

PUF についてのサーベイ論文（仮）

あらまし フィジカリー・アンクロナブル・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。

キーワード 暗号ハードウェア、ハードウェアセキュリティ、PUF

1. ま え が き

2. PUF の性質

2.1 PUF の名前の由来

2.2 一連の流れ

2.2.1 個 体

2.2.2 チャレンジ

2.2.3 試行とレスポンス

2.3 PUF に求められる性質

特にセキュリティの観点から重要なものとしては、再現性、ユニーク性、耐クロン性の3つが挙げられる。

2.3.1 再 現 性

2.3.2 ユニーク性

2.3.3 耐クロン性

他にもいくつかあるので紹介する。

2.3.4 予測困難性

2.3.5 一方向性

2.3.6 耐タンパー性

3. PUF の歴史

3.1 物理的一方向関数（POWF）

3.2 半導体製の PUF

3.3 アービター PUF

PUF の分類 PUF に対する攻撃

文 献

[1]

付 録

1.

Abstract

Key words Physically Unclonable Function