

République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
École Normale Supérieure, Kouba(Alger)



Département de Mathématiques

MÉMOIRE

Pour l'obtention du grade de

MAGISTER

Spécialité : **Mathématiques**

Option : **Algèbre et théorie des nombres**

Présenté par

Adel BRAHMI

Thème

**ANALYSE DES GÉNÉRATEURS D'ALÉAS BASÉS SUR
LES FCSR**

Soutenu le : 16 -12 -2015

Devant la Commission d'Examen

Mr. Abdelhafid MOKRANE	Professeur, E.N.S-Kouba	Président.
Mr. Abdallah DERBAL	Professeur, E.N.S-Kouba	Examinateur.
Mr. Djilali BENAYAT	Professeur, E.N.S-Kouba	Examinateur.
Mr. Abdellah MOKRANE	Professeur, Université Paris 8	Co-Directeur de mémoire.
Mr. Abdelaziz CHOUTRI	M.C.A, E.N.S-Kouba	Directeur de mémoire.

Table des matières

1	Outils mathématiques	14
1.1	Les corps finis	15
1.2	Les séries formelles	16
1.3	Les entiers p-adiques	18
1.4	Les matrices	19
2	Préliminaire	22
2.1	Introduction	23
2.2	Les séquences pseudo-aléatoires	25
2.3	Les critères de pseudo-aléatoire	26
2.4	Séquence	26
2.5	Générateurs des séquences pseudo-aléatoires	27
2.6	Registres à décalage et à rétroaction linéaire (LFSR)	29
2.6.1	Périodicité de LFSR	32
2.6.2	Fonction génératrice	32
2.7	Modes de connexion du LFSR	36
2.7.1	Mode Fibonacci	36
2.7.2	Mode Galois	37
2.8	Utilisation moderne des LFSR	39
2.8.1	Les LFSR combinés	39
2.8.2	Les LFSRs filtrés	39
2.8.3	Le générateur par rétrécissement	40
2.8.4	Les générateurs par combinaison avec retenue	41

2.9	Représentation matricielle	42
2.10	Polynôme de connexion minimal	46
2.11	Complexité linéaire	47
2.12	Séquences maximales	48
2.13	Algorithme de Berlekamp-Massey	51
3	Registres à décalage et à rétroaction avec retenue (FCSR)	53
3.1	Registres à décalage et à rétroaction avec retenue (FCSR)	54
3.1.1	Généralités sur les FCSRs	54
3.1.2	Analyse des FCSRs	56
3.2	Comportement de la mémoire	64
3.3	Mode de connexion du FCSR	66
3.3.1	FCSR en mode Fibonacci	66
3.3.2	FCSR en mode Galois	67
3.4	FCSR-Séquences maximales (l-séquence)	68
3.5	Représentation exponentielle des FCSRs séquences	70
3.6	Durée et complexité p-adique	71
4	Registres à décalage et à rétroaction avec retenue filtré (F-FCSR)	73
4.1	Introduction	74
4.2	Description du matériel de FCSR et la fonction de transition	76
4.3	Conception d'un générateur FCSR filtré	80
4.4	Description des propositions de F-FCSR	82
4.5	Nouveau Design	84
4.5.1	F-FCSR-H	84
4.5.2	F-FCSR-16	85
4.6	Faiblesses de FCSR Automaton et de la famille F-FCSR	87
4.7	L'attaque de M. Hell et T. Johansson pour briser le F-FCSR-H	90
4.8	Amélioration de la complexité d'attaque	93
5	Programmation	97
5.1	Registre à décalage et à rétroaction linéaire LFSR	98

