

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 PUF, 真贋判定, 認証, モデリング攻撃

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, Identification, Authentication, Modeling attack

1. はじめに

Internet of Things (IoT) の普及に伴い、現在、膨大な数の IoT 機器がデータを収集し通信を行っている。IoT 機器の発展がもたらす Society 5.0 の実現は人々に便利さをもたらす一方、セキュリティリスクの増大が深刻な問題となっている。この問題の一因として、製造品の偽造が挙げられる。特に半導体産業は新型コロナウイルス流行の影響で工場が一部閉鎖されるなど打撃を受けたため、半導体不足により多くの偽造 IC チップが出回っている [1]。偽造 IC チップは正規品よりも早く故障する可能性が高く、搭載されている機器の寿命を短くする恐れがある。それだけでなく偽造品は誤作動を引き起こす可能性があるため、万が一重要なインフラで使用する IoT 機器に偽造 IC チップが使用されていた場合、システム障害や情報漏えいといったセキュリティインシデントを引き起こす可能性がある。したがってセキュリティ上の観点から、偽造 IC チップの流通を防止する必要がある。

IC チップが正規品か偽造品か見分ける方法として、Physically Unclonable Function (PUF) を用いることが可能である。PUF とは、大量生産された製造物 (多くの場合、半導体技術を用いて作られたチップ) の製造時に生じる製造ばらつきを利用して、ランダムに各個体に付与された個性、またそれを利用した技術のことを指す。この個性は製造者がプログラムやシリアル番号などを書き込むことなく、自動的に付与されるものであり同時に制御不能なものである。したがって、その個性をもった個体

のクローンを作成することを防ぎ、人間を指紋や虹彩で識別するように製造物の個体識別が可能となる。

従来、シリアル番号が製造物の個体識別や品質管理に用いられていたが、シリアル番号と PUF の最も異なる点はクローンの製造が可能か否かである。シリアル番号はただの文字列であるため、悪意のある攻撃者に一度認識されれば偽造品の製造を避けることは難しい。しかし、PUF は製造時の制御不能なばらつきを利用して ID を作成するため、同じ PUF の製造物を偽造することは対象の製品の微小な個体差までを完璧に再現することに等しく、非常に困難である。

また、PUF は製造品の個体識別だけでなく、認証や秘密鍵の管理に使うことができると考えられている。秘密鍵の管理は従来であれば不揮発性メモリで行っていたが、不揮発性メモリはチップを開封して解析を行う静的リバース・エンジニアリングに耐性がない。しかし PUF を用いた鍵管理は、動作時にしか鍵が顕在しないためそのような攻撃に耐性がある。

2. Physically Unclonable Function

2.1 PUF の定義

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 [2] と Maes [3] 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。

2.3 PUF の活用法

2.3.1 真贋判定・個体識別

2.3.2 鍵の生成

2.3.3 チャレンジ・レスポンス認証

認証とは、通信において相手が本人か否かを確認する技術である。暗号を用いた認証では、認証する側と認証される側が、あらかじめ交換しておいて秘密鍵をもっているかどうか確かめることで行う。このとき秘密鍵を露出することなく認証を行う手段にチャレンジ・レスポンス認証がある。

この認証方式では共通鍵暗号アルゴリズムを用いるが、これは PUF で代用する方式が提案されている。

3. 様々な PUF

3.1 PUF の歴史と構築法

3.1.1 初期の PUF

a) 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）[4] 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ckルパターンを得る。

（3） スペck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。

b) Silicon 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なられている。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、半導体制の PUF（Silicon PUF）を提案した [5]。Silicon 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 [5] の構成は、b) 節の Ring Oscillator 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。

3.1.2 遅延ベースの PUF

a) Arbiter PUF

3.1.1 節 b) の Gassend が提案した PUF は、回路の遅延が温

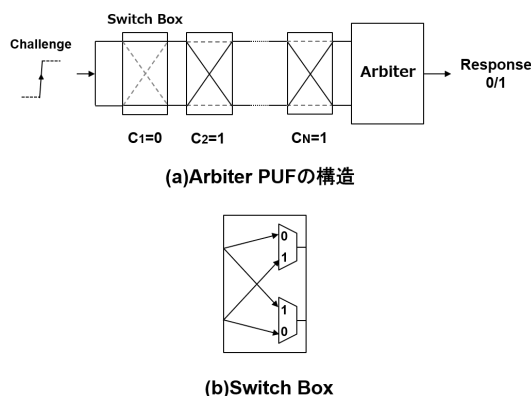


図1 Arbiter PUF の構築法

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

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[6]。そこでLimらは2004年にSillicon PUFの再現性を改善させたArbiter PUF[7]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。

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1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。

