Ecole Doctorale STIC
Sciences & Technologies de l'Information et de la Communication

ED STIC - Proposition de Sujets de Thèse

pour la campagne d'Allocation de thèses 2011

Titre du sujet :	Suites pseudo-aléatoires engendrées par des automates cellulaires et applications
Mention de thèse :	Informatique
HDR Directeur de thèse inscrit à l'ED STIC :	Martin Bruno

Co-encadrant de thèse éventuel :

Nom :	
Prénom :	
Email :	
Téléphone :	

Email de contact pour ce sujet :	Bruno.Martin@unice.fr
Laboratoire d'accueil :	I3S

Description du sujet :

Les automates cellulaires (AC) ont été inventés par Ulam et von Neumann. Il s''agit à la fois d''un modèle de système dynamique discret et d''un modèle de calcul.
Un AC est composé d''un ensemble 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 appelé son «voisinage». À chaque nouvelle unité de temps les mêmes règles sont
appliquées à l''ensemble des cellules produisant une nouvelle «configuration» de cellules dépendant entièrement de la configuration précédente. Nous considérons ici des AC
sur un anneau de N cellules et dont les états sont binaires.

En 1985 Wolfram a proposé d''utiliser une règle d''AC binaire (restreinte à ses deux cellules voisines) pour engendrer une suite pseudo-aléatoire [1]. Il a suggéré que les suites

pseudo-aléatoires engendrées par la règle 30 pourraient être utilisées comme clé d'un chiffre de Vernam. Nous avons montré [5] par une analyse exhaustive des règles
d'automates cellulaires que seule la règle 30 --ainsi que trois autres règles équivalentes-- pouvaient engendrer des suites pseudo-aléatoires convenables. Cependant ce
générateur de suites pseudo-aléatoire n'a pas résisté à différentes attaques. L'étude de la génération des suites pseudo-aléatoires par des AC ne s'est pourtant pas arrêtée.
Plusieurs pistes sont actuellement à l''étude en:
-- autorisant les cellules à exécuter des règles différentes;
-- utilisant des automates cellulaires particuliers à la manière des registres linéaires à décalage;
-- augmentant la taille du voisinage tout en conservant la même règle pour l''ensemble des cellules.
La première approche requiert la recherche des meilleures règles possibles pour engendrer des suites pseudo-aléatoires. La technique employée utilise les algorithmes
évolutionnaires; elle a été initiée par [2] et généralisée par [3]. La seconde piste provient de la «synthèse» d'un polynôme irréductible sur GF(2)[x] par des AC. L'algorithme de
synthèse proposé par Cattell et Muzio [4] permet a priori de construire des générateurs de suites pseudo-aléatoires d'une manière analogue à celle étudiée pour les registres
linéaires à décalage. Martin et Solé ont commencé des recherches dans cette direction [5]. La dernière technique concilie la théorie des fonctions booléennes et celle des
automates cellulaires. On étudie la fonction de transition comme une fonction Booléenne et on cherche une fonction à plus de trois variables avec de bonnes propriétés de
résilience et de non-linéarité [6].

Le sujet porte sur la comparaison de la qualité des suite pseudo-aléatoires engendrées par les règles d''automates cellulaires non uniformes ainsi que celles obtenues en
suivant les autres pistes. Ces résultats pourront être employés pour construire des fonctions de hachage en suivant la technique proposée par Damgard en 1990 et améliorée
par Daemen et al en 1991. La sûreté de cette fonction de hachage pourra ensuite être évaluée par une attaque différentielle utilisant la théorie des codes. Enfin
la perspective de réaliser une implémentation matérielle pourra être abordée car le modèle des automates cellulaires est assez proche de celui des FPGA.

Références
---
[1] S. Wolfram. Cryptography with cellular automata. In CRYPTO 85 volume 218 of LNCS pages 429–432. Springer Verlag 1985.
[2] M. Sipper and M. Tomassini. Co-evolving parallel random number generators. In Parallel Problem Solving from Nature – PPSN IV pages 950–959 Berlin 1996. Springer
Verlag.
[3] F. Seredynski P. Bouvry and A.Y. Zomaya. Cellular automata computations and secret key cryptography. Parallel Computing 30:753–766 May 2004.
[4] K Cattell and J.C Muzio. Synthesis of one-dimensional linear hybrid cellular automata. IEEE Trans. on Computer-aided design of integrated circuits and systems 15(3):325–
\r\n335 Apr 1996.

[5] B. Martin. A Walsh exploration of elementary CA rules. Journal of Cellular Automata 3(2):145–156 2008.
[6] P.Lacharme B.Martin andP.Sole ´.Pseudo-randomsequences booleanfunctionsandcellularautomata. In Proceedings of Boolean Functions and Cryptographic Applications
2008. A paraître.

English version: