社団法人　電子情報通信学会
THE INSTITUTE OF ELECTRONICS,
INFORMATION AND COMMUNICATION ENGINEERS

信学技報
TECHNICAL REPORT OF IEICE.

PUF に関する研究の調査と考察

岡野　舞子†

† 奈良先端科学技術大学院大学　〒630–0192 奈良県生駒市高山町 8916–5
E-mail: †okano.maiko.ol0@is.naist.jp

あらまし　フィジカリー・アンクローナブル・ファンクション（PUF）とは，主に半導体技術を用いて作られた集積回路を大量生産した際に生じる，制御不能な製造ばらつきを利用してその個体にランダムな関数を作る技術のことである．この技術は，個体の識別に用いることで模造品の作成を防ぐだけでなく，制御不能な性質を利用することで暗号アルゴリズムに組み合わせて使うことも期待されている．本稿では PUF について調査した内容を，その発展の歴史を踏まえて述べる．（全部書き終えたら，ちゃんと書き直す）

キーワード　暗号ハードウェア，ハードウェアセキュリテイ，PUF

Maiko OKANO†

† Nara Institute of Science and Technology, 8916–5 Takayama-cho, Ikoma, Nara, Japan
E-mail: †okano.maiko.ol0@is.naist.jp

Abstract

Key words　Physically Unclonable Function

1. はじめに

研究背景，PUF の使いみち

2. Physically Unclonable Function

2.1 PUF の概要

Physicallly Unclonable Function（PUF）とは，半導体技術を用いて作った集積回路などの大量生産された製造物に対し，製造時に生じる制御不能な製造ばらつきを利用して，その個体に固有なランダム関数を作成し使用する技術のことを指す．この技術は偽造品か否かどうかの真贋判定・個体識別や，主体認証，また暗号鍵やパラメータの生成に利用することが可能であると考えられている．

PUF はチャレンジとして外部から刺激を与えられたとき，レスポンスとして測定値を出力する．制御不能な製造ばらつきを利用するため，同じ PUF に同じチャレンジを入力してもレスポンスは多少異なる．しかし，同じレスポンスを異なる PUF 個体に入力したとき，出力されるレスポンスは区別可能なほどに異なるため，これがランダム関数の機能を果たす．

2.2 PUF に求められる特性

本節では，PUF に求められるセキュリティに関する特性を説明する．要求される重要な特性の説明を通して，実際の PUF がどのような機能を果たすかの理解を深めることが狙いである．しかし，本稿執筆時点（2021 年 7 月 2 日）で PUF のセキュリティ要件及び試験方法は，ISO/IEC 20879 にて議論中となっている．そのため，ここでの内容は主に菅原 [1] と Maes [2] に基づいている．

本稿では PUF の機能の根幹を支える，とりわけ重要な 3 つの特性（再現性・ユニーク性・耐クローン性）について述べる．

2.2.1 再現性（Reproducibility）

再現性とは，同一の PUF に同じチャレンジを繰り返し入力したとき，出力されるレスポンスのばらつきの小ささ，つまり安定度の高さを表す．PUF のレスポンスにはノイズが含まれており，同じ個体に同じチャレンジを入力しても出力されるレスポンスには差異が生じる．PUF の実用の観点から，同じ個体からのレスポンスは類似している必要があるため，再現性は高いほうが良い．

再現性は，同一チップの PUF 出力ビット列のハミング距離（Hamming Distance: HD），Intra-HD を評価指標としている．このとき，Intra-HD の平均の理想値は 0 である．また，この指標は，PUF のノイズの大きさを測るだけでなく，環境変化の影響を評価する場合にも用いる．

2.2.2 ユニーク性（Uniqueness）

ユニーク性とは，異なる PUF に同一のチャレンジを入力したとき，出力されるレスポンスの値の差の大きさを表す．異なる PUF のレスポンスの値の差が小さい（類似している）場合，それらを同一であると誤判定してしまう可能性が高まる．そのため，PUF の個体差，つまりユニーク性は高いほうがよい．

ユニーク性は，異なるチップの PUF 出力ビット列のハミング距離，Inter-HD を評価指標としている．このとき，Inter-HD

の平均の理想値は 0.5 であり，この値に近いほどユニーク性は高い．

2.2.3 耐クローン性（Unclonable）

耐クローン性とは，PUF のチャレンジに対するレスポンスを再現するモデルの構築が不可能，あるいは困難であることを表している．PUF を利用してある個体と別の個体を識別するためには，ある個体を模したクローンを作成できないという前提条件が必要である．

この特性には 2 つの意味があり，1 つは正規製造者であってもクローンを作ることができないこと（＝製造者耐性），もう 1 つはクローンの制作を試みる攻撃への耐性を持つ（クローンを作るための既知の攻撃が存在しない）ことである．

