# Sujet de stage M2 : Programmation par contraintes pour la résolution de problèmes de cryptographie symétrique

Marine Minier

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

## Contexte

La cryptographie et notamment la cryptographie symétrique est une pierre angulaire des communications. Elle permet de garantir des propriétés comme la confidentialité, l'intégrité ou la signature. Alors que la cryptographie à clé publique repose sur des problèmes bien connus et difficiles à résoudre, la cryptographie symétrique utilise des opérations élémentaires itérées un grand nombre de fois. Les primitives les plus importantes en cryptographie symétriques sont les fonctions de hachage permettant de garantir l'intégrité, les chiffrements à flot et les chiffrements par blocs qui eux, garantissent la confidentialité des échanges.

Au cours de la dernière décennie, beaucoup de résultats de cryptanalyse se sont intéressés à la recherche de chemins différentiels dans les chiffrements par blocs où un attaquant introduit une différence en entrée du chiffrement et prédit la différence en sortie sur les chiffrés correspondants avec une certaine probabilité que l'on veut la plus éloignée possible de la probabilité uniforme. La cryptanalyse différentielle a également étendu le modèle d'attaque au cas dit à clés liées où on s'autorise à introduire des différences non seulement dans les clairs mais également dans les clés. Ces travaux impliquent généralement la résolution de problèmes fortement combinatoires (NP-difficiles) qui peuvent être résolus par des bibliothèques de programmation par contraintes [8] : ces bibliothèques permettent de décrire le problème de façon déclarative, en termes de variables de décision, de contraintes entre ces variables, et de fonctions objectifs à optimiser ; le problème ainsi décrit est ensuite résolu par des algorithmes génériques qui explorent l'espace de recherche de façon systématique, en construisant un arbre de recherche, et propagent les contraintes à chaque nœud de l'arbre afin de l'élaguer.

La programmation par contraintes a été utilisée pour résoudre des problèmes de cryptanalyse différentielle de chiffrements par blocs [9] notamment dans le modèle dit de différentielles à clés liées contre l'AES [4, 3, 2, 5]. Récemment [1], Derbez et al. ont réussi à améliorer cette attaque grâce à un modèle MILP qui ne s'intéresse qu'à des clés liées ayant une probabilité 1 de se produire.

## Objectifs

L'objectif de ce stage est de modéliser soit en MiniZinc[1], soit directement en CP ce nouveau modèle MILP pour voir si le modèle induit est plus rapide que le modèle proposé. Dans un deuxième temps, il s'agira de programmer également directement les complexités des attaques de type Boomerang dans ce ou ces modèles.

L'ensemble des codes produits sera à développer en utilisant les langages minizinc [6] et Choco [7]. Minizinc est un langage de programmation par contraintes haut niveau permettant de compiler vers différents solvers CP comme chuffed ou des solvers SAT comme Picat-SAT. Choco est un langage de programmation par contraintes dédié, implémenté en Java.

[1] https://www.minizinc.org/.

### Conditions du stage

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

## References


1. Patrick Derbez, Marie Euler, Pierre-Alain Fouque, and Phuong Hoa Nguyen. Revisiting related-key boomerang attacks on aes using computer-aided tool. Cryptology ePrint Archive, Paper 2022/725, 2022. `https://eprint.iacr.org/2022/725`.
2. David Gérault, Pascal Lafourcade, Marine Minier, and Christine Solnon. Revisiting AES related-key differential attacks with constraint programming. *IACR Cryptology ePrint Archive*, 2017:139, 2017.
3. David Gérault, Pascal Lafourcade, Marine Minier, and Christine Solnon. Revisiting AES related-key differential attacks with constraint programming. *Inf. Process. Lett.*, 139:24–29, 2018.
4. David Gerault, Pascal Lafourcade, Marine Minier, and Christine Solnon. Computing AES related-key differential characteristics with constraint programming. *Artif. Intell.*, 278, 2020.
5. David Gerault, Marine Minier, and Christine Solnon. Using constraint programming to solve a cryptanalytic problem. In *Proceedings of the Twenty-Sixth International Joint Conference on Artificial Intelligence, IJCAI 2017, Melbourne, Australia, August 19-25, 2017*, pages 4844–4848, 2017.
6. N. Nethercote, P. J. Stuckey, R. Becket, S. Brand, G. J. Duck, and G. Tack. Minizinc: Towards a standard CP modelling language. In *Principles and Practice of Constraint Programming - CP*, volume 4741 of *LNCS*, pages 529–543. Springer, 2007.
7. Charles Prudhomme and Jean-Guillaume Fages. An introduction to choco 4.0: an open source java constraint programming library. In *CP Workshop on "CP Solvers: Modeling, Applications, Integration, and Standardization"*, 2018.
8. Francesca Rossi, Peter van Beek, and Toby Walsh. *Handbook of Constraint Programming (Foundations of Artificial Intelligence)*. Elsevier Science Inc., New York, NY, USA, 2006.
9. Siwei Sun, Lei Hu, Peng Wang, Kexin Qiao, Xiaoshuang Ma, and Ling Song. Automatic security evaluation and (related-key) differential characteristic search: Application to simon, present, lblock, DES(L) and other bit-oriented block ciphers. In *Advances in Cryptology - ASIACRYPT 2014*, volume 8873 of *Lecture Notes in Computer Science*, pages 158–178. Springer, 2014.