5.1.1	LFSR en mode Fibonacci	98
5.1.2	LFSR en mode Galois	99
5.1.3	Berlekamp-Massey	101
5.1.4	Fonction génératrice	105
5.2	Registre à décalage et à rétroaction avec retenue (FCSR)	107
5.2.1	FCSR en mode Fibonacci	107
5.2.2	FCSR en mode Galois	108
5.2.3	L'entier p-adique sur la forme $\left(\frac{s}{q}\right)$	110
5.2.4	L'ordre de p modulo q	111
5.3	Registre à décalage et à rétroaction avec retenue filtre (F-FCSR)	112
5.3.1	FCSR Filtre (F-FCSR)	112
5.3.2	F-FCSR-H	115

Table des figures

2.1	Un modèle simple pour les bits de chiffrement.	24
2.2	Une explication simple d'un chiffrement à flot.	24
2.3	Registre à décalage et à rétroaction.	28
2.4	Registre à décalage et à rétroaction linéaire LFSR.	30
2.5	Conception de LFSR de taille 4.	31
2.6	LFSR en mode Fibonacci.	37
2.7	LFSR en mode Galois.	37
2.8	LFSR combinés.	39
2.9	LFSRs Filtrés.	40
2.10	Le générateur rétrécissant.	41
2.11	Le générateur auto-rétrécissant.	41
2.12	Générateur par combinaison avec mémoire.	42
3.1	Registre à décalage et à rétroaction avec retenue ou FCSR.	55
3.2	FCSR en mode Fibonacci.	67
3.3	FCSR en mode Galois.	68
4.1	FCSR en mode Galois $\mathbb{F} = (\mathbb{F}_2, -347)$	77
4.2	L'addition avec retenue.	77
4.3	Un aperçu de F-FCSR-H.	85

Liste des tableaux

2.1	Conception de LFSR $\mathbb{L} = (\mathbb{F}_2, 4, (1, 0, 0, 1))$	31
2.2	Conception de LFSR en mode Galois $\mathbb{L} = (\mathbb{F}_2, 4, (1, 0, 0, 1))$	38
2.3	La relation entre les m-séquences et les polynômes de connexion primitifs.	49
2.4	L'application de l'algorithme de Berlekamp-Massay sur 110101100100011	52
3.1	Conception de FCSR $\mathbb{F} = (\mathbb{F}_2, 5, (1, 1, 0, 1, 1))$	56

Notations

Dans toute la suite, les notations utilisées sont, dans la plupart des cas, définies dans le texte, néanmoins, quelques notations ou définitions "standards" ont été volontairement omises. Nous les rappelons ci-dessous :

\mathbb{N}	L'ensemble des entiers naturels.
\mathbb{Z}	L'ensemble des entiers relatifs.
\mathbb{Z}_p	L'ensemble des entiers p-adiques.
\mathbb{F}_p	Un corps fini à p éléments.
p	Un nombre premier.
\underline{a}	Une séquence.
$per(\underline{a})$	La période de la séquence \underline{a} .
$Seq_p(\alpha)$	La séquence dans \mathbb{F}_p associée à l'entier p-adique α .
$a(x)$	Une série formelle.
$\mathbb{F}_p[[X]]$	L'anneau des séries formelles où les coefficients sont dans \mathbb{F} .
$Ord(q(x))$	L'ordre d'un polynôme $q(x)$.
$deg(q)$	Le degré d'un polynôme $q(x)$.
$Ord_q(p)$	L'ordre d'un entier p modulo q .
$TR(A)$	La trace d'une matrice A .
$GF(2)$	Le corps $\{\bar{0}, \bar{1}\}$.
$W_H(d)$	Le poids de Hamming de d , $d \in \mathbb{Z}$.
PSG	Pseudo-random Sequence Generators.
FSR	Feedback Shift Register.
LFSR	Linear Feedback Shift Register .
NLFSR	Non Linear Feedback Shift Register .

FCSR Feedback with Carry Shift Register.
DES Data Encryption Standard.
CDMA Code Design Multiple Access.
BER Bit Error Rate.
DES Data Encryption Standard.