3. PUF の分類

3.1 初期の PUF

3.1.1 Physical one-way functions

PUF の始祖とされているのは，2001 年に Pappu が提案した物理的一方向性関数（Physical one-way functions: POWF）[3] である．背景としては，既存の数論に基づいた一方向性関数の課題に対する解決策として提案された．POWF の簡略化した手順を以下に示す．

（1） 3 次元の不規則な構造の媒体をトークンとして用意する．具体的には，極小のガラス玉をいくつか含んだエポキシ樹脂とされている．

（2） 上記の媒体にレーザー光を照射したものを，電化結合素子カメラで記録する．これによって，2 次元のスペックルパターンを得る．

（3） スペックルパターンをガボール変換でフィルタリングし，鍵となるビット列（1 次元）を生成する．

3.1.2 Sillicon PUF

POWF は精密な光学機器で処理を行う必要があるため，アナログインターフェイスで使用するように作られている．一方で Gassend は 2002 年に，計算機やメモリと混載できるようにデジタルインターフェイスで動作する，半導体製の PUF（Sillicon PUF）を提案した [4]．Sillicon PUF は前述の POWF と異なり，暗号実装のハードウェア構成要素としてすぐに導入することができるため，現在研究されている PUF 構築の主要な種類となっている．

Gassend が提案した PUF [4] の構成は，3.2.2 節の Ring Ocillator PUF の起源となっている．この PUF は，各回路の遅延のばらつきを利用し，過渡応答を測定することで CRPs を生成する．過渡応答は，チャレンジによって刺激された経路上にある IC 内の配線やデバイスの遅延についての間接的な情報となる．この間接的な情報しかレスポンスとして与えられないことが，耐クローン性の根拠となっている．

また，“PUF” という名前や PUF の定義が明記されたのは，この論文が最初である．

3.2 遅延ベースの PUF

3.2.1 Arbiter PUF

3.1.2 節の Gassend が提案した PUF は，回路の遅延が温度や電源電圧などの環境変化に敏感であるため，PUF の信頼性を高めるためにはノイズが重大な問題となる，と Lee は指摘を行った [5]．そこで Lim らは 2004 年に Sillicon PUF の再現性を改善させた Arbiter PUF [6] を実装した．Arbiter PUF は差動構造（Arbiter）に基づいており，環境に起因するノイズに対する PUF の再現性を向上させることが可能である．これは，PUF のレスポンスに対する絶対的な遅延値を測定する代わりに，2 つの同一の遅延経路を比較し，Arbiter を用いてデジタル情報を生成するためである．

表 1 和文キャプション

Inputs		**Outputs**
G	**D**	**Q**
0	0	0
0	1	1
1	X	No Change
↑	D	d

Arbiter PUF の構造は前半と後半に分けられる．最初に 2 つの入力から立ち上がり信号（＝チャレンジ）が同時に入力され，前半部ではチャレンジによって，2 つの信号がどのような経路を伝搬するかが決定される．図**??**のとおり 2 つの MUX によってスイッチボックスが実装されており，これはチャレンジのビット数の分用意される．スイッチボックスの動作は，チャレンジのビットが 1 のときは上下に流れる信号の経路を交差，0 のときは直進となっている．

後半部では，どちらの信号が先に到達したかによって 0 か 1 のレスポンスを出力する．ここでは 1 つのトランスペアレントラッチが使用されており，これは表 1 が示すような動作を行う．2 つの立ち上がり信号が違うタイミングで D と G に入力された場合，G に立ち上がり信号が入力された瞬間の D の値を常に出力し続ける．つまり，D に先に立ち上がり信号が到達した場合，その後 G に立ち上がり信号が到達することを意味するため，レスポンスは 1 となる．逆に G に先に立ち上がり信号が到達した場合は，その時点での D には 0 が入力されていることからレスポンスは 0 となる．

3.2.2 Ring Ocillator PUF

2007 年に Suh によって提案された Ring Ocillator PUF（RO PUF）[7] は，RO の発振周波数が製造ばらつきによって異なることを基にした PUF である．RO は奇数個のインバータから構成されている．奇数個のインバータをループ上に並べ，その中のある一点の値を出力に利用することで RO の出力は一定の周期で 0 と 1 を繰り返す．インバータの個数や配線方法などがまったく同じ RO であっても，回路内部の部品の製造ばらつきによって微妙に発振周波数が異なり，RO PUF ではこの発振周波数の違いを用いて PUF の機能を提供する．RO PUF では 3 個以上の RO が用いられており，その中からチャレンジの値によって 2 つの RO を選出する．そしてその 2 つの RO の周波数の比較によってレスポンスとなる 0 か 1 のビットを出力する．

