SCIS 2022 2022 Symposium on
Cryptography and Information Security
Osaka, Japan & Online, Jan. 18 – 21, 2022
The Institute of Electronics,
Information and Communication Engineers

動的 FPGA 電源電流の RTL 解析に基づく電力解析攻撃への耐性予測
Power Analysis Attack Resistance Prediction Based on RTL Calculation of Dynamic FPGA Power Current

日室　雅貴 *　　五百旗頭　健吾 *　　豊田 啓孝 *
Masaki Himuro　　Kengo Iokibe　　Yoshitaka Toyota

キーワード サイドチャネル攻撃，相関電力解析，情報漏洩予測，AES，FPGA，レジスタ転送レベル

あらまし

筆者らは IC 外部の電源配線上における電力解析攻撃耐性を予測することを目的にしている．攻撃予測のためには基板上で観測される漏洩電圧波形をシミュレーションする必要があり，その波形は IC のスイッチング動作に起因する動的電源電流と IC から測定点までの伝達インピーダンスの畳み込み積分によって得られる．そのため，動的電流と伝達インピーダンスを正確にシミュレーションすることが求められる．

暗号回路の動的電源電流について，ゲートレベルのシミュレーションに基づいた高分解能な見積もりが行われている [1]．ただし，IC のオンチップ容量とパッケージインダクタンスの効果により、IC 外部に漏洩する高次高調波成分が減衰することが理論的に分かる．それは実験結果とも一致している。そこで，本稿では RTL でシミュレーションしたトグルレートに基づいて各クロックにおける動的電流の総和を計算 [2] し，三角波パルスに変換する．また，AES 処理のターゲットラウンドのみ電流を見積もり，その統計量に従い他ラウンドの三角波パルスの振幅をランダムに変化させた．それにより、RTL 解析の時間を短縮した (図 1)．

今回，FPGA 搭載基板に対する相関電力解析攻撃をシミュレーションした (図 2)．漏洩波形の実測と伝達インピーダンスは文献 [3] の結果を使用した．また，シミュレーションした電圧波形に対して実測したノイズフロアと同じ標準偏差の乱数を重畳した．この結果から，RTL シミュレーションに基づいて取得した三角波電流により，

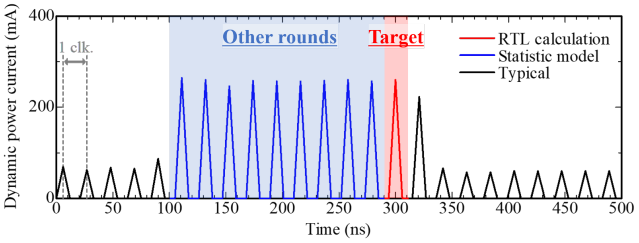
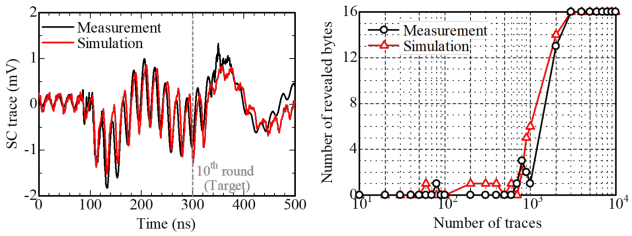


図 1: 動的電源電流シミュレーション



(a) AES 処理時の漏洩電圧波形　　(b) 相関電力解析

図 2: シミュレーション結果

基板上で観測される漏洩波形と電力解析攻撃結果を十分な精度で予測できること示した．

参考文献

[1] A. Tsukioka, et al., IEEE Letters on EMC Practice and Applications, vol. 1, no. 4, pp. 83–87, 2019.

[2] Y. Yano, et al., IEICE Trans, Vol. E104-B, No. 2, pp. 178-186, 2021.

[3] K. Iokibe, et al., ”A Study for Low Calculation Cost Side-Channel Resistance Prediction Based on Transfer Impedance of Leakage Path,” APEMC 2021, 2021.

* 岡山大学大学院自然科学研究科，〒 700-8530 岡山市北区津島中 3-1-1，The Graduate School of Okayama University, 3-1-1 Tsushima-naka, Kita-ku, Okayama, 700-8530 Japan, pw9e5u6l@s.okayama-u.ac.jp