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

ハードウェア実装 AES に対する Multi-bit ラベルを用いたノンプロファイリング深層学習サイドチャネル攻撃
Non-Profiling Deep Learning Side-Channel Attacks using Multi-bit label against Hardware-Implemented AES

福田 悠太 * 吉田 康太 * 黒田 訓宏 * 藤野 毅 *
Yuta Fukuda Kota Yoshida Kunihiro Kuroda Takeshi Fujino

キーワード 差分深層学習攻撃，ノンプロファイリング攻撃，ハードウェア実装 AES

あらまし

近年，暗号回路に対する深層学習を用いたサイドチャネル攻撃手法が活発に議論されている．深層学習を用いたサイドチャネル攻撃はプロファイリング攻撃が主として報告されてきたが，2019 年，Timon によりノンプロファイリング攻撃として差分深層学習解析 (Differential Deep-Learning Analysis: DDLA) が提案された [1]．この攻撃手法は，各鍵候補ごとに深層学習モデルを学習し，loss や accuracy といった指標を比較することで秘密鍵を明らかにする．Timon は，暗号回路動作中の中間値の 1bit(LSB または MSB) に着目し，ソフトウェア実装された AES に対して攻撃を行った．一方で我々がハードウェア実装にこの手法を適用したところ，HD リークが観察しにくいレジスタが存在することから全ての部分鍵を明らかにすることができなかった．

本稿では，この問題を解決するために，図 1 のように，1 bit のみに着目せずにすべての bit に着目する multi-bit DDLA を提案する．実験では，ASIC 実装された RSM-AES に対して multi-bit DDLA を評価した．図 2 のように，すべての部分鍵を窃取できたことを報告する．

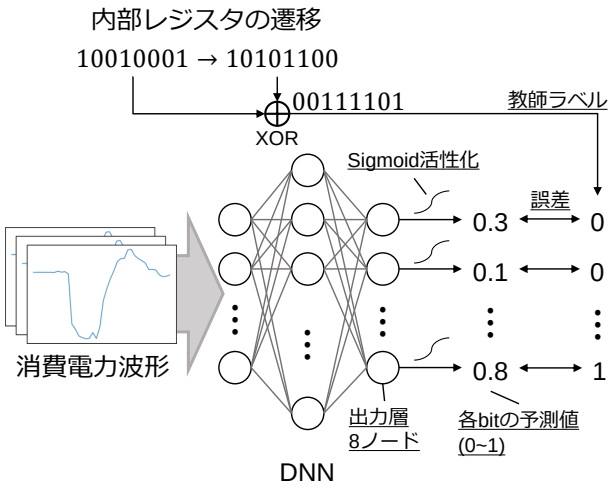

図 1: Multi-bit DDLA(提案手法) の処理フロー

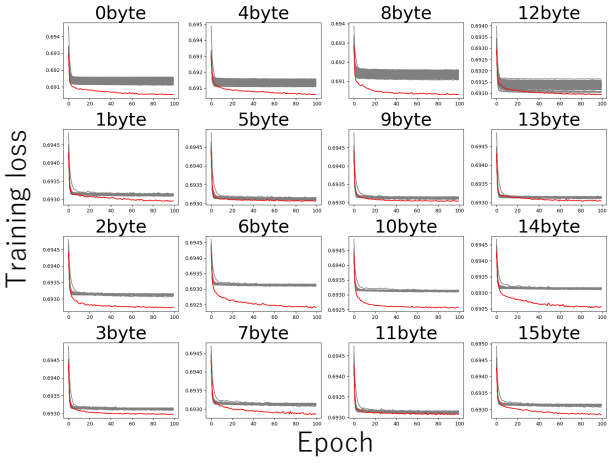

図 2: ASIC 実装 RSM-AES に対する攻撃結果

参考文献

[1] Timon B, “Non-Profiled Deep Learning-based Side-Channel attacks with Sensitivity Analysis”, IACR Transactions on Cryptographic Hardware and Embedded Systems, 2019(2), 107–131.

* 立命館大学, 〒 525-8577, 滋賀県草津市野路東 1-1-1, Ritsumeikan University, 1-1-1 Nojihigashi, Kusatsu, Shiga, Japan