Copyright ©2022 The Institute of Electronics,
Information and Communication Engineers

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

FPGA 実装した AES 回路の模擬スイッチング電流波形に基づくサイドチャネル情報漏洩帯域の考察

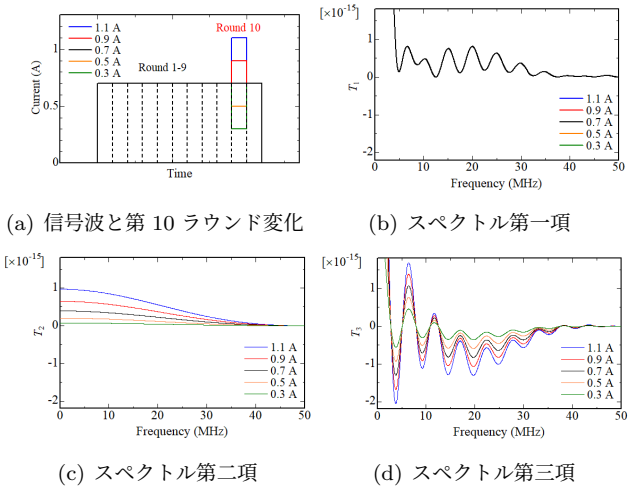
A Study on Side-Channel Information Leaking Band Based on Simulated Switching Current Waveform of AES Circuit Implemented on FPGA

下田　洸平 *　日室　雅貴 †　五百旗頭　健吾 †　豊田　啓孝 †
Kohei Shimoda　Masaki Himuro　Kengo Iokibe　Yoshitaka Toyota

キーワード サイドチャネル攻撃　AES　FPGA 相関電力解析

あらまし

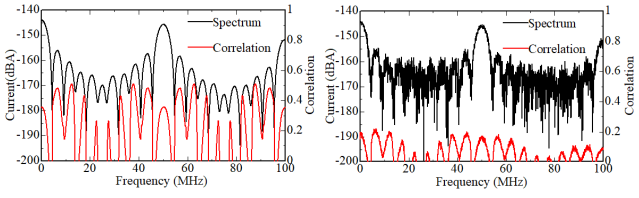
サイドチャネル情報の漏洩帯域について，暗号デバイスのクロック周波数付近の帯域で情報漏洩が起きることが報告されている [1][2]。本稿ではスイッチング電流のスペクトルの理論式を導出し，サイドチャネル情報漏洩帯域を考察した。FPGA 実装の AES 回路で発生するスイッチング電流波形を，11 個の単発三角波パルスで模擬した。振幅一定の三角波周期パルスを搬送波，HD 変化に対応して変化する方形波パルス列を信号波とする振幅変調波と考え，サイドチャネル情報である HD の時間変化を表す信号波のスペクトル理論式の導出を行った。AES の第 9-10 ラウンド間のハミング距離を漏洩モデルとした CPA を想定し，11 個のパルスのうち 10 個目の振幅 (第 10 ラウンド振幅) のみが変化する場合の信号波 (図 1(a)) のスペクトル $|F(\omega)|^2$ を導出した。$|F(\omega)|^2$ は第 10 ラウンド振幅の変化に依存しない第一項と，依存する第二，三項の足し合わせで表すことができる。図 1(b), 図 1(c), 図 1(d) より，第 10 ラウンドの振幅が変化すると 0-50 MHz の全帯域でスペクトルレベルが変動している。従って，理論的にはサイドチャネル情報はすべての高調波のサイドローブに含まれる。しかし，実測では測定系のノイズや周辺ノイズの影響により，スペクトルレベルが低い高周波やサイドローブでスペクトルレベルが低い帯域 (25 MHz, 75 MHz 付近) で相関係数が低下する (図 2)。



(a) 信号波と第 10 ラウンド変化　(b) スペクトル第一項

(c) スペクトル第二項　(d) スペクトル第三項

図 1: (a) 模擬した信号波と (b)(c)(d) そのスペクトル



(a) ノイズなし　(b) ノイズあり

図 2: 模擬波形のスペクトルと周波数領域の CPA 結果

参考文献

[1] 河田他, 信学技報, EMCJ2017-101, pp. 77-81.

[2] Sugawara *et. al.*, EMC'09/Kyoto, 2009, 21P1-6.

* 岡山大学　工学部　〒 700-8530　岡山市北区津島中 3-1-1 Faculty of Engineering, Okayama University, 3-1-1 Tsushima-naka, Kita-ku, Okayama, 700-8530, Japan
† 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 Graduate School of Natural Science and Technology, Okayama University, 3-1-1 Tsushima-naka, Kita-ku, Okayama, 700-8530, Japan