ISS-P-95

物理特性の変更が可能な RO-PUF

川述　優†　　町田　卓謙††　　崎山　一男††
† 電気通信大学 電気通信学部　†† 電気通信大学 大学院情報理工学研究科

1. はじめに

近年，セキュリティ技術として PUF(Physically Unclonable Function)の研究が行われている．PUF とは，製造ばらつきが複製・再現困難であることを利用し，物理的に複製困難な ID の生成を行う技術である．

しかし，既存 PUF では出力が所望のばらつきを示さない場合，PUF 回路の再設計を行う必要があった．そこで本研究は PUF の一種である RO(Ring Oscillator)-PUF [1] に対し，設計後に回路の一部分を変更可能な構成を設けることで，出力を変化させることが容易な RO-PUF の実現を目標とした．

2. 関連研究

RO は論理素子のインバータを奇数個リング状に接続した発振回路である．同設計の複数の RO を用意したとき，各 RO は実際に使用している配線，素子が異なることから，配線遅延，素子遅延が異なる．そのため発振周波数が異なる．RO-PUF は，任意の 2 つの RO の発振周波数の高低を比較することで，0 or 1 を出力する[2].

3. 本研究で提案する RO-PUF

本研究で提案する RO-PUF(以下，提案 RO-PUF)の構成を図 1 に示す．発振周波数のばらつきは素子や配線の物理特性に依存している．そのため既存の RO-PUF では出力を変化させる際，LSI 内の利用するインバータの個数や配置の変更が必要である．

提案 RO-PUF では，発振周波数のばらつきを LSI 内の素子や配線だけではなく，ボード上の配線やジャンパーにも依存させることで，出力を変化させることを容易にした．

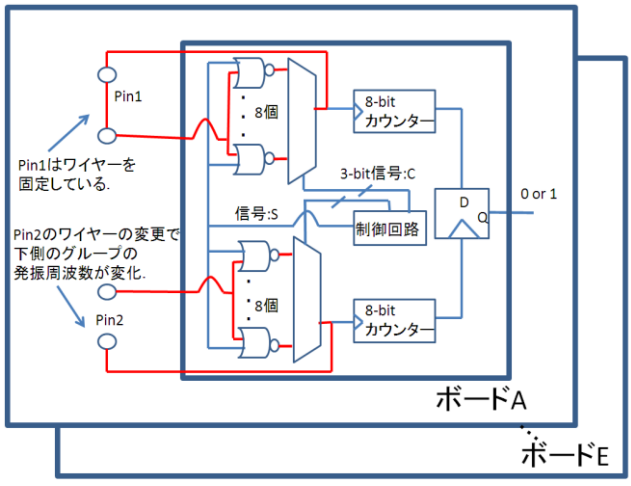

図 1：提案する RO-PUF の構成

4. 実験方法

8 個の RO を 1 組とし，2 組の RO の組を FPGA 上に実装した．各組から1つずつ RO を選び，全 64 通りの比較を行い，64-bit の出力を得た．この実験をジャンパーとして選んだ 5 本のワイヤーに対して行った．なお，ボードは A～E の 5 枚を用いた．

5. 実験結果

表1にボード A でワイヤー1～5 を用いて得られた出力を示す．また，出力は 16 進数表記で示している．

表 1:ボード A でワイヤー1～5 を用いた時の各出力

ワイヤー	64-bit の出力							
1	38	3A	18	38	38	3A	38	38
2	3A	3A	38	3A	3A	BB	3A	3A
3	3A	3A	38	3A	3A	BA	3A	3A
4	BA	BB	3A	BA	3A	BF	BF	BA
5	3A	BA	38	3A	3A	BF	BA	BA

表1から，ワイヤーの変更で出力が変化していることが判る．出力間の最大 HD は 18-bit，最低 HD は 1-bit，平均 HD は 8-bit である．

しかし，ワイヤーの変更で出力が変化しないビットも確認出来る．また，ボード B～E でも同じ様な傾向の結果が得られたことから，設計に改善の余地があることが判る．

7. まとめ

セキュリティ技術の一つである PUF では，出力の変更には再設計が必要という問題点がある．これに対し，設計後に回路構成を変更可能とすることで，出力を変化させることが可能な RO-PUF の実現を目標とした研究であった．結果としてワイヤーの変更が出力を変化させていることが判った．しかし，変化を示さないビットも各ボードで確認できたことから，改善の余地があることが判った．

今後の課題として，再現性の評価，出力のばらつき向上に向けた考察が挙げられる．

参考文献

[1] Blaise Gassend, Dwaine E. Clarke, Marten van Dijk, Srinivas Devadas, “Silicon Physical Random Functions,” In ACM Conference on Computer and Communications Security-CCS 2002, pp.148-160, 2002.

[2] G. Edward Suh, Srinivas Devadas, “Physical Unclonable Functions for Device Authentication and Secret Key Generation, ” In Proceedings of the 44th annual Design Automation Conference, DAC’07, pp.9-14, 2007.