回路構造の変化を捉えるインピーダンス解析

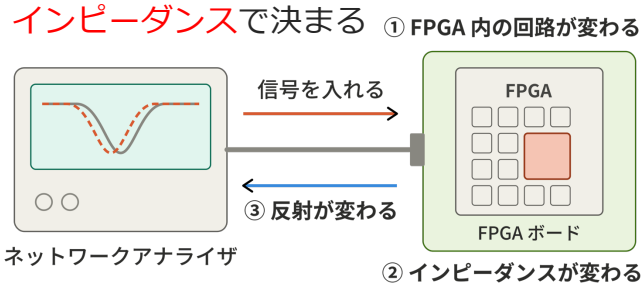
崎山·李·宮原 研究室

インピーダンス解析

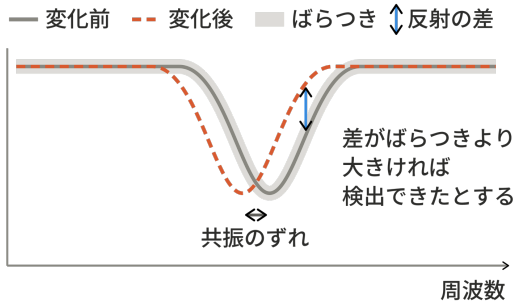
- チップの電源に信号を入れ、返ってくる反射から内部の様子を調べる手法
- 回路の構造（改ざん・ハードウェアトロイ）や、回路が持つ値（秘密鍵）まで見分けられることが報告されている [1, 2]

反射の測定

- 入力した信号に対する反射は、チップのインピーダンスで決まる

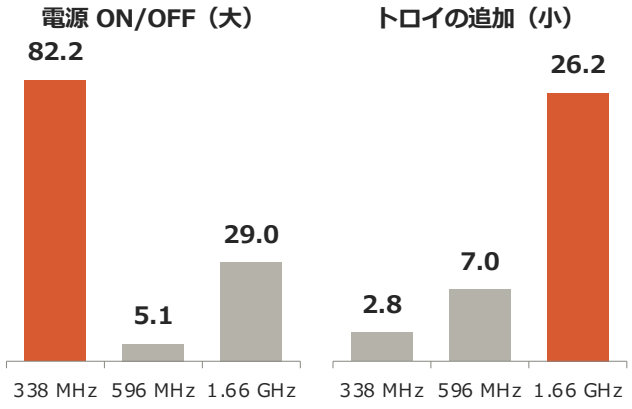


- 共振する周波数で反射に谷ができ、回路が変わると谷の位置や深さが変わる



先行研究

- 変化が大きいと低い周波数、小さいと高い周波数で検出しやすい [2]
- 具体的に回路がどう変わると検出のしやすさが変化するのかは未解明

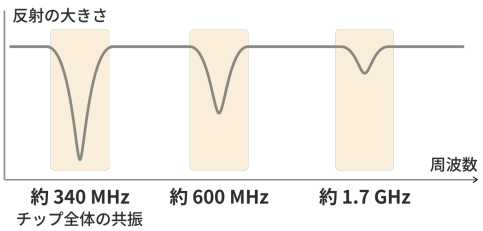


縦軸：検出のしやすさ（変化前後の差 ÷ 同じ回路どうしの差）。目盛りは左右で異なる。[2] Table 1 より作成

実験内容

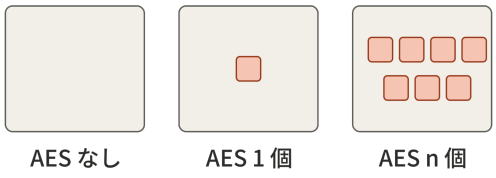
回路の量を変えると、差の大きさと見える周波数帯はどう変わるのか？

- 特定の3 つの周波数帯で、差の大きさと形を比べる



先行研究で回路の変化に敏感と報告された帯域 [2](模式図)

- AES 暗号回路の個数だけを変えた回路を比べる



変化の種類をそろえ、回路の量だけを変えることで、量と検出しやすい帯域の関係が分かる。

まとめと展望

- 回路のAES書き込みあり／なしの差は、3 帯域すべてで検出できた
- 回路の量を変えて、検出しやすい帯域がどう変わるか、また差を決めるのが変化の「量」か「回路全体に対する割合」かを明らかにする。

[1] S. K. Monfared, T. Mosavirik, S. Tajik, “LeakyOhm: Secret bits extraction using impedance analysis,” Cryptology ePrint Archive, 2023/693.
[2] T. Mosavirik, S. K. Monfared, M. S. Safa, S. Tajik, “Silicon Echoes: Non-invasive trojan and tamper detection using frequency-selective impedance analysis,” Cryptology ePrint Archive, 2023/075.

製作者:疋出 真翔(李研究室)