CCPBAC:un cryptosystème à clés publiques basés sur des automates cellulaires

Gilbert TINDO

Département d'informatique
Faculté des sciences
Université de Yaoundé I
B.P. 812 Yaoundé
CAMEROUN
gtanedon@yahoo.com
gtindo@uycdc.uninet.cm

RÉSUMÉ. Dans ce papier, nous nous intéressons aux automates cellulaires de dimension deux inversibles et proposons une approche pour la construction de tels automates. L'approche proposée est ensuite utilisée pour construire un cryptosystème à clés publiques basé sur des automates cellulaires de dimension deux inversibles. La clé publique du système est l'automate cellulaire utilisé pour le chiffrement. La sécurité du cryptosystème est baseé sur le fait qu'il n'y a pas de procédure efficace connue pour calculer l'inverse d'un automate cellulaire de dimension supérieure ou égal à 2.

ABSTRACT. In this paper, we are interested in invertible two dimensional cellular automata, and we exhibit a method for building some automata of this class. Method exhibited is used to build a public key cryptosystem based on invertible two dimensional cellular automata. The public key is the automaton used to encrypt messages. The security of this cryptosystem is based on the fact that there is no known efficient procedure for computing the inverse of a cellular automata of dimension greater than or equal to two.

MOTS-CLÉS : Automate cellulaire réversible, cryptographie, clé publique, sécurité

KEYWORDS : invertible cellular automata, cryptography,public key, security

1. Introduction

Un automate cellulaire est un outil mathématique permettant de modéliser certains phénomènes physiques. Récemment les automates cellulaires ont été proposés par de nombreux auteurs [3, 4, 6, 8, 10, 11] comme outil de construction de systèmes cryptographiques (cryptosystèmes). La plupart des cryptosystèmes basés sur les automates cellulaires sont à clés symétriques [4, 8, 10, 11] et l'automate cellulaire joue le rôle de clé secrète. Suite aux travaux de Kari [6, 7] et de Toffoli et Margolus [9], montrant l'indécidabilité du problème de savoir si un automate cellulaire en dimension au moins égale à deux est inversible, des systèmes cryptographiques à clés publiques basés sur les automates cellulaires ont été proposés [3, 6]. La confidentialité d'un système cryptographique à clés publiques est basée en général sur la difficulté de trouver la fonction inverse de la fonction de chiffrement. Le calcul de cet inverse peut se faire cependant très facilement si on connaît une brèche secrète dans la construction de la fonction de chiffrement. En ce qui concerne les cryptosystèmes basés sur les automates cellulaires, la clé publique utilisée pour crypter les messages est un automate cellulaire. Pour déchiffrer le message, il suffit d'appliquer au message crypté l'automate inverse de celui utilisé pour le chiffrement. Or il n'existe pas de procédure connue pour calculer l'inverse d'un automate cellulaire de dimension supérieure ou égale à 2. La brèche secrète utilisée généralement est le fait que l'automate de chiffrement est la composée d'un certain nombre d'automates triviaux que l'on sait inverser facilement. Depuis que les automates cellulaires ont été proposés comme une alternative pour la conception de cryptosystèmes à clés publiques, leur usage n'est pas devenu très populaire. Le problème est sans doute dû au fait que l'on ne sait pas toujours construire une grande famille d'automates cellulaires non triviaux inversibles. Dans la section suivante, nous proposons une approche de construction d'automates cellulaires inversibles de dimension supérieur ou égale à deux. La section 3 est consacrée à la construction d'un cryptosystème à clés publiques basé sur des automates cellulaires inversibles obtenus en utilisant l'approche proposée. Le procédé de construction constitue la brèche secrète qui, si elle n'est pas connue, le problème de l'inversion des automates construits se ramène à la recherche exhaustive d'un m-uplet dans l'ensemble Z^B, où m et B sont des entiers, Z^B est l'ensemble des entiers modulo B.

