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についてのサーベイ論文（仮）

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

Survey paper of 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. PUF とは

2.1 PUF の概要

フィジカリー・アンクローナブル・ファンクション（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て，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る技術のことを指す．

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．

まず，再現性・ユニーク性・耐クローン性の 3 つの特性について述べる．この 3 つの特性は，PUF の機能の根幹を支えるとりわけ重要な特性である．

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 節で紹介する．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 節で説明した Sillicon 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である，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できる．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

3.3 メモリベースの PUF

3.3.1 SRAM PUF

3.3.2 Butterfly PUF

3.4 その他の特徴を持つ PUF

3.5 Strong/Weak PUF

3.6 Controlled/Uncontrolled PUF

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

4.2.1 モデリング解析

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.