 値を示している．ここで，どの実験においても，式(6)から算出した自由度 f は 400 以上であったため, 自由度∞の t 分布に従い, 両側検定を行った. このとき，有意水準 0.05 での棄却域は，1.96 以上または-1.96 以下である．図 8 から図 10 に示すように，無対策ではどの選択関数を用いた場合でも，t 値は-1.96 以下であり棄却域に入るため，有意水準 0.05 で帰無仮説 h0 は棄却される．すなわち，有意水準 0.05 において，どの選択関数でも 2 つの消費電力波形の母集団には有意な差がある．したがって，無対

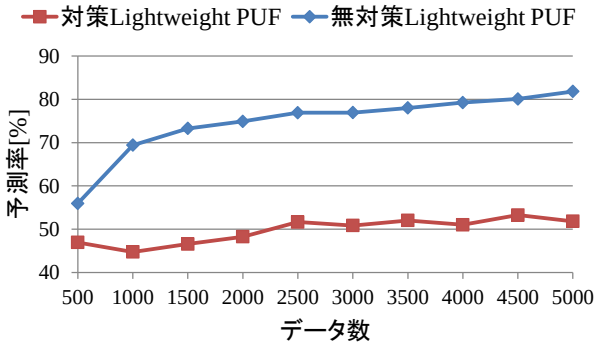

図 7　実際のサイドチャネル解析結果
Figure 7　Results of side-channel analysis.

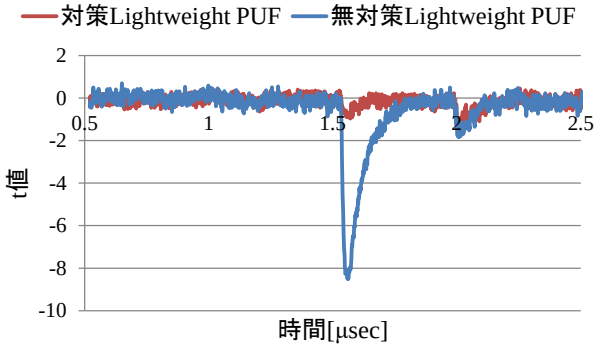

図 8　実験結果（選択関数①）
Figure 8　Experimental results using selection function (i).

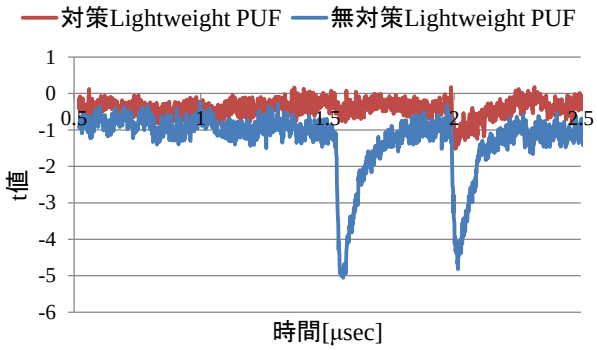

図 9　実験結果（選択関数②）
Figure 9　Experimental results using selection function (ii).

ⓒ 2018 Information Processing Society of Japan

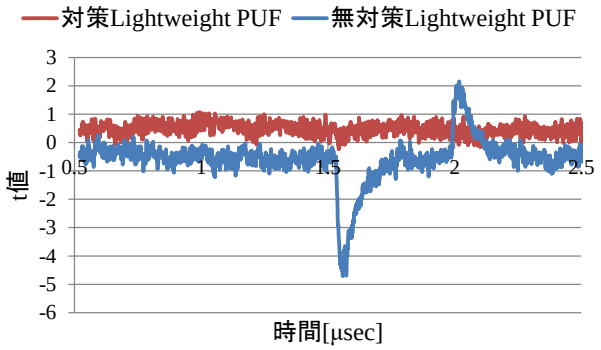

図 10　実験結果（選択関数③）
Figure 10　Experimental results using selection function (iii).

策 Lightweight PUF において，PUF の動作に依存したサイドチャネル情報が漏えいしていると考えられる．

一方で，対策 Lightweight PUF では，どの選択関数においても算出した t 値は 1.96 以上または-1.96 以下でないことが確認できる．したがって，帰無仮説 h0 は採択され，2 つのグループにおいて，有意な差は見られない．すなわち，サイドチャネル情報は漏洩していないと考えられる．以上のように，提案手法を用いることで，実際にサイドチャネル解析を行わなくても，簡易的にサイドチャネル解析に対する安全性を評価することができる．

5. まとめ

本研究では，PUF のサイドチャネル解析に関する安全性評価手法を提案した．提案手法では，取得した消費電力波形データに対して，統計的検定を適用することで PUF 内部の動作に起因したサイドチャネル情報が漏えいしているかを検定する，すなわち，実装した PUF がサイドチャネル解析に対して安全かどうかを評価する．FPGA を用いた評価実験では，無対策の Lightweight PUF では提案手法により，サイドチャネル情報の漏えいに関して，有意な差が確認され，対策 Lightweight PUF では有意な差は確認されなかった．したがって，提案手法により簡易的にサイドチャネル解析に対する安全性の評価が可能であり，提案手法が有効であることを実証した．