2. Automates cellulaires et inversibilité

2.1. Automates cellulaires

Un automate cellulaire est un quadruplet $A = (Q, Z^n, f, V)$, où Q est un ensemble fini appelé ensemble des états, Z est l'ensemble des entiers relatifs, Z^n est l'espace cellulaire, f est la fonction locale de transition, n est la dimension de l'automate, et V est le vecteur de voisinage. Une cellule de l'automate à un instant t est caractérisé par un couple $(i, z_i(t))$, où $i = (i_1, i_2, \ldots, i_n)$ est un élément de Z^n qui permet de repérer la cellule dans l'espace cellulaire et $z_i(t)$ est un élément de Q qui représente l'état de cette cellule. Le vecteur de voisinage V est un vecteur qui permet de définir le voisinage d'une cellule quelconque. Si V est égal à $\{v_1, v_2, \ldots, v_i, \ldots, v_m\}$, où , $1 \leq i \leq m$, alors le voisinage de la cellule de coordonnées i est $i + v_1, i + v_2, \ldots, i + v_m$. Dans un automate cellulaire, le vecteur de voisinage est le même pour chaque cellule. En dimension deux, les voisinages les plus célèbres sont le voisinage de Von Neumann donné par le vecteur de voisi-

nage $\{(0,-1),(-1,0),(1,0),(0,1),(0,0)\}$ et le voisinage de Moore donné par le vecteur de voisinage $\{(-1,-1),(-1,1),(1,-1),(0,-1),(-1,0),(0,0),(0,1),(1,0),(1,1)\}$.
La fonction locale de transition f est une application de Q^m vers Q, c'est-à-dire que pour calculer le nouvel état d'une cellule, on prend l'état de chaque cellule dans le voisinage de la cellule considérée et on applique au m-uplet obtenu la fonction locale de transition. La fonction locale de transition peut être la même pour toutes les cellules , on parle alors d'automates cellulaires uniformes (ou homogènes) ; elle peut être différente d'une cellule à l'autre, on parle alors d'automates cellulaires hétérogènes. Toutes les cellules changent d'état de façon asynchrone. Soit $Z(t)$ l'ensemble des états de toutes les cellules de l'automate cellulaire à l'instant t. On dit que $Z(t)$ est la configuration de l'automate cellulaire à l'instant t. On peut ainsi définir une fonction F qui à la configuration de l'automate à l'instant t associe la configuration de l'automate à l'instant $t+1$, c'est-à-dire $Z(t+1) = F(Z(t))$. F est la fonction globale de transition de l'automate cellulaire.

2.2. Quelques résultats sur l'inversibilité des automates cellulaires

Le problème de savoir si un automate cellulaire tel que défini ci-dessus est inversible à longtemps préoccupé les scientifiques. Quelques résultats intéressants sur le sujet ont été publiés suite aux travaux de pionniers de Richardson [12] et, Amoroso et Patt [1].
Lemme 1 : (Richardson [12]) Si un automate cellulaire est inversible, alors son inverse est un automate cellulaire.
Ce résultat nous permet de savoir que si la fonction globale de transition d'un automate est inversible, alors la fonction globale inverse peut aussi être décrite localement par une fonction locale de transition.
Théorème 1 : (Amoroso et Patt [1]) Il existe une procédure efficace pour décider si oui ,ou non un automate cellulaire quelconque en dimension un, défini par sa fonction locale de transition est inversible.
Dans [5], Karel Culik propose une démonstration de ce résultat pour des fonctions locales de transition linéaires. Ce résultat permet a priori d'écarter tout automate cellulaire inversible à une dimension comme candidat pour l'utilisation en tant que cryptosystème à clés publiques.
Théorème 2 : [6, 7] Le problème de savoir si un automate cellulaire de dimension au moins égale à deux, défini par sa fonction locale de transition est inversible, est indécidable.
Ce résultat nous permet de dire que si l'on dispose d'une brèche secrète pour calculer l'inverse d'un automate cellulaire A de dimension supérieure ou égale à deux, on peut utiliser A comme cryptosystème à clés publiques. L'automate A peut être publié pour chiffrer des messages. Les messages chiffrés par A ne pourront être déchiffrés facilement que par ceux qui ont l'automate inverse A^{-1}.