図**??**のように複数（この場合は N 個）の RO は MUX に接続され，チャレンジはその MUX のセレクタとして用いられる．

セレクタにより選ばれた 2 つの信号はそれぞれ別のカウンター回路に入力しており，カウンター回路で計測された一定時間あたりの発振回数が比較されその結果によって RO PUF から 0 か 1 の値が出力される．

3.3 メモリベースの PUF

3.3.1 SRAM PUF

SRAM PUF とは，電源投入直後にまだ何も書き込んでいない SRAM から読みだした値（初期値）を個体差として利用する PUF である [1]．2006 年に Simpson によって，PUF を利用して FPGA の IP 保護を行うというアプローチ [8] が提案された．この提案を元に，2007 年に Guajardo は FPGA に搭載されている SRAM を PUF として実装 [9] した．また，同時期の類似研究として Holcomb の FERNS（Fingerprint Extravtion and Random Numbers in SRAM）[10] がある．FERNS は SRAM PUF と非常に類似しているが，市販の SRAM チップとマイクロコントローラチップに組み込まれた SRAM という 2 つの異なるプラットフォームで実装がされている点で，Guajaudo の研究とは異なっている [2].

SRAM PUF の動作原理は，SRAM セルの電源投入時の過渡的な動作に基づいている．電源投入直後，セルは動作点が定まらず不安定な状態となるが，ごく短時間のうちに動作点は定まり安定する．この初期の動作点（初期値）は，電源投入時，毎回高い確率で同じになる．何故なら，製造ばらつきによってトランジスタに僅かな電圧差が生じるため，クロスカップリングされたインバータ回路の MOSFET の「強さ」に違いが出るためである [2]．したがって，各 SRAM セルはランダムに 0 と 1 のいずれかに遷移していくため，これが PUF のユニーク性の根拠となる．また，チャレンジは SRAM 内の特定のセルのアドレスである．

3.3.2 Butterfly PUF

2008 年に Kumar らは，起動時に SRAM セルと同様の動作をする構造を FPGA マトリクス内に実装し，これを Butterfly PUF [14] として提案した．これはほとんどの市販 FPGA に搭載されている SRAM は，電源投入直後に強制的にクリアされるため，3.3.1 節で説明したセルごとのランダムな初期値を PUF として利用することができないからである．

Butterfly PUF の実装は，2 つの透過的なデータラッチを交差結合し，SRAM セルの動作を FPGA のりコンフィギュレーションロジックで模倣することで行われる．ラッチを使って交差結合構造を作り，これにより励起状態によって不安定な状態となる．そして，しばらくすると 2 種類の安定状態のうちの 1 つに落ち着くため，これが PUF のレスポンスとなる．

3.4 その他の特徴を持つ PUF

3.5 Strong/Weak PUF

PUF は，CRP の空間の広さによって Strong PUF と Weak PUF の 2 つに分けられる．

Strong PUF は CRP の空間が極めて広い PUF であり，チャレンジ長が増大すると CRP 空間が指数関数的に増大する．また十分に長いチャレンジを与えることができる，という特徴をもつ．例としては Arbiter PUF が挙げられる．スイッチボックスの個数が n 個の場合チャレンジ数は 2^n 個となるため，$n = 128$ のときペア数は 2^{128} となり CRP を全通り試すことは困難になる．

Weak PUF は CRP 空間が狭い PUF であり，物理的な制約によって十分なチャレンジ長を確保することができない PUF である．例として RO PUF と SRAM PUF が挙げられる．RO PUF ではチップに搭載できる RO の数が制限されるので，チャレンジ長が短くなる．SRAM PUF は搭載できるメモリ素子の数に限りがあるので，チャレンジ長は高々アドレス長までとなる．典型的な SRAM のサイズは数キロバイトから数メガバイトであり，SRAM PUF を全探索攻撃から防ぐことは困難である．

ところで，Strong/Weak PUF の"Strong/Weak"は PUF の実利用におけるセキュリティ強度とは，直接結びつかないことに注意する必要がある．例として，PUF を製品の真贋鑑定の認証として用いるか，セキュリティパラメータの生成として用いるかでは，求められる CRP 空間の広さは異なる．現在，Strong/Weak の名前はしばしば誤解を生じさせることがあるので，ISO/IEC 29897 で別の名称（Extensive/Confined）が提案されている [11].

