Sujet TER M1 – Cryptographie – Détection efficace de propriétés statistiques de chiffrements symétriques

Jules Baudrin
jules.baudrin@uvsq.fr

2026

Contexte. Comme vu en cours de cryptographie, il est très difficile (si ce n'est impossible) de prouver la sécurité *inconditionnelle* des algorithmes cryptographiques utilisées dans la vie de tous les jours. C'est la raison pour laquelle seule une *cryptanalyse* continue, précise et la plus vaste possible permet de gagner confiance en les primitives actuelles.

Depuis plus de 35 ans, la *cryptanalyse différentielle* est incontestablement la méthode d'analyse de primitives *symétriques* la plus développée, mais également l'une des plus redoutables. Elle s'intéresse à la distribution de probabilités des différences entre deux messages *chiffrés* dont les messages *clairs* associés différent d'une valeur choisie. Autrement dit, elle s'intéresse, pour toutes différences $\Delta^{\text{in}}, \Delta^{\text{out}}$, au nombre de solutions de l'équation suivante (d'inconnue x):

$$F(x + \Delta^{\text{in}}) + F(x) = \Delta^{\text{out}}.$$

En particulier, dès qu'il est possible de mettre en avant un couple $(\Delta^{\text{in}}, \Delta^{\text{out}})$ (communément appelé *différentielle*) pour lequel ce nombre de solutions est anormalement élevé, la primitive est largement fragilisée ; son comportement n'étant pas assez proche du comportement aléatoire attendu d'une fonction cryptographique robuste.

En pratique, la taille n du domaine (et co-domaine) de la plupart des fonctions cryptographiques est trop grosse (typiquement $n = 2^{128}$) pour permettre une recherche exhaustive des équations admettant un maximum de solutions. La grande majorité des analyses différentielles utilisent donc des heuristiques de recherche adaptées aux constructions usuelles de primitives *itérées* mais aussi (et surtout) les spécificités du design.

Récemment, de nouveaux cas d'utilisation sont apparus et nécessitent des primitives dont la taille de domaine/co-domaine sont nettement plus petits ($n = 2^{32}, 2^{48}$ ou 2^{64}). C'est le cas par exemple des familles de *chiffrements par bloc* SIMON et SPECK, conçue par la NSA en 2013 et dont l'objectif est d'atteindre des performances compétitives avec des implémentations matérielles pour SIMON ou logicielles pour SPECK.

De plus, un nouvel algorithme probabiliste de recherche de différentielles a été proposé en 2023. Il permet de convertir la recherche de différentielles pour une fonction F en un problème de recherche de *collisions* pour certaines *dérivées* de F. Ce changement de point de vue permet donc d'obtenir une complexité de l'ordre de $2^{\frac{n}{2}}$, d'après le *paradoxe des anniversaires*. Néanmoins, il nécessite des hypothèses sur F qui ne sont pas forcément vérifiées par des fonctions cryptographiques, mais également des optimisations algorithmiques pour pouvoir être utilisé en pratique sur des chiffrements de petites tailles.

Objectifs. Les objectifs de ce projet sont donc:

1. Se (ré)approprier les concepts sous-jacents (chiffrement par blocs, cryptanalyse différentielle, recherche de collisions) ;
2. Lire et comprendre l'article de 2023 ;
3. Implémenter l'algorithme de recherche de différentielles et un chiffrement « jouet » afin de vérifier son bon fonctionnement ;

4. Implémenter certaines des optimisations décrites dans le papier ;

5. Implémenter SPECK et reproduire les résultats énoncés dans l'article de 2023 (l'algorithme permet « de retrouver automatiquement toutes les propriétés différentielles de l'état de l'art mises en avant par une précédente analyse dédiée » de SPECK.) ;

6. Expliquer les résultats obtenus dans un rapport.

En fonction des envies du groupe, il est également possible de reproduire l'analyse de sécurité du chiffrement BEANIE, de comparer l'impact du choix de la clé sur la recherche de différentielles, d'étudier plus en détails les hypothèses d'indépendance ou encore de comprendre comment l'algorithme s'étend à la recherche d'approximations linéaires (l'équivalent des différentielles pour la cryptanalyse linéaire).

Le projet porte donc sur des aspects à la fois théorique et pratique de la cryptographie symétrique moderne. Afin d'obtenir les performances nécessaires sur un ordinateur personnel, la programmation s'effectuera dans un langage compilé (C, C++ ou Rust par exemple).

Groupe. Ce projet s'adresse à un groupe de 4 étudiant.e.s.

Bibliographie.

- *Efficient Detection of High Probability Statistical Properties of Cryptosystems via Surrogate Differentiation*, Eurocrypt 2023, I. Dinur, O. Dunkelman, N. Keller, E. Ronen & A. Shamir `https://eprint.iacr.org/2023/288.pdf`

- *The SIMON and SPECK Families of Lightweight Block Ciphers*, 2013, R. Beaulieu, D. Shors, J. Smith, S. Treatman-Clark, B. Weeks & L. Wingers `https://eprint.iacr.org/2013/404.pdf`