3. Une approche de construction d'automates cellulaires inversibles

Considérons une grille de dimension deux . Cette grille peut être considérée comme une agrégation de grilles de dimension un dans le sens horizontal, le sens vertical ou le sens oblique. Si on considère une grille finie, elle est généralement vue comme un tore, et dans ce cas elle peut toujours être considérée comme une agrégation de grilles finies de dimension un. Considérons deux automates cellulaires $H1$ et $H2$, de dimension un et

dont les voisinages ont pour longueurs respectives $R1$, et $R2$. Nous appelons longueur du voisinage d'un automate cellulaire de dimension un, la distance entre les points à l'extrémité du segment passant par tous les points de ce voisinage. Les espaces cellulaires associés aux automates $H1$ et $H2$ ne sont pas orientés dans le même sens si on les place dans la grille de dimension deux.
Initialisons une grille carrée $L \times L$, avec une configuration $Z(t)$. Cette configuration définit un ensemble de configurations pour les automates à une dimension $H1$ et $H2$. Elle définit exactement L configurations pour $H1$ et L configurations pour $H2$, où L est la racine carrée du nombre de cellules de la grille. Nous pouvons supposer sans nuire à la généralité que la longueur du voisinage de $A1$ est la plus petite. Faisons évoluer chaque configuration de $H1$ induite de $Z(t)$ d'une seule itération. On obtient une configuration $Y(t)$ sur la grille. Faisons évoluer chaque configuration de $H2$ induite de $Y(t)$ d'une seule itération. On obtient une configuration $U(t)$ sur la grille.

Proposition 1 : La relation qui fait passer la configuration $Z(t)$ à $U(t)$ définit un automate cellulaire de dimension deux homogène ou non homogène, dont le voisinage de chaque cellule une est grille de $R1 \times R2$ cellules.
Preuve : Il est clair que pour une cellule donnée, le calcul de son nouvel état fait intervenir les états de toutes les cellules d'une grille autour de cette cellule contenant $R1 \times R2$ cellules. Cette grille de taille $R1 \times R2$, étant la même pour toutes les cellules, on peut en déduire un vecteur de voisinage en dimension deux. La fonction locale de transition fait intervenir toutes les cellules de la grille.

Illustration :
Supposons que les deux automates cellulaires $H1$ et $H2$ soient uniformes et linéaires et que l'espace cellulaire de $H1$ est orienté dans le sens vertical et celui de $H2$ est orienté dans le sens horizontal. Les autres caractéristiques de l'automate cellulaire $H1$ sont ainsi définies : Le vecteur de voisinage est $V = (0,-1),(0,0),(0,1)$ La fonction locale de transition est une fonction de Q^3 dans Q et son expression est donnée par :

$$\begin{aligned} z_{ij}(t+1) &= f_1(z_{ij}(t), z_{ij-1}(t), z_{ij+1}(t)) \\ &= \beta_1 z_{ij}(t) + \beta_2 zij - 1(t) + \beta_3 z_{ij+1}(t) + \beta \end{aligned}$$

et celles de $H2$ sont ainsi définies : Le vecteur de voisinage est $V = (-1,0),(0,0),(1,0)$ La fonction locale de transition est une fonction de Q^3 dans Q et son expression est donnée par :

$$\begin{aligned} z_{ij}(t+1) &= f_2(z_{ij}(t), z_{i-1j}(t), z_{i+1j}(t)) \\ &= \mu_1 z_{ij}(t) + \mu_2 z_{i-1j}(t) + \mu_3 z_{i+1j}(t) + \mu \end{aligned}$$

La configuration $U(t)$ obtenue est entièrement définie par une fonction locale de transition telle que :

$$\begin{aligned} U_{ij}(t+1) &= f(z_{ij}, z_{ij-1}, z_{ij+1}, z_{i-1j-1}, z_{i-1j}, z_{i-1j+1}, z_{i+1j-1}, z_{i+1j}, z_{i+1j+1})(t+1) \\ &= \alpha_1 z_{ij}(t) + \alpha_2 z_{ij-1}(t) + \alpha_3 z_{ij+1}(t) + \alpha_4 z_{i-1j}(t) + \alpha_5 z_{i-1j-1}(t) \\ &+ \alpha_6 z_{i-1j+1}(t) + \alpha_7 z_{i+1j}(t) + \alpha_8 z_{i+1j-1}(t) + \alpha_9 z_{i+1j+1}(t) + \alpha \end{aligned}$$

