Centre d'Etudes Doctorales : Sciences et Techniques et Sciences Médicales

Avis de Soutenance

THESE DE DOCTORAT

Présentée par

Monsieur ZAKARIAE CHEDDOUR

Discipline : Mathématiques
Spécialité : Mathématiques fondamentales et appliquées

Sujet de la thèse

Sur des problèmes liés aux courbes elliptiques

Formation Doctorale " Sciences de l'Ingénieur, Sciences Physique, Mathématiques et Informatique"

Thèse présentée et soutenue **le samedi 30 septembre 2023 à 10h** à la Faculté Polydisciplinaire de Taza, devant le jury composé de :

Nom et Prénom	Titre	Etablissement	
M'hammed ZIANE	PES	Faculté des Sciences d'Oujda	Président
Abdelhamid TADMORI	PH	Faculté des Sciences et Techniques d'Al Hoceima	Rapporteur
Khadija BOUZKOURA	PH	Faculté des Sciences Ben M'sik de Casablanca	Rapporteur
Abdelkarim BOUA	PH	Faculté Polydisciplinaire de Taza	Rapporteur
Soumia LALAOUI RHALI	PES	Faculté Polydisciplinaire de Taza	Examinateur
ABDELALIM SEDDIK	PH	Faculté des Sciences Ain Chock de Casablanca	Examinateur
Ali MOUHIB	PES	Faculté Polydisciplinaire de Taza	Directeur de Thèse
Abdelhakim CHILLALI	PH	Faculté Polydisciplinaire de Taza	Co-Directeur de Thèse

Laboratoire de recherche : Sciences de L'Ingénieur
Etablissement : Faculté Polydisciplinaire de Taza

Résumé de la thèse

Cette thèse explore les principes fondamentaux des courbes elliptiques, puis étend leur applicabilité au-delà des nombres rationnels, englobant les corps de nombres cyclotomiques quadratiques et s'étendant des corps finis aux extensions de corps finis. L'étude commence par un examen des courbes elliptiques sur le corps des nombres rationnels Q, fournissant ainsi une base solide dans la théorie de base. En s'appuyant sur ces bases, la thèse se plonge dans l'exploration des courbes elliptiques sur les corps de nombres cyclotomiques quadratiques, introduisant de nouvelles perspectives et des défis. De plus, l'enquête élargit le champ d'application des courbes elliptiques des corps finis F_q aux extensions des corps finis $F_q[\alpha]$. En étudiant ces extensions, la thèse met en lumière les relations complexes et les propriétés qui émergent dans ces contextes augmentés. Grâce à cette recherche, la thèse contribue à une meilleure compréhension des courbes elliptiques, de leur comportement et de leurs applications dans divers domaines mathématiques et cryptographiques.

Mots clés :

Courbe elliptique, sous-groupes de torsion, corps de nombres quadratiques cyclotomiques, crypto système, cryptage entièrement homomorphe, suite de type k-Fibonacci, matrices, problème du logarithme discret sur les courbes elliptiques, corps de nombres multiquadratiques imaginaires, courbes hyper elliptiques, anneau de groupes, cryptographie à clé publique, Diffie-Hellman, protocole d'échange de clés.