Cryptanalyse Boomerang de Chiffrements par Bloc

Encadrantes: Virginie Lallemand et Marine Minier
virginie.lallemand@loria.fr, marine.minier@loria.fr

Équipe CARAMBA
Université de Lorraine, CNRS, Inria, LORIA
Nancy, France

Mots clés : Cryptographie symétrique · Chiffrement par bloc · Attaque

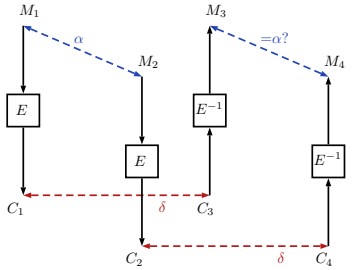
1 Contexte du Stage

La technique de cryptanalyse dite *boomerang* a été introduite en 1999 par David Wagner [Wag99] et peut être vue comme une variante de la cryptanalyse différentielle [BS91].

Au lieu d'étudier les biais dans l'apparition des couples de différences en entrée et en sortie du chiffrement E, un attaquant recherche une paire de différences (α, δ) reliant un quartet de messages par la relation :

$$E^{-1}(E(M_1) \oplus \delta) \oplus E^{-1}(E(M_1 \oplus \alpha) \oplus \delta) = \alpha,$$

comme illustré ci-contre. Plusieurs outils automatiques ont été développés pour aider un attaquant à trouver un tel distingueur boomerang ([DDV20, HBS21, BL23] pour n'en citer que quelques-uns), reposant chacun sur des hypothèses plus ou moins fortes d'indépendance.



2 Objectifs

Le ou la stagiaire commencera par s'approprier les différentes techniques de modélisation et comparera les différents outils automatiques proposés dans la littérature pour rechercher un distingueur boomerang. L'objectif sera ensuite d'adapter un de ces outils pour proposer une analyse d'un chiffrement proposé récemment (comme SAND [CFS+22] ou SKINNYee [NSS22] par exemple) et de monter une attaque boomerang sur une version réduite de celui-ci.

Une première piste intéressante pourra être de suivre les idées de [BL23] et de faire une analyse fine des opérations non-linéaires pour rendre le modèle plus précis.

Conditions du Stage. Le stage se déroulera au sein du Laboratoire d'Informatique Lorrain (le LORIA) à Nancy et sera gratifié à hauteur d'environ 473 euros par mois.

Contact. Pour candidater, contactez Virginie Lallemand et Marine Minier (voir ci-dessus) en joignant :
- un CV,
- les relevés de notes des deux dernières années,
- une liste des cours suivis lors de l'année universitaire, ainsi que les noms des responsables de ces cours.

Références

[BL23] Xavier Bonnetain and Virginie Lallemand. On boomerang attacks on quadratic feistel ciphers : New results on katan and simon. *IACR Transactions on Symmetric Cryptology*, (3) :101–145, Sep. 2023.

[BS91] Eli Biham and Adi Shamir. Differential cryptanalysis of DES-like cryptosystems. pages 2–21, 1991.

[CFS+22] Shiyao Chen, Yanhong Fan, Ling Sun, Yong Fu, Haibo Zhou, Yongqing Li, Meiqin Wang, Weijia Wang, and Chun Guo. SAND : an AND-RX feistel lightweight block cipher supporting s-box-based security evaluations. *Des. Codes Cryptogr.*, 90(1) :155–198, 2022.

[DDV20] Stéphanie Delaune, Patrick Derbez, and Mathieu Vavrille. Catching the fastest boomerangs application to SKINNY. 2020(4) :104–129, 2020.

[HBS21] Hosein Hadipour, Nasour Bagheri, and Ling Song. Improved rectangle attacks on SKINNY and CRAFT. 2021(2) :140–198, 2021.

[NSS22] Yusuke Naito, Yu Sasaki, and Takeshi Sugawara. Secret can be public : Low-memory AEAD mode for high-order masking. pages 315–345, 2022.

[Wag99] David Wagner. The boomerang attack. pages 156–170, 1999.