En faisant évoluer $H1$ et $H2$, on obtient :

$$\begin{aligned} U_{ij}(t) &= \mu_1 y_{ij}(t) + \mu_2 y_{i-1j}(t) + \mu_3 y_{i+1j}(t) + \mu \\ &= \mu_1(\beta_1 z_{ij}(t) + \beta_2 z_{ij-1}(t) + \beta_3 z_{ij+1}(t) + \beta) \\ &+ \mu_2(\beta_1 z_{i-1j}(t) + \beta_2 z_{i-1j-1}(t) + \beta_3 z_{i-1j+1}(t) + \beta) \\ &+ \mu_3(\beta_1 z_{i+1j}(t) + \beta_2 z_{i+1j-1}(t) + \beta_3 z_{i+1j+1}(t) + \beta) + \mu \end{aligned}$$

Il suffit de prendre :

$\alpha_1 = \mu_1\beta_1$ $\alpha_2 = \mu_1\beta_2$ $\alpha_3 = \mu_1\beta_3$
$\alpha_4 = \mu_2\beta_1$ $\alpha_5 = \mu_2\beta_2$ $\alpha_6 = \mu_2\beta_3$
$\alpha_7 = \mu_3\beta_1$ $\alpha_8 = \mu_3\beta_2$ $\alpha_9 = \mu_3\beta_3$
$\alpha = (\mu_1 + \mu_2 + \mu_3)\beta + \mu$

L'automate de dimension deux obtenu est homogène et linéaire. Si les fonctions locales de transition de $H1$ ou de $H2$ sont non linéaires, on obtient un automate de dimension deux non linéaire.

Proposition 2 : Si à partir de l'automate composé A, on veut obtenir directement les automates utilisés pour le construire, on devra résoudre un système d'équations non linéaires à nombres entiers au moins aussi complexe que :

$\alpha_1 = \mu_1\beta_1$ $\alpha_2 = \mu_1\beta_2$ $\alpha_3 = \mu_1\beta_3$
$\alpha_4 = \mu_2\beta_1$ $\alpha_5 = \mu_2\beta_2$ $\alpha_6 = \mu_2\beta_3$
$\alpha_7 = \mu_3\beta_1$ $\alpha_8 = \mu_3\beta_2$ $\alpha_9 = \mu_3\beta_3$
$\alpha = (\mu_1 + \mu_2 + \mu_3)\beta + \mu$

où les inconnues sont $\mu_1, \mu_2, \mu_3, \mu, \beta_1, \beta_2, \beta_3$ et β.

Preuve : Ce résultat est immédiat si la fonction de transition de l'automate composé est linéaire. On obtient exactement l'équation ci-dessus (voir illustration). Avec des fonctions de transition non linéaires, le système d'équations non linéaires obtenu est plus complexe .

En dimension un, on sait construire des automates cellulaires inversibles. Si $H1$ et $H2$ sont inversibles, alors les deux automates $A1$ et $A2$ qui sont des agrégations des automates $H1$ et $H2$ le sont également. L'automate $A = A2oA1$ est à deux dimensions et est inversible. En vue d'utiliser A comme clé publique d'un cryptosystème, on peut construire d'abord $A1$ et $A2$, de sorte qu'ils soit inversibles et en déduire A, comme composition de $A2$ et $A1$. La clé publique sera $A = A2oA1$ et la clé privée sera $A^{-1} = A1^{-1}oA2^{-1}$.

4. Un cryptosystème à clés publiques

4.1. Exemple de construction d'un automate cellulaire à deux dimensions inversible

L'automate cellulaire que nous considérons ici a des configurations périodiques. On peut dont l'implémenter en utilisant une grille carrée de $L \times L$ cellules. La grille ainsi définie peut être considérée comme une agrégation de grilles de dimension un dans le sens horizontal et dans le sens vertical.