3.6 Controlled/Uncontrolled PUF

Controlled PUF とは，特定の API でしかアクセスできないようにアルゴリズムで制御された PUF である [12] [13]．逆に PUF へのアクセス制御がなく，誰でも PUF の生の入出力にアクセスできる場合は，Uncontrolled PUF と呼ぶ．

Uncontrolled PUF はシンプルな利用法であり，アクセス制御のためのデジタル回路が不要であることから，回路をより小型にすることができるという利点がある [1]．しかし，攻撃者はありうるすべてのチャレンジを PUF に入力することで，対応するレスポンスを入手して対応表を作るクローン攻撃が可能となる．このような攻撃に対し Uncontrolled PUF は，CRP を全探索できないほど大きくする方法でしか対策を行えない．

Controlled PUF は PUF の生データを秘匿するため，攻撃者に CRPs を知られることを防ぎモデリング解析の対策になると考えられている．そのため，SRAM PUF や RO PUF などの Weak PUF は Controlled PUF として実装されることが望ましい．

4. 問題点や攻撃

4.1 暗号としての PUF 利用（仮）

4.2 PUF に対する攻撃と対策

4.2.1 モデリング解析

Arbiter,RO

5. ま と め

文　献

[1] 菅原健，“暗号ハードウェアの研究開発動向：フィジカリー・アンクローナブル・ファンクション，”金融研究，vol.39，no.4，pp.25-54，Oct. 2020.

[2] R. Maes, Physically Unclonable Functions: Properties, Springer, Berlin, Heidelbelg, 2013.（DOI:10.1007/978-3-642-41395-7_3）

[3] P.S. Ravikanth, “Physical One-Way Functions,” PhD thesis, Massachusetts Institute of Technology, March 2001.

[4] B. Gassend, D. Clarke, M. van Dijk, S. Devadas, “Silicon physical random funcions,” CCS ’02: Proceedings of the 9th ACM conference on Computer and communications security, pp.148-160, November

2002.（DOI: 10.1145/586110.586132）
[5] J.W. Lee, D. Lim, B. Gassend, G.E. Suh, M. van Dijk, S. Devadas,“A Technique to Build a Secret Key in Integrated Circuits for Identification and Authentication Applications,”2004 Symposium on VLSI Circuits. Digest of Technical Papers (IEEE Cat. No.04CH37525), pp. 176-179, June 2004.（DOI: 10.1109/VLSIC.2004.1346548）
[6] D. Lim,“Extracting Secret Keys from Integrated Circuits,”Master's Thesis, Massachusetts Institute of Technology, March 2004.
[7] G.E. Suh, S. Devadas,“Physical Unclonable Functions for Device Authentication and Secret Key Generation,”2007 44th ACM/IEEE Design Automation Conference, pp.9-14, June 2007.
[8] E. Simpson, P. Schaumont, Offline Hardware/Software Authentication for Reconfigurable Platforms. In: Goubin L., Matsui M. (eds) Cryptographic Hardware and Embedded Systems - CHES 2006. CHES 2006. Lecture Notes in Computer Science, vol 4249, Springer, Berlin, Heidelberg, 2006.（DOI: 10.1007/11894063_25）
[9] J. Guajardo, S.S. Kumar, GJ. Schrijen, P. Tuyls, FPGA Intrinsic PUFs and Their Use for IP Protection, Proceedings of International Workshop on Cryptographic Hardware and Embedded Systems (CHES) 2007, Lecture Notes in ComputerScience, vol 4727, Springer-Verlag, pp. 63–80, 2007.（DOI: 10.1007/978-3-540-74735-2_5）
[10] D. E. Holcomb, W. P. Burleson , K. Fu, "Power-Up SRAM State as an Identifying Fingerprint and Source of True Random Numbers," in IEEE Transactions on Computers, vol. 58, no. 9, pp. 1198-1210, Sept. 2009.（DOI: 10.1109/TC.2008.212.）
[11] 堀洋平,“Physically Unclonable Function（PUF）の基礎, 応用と標準化について,”https://www.iot-aidevice.org/app/download/14287213230/AI2oT3_堀_+PUF の基礎_応用と標準化.pdf?t=1548407303, 参照 July 16, 2021.
[12] B. Gassend, D. Clarke, M. van Dijk and S. Devadas, "Controlled physical random functions," 18th Annual Computer Security Applications Conference, 2002. Proceedings., pp. 149-160, Nov. 2002.（Doi: 10.1109/CSAC.2002.1176287）
[13] B. Gassend, M. van Dijk, D.Clarke, E.Torlak, S. Devadas, P.Tuyls, "Controlled physical random functions and applications," ACM Transactions on Information and System Security, Volume 10, Issue 4, Article No.3, pp 1–22, Jan. 2008.（DOI:10.1145/1284680.1284683）
[14] S.S. Kumar, J. Guajardo, R. Maes, G. Schrijen, P. Tuyls, "Extended abstract: The butterfly PUF protecting IP on every FPGA," 2008 IEEE International Workshop on Hardware-Oriented Security and Trust, pp.67-70, June 2008.（DOI: 10.1109/HST.2008.4559053）