AVIS DE SOUTENANCE DE THESE

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

Mr. EL HAMAM Moha Ben Taleb

Soutiendra : le 10/12/2022 à 10H

Lieu : Faculté des Sciences Dhar el Mehraz-Département de Géologie.

Une thèse intitulée :

" ***Courbes hessiennes tordues sur un anneau non-local et leurs applications en cryptograghie*** "

En vue d'obtenir le Doctorat

FD : Mathématiques et Application *(MA***)**
Spécialité : *Algèbre*

Devant le jury composé comme suit :

	Nom et prénom	**Grade**	**Etablissement**
Président	Pr MOUANIS Hakima	PES	Faculté des Sciences Dhar El Mahraz - Fès
Directeur de thèse	Pr EL FADIL Lhoussain	PES	Faculté des Sciences Dhar El Mahraz - Fès
Co- Directeur de thèse	Pr Abdelhakim CHILLALI	PH	Faculté polydisciplinaire - Taza
Rapporteurs	Pr Soumia LALAOUI RHALI	PES	Faculté polydisciplinaire - Taza
	Pr Seddik ABDELALIM	PH	Faculté des Sciences Ain Chock- Casa
	Pr El Mostafa Kalmoun	PES	Université Al Akhawayn - Ifrane
Membres	Pr Mohammed Sahmoudi	PH	Faculté des Sciences - Meknès

Résumé :

Le but de cette thèse est d'étudier les courbes hessiennes tordues définies sur un anneau fini et non-local et ces applications cryptographiques.

Plus précisément, nous étudions les courbes hessiennes tordues sur un anneau non-local $F_q[e]$ avec $e^n = e^{n-1}$ dans le cas n = 2 et n = 3 avec F_q est le corps fini à q éléments et leurs applications cryptographiques, où q est une puissance d'un nombre premier p.

En utilisant l'équation hessienne tordue, nous définissons les courbes hessiennes ´ tordues $H_{a,d}(F_q[e])$ sur l'anneau non-local $F_q[e]$, $e^2 = e$. Ensuite, nous montrons que $H_{\pi_0(a),\pi_0(b)}(F_q)$ et $H_{\pi_1(a),\pi_1(b)}(F_q)$ sont deux courbes hessiennes tordues sur le corps F_q. Plus précisément, nous donnons une bijection entre les ensembles $H_{a,d}(F_q[e])$ et $H_{\pi_0(a),\pi_0(b)}(F_q) \times H_{\pi_1(a),\pi_1(b)}(F_q)$. De plus, nous classifions les éléments de $H_{a,d}(F_q[e])$. Apres avoir munir l'ensemble $H_{a,d}(F_q[e])$ d'une nouvelle structure du groupe, nous vérifions que la bijection mentionnée ci-dessus est un isomorphisme de groupes. De cette isomorphisme, on en déduit que le problème du logarithme discret sur $H_{a,d}(F_q[e])$ est équivalent à celui de $H_{\pi_0(a),\pi_0(b)}(F_q) \times H_{\pi_1(a),\pi_1(b)}(F_q)$. Les opérations effectuées par cette nouvelle loi sur $H_{a,d}(F_q[e])$ sont moins couteuses.

En outre, nous définissons les courbes hessiennes tordues $H_{a,d}(F_q[e])$ sur un anneau non-local $F_q[e]$ avec $e^3 = e^2$. Nous montrons que $H_{\pi_0(a),\pi_0(b)}(F_q)$ et $H_{\pi_1(a),\pi_1(b)}(F_q)$ sont deux courbes hessiennes tordues sur le corps F_q. Puis nous donnons la classification des éléments de ces courbes $H_{a,d}(F_q[e])$.

Enfin, nous présentons quelques applications cryptographiques sur $H_{a,d}(F_q[e])$ en utilisant les resultats trouvés.

Mots clés : Courbe elliptique, Courbe hessienne tordue, Anneau fini, Corps fini, Cryptographie.

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

Abstract:

The aim of this thesis is to study twisted Hessian curves defined on finite and nonlocal rings and their cryptographic applications. More precisely, we study twisted Hessian curves on the non-local rings $F_q[e]$, $e^n = e^{n-1}$ in cases $n = 2$ and $n = 3$ with F_q the finite field of order q, and their cryptographic applications, where q is a power of a prime number p. Using the twisted Hessian equation, we define the twisted Hessian curves $H_{a,d}(F_q[e])$ on non-local ring $F_q[e]$, $e^2 = e$ We next, show that $H_{\pi_0(a),\pi_0(b)}(F_q)$ and $H_{\pi_1(a),\pi_1(b)}(F_q)$ are two twisted Hessian curves over the field F_q. More precisely, we give a bijection between the sets $H_{a,d}(F_q[e])$ and $H_{\pi_0(a),\pi_0(b)}(F_q) \times H_{\pi_1(a),\pi_1(b)}(F_q)$ Moreover, we classify the elements of $H_{a,d}(F_q[e])$. After equipping the set $H_{a,d}(F_q[e])$ with a new group structure, we check that the mentioned bijection above is an isomorphism of groups. From this isomorphism, we deduce that the problem of the discrete logarithm on $H_{a,d}(F_q[e])$ is equivalent to $H_{\pi_0(a),\pi_0(b)}(F_q) \times H_{\pi_1(a),\pi_1(b)}(F_q)$. The computation cost of this new law on $H_{a,d}(F_q[e])$ is less expensive. Furthermore, we define the twisted Hessian curves $H_{a,d}(F_q[e])$ on the non-local ring $F_q[e]$, $e^3 = e^2$. We show that $H_{\pi_0(a),\pi_0(b)}(F_q)$ and $H_{\pi_1(a),\pi_1(b)}(F_q)$ are are two twisted Hessian curves over the field F_q. We give the classification of the elements of the curve twisted hessian $H_{a,d}(F_q[e])$, $e^3 = e^2$.

Key words: Elliptic curve, Twisted Hessian curve, Finite ring, Finite field, Cryptography.