Considérons l'automate cellulaire fini à une dimension de L cellules, dont la fonction lo-

cale de transition est définie par :

$$x_i(t) \quad = \quad (a_0 x_i(t-1) + a_1 x_{i-1}(t-1) + d) mod B \qquad [1]$$

où B est un entier premier strictement supérieur à 2, les a_j $(0 \leq j < L)$ et d sont des éléments de l'ensemble des entiers modulo B (x mod r représente le reste de la division de x par r), $V(i)$ est égal à $i, i-1$. Cet automate cellulaire a été largement étudié dans [8]. Les trajectoires décrites par les configurations de cet automate peuvent être toutes cycliques si ses paramètres sont convenablement choisis [8].Chaque cellule de cet automate prend ses états dans l'ensemble $0, 1, 2, ?, B-2, B-1$ que nous notons par la suite Z^B, où B est un nombre premier. Si L le nombre de cellules de chaque automate de l'ensemble est aussi un nombre premier, on montre qu'il y a soit zéro soit $\Phi(B_{L-1-1})$ automates cellulaires de l'ensemble que nous considérons qui exhibent dans leurs graphes de transition le cycle de longueur maximale $B^L - B$, où Φ est la fonction indicatrice d'Euler ($\Phi(x)$ est le nombre d'entiers inférieurs à x premier avec x).
Exemple 1 : Quelques automates inversibles définis par la relation (1)
a)$B = 5, l = 3, x_i(t+1) = (4x_i(t) + 2x_{i-1}(t) + 1) mod 5$
b)$B = 131, l = 7, x_i(t+1) = (130x_i(t) + 2x_{i-1}(t) + 2) mod 131$
c)$B = 16087, l = 5, x_i(t+1) = (6904x_i(t) + 9184x_{i-1}(t) + 3) mod 16087$

Considérons un autre automate défini de la façon suivante : - le nombre de cellules est $N = 2L$. Une configuration $Z(t) = (z_0(t), z_1(t), \cdots, z_{L-1}(t), Z_0(t), Z_1(t), \ldots, Z_{L-1}(t))$
- la fonction locale de transition est la même pour les L premières cellules. Cette fonction qui est non linéaire est définie de la façon suivante :

$z_j(t+1) = (b_0 Z_j(t) + b_1 Z_{j-1}(t) + d_1 + a_0^2 Z_j(t) Z_{j+1}(t) + a_0 a_1 Z_j(t)^2 + a_0 d_0 Z_j(t) + a_0 z_j(t) z_{j+1}(t) z_{j+2}(t)$
$+ a_0 a_1 Z_{j-1}(t) Z_{j+1}(t) + a_1^2 Z_{j-1}(t) Z_j(t) + a_1 d_0 Z_{j-1}(t) + a_1 Z_{j_1}(t) z_{j+1}(t) z_{j+2}(t) + d_0 a_0 Z_{j+1}(t)$
$+ d_0 a_1 Z_j(t) + d_0^2 + d_0 z_{j+1}(t) z_{j+2}(t) + a_0 z_j(t) z_{j+1}(t) Z_{j+1}(t) + a_1 z_j(t) z_{j+1}(t) Z_j(t)$
$+ d_0 z_j(t) z_{j+1}(t) + z_j(t) z_{j+1}(t)^2 z_{j+2}(t)) mod B$

- la fonction locale de transition est la même pour les L dernières cellules. Cette fonction qui est aussi non linéaire est définie de la façon suivante :
$Z_j(t) = (a_0 Z_j(t) + a_1 Z_{j-1}(t) + d_0 + z_j(t) z_{j+1}(t)) mod B$
Proposition 3 : L'automate défini ci-dessus dont la fonction locale de transition est donnée par les équations (2) et (3) est une composition de deux automates partiellement linéaire de dimension un.
Preuve : Elle peut se faire par construction. Considérons deux automates cellulaires de dimension un de taille L dont la fonction locale de transition est définie par la relation (1) : le premier automate a pour coefficients de la fonction locale de transition (a_0, a_1) le second automate a pour coefficients de la fonction locale de transition (b_0, b_1)

