Optimisation automatique de l'implémentation de boîtes-S pour la cryptographie symétrique

Sébastien Duval

Université de Lorraine, CNRS, Inria, LORIA, F-54000 Nancy, France sebastien.duval@loria.fr

Contexte

La cryptographie symétrique emploie des fonctions de grande taille qui simulent l'aléatoire pour qui ne connaît pas la clef secrète. Cependant, d'aussi grandes fonctions aléatoires sont impossibles à implémenter à un coût pratique. Ainsi, l'approche usuelle est de structurer les grandes fonctions cryptographiques, en les découpant comme assemblage de deux types de composants : des composants simples (et grands) et des composants petits (et complexes). Ces derniers composants sont appelés boîtes-S. Une boîte-S est la part la mieux maîtrisée des fonctions cryptographiques, et celle qui a le plus d'incidence à la fois sur le coût et la sécurité de la fonction complète.

Problématique : plus la boîte-S est petite, plus elle est simple à implémenter à un coût optimal, mais plus le passage de la sécurité de la boîte-S à la sécurité de la fonction complète est approximatif.

Les boîtes-S récentes ne manipulent que 4 bits à la fois, pour la simple raison qu'aucun outil automatique ne permet d'implémenter optimalement toute fonction de 5 bits ou plus. Pourtant, des boîtes-S de plus grande taille permettent une meilleure analyse de sécurité et, comme observé récemment [BDD+20], les plus grandes boîtes-S offrent un meilleur compromis entre coût et sécurité.

Travaux antérieurs : l'optimisation de l'implémentation des fonctions est un problème ancien en cryptographie, et il existe actuellement plusieurs outils, généralement limités à l'optimisation de fonctions de 4 bits. Une exception est l'outil développé par Stoffelen [Sto16], qui fonctionne pour quelques fonctions de 5 bits, outil amélioré dans [BDD+20] pour fonctionner sur de nombreuses fonctions de 5 bits et certaines de 6 bits.

De nombreuses approches existent, pas toutes exploitées aujourd'hui :

1. Approches mathématiques
    - par classes d'équivalence de fonctions [LP07, BL08, Saa11],
    - par construction de boîtes-S grandes à partir de boîtes-S petites [LW14, CDL15, BDD+20].
2. Approches algorithmiques
    - par composition des bits d'entrée / par décomposition des bits de sortie de la fonction [LWF+22],
    - en découpant la fonction en plusieurs morceaux implémentés, puis en implémentant chaque morceau et en recombinant le tout à la fin [JPST17, MB19, BDD+20],
    - parours de graphe : en largeur, en profondeur, plus court chemin (A*), ...
3. Approches par résolution de contraintes

- Mixed-Integer Linear Programming (MILP) : contraintes sous forme d'équations linéaires,
- Programmation par Contraintes (CP) : contraintes sous forme de bornes sur les domaines des variables,
- SATisfiabilité (SAT) : contraintes sous forme de clauses logiques.

Objectifs

Les outils actuels sont loin d'être optimaux. Même le meilleur outil actuel [BDD+20], basé sur un solveur SAT, n'est pas efficace. L'objectif de ce stage est d'explorer de nouvelles approches pour optimiser automatiquement les implémentations de petites fonctions. Il peut s'agir de combiner certaines approches ci-dessus intelligemment, ou d'imaginer une nouvelle approche ad-hoc.

Ce stage requiert avant tout un goût pour l'algorithmique et des compétences en code optimisé (certains outils sont en Java ou Python, mais idéalement les algorithmes imaginés devraient être implémentés efficacement en C).

Conditions du stage

Le stage se déroulera au sein du Laboratoire d'Informatique Lorrain (LORIA) à Nancy, au sein de l'équipe CARAMBA, et sera gratifié à hauteur de 473 euros par mois.

References

[BDD+20] Begül Bilgin, Lauren De Meyer, Sébastien Duval, Itamar Levi, and François-Xavier Standaert. Low and depth and efficient inverses: a guide on s-boxes for low-latency masking. *IACR Transactions on Symmetric Cryptology*, 2020(1):144–184, May 2020.

[BL08] Marcus Brinkmann and Gregor Leander. On the classification of APN functions up to dimension five. *Des. Codes Cryptogr.*, 49(1-3):273–288, 2008.

[CDL15] Anne Canteaut, Sébastien Duval, and Gaëtan Leurent. Construction of lightweight s-boxes using feistel and MISTY structures. In Orr Dunkelman and Liam Keliher, editors, *Selected Areas in Cryptography - SAC 2015 - 22nd International Conference, Sackville, NB, Canada, August 12-14, 2015, Revised Selected Papers*, volume 9566 of *Lecture Notes in Computer Science*, pages 373–393. Springer, 2015.

[JPST17] Jérémy Jean, Thomas Peyrin, Siang Meng Sim, and Jade Tourteaux. Optimizing implementations of lightweight building blocks. *IACR Trans. Symmetric Cryptol.*, 2017(4):130–168, 2017.

[LP07] Gregor Leander and Axel Poschmann. On the classification of 4 bit s-boxes. In Claude Carlet and Berk Sunar, editors, *Arithmetic of Finite Fields, First International Workshop, WAIFI 2007, Madrid, Spain, June 21-22, 2007, Proceedings*, volume 4547 of *Lecture Notes in Computer Science*, pages 159–176. Springer, 2007.

[LW14] Yongqiang Li and Mingsheng Wang. Constructing s-boxes for lightweight cryptography with feistel structure. In Lejla Batina and Matthew Robshaw, editors, *Cryptographic Hardware and Embedded Systems - CHES 2014 - 16th*

International Workshop, Busan, South Korea, September 23-26, 2014. Proceedings, volume 8731 of *Lecture Notes in Computer Science*, pages 127–146. Springer, 2014.

[LWF+22] Qun Liu, Weijia Wang, Yanhong Fan, Lixuan Wu, Ling Sun, and Meiqin Wang. Towards low-latency implementation of linear layers. *IACR Trans. Symmetric Cryptol.*, 2022(1):158–182, 2022.

[MB19] Lauren De Meyer and Begül Bilgin. Classification of balanced quadratic functions. *IACR Trans. Symmetric Cryptol.*, 2019(2):169–192, 2019.

[Saa11] Markku-Juhani O. Saarinen. Cryptographic analysis of all 4 × 4-bit s-boxes. In Ali Miri and Serge Vaudenay, editors, *Selected Areas in Cryptography - 18th International Workshop, SAC 2011, Toronto, ON, Canada, August 11-12, 2011, Revised Selected Papers*, volume 7118 of *Lecture Notes in Computer Science*, pages 118–133. Springer, 2011.

[Sto16] Ko Stoffelen. Optimizing s-box implementations for several criteria using SAT solvers. In Thomas Peyrin, editor, *Fast Software Encryption - 23rd International Conference, FSE 2016, Bochum, Germany, March 20-23, 2016, Revised Selected Papers*, volume 9783 of *Lecture Notes in Computer Science*, pages 140–160. Springer, 2016.