Lightning Talk #1

Création d'une bibliothèque unifiée de Cryptanalyse

William Mathey
EPITA - Laboratoire de Recherche de l'EPITA (LRE)
12 mars 2026

Table des matières

01

Contexte et État de l’art

L'évolution des solutions

Les algorithmes Ad-Hoc (ex : César, chiffrements manuels)

- “Structural evaluation of AES and chosen-key distinguisher of 9-round AES-128” [4]
- “Automatic search for related-key differential characteristics in byte-oriented block ciphers : Application to AES, Camellia, Khazad and others” [2]

L’ère de la modélisation : SAT, (M)ILP & CP (ex : chiffrements par blocs comme AES)

- “Differential and linear cryptanalysis using mixed-integer linear programming” [7]
- “Constraint programming models for chosen key differential cryptanalysis” [5]

Une évolution vers plus d'automatisation : Pourquoi ?

Les algorithmes automatisés (ex : machine Enigma)

- **Augmentation massive de la puissance de calcul :** permet d'envisager des attaques impossibles à traiter manuellement.
- **Complexité des chiffrements modernes grandissante :** l'automatisation est devenue nécessaire pour des algorithmes comme l'AES.
- **Permet la généricité et la rapidité**

Les solutions modernes : TAGADA [6, 3] & CLAASP [1] & OCP & BONC

On veux unifier un maximum de chiffrement dans une meme bibliothèque.

Limitations des approches existantes

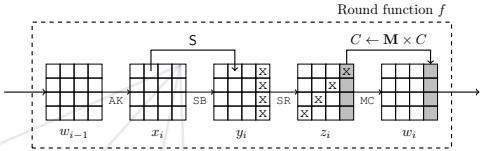
Complexité de traitement et Perte d'information

- TAGADA génère des graphes peu lisibles pour des tours d'AES (cf. figures).
- Comment retrouver les informations des états/opérateurs après modélisation ?
- CLAASP booléanise tout, perdant le contexte arithmétique.

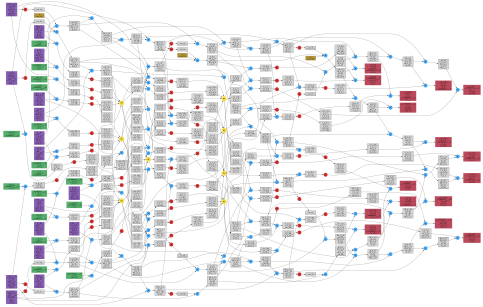
Généralisation

- Modélisation différentes (SAT, MILP, CP).
- Généralisation à d'autres primitives (fonctions de hashage/fonctions asymétriques)
- Unification de familles de chiffrement SPN/Feistel/ARX (problème d'uniformisation vs différentiation)

Crypanalystes vs TAGADA



(a) Schéma d'un tour d'AES-128.



(b) Schéma de 3 tours d'AES-128 avec TAGADA.

02

Problématique et Perspectives

Objectif

Objectif : Développer une bibliothèque unifiée, efficace, et facile à utiliser.

Roadmap

Jusqu'à fin mars : Finalisation de l'état de l'art et traduction des fonctionnalités existantes en python.

Avril - Mai : Recherche itérative de modèles/architectures de représentation.

Juin - Juillet : POC en Python.

Des Questions ?

Références i

[1] Emanuele Bellini et al. *CLAASP : a Cryptographic Library for the Automated Analysis of Symmetric Primitives*. Cryptology ePrint Archive, Paper 2023/622. 2023. url : `https://eprint.iacr.org/2023/622`.

[2] Alex Biryukov et Ivica Nikolić. “Automatic search for related-key differential characteristics in byte-oriented block ciphers : Application to AES, Camellia, Khazad and others”. In : *Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Springer. 2010, p. 322-344.

[3] François Delobel et al. “A CP-based Automatic Tool for Instantiating Truncated Differential Characteristics ⋆”. In : *LNCS*. Goa, India : Springer, déc. 2023, p. 1-23. url : `https://hal.science/hal-04343593`.

[4] Pierre-Alain Fouque, Jérémy Jean et Thomas Peyrin. “Structural evaluation of AES and chosen-key distinguisher of 9-round AES-128”. In : *Annual Cryptology Conference*. Springer. 2013, p. 183-203.

Références ii

[5] David Gerault, Marine Minier et Christine Solnon. “Constraint programming models for chosen key differential cryptanalysis”. In : *International conference on principles and practice of constraint programming*. Springer. 2016, p. 584-601.

[6] Luc Libralesso et al. “Automatic Generation of Declarative Models for Differential Cryptanalysis”. In : *LIPIcs–Leibniz International Proceedings in Informatics*. LIPIcs–Leibniz International Proceedings in Informatics. Montpellier, France, oct. 2021. doi : `10.4230/LIPIcs.CP.2021.19`. url : `https://hal.science/hal-03320980`.

[7] Nicky Mouha et al. “Differential and linear cryptanalysis using mixed-integer linear programming”. In : *International Conference on Information Security and Cryptology*. Springer. 2011, p. 57-76.