Sujet de stage :

Étude des boîtes-S cryptographiques pour améliorer la complexité des attaques statistiques

Encadrants: Christina Boura et Yann Rotella
christina.boura@uvsq.fr, yann.rotella@uvsq.fr

Étudier la résistance des primitives cryptographiques à clé secrète contre des attaques statistiques (cryptanalyse différentielle, linéaire, etc.) est un sujet primordial afin d'établir le niveau de sécurité réel des primitives symétriques. La plupart des attaques contre des primitives symétriques se construisent autour d'un distingueur. Un distingueur est une propriété qui est vérifiée sur la primitive cible avec une probabilité significativement plus élevée que pour une permutation aléatoire. Cette propriété peut être ensuite utilisée pour retrouver la clé du chiffrement ou pour mener d'autres attaques contre la primitive.

Dans un article récent [1] (version librement accessible ici [2]), Marek Broll, Federico Canale, Antonio Flórez-Gutiérrez, Gregor Leander et María Naya-Plasencia ont proposé une nouvelle technique générique pour améliorer la phase des attaques qui consiste à retrouver la clé. Cette technique consiste à étudier les propriétés spécifiques des boîtes-S utilisées pour la partie non-linéaire des algorithmes. Plus précisément, ils ont proposé une représentation par arbre des boîtes-S et un algorithme pour retrouver la meilleure représentation qui faciliterait les attaques. Cependant, l'algorithme proposé est assez lent et fonctionne très mal pour des boîtes-S de grande taille. Un premier objectif du stage serait de proposer un algorithme alternatif, ainsi qu'une implémentation de celui-ci pour des grandes boîtes-S. Une autre question restée ouverte dans [1] est la définition du critère exact qui permettrait de déterminer si une représentation est meilleure qu'une autre. Répondre à cette question pour les cryptanalyses les plus importantes est primordial afin de choisir la représentation de la boîte-S qui accélèrerait l'attaque de la manière la plus significative possible. Enfin, utiliser les résultats des deux étapes précédentes pourrait permettre par la suite d'améliorer des attaques existantes contre certaines primitives cryptographiques.

Lieu du stage : Laboratoire de Mathématiques de Versailles (LMV), UVSQ
Durée du stage : 6 mois (de mars à août 2023)
Rémunération : autour de 473 euros par mois

Références

[1] Marek Broll, Federico Canale, Antonio Flórez-Gutiérrez, Gregor Leander, and María Naya-Plasencia. Generic framework for key-guessing improvements. In *ASIACRYPT 2021, Proceedings, Part I*, volume 13090 of *Lecture Notes in Computer Science*, pages 453–483. Springer, 2021.

[2] Marek Broll, Federico Canale, Antonio Flórez-Gutiérrez, Gregor Leander, and María Naya-Plasencia. Generic framework for key-guessing improvements. *IACR Cryptol. ePrint Arch.*, page 1238, 2021.