

UNIVERSITÉ Paris 8 - Vincennes Saint-Denis  
**ÉCOLE DOCTORALE**  
COGNITION, LANGAGE, INTERACTION  
**LABORATOIRE**  
ANALYSE, GÉOMÉTRIE ET APPLICATION (LAGA), UMR 7539

# THÈSE

pour obtenir le titre de

**Docteur**

de l'Université Paris 8

**En : Informatique**

**Option : Cryptographie**

Présentée et soutenue par

Boufeldja ALLAILOU

## Conception et Évaluation des Générateurs d'Aléa

soutenue le 18 Décembre 2010

**Jury :**

<i>Directeur :</i>	Farid MOKRANE	- Université Paris 8
<i>Co-Directeur :</i>	Karim DROUCHE	- Université de Cergy-Pontoise
<i>Rapporteurs :</i>	Jean-Marc COUVEIGNES	- Université de Toulouse II
	Makoto MATSUMOTO	- University of Tokyo
<i>Examineurs :</i>	Nicolas T. COURTOIS	- University College London
	Philippe GUILLOT	- Université Paris 8.



# Table des matières

<b>1</b>	<b>Introduction</b>	<b>1</b>
1.1	Registres à décalage à rétroaction . . . . .	2
1.2	Construction des Générateurs de flot de chiffrement . . . . .	4
1.2.1	Le générateur à combinaison non linéaire . . . . .	4
1.2.2	Le générateur filtré . . . . .	4
1.2.3	Le générateur par combinaison avec mémoire . . . . .	5
1.2.4	Le générateur par rétrécissement . . . . .	5
1.3	Quel standard pour les chiffrement par flot . . . . .	6
1.4	Travaux développés dans cette thèse . . . . .	8
1.5	Plan de la Thèse . . . . .	9
<b>I</b>	<b>Théorie des Registres à décalage à Rétroaction</b>	<b>11</b>
<b>2</b>	<b>Registres à Décalage à Rétroaction Linéaire (LFSRs)</b>	<b>13</b>
2.1	Introduction . . . . .	13
2.2	Définition et propriété périodique des LFSR séquence . . . . .	13
2.3	Opérateur de décalage à gauche . . . . .	13
2.4	Polynôme minimal d'une LFSR séquence . . . . .	14
2.5	Périodicité . . . . .	15
2.6	Structure de $G(f)$ pour $f$ irréductible . . . . .	16
2.7	Structure de $G(f)$ pour $f$ produit de polynômes irréductibles distincts . . . . .	16
2.8	Représentation matricielle . . . . .	17
2.9	Représentation par trace . . . . .	17
<b>3</b>	<b>Registres à Décalage à Rétroaction avec Retenues (FCSRs)</b>	<b>19</b>
3.1	Théorie des nombres 2-adiques . . . . .	19
3.2	Généralités Sur les FCSRs . . . . .	22
3.3	Analyse des FCSRs . . . . .	22
3.3.1	Comportement de la mémoire . . . . .	23
3.3.2	Initialisation et Algorithme . . . . .	23
3.3.3	Représentation exponentielle des FCSRs séquences . . . . .	24
3.3.4	État initial dégénéré . . . . .	24
3.4	Représentations . . . . .	25
3.4.1	Fibonacci FCSR . . . . .	25
3.4.2	Galois FCSR . . . . .	25

