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

電磁波サイドチャネルとスクリーミングチャネルの同時収集攻撃の検証
Attack Verification Using Simultaneous Measurements From Electromagnetic Side-Channel and Screaming Channel

松川 侑生 * 杉本 悠馬 * 菅原 健 * 崎山 一男 * 李 陽 *
Yuki Matsukawa Yuma Sugimoto Takeshi Sugawara Kazuo Sakiyama Yang Li

キーワード サイドチャネル攻撃, 秘密鍵復元, 相関攻撃, SoC, AES,

1 はじめに

暗号モジュールの解析手法の一つとして，実装上の脆弱性を利用した実装攻撃が挙げられる．その中でも近年，暗号化中に発生するサイドチャネル情報（処理時間や消費電力，漏洩電磁波など）を利用したサイドチャネル攻撃が盛んに研究されている．本研究で注目するのは電磁波チャネルとスクリーミングチャネルである．両者の漏洩の原因はどちらも漏洩電磁波にあるが，漏洩モデルは異なる．両者が異なる情報が漏洩しているならば，同時に収集し攻撃することで鍵復元効率を改善させることができる．

本発表では，BLE Nano V2 をターゲットとした波形の同時収集環境を構築し，2 つのサイドチャネルの独立収集時と同時収集時の波形の歪みを検証した．また，スクリーミングチャネルの Sbox 入力の MSB4bit に注目した簡易的な漏洩モデルと相関同時攻撃を提案し，擬似波形と実際に収集した波形でそれぞれ検証した．

2 スクリーミングチャネル

スクリーミングチャネル (SC) とは，遠距離でも観測可能なサイドチャネル情報であり，Camurati らが tinyAES や mbedTLS に対して鍵復元を達成した [1]．SC の漏洩 [1, 2] は，ミックストシグナルチップという，一つのシリコンダイ上にデジタル回路とアナログ回路を搭載した SoC（System on a chip）で発生する．具体的には BLE Nano V2 を使用していた．遠距離でも漏洩を獲得できる原因は，デジタル回路部で発生する漏洩電磁波が無線通信部であるアナログ回路に混入するためである．SC の漏洩特性は，EM と違い，漏洩の特性をハミングウェイトモデルでは表現することができない．この漏洩の特性の違いを Camurati らは両者のサイドチャネル情報を単独で収集し示した．

3 同時収集攻撃

EM と SC が互いに異なる漏洩情報を持つならば，両者を同時収集し，攻撃に適用することで容易に鍵復元を達成できる．我々は Camurati らと同様のターゲットを用いて，同時収集攻撃のために波形の同時収集環境の構築を行った．また，EM と SC の独立収集時と同時収集時の波形の違い，同時収集攻撃の検証を行った．同時収集でも鍵復元が困難になるような歪みは生じず，相関同時攻撃により擬似波形と実際に収集した波形，共にターゲットへのアクセス回数を削減できた．

参考文献

[1] Giovanni Camurati, Sebastian Poeplau, Marius Muench, Tom Hayes, and Aurélien Francillon. Screaming channels: When electromagnetic side channels meet radio transceivers. In *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, pp. 163–177, 2018.

[2] Giovanni Camurati, Aurélien Francillon, and François-Xavier Standaert. Understanding screaming channels: From a detailed analysis to improved attacks. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, pp. 358–401, 2020.

* 電気通信大学, 東京都調布市調布ヶ丘 1-5-1, Faculty of Informaticsand Engineering, The University of Electro-Communications, 1-5-1 Chofu-shi, Tokyo 182-8585, Japan, y.matsukawa@uec.ac.jp