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

プロービング攻撃による漏洩情報を用いたAES鍵復元アルゴリズムの改良
An Improved AES Key Recovery Algorithm Using Key Leakage by Probing Attacks

植村 友紀 * 渡邉 洋平 *† 李 陽 * 三浦 典之 ‡
Tomoki Uemura Yohei Watanabe Yang Li Noriyuki Miura
岩本 貢 * 崎山 一男 * 太田 和夫 *†
Mitsugu Iwamoto Kazuo Sakiyama Kazuo Ohta

キーワード 漏洩鍵，AES鍵スケジュール，cold boot attack，リーケージセンサ

あらまし

ISITA2020において，AES暗号に対するプロービング攻撃の脅威を評価するため，Uemuraら [1] はプロービング攻撃による漏洩情報を用いたAES鍵復元アルゴリズムを提案した．本研究では，Uemuraらの鍵復元アルゴリズムでは漏洩情報を十分に利用できていないことを指摘した上で，すべての漏洩情報を利用した鍵復元アルゴリズムを提案する．具体的には，Uemuraらのアルゴリズムにおける拡大フェイズ，枝刈りフェイズに加え，新たに検査フェイズを設けることで，漏洩情報を全て攻撃に用いるよう改良する．

Uemuraらのアルゴリズムでは，拡大フェイズと枝刈りフェイズを繰り返すことで8ラウンド鍵を復元し，直ちにAES秘密鍵を復元していたが，アルゴリズムの構造上，これらのフェイズで利用されない漏洩情報が存在していた．提案アルゴリズムで導入する検査フェイズでは，8ラウンド鍵を復元した後，すべての鍵スケジュール（秘密鍵と1–10ラウンド鍵）を復元し，拡大フェイズや枝刈りフェイズで利用していない漏洩情報と矛盾がないかどうかを検査する．その結果，より効果的な鍵復元アルゴリズムを実現することができ，実装実験を通じてプロービング攻撃の脅威をより正確に評価することができた．たとえば，鍵の漏洩割合が11%の場合において，Uemuraらの実験ではほぼ0%の復元成功確率だったことに対し，本実験では約40%の確率で復元に成功した．

参考文献

[1] T. Uemura, Y. Watanabe, Y. Li, N. Miura, M. Iwamoto, K. Sakiyama, and K. Ohta, “A key recovery algorithm using random key leakage from AES key schedule,” in *2020 International Symposium on Information Theory and its Applications (ISITA2020)*, (Kapolei, USA), Oct. 2020.

* 電気通信大学, 〒182–8585 東京都調布市調布ヶ丘 1–5–1, The University of Electro-Communications, 1–5–1 Chofugaoka, Chofu, Tokyo, 182–8585, Japan
† 国立研究開発法人 産業技術総合研究所, 〒135–0064 東京都江東区青海 2–4–7 National Institute of Advanced Industrial Science and Technology (AIST) 2–3–26 Aomi, Koto-Ku, Tokyo, 135–0064, Japan
‡ 大阪大学, 〒565–0871 大阪府吹田市山田丘 1–1, Osaka University, 1–1 Yamadaoka, Suita, Osaka, 565–0871 Japan