サーベイ論文

PUF についてのサーベイ論文（仮）

岡野　舞子†

Survey paper of PUF()

Maiko OKANO†

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

1. はじめに

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．この技術は，集積回路の

2.2 歴　　史

2.2.1 物理的一方向関数（POWF）

2.2.2 半導体製の PUF

2.3 PUF の動作

2.3.1 個　　体

2.3.2 チャレンジ

2.3.3 試行とレスポンス

2.4 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 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．

2.4.1 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．

2.4.2 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．

DOI:10.14923/transfunj.???????????

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．

2.4.3 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．

2.4.4 予測困難性

2.4.5 一 方 向 性

2.4.6 耐タンパー性

3. PUF の分類

4. 問題点や攻撃

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

Abstract

Key words Physically Unclonable Function