<b>4</b>	<b>Registres à Décalage à Rétroaction avec Retenues Vectoriel (VFCSRs)</b>	<b>27</b>
4.1	Introduction . . . . .	27
4.2	Formalisme . . . . .	27
4.3	Calcul sur $(\mathbb{F}_2, P, \mathcal{B})$ . . . . .	28
4.4	Analyse des VFCSRs sur $(\mathbb{F}_2, P, \mathcal{B})$ . . . . .	28
4.4.1	Norme et Analyse par rapport à une autre base . . . . .	29
4.4.2	Périodicité et $l$ -séquences . . . . .	29
4.4.3	Représentation exponentielle Vectorielle . . . . .	30
4.4.4	Comportement de la mémoire dans le cas vectoriel . . . . .	31
4.4.5	Etat initial . . . . .	31
4.5	Conclusion . . . . .	32
<b>5</b>	<b>Conception et analyse des FCSRs Vectorielles sur <math>\mathbb{F}_4</math></b>	<b>33</b>
5.1	Introduction . . . . .	33
5.2	Conception des VFCSRs $\mathbb{F}_4$ . . . . .	33
5.2.1	Fonctionnement du registre . . . . .	33
5.2.2	Relations de récurrence et matrice de connexion . . . . .	34
5.3	Analyse . . . . .	35
5.3.1	Correspondance avec $(\mathbb{Z}_2)^2$ . . . . .	35
5.3.2	Matrice de connexion . . . . .	35
5.3.3	Déterminant . . . . .	36
5.3.4	Cas de Goresky-Klapper ( $\mathbb{F}_2$ ) . . . . .	36
5.4	$l$ -séquences sur $\mathbb{F}_4$ . . . . .	37
5.5	Implantation . . . . .	37
5.5.1	Cas quadratique . . . . .	37
5.5.2	Recherche des paramètres . . . . .	38
5.5.3	Exemples . . . . .	40
5.6	Propriétés pseudo-aléatoires des VFCSRs . . . . .	41
5.7	Conclusion . . . . .	45
<b>II</b>	<b>Chiffrement par flot</b>	<b>47</b>
<b>6</b>	<b>Chiffrement par flot F-FCSR</b>	<b>49</b>
6.1	Introduction . . . . .	49
6.2	Automate FCSR . . . . .	49
6.2.1	Déscription de l'automate FCSR . . . . .	50
6.2.2	Fonction de transition . . . . .	51
6.3	Chiffrement par flot F-FCSR-H v2 . . . . .	51
6.3.1	Paramètres du F-FCSR-H v2 . . . . .	51
6.3.2	Conception du filtre . . . . .	52
6.3.3	Initialisation (Key+IV setup) . . . . .	52
6.3.4	Extraction des données pseudo-aléatoires . . . . .	53
6.4	Attaque du F-FCSR-H v2 . . . . .	54
6.5	Conclusion . . . . .	54

<b>7</b>	<b>Nouvelle famille de chiffrement par flot</b>	<b>57</b>
7.1	Introduction . . . . .	57
7.2	Galois VFCSR . . . . .	57
7.2.1	Formalisme . . . . .	57
7.2.2	Cas quadratique . . . . .	59
7.3	Automate VFCSR Quadratique (VFCSR-Q) . . . . .	59
7.3.1	Description de l'automate . . . . .	60
7.3.2	Fonction de transition . . . . .	61
7.4	Description hardware de l'automate VFCSR-Q . . . . .	66
7.4.1	Analyse . . . . .	66
7.4.2	Implantation des éléments des fonctions de transitions . . . . .	68
7.5	Implantation du VFCSR-Q-H . . . . .	77
7.5.1	Les paramètres proposés . . . . .	77
7.5.2	Propriétés pseudo-aléatoire du Galois VFCSR . . . . .	77
7.5.3	Aspect d'équivalence . . . . .	78
7.6	Conception de l'algorithme de chiffrement par flot version Hardware . . . . .	79
7.6.1	Conception du filtre . . . . .	79
7.6.2	Extraction des données pseudo-aléatoires . . . . .	79
7.7	Sécurité du F-VFCSR-Q-H . . . . .	81
7.8	Conclusion . . . . .	82

### **III Les Générateurs Pseudo-aléatoires Cryptographiquement sûrs** **83**

<b>8</b>	<b>Génération de courbes elliptiques cryptographiques</b>	<b>85</b>
8.1	Introduction . . . . .	85
8.2	Arithmétique des courbes elliptiques . . . . .	86
8.2.1	Les courbes elliptiques sur l'ensemble $\mathbb{R}$ . . . . .	87
8.2.2	Les courbes elliptiques sur les corps finis . . . . .	89
8.3	Génération des courbes elliptiques cryptographiques . . . . .	90
8.3.1	Les courbes elliptiques sur $\mathbb{F}_p$ . . . . .	90
8.3.2	Génération par l'approche aléatoire[62] . . . . .	91
8.4	Conclusion . . . . .	93
<b>9</b>	<b>Générateur pseudo-aléatoire basé sur les courbes elliptiques</b>	<b>95</b>
9.1	Introduction . . . . .	95
9.2	Algorithme DEC-PRNG . . . . .	96
9.3	Attaque supposée sur le DEC-PRNG . . . . .	97
9.3.1	Description de l'attaque . . . . .	98
9.3.2	Implantation . . . . .	98
9.4	Test proposé . . . . .	99
9.4.1	Formalisme . . . . .	99
9.4.2	Implantation . . . . .	101
9.5	Conclusion . . . . .	103

8.1	Arithmétique sur les courbes elliptiques. . . . .	88
9.1	Diagramme du DEC-PRNG. . . . .	97