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

パイプライン化されたAES S-boxへのフォールト攻撃に対する安全性評価
Security Evaluation against Fault Attacks on Pipelined AES S-box

平田 遼 * 宮原 大輝 * 李 陽 * 三浦 典之 † 崎山 一男 *
Haruka Hirata Daiki Miyahara Yang Li Noriyuki Miura Kazuo Sakiyama

キーワード 故障利用解析, AES, S-box, Masks and Macs

あらまし

暗号ハードウェアに対する物理攻撃が驚異とされており，攻撃への対策手法の安全性検証は重要である．物理攻撃には，デバイスの物理特性を観察し秘密情報を得るPassive 型の攻撃や，攻撃者が暗号デバイスに影響を与えるActive 型の攻撃がある．Passive 型と Active 型を組み合わせた攻撃も報告されており，これらの攻撃への対策としてCHES2019 でM&M（Masks and Macs）という手法が提案された [1]．SCIS2021 では，M&M により対策されたAES 暗号ハードウェアに対するDFA 攻撃を検討し，実験により鍵復元が可能であることを示した [2]．本稿では，パイプライン化されたS-box に対するフォールト攻撃の可能性を議論する．また，フォールト攻撃の検証として，M&M により対策されたAES 暗号を実装したASIC[3] を用いた実験を行う．

参考文献

[1] De Meyer, L., Arribas, V., Nikova, S., Nikov, V., & Rijmen, V. (2018). M&M: Masks and Macs against Physical Attacks. IACR Transactions on Cryptographic Hardware and Embedded Systems, 2019(1), 25–50. https://doi.org/10.13154/tches.v2019.i1.25-50

[2] 平田遼，羽田野凌太，李陽，三浦典之，崎山一男，“M&M により対策されたAES 暗号ハードウェアに対するサイドチャネル攻撃，” 2021 年暗号と情報セキュリティシンポジウム (SCIS2021), (Jan., 2021)

[3] 平田遼, 羽田野凌太, 李陽, 三浦典之, Svetla Nikova, 崎山一男, “M&M により対策されたAES ハードウェアの安全性評価について，” IEICE2020 年ソサイエティ大会, (Sep., 2020).

* 電気通信大学, 東京都調布市調布ケ丘 1 丁目 5-1, The University of Electro-Communications, 1-5-1 Chofugaoka, Chofu, Tokyo 182-8585, Japan
† 大阪大学, 大阪府吹田市山田丘 1 番 1 号, Osaka University, 1-1 Yamadaoka, Suita, Osaka, 565-0871, Japan