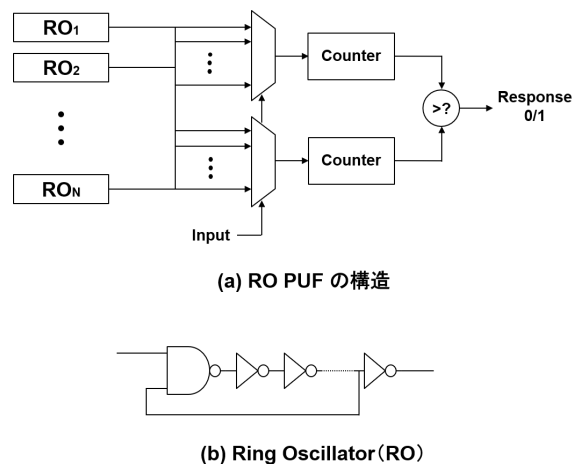


図2 RO PUF の構築法

b) Ring Oscillator PUF

2007年にSuhによって提案されたRing Oscillator PUF (RO PUF)[8]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(図2(b))、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2(a)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のセレクトとして用いられる。セレクトにより選ばれた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。

3.1.3 メモリベースのPUF

a) 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[2]。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[9]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[10]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)[11]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されている点で、Guajardoの研究とは異なっている[3]。

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 [3]。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。

b) 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 [15] 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、a) 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 のリ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。

3.1.4 その他の特徴を持つ PUF

3.2 PUF の分類

3.2.1 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 SRAM PUF が挙げられる。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 [12]。

3.2.2 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 [13] [14]。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 [2]。しかし、攻撃者はあらゆ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 などの Weak PUF は Controlled PUF として実装されることが望ましい。

4. PUF の問題

4.1 PUF への攻撃

4.1.1 モデリング攻撃

モデリング攻撃とは、PUF から CRPs やサイドチャネルなどの情報を取得して、それを用いて PUF のクローンとなる関数を生成する攻撃である。2.3 節で紹介したように PUF をセキュリティの要素として使うためには、あるチャレンジに対応するレスポンスが推定されないことが重要である。

3.1.2 節 a) の Arbiter PUF は導入当初から、モデリング攻撃を受けやすいことが認識されていた [3] [7]。これは、PUF の再現性を高めるために Arbiter PUF のチャレンジとレスポンスの間の依存関係の複雑さが軽減されたためである。とはいえ、Arbiter PUF 以外の PUF も機械学習の発展により、モデリング攻撃の研究が多数存在する。

モデリング攻撃は PUF に対する攻撃として最も主流であり、現在に至るまで多くの結果が報告されている。今回、モデリング攻撃をするにあたってどの PUF 情報を利用したかによって、モデリング攻撃の分類を行う。

a) CRPs の取得による攻撃

取得した CRPs を機械学習を用いて学習することで、PUF の近似となる関数を取得する攻撃である。b)、4.1.2 節で紹介する攻撃手法と違い、電磁波を測定する装置や対象の機器に接触する必要がないため、解析難易度は比較的低いと考えられている [16]。したがって、モデリング攻撃の中ではこの攻撃手法が主流であると考えられる。

調査したところ、この攻撃手法の対象となる PUF は Arbiter PUF [17]~[24] と RO PUF [16], [17], [25] をベースにした PUF に多く確認した。これは、これらの PUF は一般的な使い方では Strong PUF に分類され、CRPs の空間が広く Uncontrolled PUF として使用されるため機械学習を行いやすいためであると考えられる。また、機械学習アルゴリズムの発展により、少ない CRPs でモデリング攻撃を行う研究もなされている [16]。対策としては、Strong PUF に機械学習によるクローン生成が難しい Weak PUF を組み合わせたマルチ PUF [20], [22] や改良された PUF [24] を構築することで CRPs の規則性をなくすアプローチ

がとられている。

b) サイドチャネル情報による攻撃

攻撃者は消費電力や漏洩する電磁波を観測することで PUF 内部の情報を取得し、それを基にモデリング攻撃を行うことも可能である。

Controlled Arbiter PUF は a) のような CRPs の機械学習による攻撃には耐性があると考えられているが、消費電力を測定することで得た情報を元に機械学習することでモデリング攻撃が可能であると指摘されている [26]。また、RO PUF の漏洩電磁波を用いた手法 [27]～[29] もいくつか提案されている。

