COURBURE ET NORMALITÉ

SUJET DE THÈSE PROPOSÉ PAR PHILIPPE LANGEVIN

Depuis les années 1950, la théorie de l'information a suscité un flot continu de questions complexes sur les fonctions booléennes. Quelques problèmes fondamentaux d'optimalité pour la théorie des codes et la cryptographie symétrique restent partiellement non résolus. Les approches théoriques qui permettent d'obtenir des résultats asymptotiques utiles dans un cadre probabiliste, peinent à fournir des réponses précises à distance finie ! Concrètement, on sait bien qu'une fonction booléenne cryptographique doit être équilibrée et de faible linéarité. Pour autant, la linéarité optimale d'une fonction équilibrée de 8 bits est toujours une question ouverte depuis les travaux Hans Dobbertin de 1994.

*

Aujourd'hui, nous constatons que la puissance de calcul des machines, combinée aux méthodes de classification des fonctions booléennes, ouvre des perspectives prometteuses pour des avancées significatives le domaine des fonctions booléennes en cryptographie en dimension 8. En effet, l'année dernière, nous avons franchi une étape importante en prouvant que toutes les fonctions courbes de 8 bits sont normales, résolvant un autre problème ouvert vieux de 30 ans, posé par Hans Dobbertin dans [4]. Nous pensons que les méthodes utilisées s'appliquent pour appréhender la non linéarité des fonctions booléennes équilibrées de 8 variables, et c'est un des trois objectifs que nous proposons d'atteindre.

*

Dans ses travaux, Hans Dobbertin s'appuie sur deux notions importantes du domaine des fonctions booléennes [2] : normalité et non linéarité. La non linéarité d'une fonction booléenne mesure la distance de cette fonction à l'espace des fonctions affines. Les fonction de nonlinéarité optimale en dimension m paire, sont appelés des fonctions courbes, une terminologie popularisé par Oscar Rothaus [17] lors de la classification des fonction de $m = 6$ variables. Les fonctions courbes occupent une place centrale dans la théorie des designs, des codes et de la cryptographie symétrique. Pour construire des fonctions équilibrées de faible linéarité, Dobbertin propose de déformer les fonctions courbes constantes sur des sous-espaces de dimension bien choisie. Il introduit la notion de normalité en qualifiant de normale toute fonction booléenne constante sur un sous-espace de dimension t. Notons bien que la terminologie est justifiée par le fait que toutes les fonctions courbes obtenues par des construction primaires, Maiorana-Marland, partial spread Dillon [16] sont normales. Sous cette hypotèse, les résultats classiques de l'analyse harmonique permettent de contrôler la non linéarité des déformation de ces fonctions courbes. L'article de Dobbertin termine son étude en posant une question :

existe-t-il une fonction courbe anormale ?

*

Date: janvier 2025.

La réponse est négative petite dimension, car toutes les fonctions de petit degré, et donc en particulieri, les fonction courbes, sont normales. La réponse est positive en grande dimension supérieure ou égale à 10 [1, 12]. L'année dernière, nous avons adapté les travaux de comptage [11] basés sur les résultats de [10] pour classifier l'ensemble des fonctions coubes de 8-bit sous l'action du groupe général linéaire. Un travail numérique annoncé dans la conférence [9] qui nous permet d'affirmer que

toutes les fonctions courbes de 8 bits sont normales.

*

Fort de ces expériences et des travaux en cours, nous pensons qu'il est désormais possible de percer sur trois autres grandes questions ouvertes concernant les fonctions booléennes à 8 variables :

(1) non-linéarité maximale d'ordre 2 et 3;
(2) linéarité minimale des fonctions équilibrées;
(3) nouvelle construction primaires de fonctions courbes.

Les travaux s'inscriront dans la continuité des méthodes que nous avons décrites, en particulier pour l'étude de la non linéarité maximale, et des interactions avec la notions de normalité. La dernière question sur les constructions primaires pourrait bien nécessiter une approche innovante exploitant des techniques d'intelligence artificielle pour identifier de nouvelles connstruction à partir de données massives sur les fonctions courbes.

*

Pour relever ce type de défi, le candidat doit avoir le goût pour le challenge numérique, il doit posséder des compétence en mathématiques discrètes, doubler de solides base en programmation.

References

[1] Anne Canteaut, Magnus Daum, Hans Dobbertin, and Gregor Leander. Finding nonnormal bent functions. *Discret. Appl. Math.*, 154(2):202–218, 2006.

[2] Claude Carlet, editor. *Boolean Functions for Cryptography and Coding Theory*. Cambridge University Press, 2020.

[3] Pascale Charpin. Normal Boolean functions. *Journal of Complexity*, 20(2):245–265, 2004. Festschrift for Harald Niederreiter, Special Issue on Coding and Cryptography.

[4] Hans Dobbertin. Construction of bent functions and balanced Boolean functions with high nonlinearity. In Bart Preneel, editor, *Fast Software Encryption*, pages 61–74, Berlin, Heidelberg, 1995. Springer Berlin Heidelberg.

[5] Sylvie Dubuc. *Etude des propriétés de dégénérescence et de normalité des fonctions booléennes et construction de fonctions q-aires parfaitement non-linéaires*. PhD thesis, University of Caen, 2001.

[6] Valérie Gillot and Philippe Langevin. Classification of some cosets of Reed-Muller codes. *Cryptography and Communications*, 15:1129–1137, 2023. doi:10.1007/s12095-023-00652-4.

[7] Valérie Gillot and Philippe Langevin. Classification of 8-bit bent functions. `https://langevin.univ-tln.fr/project/genbent/genbent.html`.

[8] Valérie Gillot and Philippe Langevin. Classification of $B(s,t,m)$. `http://langevin.univ-tln.fr/data/bst/`.

[9] Valérie Gillot, Philippe Langevin, and Alexandr Polujan. In *Boolean Function and Their Application*.

[10] Xiang-Dong Hou and Philippe Langevin. Results on bent functions. *Journal of Combinatorial Theory (A)*, 80(2):232–246, 1997.

[11] Philippe Langevin and Gregor Leander. Counting all bent functions in dimension eight 99270589265934370305785861242880. *Designs, Codes Cryptography 59(1-3)*, 59(1-3):193–205, 2011.

[12] Gregor Leander and Gary McGuire. Construction of bent functions from near-bent functions. *J. Combin. Theory Ser. A*, 116(4):960–970, 2009.
[13] Qingshu Meng, Huanguo Zhang, Jingsong Cui, and Min Yang. almost enumeration of 8-variable bent functions. *IACR Cryptol. ePrint Arch.*, page 100, 2005.
[14] Alexandr Polujan, Luca Mariot, and Stjepan Picek. Normality of Boolean bent functions in eight variables, revisited. In *The 8th International Workshop on Boolean Functions and their Applications*, pages 79–83, 2023.
[15] Alexandr Polujan, Luca Mariot, and Stjepan Picek. On two open problems on the normality of bent functions. *Accepted in Discrete Applied Mathematics*, 2024.
[16] Dillon J. F. *Elementary Hadamard Difference Sets*. PhD thesis, University of Maryland, 1974.
[17] Rothaus O. S. On bent functions. *Journal of Combinatorial Theory (A)*, 20:300–305, 1976.

Imath, université de Toulon
Email address: {philippe.langevin}@univ-tln.fr