UNIVERSITE SIDI MOHAMED BEN ABDELLAH
FACULTE DES SCIENCES ET TECHNIQUES - FES
Centre d'Etudes Doctorales : Sciences et Techniques de l'Ingénieur

Fès, le 12/10/2013

N° d'ordre : 15/2013

THESE DE DOCTORAT

Présentée par

Mr: Abdelhakim Chillali

Spécialité : **Mathématiques / Informatique**

Sujet de la thèse :

Crypto système à clef publique et courbes elliptiques sur $\mathbb{F}_q[\varepsilon]$.

Thèse présentée et soutenue le 12/10/2013 devant le jury composé de :

Nom Prénom	Titre	Etablissement	
M'hamed Ziane	PES	Faculté des Sciences d'Oujda	Président
Fayçal Lamrini	PES	Faculté des Sciences Dhar El Mehraz de Fès	Rapporteur
Abdelmalek Azizi	PES	Faculté des Sciences d'Oujda	Rapporteur
Mohammed A. Elomary	PH	Faculté des Sciences et Techniques Errachidia	Rapporteur
Mostapha Azizi	PES	Ecole Supérieure de Technologie d'Oujda	Examinateur
Med Charkani El Hassani	PES	Faculté des Sciences Dhar El Mehraz de Fès	Directeur de thèse

Laboratoire d'accueil: Algèbre, Analyse Fonctionnelle et Applications
Etablissement: Faculté des sciences et Techniques
Laboratoire d'accueil: Algèbre, Géométrie et Arithmétique (LAGA)
Etablissement: Faculté des Sciences Dhar El Mehraz

Résumé de la thèse

Ce travail a été réalisé au sein du Laboratoire: Algèbre, Analyse Fonctionnelle et Applications à la Faculté des sciences et Techniques de Fès.

Nous avons abordé dans cette thèse des axes de recherche importants pour les protocoles cryptographiques, à savoir, d'une manière générale :

1. Groupe générique
2. Crypto système
3. Méthode d'identification

Dans le chapitre 2, on a généralisé de nombreuses propriétés sur les courbes elliptiques sur l'anneau $\mathbb{F}_q[\varepsilon]$, $\varepsilon^n = 0$.

Dans le chapitre 3, nous avons ainsi proposé un crypto système à base des matrices. Et enfin dans le chapitre 4, nous avons présenté des algorithmes de représentation, des procédures pour montrer que ces courbes peuvent former des groupes génériques et une méthode d'identification sur ces courbes.

Mots clés:
Courbes elliptiques, Anneau local, Corps fini, Cryptosystème, Algorithme, Logarithme discret..

Table des matières

Table des figures **vii**

I Principe de base de la cryptographie **7**

1 Article de Diffie Hellman (1976) 7

1.1 Cryptographie 8

1.2 Mécanismes de la cryptographie 9

1.3 Qu'entend-on par clé ? 9

2 La Cryptanalyse 10

3 Algorithmes de chiffrement 10

3.1 Sécurité de l'information 11

3.2 Chiffrement symétrique ou à clef secrète 12

3.2.1 Avantages 12

3.2.2 Faiblesses 12

3.3 Chiffrement asymétrique ou à clef publique 13

3.3.1 Algorithmes à empilement 13

3.3.2 Exemples 13

3.3.3 Avantages 14

3.4 Attaques sur les algorithmes asymétriques 14

3.4.1 Attaques au niveau des clefs 14

3.4.2 Attaque temporelle 15

II Courbe Elliptique Sur L'anneau $\mathbb{F}_q[\epsilon]$, $\epsilon^n = 0$ **17**

1 L'anneau $A_n = \mathbb{F}_q[\epsilon]$, $\epsilon^n = 0$ 17

2 Courbe Elliptique 21
2.1 Courbe elliptique sur un corps 21
2.2 Loi de groupe explicite 22
2.3 Isogénie 22
2.4 Courbes elliptiques sur A_n, $n \geq 1$ 24
2.5 Les morphismes π^k et θ_k 27
2.6 Les applications fondamentales 34

III Crypto système à clef publique **41**
1 Taille d'un entier naturel en base b 41
2 Fonction à sens unique 42
3 Le logarithme discret 43
4 Groupe Générique 44
5 Cryptosystème à bases des matrices 44
5.1 Principe de Diffie-Hellman 45
5.2 Loi du groupe 46
5.3 Description du MDLP Cryptosystème 47
5.4 Echange de clefs 47
5.5 Exemple 49
5.6 Exemple de cryptographie 50
6 Fonctions de chiffrement et de déchiffrement 54

IV Algorithmes de Représentation du groupe $E^n_{a,b}$ **57**
1 Représentation des éléments de A_n 57
1.1 Algorithme(1) : somme(p) 57
1.2 Algorithme(2) : produit(p) 57
1.3 Algorithme(3) : inverse(p) 58
1.4 Algorithme(4) :projection(1) 59
1.5 Algorithme(5) :projection(2) 60
2 Représentation du groupe $E^n_{a,b}$ 60
2.1 Algorithme(6) : Neutre 60
2.2 Algorithme(7) : projection(a) 61
2.3 Algorithme(8) : projection(b) 61
2.4 Algorithme(9) : appartient 62
2.5 Algorithme(10) : Egal 63

3 Loi de groupe sur $G^n_{a,b}$ 66
3.1 Les procedures $p1, p2, p3, p4, p5$ `et` $p6$ 66
3.2 Algorithme(11) : Somme 69
4 Structure de ($G^n_{a,b}$,Somme,Neutre,appartient,Egal) 70
4.1 Procedure msomme 70
4.2 Exemples 71
5 Méthodes d'identification sur $E^k_{a,b}$ 72
5.1 Une fonction fortement résistante aux collisions sur $E^k_{a,b}$ 72
5.2 Procédés d'identification sur $E^k_{a,b}$ 73

Conclusion générale et perspectives **75**

Références bibliographiques **77**