AVIS DE SOUTENANCE DE THESE

Le Doyen de la Faculté des Sciences Dhar El Mahraz –Fès – annonce que

Mr **: GRINI Abdelâli**

Soutiendra : **le 21/01/2022** à **10h**

Lieu **: Centre de visioconférence**

Une thèse intitulée :

Courbes Hessiennes tordues sur un anneau local et leurs applications en cryptographie

En vue d'obtenir le Doctorat
FD : Mathématiques et Applications (MA)
Spécialité: Algèbre

Devant le jury composé comme suit :

	NOM ET PRENOM	GRADE	ETABLISSEMENT
Président	Pr EL FADIL Lhoussain	PES	Faculté des Sciences Dhar El Mahraz - Fès
Directrice de thèse	Pr MOUANIS Hakima	PES	Faculté des Sciences Dhar El Mahraz – Fès
Co-directeur de thèse	Pr CHILLALI Abdelhakim	PH	Faculté poly-disciplinaire - Taza
Rapporteurs	Pr ZIANE M'hamed	PES	Faculté des Sciences - Oujda
	Pr EL OMARY Mohamed Abdou	PES	Faculté des Sciences et Techniques - Settat
	Pr EZZOUAK Siham	PH	Faculté des Sciences Dhar El Mahraz - Fès
Membres	Pr BOUA Abdelkarim	PH	Faculté poly-disciplinaire - Taza
	Pr MEKKOUR Mounir	PH	Faculté des Sciences Dhar El Mahraz - Fès

Résumé :
Cette thèse est consacrée à l'étude des courbes hessiennes tordues sur l'anneau local $F_q[\varepsilon],\ \varepsilon^2 = 0$ et leurs applications cryptographiques. Après avoir défini les courbes hessiennes tordues sur cet anneau, on a classifié ses éléments en deux types, ce qui nous a permis de montrer que les éléments du deuxième type forment un sous-groupe de la courbe hessienne tordue $H^2_{a,d}$, et qui est isomorphe au corps F_q. À partir de cet isomorphisme on a déduit que; le problème du logarithme discret sur $H^2_{a,d}$ est équivalent à celui sur H_{a_0,d_0}et # $(H^2_{a,d}) = p^b$ # (H_{a_0,d_0}), ce qui représente un facteur important et utile en cryptographie puisqu'il permet d'obtenir un nombre énorme de points avec un nombre premier p plus petit. En conséquence, nous pouvons remarquer que le temps nécessaire pour résoudre le problème du logarithme discret sur $H^2_{a,d}$ est plus grand que celui de la courbe hessienne tordue sur un corps fini.

Enfin, on a illustré leur utilité cryptographique en donnant des applications cryptographiques sur $H^2_{a,d}$ en utilisant les résultats trouvés. On a implémenté ces exemples en utilisant le codage des éléments de la courbe $H^2_{a,d}$ à l'aide du logiciel de calcul Maple.

Mots clés : Courbe hessienne tordue, anneau fini, cryptographie, Cramer-Shoup, courbe elliptique, ElGamal, Diffie-Hellman, Corps fini.

Twisted Hessian curves on a local ring and their applications in cryptography

Abstract:
This thesis is devoted to the study of twisted Hessian curves on the local ring $F_q[\varepsilon],\ \varepsilon^2 = 0$ and their cryptographic applications. After defining the twisted Hessian curves on this ring, we classified its elements into two types, which allowed us to show that the elements of the second type form a subgroup of the twisted Hessian curve $H^2_{a,d}$, and which is isomorphic to the field F_q. From this isomorphism we deduced that; the discrete logarithm problem on $H^2_{a,d}$ is equivalent to the one on H_{a_0,d_0} and # $(H^2_{a,d}) = p^b$ # (H_{a_0,d_0}), which is an important and useful factor in cryptography since it allows to obtain a huge number of points with a smaller prime p. As a consequence, we can notice that the time needed to solve the discrete logarithm problem on $H^2_{a,d}$ is greater than that of the twisted Hessian curve on a finite field.
Finally, we illustrated their cryptographic interest by giving cryptographic applications on $H^2_{a,d}$ using the results found. These examples were implemented using the encoding of the elements of the curve $H^2_{a,d}$ with the help of Maple.

Key Words : Twisted Hessian curve, Finite ring, Cryptography, Cramer-Shoup, Elliptic curve, ElGamal, Diffie-Hellman.