AVIS DE SOUTENANCE

THESE DE DOCTORAT

Présentée par

Mr: AZIZ BOULBOT

Spécialité : Mathématiques fondamentales et appliquées

Sujet de la thèse: Courbes elliptiques sur certains anneaux finis et application en cryptographie.

Formation Doctorale : Sciences de l'ingénieur Sciences Physiques, Mathématiques et Informatique.

Thèse présentée et soutenue le lundi 20 juillet 2020 à 10h au Centre de Conférence devant le jury composé de :

Nom Prénom	Titre	Etablissement	
Lhoussain EL FADIL	PES	Faculté des Sciences Dhar El Mehraz de Fès	Président
Mohamed Abdou ELOMARY	PES	Faculté des Sciences et Techniques de Settat	Rapporteur
Ali KACHA	PES	Faculté des Sciences de Kenitra	Rapporteur
Abdelkarim BOUA	PH	Faculté Polydisciplinaire de Taza	Rapporteur
Ismail AKHARRAZ	PH	Faculté Polydisciplinaire de Taza	Examinateur
Abdelhakim CHILLALI	PH	Faculté Polydisciplinaire de Taza	Examinateur
Ali MOUHIB	PES	Faculté Polydisciplinaire de Taza	Directeur de thèse

Laboratoire d'accueil : Sciences de l'Ingénieur.

Etablissement : Faculté Polydisciplinaire de Taza

Titre de la thèse : Courbes elliptiques sur certains anneaux finis et application en cryptographie.

Nom du candidat : AZIZ BOULBOT

Spécialité : Mathématiques fondamentales et appliquées

Résumé de la thèse

Le but de cette thèse est d'étudier les applications cryptographiques des courbes elliptiques définies sur des anneaux finis et non locaux.

Dans le premier chapitre, nous avons donné sous forme d'une introduction aux courbes elliptiques, des préliminaires nécessaires à l'élaboration de cette thèse.

Dans le deuxième chapitre, nous avons étudié les courbes elliptiques définies sur l'anneau $\mathbb{F}_q[e]$, où $e^2 = e$ et $\mathbb{F}_q$ est un corps fini d'ordre $q = p^d$avec p un nombre premier et d un entier positif. Le résultat essentiel, que nous avons montré, est l'isomorphisme entre la courbe elliptique $E_{a,b}(\mathbb{F}_q[e])$ et le groupe $E_{\pi_0(a),\pi_0(b)}(\mathbb{F}_q) \times E_{\pi_1(a),\pi_1(b)}(\mathbb{F}_q)$. Ce résultat nous a permis de munir la courbe elliptique $E_{a,b}(\mathbb{F}_q[e])$ d'une structure de groupe et de donner explicitement sa loi de groupe.

Dans le troisième chapitre, nous avons étudié les courbes elliptiques définies sur l'anneau $\mathbb{F}_q[e]$, où $e^3 = e^2$ et q est une puissance d'un nombre premier supérieur ou égal à 5. Après avoir classifié les points dans ces courbes elliptiques, nous avons donné explicitement leur loi du groupe.

Enfin dans le quatrième chapitre, nous avons donné deux systèmes de chiffrement entièrement homomorphe sur ces courbes.

Mots clés : Anneau fini, Anneau non-local, Caractéristique, Corps finis, Courbes elliptiques, Cryptographie, Chiffrement entièrement homomorphe, Equation de Weierstrass, Isomorphisme, Logarithme discret.