Résumé

Dans ce mémoire, nous avons étudié les séquences et les générateurs des séquences pseudo-aléatoires (LFSR, FCSR, F-FCSR, F-FCSR-H), et nous avons détaillé l'article "Breaking the F-FCSR-H Stream Ciphers in Real Time" de M. Hell and T. Johansson publié dans "International Association for Cryptologic Research 2008".

Dans le premier chapitre, nous définissons les séquences pseudo-aléatoires et leurs caractéristiques, comment les obtenir grâce à leur génération par des générateurs pseudo-aléatoires qui sont basés sur une fonction de rétroaction linéaire. On utilise quelques définitions et théorèmes d'algèbre pour étudier les propriétés de ces générateurs et chercher comment obtenir une période maximale. Aussi, nous rappelons comment analyser un "LFSR" et récupérer la séquence par l'algorithme de "Berlekamp-Massey".

Dans le deuxième chapitre nous avons étudié les mêmes éléments que dans le chapitre précédent appliqué à un autre type de générateurs qui utilise une fonction de rétroaction non linéaire "FCSR".

Dans le troisième chapitre nous avons détaillé l'article "Breaking the F-FCSR-H Stream Ciphers in Real Time". Nous avons étudié un "F-FCSR", qui est un générateur de séquence pseudo-aléatoire basé sur un FCSR on mode Galois avec un filtre. Pour éviter une cryptanalyse par l'algorithme d'approximation rationnelle. Et nous sommes concentrés sur l'étude "F-FCSR-H" et toutes ses propriétés. Nous avons expliqué le fossé et comment l'exploiter afin d'analyser le F-FCSR-H et extraire la séquence.

Dans le quatrième chapitre nous avons programmé tous les générateurs que nous avons étudié précédemment ainsi que l'algorithme de "Berlekamp-Massey" avec des exemples en fortran 95 et en scilab.

Mots clés

cryptologie, cryptographie, cryptanalyse, séquence pseudo-aléatoire, générateur de séquence(LFSR, FCSR, F-FCSR, F-FCSR-H), m-séquence, l-séquence, fonction de rétroaction.

ملخص

تتمحور هذه المذكرة حول دراسة سلاسل الشفرات و مولداتها الشبه عشوائية $LFSR$ ، $FCSR$ ، $F - FCSR - H$ ، $F - FCSR$. وقمنا بدراسة تحليلية للمقال "Breaking the F-FCSR-H Stream Ciphers in Real Time" de M. Hell and T. Johansson publié dans "International Association for Cryptologic Research 2008".

في البداية قدّمنا سلاسل الشفرات و خصائصها و كيفية الحصول عليها من مولدات تعتمد على دوال إرجاع خطية $LFSR$. و استعملنا بعض التعاريف و النظريات في الجبر لدراسة خصائصها و كيفية توليد سلسلة شفرات مثالية تمتلك أكبر دور ممكن . و عرضنا أيضا كيفية كسر تشفير $LFSR$ و استعادة الشفرة باستعمال خوارزمية "Berlekamp - Massey" . ثمّ درسنا نفس العناصر في الفصل السابق مطبقة على مولد شفرات آخر يعتمد على دالة إرجاع غير خطية هو $FCSR$.

في الفصل الثالث قمنا بدراسة تحليلية للمقال المذكور سابقا، والذي يتعمق في دراسة مولد شفرات مصمّم على $FCSR$ بإضافة فلتر هو $F - FCSR$. و ركزنا الدراسة على $F - FCSR - H$ مع ذكر تركيبه. و شرحنا الثغرة التي اكتشفت في برمجته و كيفية كسر الشفرة و استرجاعها.

و في الأخير وضعنا خوارزميات و برمجنا كل مولدات الشفرات المدروسة سابقا و كذا خوارزمية "Berlekamp - Massey" بلغة 95 - fortran و scilab .

كلمات مفتاحية

علم التعمية، سلاسل شفرات، مولد شفرات ($LFSR, FCSR, F - FCSR, F - FCSR - H$) ، دور أعظمي لسلسلة شفرات، خوارزمية، برمجة، دالة إرجاع.