今後は，他の PUF に関する検討を進める予定である．

謝辞　この成果は，国立研究開発法人新エネルギー・産業技術総合開発機構（ＮＥＤＯ）の委託業務の結果，得られたものです．

参考文献

[1] Lee, J.-W., Lim, D., Gassend, B., Suh, G. E., Dijk, M. V., and Debadas, S.: A Technique to Build a Secret Key in Integrated Circuits for Identification and Authentication Applications, Proc. of IEEE VLSI Circuits Symposium, pp. 176–179 (2004).
[2] Majzoobi, M., Koushanfar, F., and Potkonjak, M.: Lightweight Secure PUFs, Proc. of IEEE/ACM Int. Conf. on Computer Aided Design (ICCAD), pp. 670–673 (2008).
[3] Suh, G. E. and Devadas, S.: Physical Unclonable Functions for Device Authentication and Secret Key Generation, Proc. of 44th ACM/IEEE Design Automation Conf. (DAC), 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, Proc. of 9th Int. Workshop on Cryptographic Hardware and Embedded Systems (CHES 2007), LNCS 4272, pp. 63–80, Speinger-Verlag (2007).
[5] Mahmoud, A., Rührmair, U., Majzoobi, M., and Koushanfar, F.: Combined Modeling and Side Channel Attacks on Strong PUFs, IACR Cryptology ePrint Archive: Report 2013/632 (2013).
[6] Rührmair, U., Xu, X., Sölter, J., Mahmoud, A., Majzoobi, M., Koushanfar, F., and Burleson, W.: Efficient Power and Timing Side Channels for Physical Unclonable Functions, Proc. of 16th Int. Workshop on Cryptographic Hardware and Embedded Systems (CHES 2014), LNSC 8731, pp. 476–492, Springer, (2014).
[7] Merli, D., Schuster, D., Stumpf, F., and Sigl, G.: Semi-invasive EM attack on FPGA RO PUFs and countermeasures, Proc. of 6th Workshop on Embedded Systems Security (WESS'11), no. 2, pp. 1–9, (2011).
[8] Delvaux, J. and Verbauwhede, I.: Side Channel Modeling Attacks on 65nm Arbiter PUFs Exploiting CMOS Device Noise, Proc. of IEEE Int. Symp. on Hardware-Oriented Security and Trust (HOST 2013), pp. 137–142, (2013).
[9] Kumar, R. and Burleson, W.: Side-Channel Assisted Modeling Attacks on Feed-Forward Arbiter PUFs Using Silicon Data, Proc. of RFIDSec 2015, LNCS 9440, pp. 53–67, Springer, (2015).
[10] 野崎佑典，吉川雅弥：耐タンパ PUF に対する電磁波解析の基礎検討，情報処理学会研究報告，IPSJ-CDS，vol. 20，no. 9，pp. 1–6，(2017).
[11] 野崎佑典，吉川雅弥：XOR 型 PUF のサイドチャネル対策手法とその評価，電子情報通信学会技術研究報告，IEICE-HWS，vol. 118，no. 153，pp. 337–342，(2018).
[12] Lim, D.: Extracting Secret Keys from Integrated Circuits, M.S. thesis, MIT (2004).
[13] Rührmair, U., Sölter, J., Sehnke, F., Xu, X., Mahmoud, A., Stoyanova, V., Dror, G., Schmidhuber, J., Burleson, W., and Devadas, S.: PUF Modeling Attacks on Simulated and Silicon Data, IEEE Trans. on Information Forensics and Security, vol. 8, no. 11, pp. 1876–1891 (2013).
[14] Goodwill, G., Jun, B., Jaffe, J., and Rohatgi, P.: A Testing Methodology for Side-Channel Resistance Validation, Non-Invasive Attack Testing Workshop (NIAT 2011), pp. 1–15, (2016).
[15] ISO/IEC 17825:2016, Information technology -- Security techniques -- Testing methods for the mitigation of non-invasive attack classes against cryptographic modules, (2016).
[16] ヘンドラ　グントゥル，佐藤　証，菅原崇彦，油谷大武，吉村　紀：ISO/IEC 17825 による暗号回路の電力解析に対する安全性評価と偏りを有するデータセットを用いた解析精度の向上，2017 年暗号と情報セキュリティシンポジウム講演論文集，3C3-3，pp. 1–8，(2017).
[17] 松山直樹，岸田治展，菅原崇彦：ISO/IEC 17825 による電力解析評価と DPA/CPA 解析評価との相関性，2018 年暗号と情報セキュリティシンポジウム講演論文集，1D1-2，pp. 1–6，(2018).
[18] Welch, B. L.: The significance of the Difference Between Two Means when the Population Variances are Unequal, Biometrika, vol. 29, no. 3–4, pp. 350–362, (1938).
[19] Riedmiller, M. and Braun, H.: A direct adaptive method for faster backpropagation learning: The RPROP algorithm, Proc. of IEEE Int. Conf. on Neural Networks (ICNN'93), vol. 1, pp. 586–591, (1993).

ⓒ 2018 Information Processing Society of Japan