Considérons l'automate cellulaire de dimension un de taille $2L$ dont la fonction globale de transition est donnée par :
$Y(t+1) = f(z_0(t), z_1(t), \ldots, z_{L-1}(t), Z_0(t), Z_1(t), \ldots, Z_{L-1}(t))$ Il suffit d'appliquer à la configuration $Y(t)$ les deux fonctions globales G et H définies par :

$G_j(t+1) = a_0 Z_j(t) + a_1 Z_{j-1}(t) + d_0 + z_j(t) z_{j+1}(t) \quad si 0 \leq j \leq L-1$
$G_{j+L}(t+1) = z_j(t) \quad si 0 \leq j \leq L-1$
$H_j(t+1) = b_0 Z_j(t) + b_1 Z_{j-1}(t) + d_1 + z_j(t) z_{j+1}(t) \quad si 0 \leq j \leq L-1$
$H_{j+L}(t+1) = z_j(t)$

On vérifie aisément qu'on a bien $Y = HoG$?

Si les coefficients $(a_i)0 \leq i \leq 1$ et $(b_i)0 \leq i \leq 1$ sont convenablement choisies [8], alors les fonctions H et G sont inversibles et donc Y est inversible. L'automate cellulaire défini par Y est de dimension un, n'est pas uniforme, est inversible et sa fonction locale de transition est non linéaire. Nous l'utilisons pour construire notre automate de dimension deux comme indiqué dans la section 2.

Exemple : si $B = 5$ et $L = 3$, l'automate Y associé est défini par : la fonction locale de transition est la même pour les 3 premières cellules : $z_j(t+1) = (4Z_j(t)+2Z_{j-1}(t)+ Z_j(t)Z_{j+1}(t) + 3Z_j(t)^2 + 4Z_j(t) + 4z_j(t)z_{j+1}(t)z_{j+2}(t) + 3Z_{j-1}(t)Z_{j+1}(t) + 4Z_{j-1}(t)Z_j(t) + 2Z_{j-1}(t) + 2Z_{j_1}(t)z_{j+1}(t)z_{j+2}(t) + 4Z_{j+1}(t) + 2Z_j(t) + z_{j+1}(t)z_{j+2}(t) + 4z_j(t)z_{j+1}(t)Z_{j+1}(t) + 2z_j(t)z_{j+1}(t)Z_j(t) + z_j(t)z_{j+1}(t) + z_j(t)z_{j+1}(t)^2z_{j+2}(t) + 2)mod5$

- la fonction locale de transition est la même pour les 3 dernières cellules :
$Z_j(t) = (4Z_j(t) + 2Z_{j-1}(t) + z_j(t)z_{j+1}(t) + 1)modB$

En appliquant cette fonction d'abord sur les lignes d'une grille de dimension deux, ensuite sur les colonnes de la même grille, on obtient un automate de dimension 2 inversible, dont la fonction locale de transition est non linéaire.
Pour crypter des messages, il suffit de décomposer le texte clair en chaîne de bits, et de regrouper les bits par blocs de k bits tels que $2^k \leq B < B^{k+1}$. $N2$ blocs qui se suivent sont ensuite organisés en grille de $N \times N$ blocs, et définissent ainsi une configuration de l'automate cellulaire de dimension deux.

4.2. Publication de la clé publique

Deux approches peuvent être utilisées pour transférer la clé publique à tout utilisateur devant expédier des messages cryptés :

– la première approche consiste à transmettre une procédure qui calcule l'état d'une cellule connaissant l'état de ses voisines. Les paramètres de cette procédure sont les coefficients appliqués aux différents états des voisins d'une cellule, le nombre de lignes (ou de colonnes) L de la grille, une éventuelle constante additive finale.

– la deuxième approche est à utiliser si on n'a pas une expression analytique de la fonction locale de transition de l'automate A. On transmet la table qui à chaque m-uplet possible d'états des voisins d'une cellule associe un nouvel état de la cellule considérée. La taille de la table peut être très grande. Elle est de l'ordre de $B^m log(B)$ où m est la taille du voisinage et B est le nombre des états d'une cellule.

