– Sujet de stage –

Université	Nice-Sophia Antipolis	
Laboratoire	Informatique Signaux et Systèmes de Sophia-Antipolis	UMR 6070
Equipe interne	Modèles de calcul, complexité et codes	MC3
Localisation	2000 Route des Lucioles, Sophia Antipolis cedex	F-06903
Directeur du laboratoire	Luc PRONZATO (mailto:pronzato@i3s.unice.fr)	DR CNRS
Directeur de stage	Bruno MARTIN (mailto:Bruno.Martin@unice.fr)	PR

L'aléatoire déterministe par des automates cellulaires, liens avec les fonctions Booléennes

Thématique : sécurité/cryptologie

Présentation générale

Les *automates cellulaires* (AC) constituent à la fois un modèle de système dynamique discret et un modèle de calcul. Un AC est composé d'un ensemble infini de cellules identiques qui peuvent prendre à un instant donné un état à valeurs dans un ensemble fini. Le temps est également discret et l'état d'une cellule au temps t est fonction de l'état au temps $t-1$ d'un nombre fini de cellules, son «voisinage». À chaque instant, la même règle est appliquée à l'ensemble des cellules, produisant une nouvelle «configuration» dépendant entièrement de la configuration précédente. Nous considérons ici des AC sur un anneau de N cellules dont les états sont binaires et dont la règle est vue comme une fonction Booléenne.

Wolfram [6] a proposé d'utiliser une règle d'AC binaire (restreinte aux seules cellules voisines) pour engendrer une suite pseudo-aléatoire qui pourrait être utilisée comme la clé d'un chiffre de Vernam. Nous avons montré [4] qu'une seule règle pouvait engendrer des suites pseudo-aléatoires convenables. Cependant, ce générateur de suites pseudo-aléatoires n'a pas résisté à diverses attaques [1, 5].

Objectifs du stage

L'étude de la génération des suites pseudo-aléatoires par des automates cellulaires ne s'est pas arrêtée. Plusieurs pistes sont actuellement à l'étude [3] :

– autoriser les cellules à exécuter des règles différentes (AC non uniformes) ;
– augmenter la taille du voisinage tout en conservant la même règle pour l'ensemble des cellules.

On se propose d'étudier la règle de l'AC comme une fonction Booléenne et d'utiliser la dynamique des AC pour étendre l'arité de la règle en une fonction Booléenne à N variables afin d'en extraire une suite pseudo-aléatoire. Pour cela, on cherche des fonctions Booléennes à plus de trois variables avec de bonnes propriétés de résilience et de non-linéarité. Une partie de l'étude a déjà été faite [2] et devra être étudiée.

Le but du stage est de comparer la qualité des suite pseudo-aléatoires engendrées par les deux approches citées en faisant le lien entre les propriétés des fonctions Booléennes et la dynamique d'un automate cellulaire du point de vue de la génération déterministe de suites pseudo-aléatoires.

Compétences souhaitées

Connaissances en informatique théorique (complexité, cryptographie). Programmation en `C` ou `C++`.

Références

[1] A.M. Apohan and C.K. Koc. Inversion of cellular automata iterations. In *Computer and Digital Techniques*, volume 144, pages 279–284, 1997.

[2] A. Braeken, Y. Borissov, S. Nikova, and B. Preneel. Classification of boolean functions of 6 variables or less with respect to cryptographic properties. Technical report, IACR248, 2008.

[3] P. Lacharme, B. Martin, and P. Solé. Pseudo-random sequences, boolean functions and cellular automata. In *Proceedings of Boolean Functions and Cryptographic Applications*, 2008. A paraître.

[4] B. Martin. A Walsh exploration of elementary CA rules. *Journal of Cellular Automata*, 3(2) :145–156, 2008.

[5] W. Meier and O. Staffelbach. Analysis of pseudo random sequences generated by cellular automata. In *EUROCRYPT '91*, Lecture Notes in Computer Science, pages 186–200. Springer Verlag, 1991.

[6] S. Wolfram. Cryptography with cellular automata. In *CRYPTO 85*, volume 218 of *LNCS*, pages 429–432. Springer Verlag, 1985.