Attaque structurelle par échange contre des versions réduites d'AES-128

Rachelle Heim Boissier

rachelle.heim@uvsq.fr

Université Paris-Saclay, UVSQ, CNRS, Laboratoire de Mathématiques de Versailles, 78000, Versailles, France

AES [DR02] est l'algorithme de chiffrement symétrique le plus utilisé et par conséquent l'un des plus étudiés depuis sa standardisation par le NIST en 2000. Dans sa version la plus courante, AES-128, il comporte 10 tours. Après plus de 20 ans de cryptanalyse, les meilleures attaques par recouvrement de clé contre AES-128 atteignent 7 tours et ont des complexités en temps et en données légèrement inférieures, resp. légèrement supérieures à 2^{100} [DFJ13, BLNS18].

Dans un article de 2019, Rønjom et Bardeh proposent de nouveaux distingueurs d'AES réduit à 5 et 6 tours dits par échange [BR19]. Ces distingueurs utilisent une propriété structurelle de 4 tours d'AES mise en évidence pour la première fois par Rønjom, Bardeh et Helleseth dans un article de 2017 [RBH17]. À partir de cette propriété, nous proposons une nouvelle attaque en recouvrement de clef à clair choisi contre AES-128 réduit à 6 tours [1]. Cette attaque, comme [BR19], utilise des techniques dites par échange. Son coût est toutefois plus faible que l'ensemble des attaques utilisant la propriété de [RBH17] pour analyser 6 tours. Sa complexité en temps est proche de 2^{64} applications d'AES réduit à 6 tours. Elle nécessite par ailleurs 2^{48} couples clair/chiffré ainsi que le stockage en mémoire de 2^{52} états d'AES.

Si sa complexité demeure élevée au regard de celle des meilleures attaques contre 6 tours qui lui pré-existent, ces dernières appartiennent à des familles cryptanalytiques plus anciennes et qui, par conséquent, ont été davantage étudiées.

Rétrospectivement, il apparaît que notre attaque a une parenté étroite avec une attaque contre AES-128 réduit à 5 tours proposée par Grassi dans [Gra18] et une attaque contre AES-128 réduit à 6 tours proposée par Bar-On, Dunkelman, Keller, Ronen et Shamir dans [BDK+20]. Notre attaque a toutefois une meilleure complexité en temps que cette dernière.

Références

[BDK+20] Achiya Bar-On, Orr Dunkelman, Nathan Keller, Eyal Ronen, and Adi Shamir. Improved key recovery attacks on reduced-round AES with practical data and memory complexities. *J. Cryptol.*, 33(3) :1003–1043, 2020.

[BLNS18] Christina Boura, Virginie Lallemand, María Naya-Plasencia, and Valentin Suder. Making the impossible possible. *J. Cryptol.*, 31(1) :101–133, 2018.

1. Ce travail a été réalisé en coopération avec Henri Gilbert (ANSSI et UVSQ) et Jean-René Reinhard (ANSSI)

[BR19] Navid Ghaedi Bardeh and Sondre Rønjom. The exchange attack : How to distinguish six rounds of AES with $2^{88.2}$ chosen plaintexts. In Steven D. Galbraith and Shiho Moriai, editors, *Advances in Cryptology - ASIACRYPT 2019 - 25th International Conference on the Theory and Application of Cryptology and Information Security, Kobe, Japan, December 8-12, 2019, Proceedings, Part III*, volume 11923 of *Lecture Notes in Computer Science*, pages 347–370. Springer, 2019.

[DFJ13] Patrick Derbez, Pierre-Alain Fouque, and Jérémy Jean. Improved key recovery attacks on reduced-round AES in the single-key setting. In Thomas Johansson and Phong Q. Nguyen, editors, *Advances in Cryptology - EUROCRYPT 2013, 32nd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Athens, Greece, May 26-30, 2013. Proceedings*, volume 7881 of *Lecture Notes in Computer Science*, pages 371–387. Springer, 2013.

[DR02] Joan Daemen and Vincent Rijmen. In Springer, editor, *The Design of Rijndael : AES - The Advanced Encryption Standard*, 2002.

[Gra18] Lorenzo Grassi. Mixture differential cryptanalysis : a new approach to distinguishers and attacks on round-reduced AES. *IACR Trans. Symmetric Cryptol.*, 2018(2) :133–160, 2018.

[RBH17] Sondre Rønjom, Navid Ghaedi Bardeh, and Tor Helleseth. Yoyo tricks with AES. In Tsuyoshi Takagi and Thomas Peyrin, editors, *Advances in Cryptology - ASIACRYPT 2017 - 23rd International Conference on the Theory and Applications of Cryptology and Information Security, Hong Kong, China, December 3-7, 2017, Proceedings, Part I*, volume 10624 of *Lecture Notes in Computer Science*, pages 217–243. Springer, 2017.