4.3. Sécurité du cryptosystème

La sécurité du cryptosystème que nous proposons repose sur deux résultats théoriques . Le premier résultat dit qu'en dimension au moins égale à deux, le problème de savoir si un automate cellulaire est inversible est indécidable [6]. Si on sait a priori qu'un automate cellulaire de ce type est inversible et est la composée de M autres automates cellulaires, on peut essayer de trouver les automates composés en suivant le processus de construction de la section 2. Dans ce cas , on sera amené à résoudre un grand système d'équations non linéaires dont les inconnues et les coefficients sont des entiers. Le temps de résolution d'un tel système est en général exponentiel [13]. Si un pirate intercepte la clé publique il y a très peu de chances qu'il découvre la clé privée.

5. Conclusion

Nous avons dans ce papier , proposé une approche de construction des automates cellulaires de dimension deux inversibles, et nous avons construit un cryptosystème basé sur cette approche. La sécurité de ce système est fondée sur le fait qu'il n'existe pas de procédure efficace connue pour calculer l'inverse d'un automate cellulaire de dimension deux. Il est clair que le temps nécessaire pour crypter une grille de L^2 cellules de données est proportionnel à L^2m, où m est la taille du voisinage d'une cellule. Le temps de déchiffrement est pratiquement du même ordre. Ces deux opérations peuvent se faire donc efficacement. Les constructions faites dans ce papier aboutissent à un automate de dimension deux. Elles peuvent s'étendre sans problème aux automates cellulaires de dimension d quelconque. Le logiciel qui implémente ce cryptosystème est en cours de mise en oeuvre. Nous expérimenterons alors d'autres techniques de cryptanalyse telle que la cryptanalyse à texte clair connu, la cryptanalyse à texte chiffré connu.

Remerciements : Ce travail a été fait en partie grâce au soutien du GIS SARIMA, qui a financé un séjour de l'auteur à l'université d'Artois, en France.

6. Bibliographie

[1] S. AMOROSO, N. PATT, « Decision procedures for surjectivity and injectivity of parallel maps for tessalation structures », *J. Comp. Syst. Sci.*,n° 6,448-464,1972.

[2] B. DURAND « Automates cellulaires : réversibilité et complexité », *Thèse de Doctorat*, Ecole Normale Suprieure de Lyon, Université Claude Bernard-Lyon I, 1994

[3] P. GUAN « Cellular automata public-key cryptosystems » *Complex Systems*,vol. 1, 1987

[4] H. GUTOWITZ « Cryptography with dynamical systems », in *cellular automata and cooperative phenomena*, Eds, E. Goles and N. Boccara, Kluwer Academic Pres, 1993

[5] KAREL CULIK II « On invertible cellular automata » *Complex System*, vol. 1 , 1987

[6] J. KARI « Cryptosystems based reversible cellular automata » *Preprint*, University of Turku, Finland

[7] J. KARI « Reversibility of 2D cellular automata is undecidable » *Physica D* vol. 45 ,pp379-385, 1990

[8] G. TINDO « Un algorithme de cryptographie à clés symétriques » *Annales de la faculté des sciences* Série Math-Phys-Info, vol. 33, pp51-60,2004

[9] T. TOFFOLI , N. MARGOLUS « Invertible cellular automata : A review » *Physica D*,vol. 666, pp1-23, 1994

[10] J. URIAS , E. ULGADE , G. SALAZAR « A cryptosystem based on cellular automata » *Chaos* vol. 8 n° 4 , pp819-822, 1998

[11] S. WOLFRAM « Cryptography with cellular automata » *Proceedings of Crypto*, vol. 85, pp429-432, 1985

[12] D. RICHARDSON « Tessellation with local transformation » *J. Comp. Syst. Sci* n° 6, pp373-388, 1972

[13] P. GUAN , H. ZASSENHAUS « Solving systems of equations over finite fields » *Journal of Number Theory* 1987