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

RAMBleed による OpenSSL 暗号鍵導出
Derivation of OpenSSL Cryptographic Key with RAMBleed

冨田 千尋 * 瀧田 愼 † 福島 和英 ‡ 仲野 有登 ‡
Chihiro Tomita Makoto Takita Kazuhide Fukushima Yuto Nakano
白石 善明 * 森井 昌克 *
Yoshiaki Shiraishi Masakatu Morii

キーワード Rowhammer, RAMBleed, サイドチャネル攻撃, OpenSSL, 秘密鍵

あらまし

半導体の高密度化が進み，DRAM 内のあるセルへのアクセスにより別のセルに影響を与え，意図しないビット反転を引き起こす Rowhammer[1] と呼ばれる攻撃が発見された．また，Kwong らは，Rowhammer によるビット反転を観察し，任意のメモリ位置に秘密情報を誘導することで，アクセス権限のない情報の一部を高い精度で回復する RAMBleed 呼ばれるサイドチャネル攻撃を提案した [2]

本論文では RAMBleed を利用して，OpenSSL で用いられる秘密鍵を回復する手法を提案する．秘密鍵はサーバのみが保持し，管理者権限なしにその情報を読み取ることができないため，第三者がその情報を直接取得することは不可能である．筆者らは，既に OpenSSL により SSL/TLS 通信に対応した Apache Web サーバの動作を解析し，RSA 秘密鍵を構成する二つの素数 p, q を RAMBleed により管理者権限なしで間接的に読み取ることができる可能性を明らかにしている [3]．本論文では，先の筆者らの手法を発展させ，p, q を実際に回復する具体的な手法を与える．今まで OpenSSL に対して，実際に利用されている現実的なパラメータおよび環境において RSA 秘密鍵を導出する手法は提案されていなかった．本手法は RAMBleed に対して対策が取られていない DRAM を利用したサーバ上で，RSA 方式を採用する OpenSSL に対して一般的に適用可能であり，OpenSSL に対する大きな脅威が明らかとなった．

実際に提案手法を用いて，2048 ビットの RSA 秘密鍵を構成する 1024 ビットの p, q を RAMBleed により読み取り，それを元に秘密鍵を復元する実験を行った．実験の結果，RAMBleed により p, q それぞれの下位 570 ビットを約 93%の 精度で読み取ることができた．また，RSA 暗号に対する暗号鍵導出攻撃 [4][5] を組み合わせることで，読み取り結果に含まれる誤りを訂正し，得られた p, q それぞれの下位 570 ビットから秘密鍵の全てのビット値を復元することに成功した．

* 神戸大学大学院工学研究科, Kobe University
† 兵庫県立大学大学院情報科学研究科, University of Hyogo
‡ 株式会社 KDDI 総合研究所, KDDI Research, Inc.

謝辞

本研究は、総務省の「電波資源拡大のための研究開発（JPJ000254）」における委託研究「安全な無線通信サービスのための新世代暗号技術に関する研究開発」 の成果の一部である。

参考文献

[1] Y. Kim, R. Daly, J. Kim, C. Fallin, J. Lee, D. Lee, C.Wilkerson, K. Lai, and O. Mutlu, “Flipping bits in memory without accessing them: An experimental study of DRAM disturbance errors,” ACM/IEEE 41st International Symposium on Computer Architecture, 2014, pp.361-372, 2014.

[2] A. Kwong, D. Genkin, D. Gruss and Y. Yarom,“RAMBleed: Reading Bits in Memory Without Accessing Them,”in 2020 IEEE Symposium on Security and Privacy (SP), 2020 pp. 695-711.

[3] 冨田千尋，瀧田愼，福島和英，仲野有登，白石善明，森井昌克，“RAMBleed による OpenSSL の秘密情報の回復，” CSS2021, 2021.

[4] K. G. Paterson, A. Polychroniadou, and D. L. Sibborn,“A coding-theoretic approach to recovering noisy RSA keys,” ASIACRYPT 2012. LNCS, vol. 7658, pp. 386–403. Springer, Heidelberg (2012).

[5] D. Coppersmith,“Small solutions to polynomial equations, and low exponent RSA vulnerabilities,”J. Cryptology, 10(4):233–260, 1997.