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

Table des figures

Liste des tableaux

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-adique.
$\mathbb{F}_p$	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 $\{\overline{0}, \overline{1}\}$.
$W_H(d)$	Le poids de Hamming de d, $d \in \mathbb{Z}$.
PSG	Pseudo-random Seqence 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.

ملخّص

تتمحور هذه المذكّرة حول دراسة سلاسل الشفرات و مولّداتها الشبه عشوائية $LFSR$ ، $FCSR$ $F-FCSR$ ، $F-FCSR-H$. 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 كيفيّة 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 مطبّقة 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 خوارزميّة "$Berlekamp-Massey$" بلغة $fortran-95$ و $scilab$.

كلمات مفتاحيّة

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