Stage de M2 : Cryptanalyse du schéma ZIP-AES

Encadrants: Sébastien Duval, Marine Minier
sebastien.duval@loria.fr marine.minier@loria.fr

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

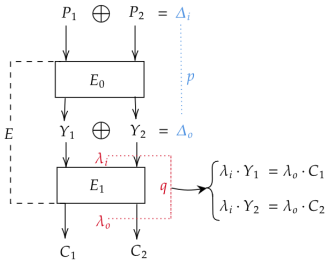
Mots clés : Cryptographie symétrique · Chiffrement par bloc · Attaque

1 Contexte du Stage de M2

La technique de cryptanalyse dite *différentiel-linéaire* a été introduite en 1994 par Langford et Hellman [LH94] et peut être vue comme une variante des cryptanalyses différentielle [BS91, Hey02] et linéaire [Mat94].

On cherche ici à regarder les biais linéaires induits par une paire de textes clairs, une fois qu'on a effectué le chiffrement. Voir Figure.

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 (différence, masque) (Δ_i, λ_o) reliant une paire de messages P_1 et $P_2 = P_1 \oplus \Delta_i$ et tel que $\lambda_o \cdot C_1 = \lambda_o \cdot C_2$. Si la probabilité d'apparition de cette relation est suffisament éloignée de la probabilité uniforme, on peut alors monter une attaque sur le chiffrement.



2 Objectifs

Le but de ce stage est de regarder la primitive appelée ZIP-AES et décrite dans [FGGL+24]. ZIP-AES est une primitive construite sur deux branches qui d'un coté font intervenir 5 tours d'AES et de l'autre 5 tours d'AES en déchiffrement.

L'idée est de regarder non pas la cryptanalyse différentielle-linéaire sur ce chiffrement mais une variante appelée cryptanalyse linéaire-différentielle, ou plutôt car nous savons que cette cryptanalyse est inefficace, les variantes dites linéaire-différentielle tronquée et multiple linéaire-différentielle. La cryptanalyse par différentielle tronquée à été introduite par L. Knudsen dans [Knu95] et la cryptanalyse multiple linéaire a été étudié par C. Blondeau et K. Nyberg dans [BN17].

L'idée est ici d'implémenter de telles attaques sur des versions réduites du chiffrement ZIP-AES afin de se rendre compte si un biais existe réellement.

Le ou la stagiaire commencera par comprendre ce qu'est une attaque différentielle-linéaire ou linéaire-différentielle (et linéaire multiple ou différentiel tronqué ou les deux) avant de se familiariser avec les différents outils de modélisation (MILP, SAT, CP ou méthodes Ad-Hoc) permettant de générer automatiquement un distingueur du type précédent. Les résultats seront bien évidemment vérifiés par une étude empirique sur quelques tours du chiffrement.

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 pour une durée maximale de 6 mois.

Contact. Pour candidater, contactez Sébastien Duval et Marine Minier (voir ci-dessus) en envoyant un CV et une lettre de motivation.

Profil. Etudiant·e de M2 de cryptographie cherchant un stage de fin de cursus.

Références

[BN17] Céline Blondeau and Kaisa Nyberg. Joint data and key distribution of simple, multiple, and multidimensional linear cryptanalysis test statistic and its impact to data complexity. *Des. Codes Cryptogr.*, 82(1-2) :319–349, 2017.

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

[FGGL+24] Antonio Flórez-Gutiérrez, Lorenzo Grassi, Gregor Leander, Ferdinand Sibleyras, and Yosuke Todo. General practical cryptanalysis of the sum of round-reduced block ciphers and ZIP-AES. Cryptology ePrint Archive, Paper 2024/2033, 2024.

[Hey02] Howard M Heys. A tutorial on linear and differential cryptanalysis. *Cryptologia*, 26(3) :189–221, 2002. available at : `http://www.cs.bc.edu/~straubin/crypto2017/heys.pdf`.

[Knu95] Lars R. Knudsen. Truncated and higher order differentials. pages 196–211, 1995.

[LH94] Susan K. Langford and Martin E. Hellman. Differential-linear cryptanalysis. pages 17–25, 1994.

[Mat94] Mitsuru Matsui. Linear cryptanalysis method for DES cipher. pages 386–397, 1994.