4.1.2 リバース・エンジニアリングによる攻撃

PUF は電源投入後にしか鍵が顕在しないため、電源オフ時に行う静的リバース・エンジニアリングに耐性がある。しかし、

5. ま と め

文 献

- [1] Gigazine, “世界的な半導体不足によって偽造チップが広がっている,” <https://gigazine.net/news/20210615-chip-shortages-lead-counterfeit/>, 参照 July 18, 2021.
- [2] 菅原健, “暗号ハードウェアの研究開発動向: フィジカリー・アンクロナブル・ファンクション,” 金融研究, vol.39, no.4, pp.25-54, Oct. 2020.
- [3] R. Maes, Physically Unclonable Functions: Properties, Springer, Berlin, Heidelberg, 2013. (DOI:10.1007/978-3-642-41395-7_3)
- [4] P.S. Ravikanth, “Physical One-Way Functions,” PhD thesis, Massachusetts Institute of Technology, March 2001.
- [5] B. Gassend, D. Clarke, M. van Dijk, S. Devadas, “Silicon physical random functions,” CCS’02: Proceedings of the 9th ACM conference on Computer and communications security, pp.148-160, November 2002. (DOI: 10.1145/586110.586132)
- [6] 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)
- [7] D. Lim, “Extracting Secret Keys from Integrated Circuits,” Master’s Thesis, Massachusetts Institute of Technology, March 2004.
- [8] 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.
- [9] 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)
- [10] J. Guajardo, S.S. Kumar, G.J. 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 Computer Science, vol 4727, Springer-Verlag, pp. 63–80, 2007. (DOI: 10.1007/978-3-540-74735-2_5)
- [11] D. E. Holcomb, W. P. Burtson, 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.)
- [12] 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.
- [13] 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)
- [14] 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)
- [15] 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)
- [16] 野崎佑典, 梅田大知, 竹本修, 吉川雅弥, “リングオシレータ PUF に対する遺伝的アルゴリズムを用いたハイブリッドモデリング解析とその評価,” 電気学会論文誌 C (電子・情報・システム部門誌), 140 巻, 12 号, p. 1307-1315, Dec. 2020. (DOI: 10.1541/ieej.iss.140.130)
- [17] U. Rührmair et al., “PUF Modeling Attacks on Simulated and Silicon Data,” in IEEE Transactions on Information Forensics and Security, vol. 8, no. 11, pp. 1876-1891, Nov. 2013. doi: 10.1109/TIFS.2013.2279798.
- [18] J. Ye, Y. Hu and X. Li, “RPUF: Physical Unclonable Function with Randomized Challenge to resist modeling attack,” 2016 IEEE Asian Hardware-Oriented Security and Trust (AsianHOST), pp. 1-6, Dec. 2016. (Doi: 10.1109/AsianHOST.2016.7835567)
- [19] C. Gu, C. H. Chang, W. Liu, S. Yu, Q. Ma and M. O’neill, “A Modeling Attack Resistant Deception Technique for Securing PUF based Authentication,” 2019 Asian Hardware Oriented Security and Trust Symposium (AsianHOST), pp. 1-6, Dec. 2019. (Doi: 10.1109/Asian-HOST47458.2019.9006710)
- [20] Q. Ma, C. Gu, N. Hanley, C. Wang, W. Liu and M. O’Neill, “A machine learning attack resistant multi-PUF design on FPGA,” 2018 23rd Asia and South Pacific Design Automation Conference (ASP-DAC), pp. 97-104, Jan. 2018. (doi: 10.1109/ASPDAC.2018.8297289)
- [21] T. Kroeger, W. Cheng, S. Guilley, J. -L. Danger and N. Karimi, “Effect of Aging on PUF Modeling Attacks based on Power Side-Channel Observations,” 2020 Design, Automation & Test in Europe Conference & Exhibition (DATE), pp. 454-459, March 2020. doi: 10.23919/DATE48585.2020.9116428.
- [22] Y. Cui, C. Gu, Q. Ma, Y. Fang, C. Wang, M. O’Neill, and W. Liu, “Lightweight Modeling Attack-Resistant Multiplexer-Based Multi-PUF (MMPUF) Design on FPGA,” Electronics, vol. 9, no. 5, p. 815, May 2020.
- [23] M. Ebrahimabadi, M. Younis, W. Lalouani and N. Karimi, “A Novel Modeling-Attack Resilient Arbiter-PUF Design,” 2021 34th International Conference on VLSI Design and 2021 20th International Conference on Embedded Systems (VLSID), pp. 123-128, Feb. 2021. doi: 10.1109/VLSID51830.2021.00026.
- [24] E. Dubrova, O. Näsund, B. Degen, A. Gawell and Y. Yu, “CRC-PUF: A Machine Learning Attack Resistant Lightweight PUF Construction,” 2019 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), pp. 264-271, June 2019. doi: 10.1109/EuroSPW.2019.00036.
- [25] Q. Wang, M. Gao, and G. Qu, “A Machine Learning Attack Resistant Dual-mode PUF,” In Proceedings of the 2018 on Great Lakes Symposium on VLSI (GLSVLSI ’18), Association for Computing Machinery, pp.177–182, May 2018.
- [26] G.T. Becker, R. Kumar, “Active and Passive Side-Channel Attacks on Delay Based PUF Designs,” IACR Cryptology ePrint Archive, vol. 2014, pp.287, 2014.
- [27] Y. Cao, X. Zhao, W. Ye, Q. Han, and X. Pan, “A Compact and Low Power RO PUF with High Resilience to the EM Side-Channel Attack and the SVM Modelling Attack of Wireless Sensor Networks,” Sensors, vol. 18, no. 2, p. 322, Jan. 2018.
- [28] M. Shiozaki, T. Fujino, “Simple electromagnetic analysis attack based on geometric leak on ASIC implementation of ring-oscillator PUF,” J Cryptogr Eng, Sep. 2020.
- [29] D. Merli, D. Schuster, F. Stumpf, G. Sigl, “Semi-invasive EM attack on FPGA RO PUFs and countermeasures,” Association for Computing Machinery, New York, NY, USA, 2011.