«ALGORITHMIQUE DES COUPLAGES ET CRYPTOGRAPHIE» PAR SORINA IONICA

Présentée par : Melle Sorina IONICA Discipline : Informatique Laboratoire : PRISM

Les couplages ont été utilisés pour la première fois en cryptographie pour attaquer le problème du logarithme discret sur la courbe elliptique. Plus tard, des nombreux schémas cryptographiques à base de couplages sont proposés. Dans cette thèse, nous proposons l'utilisation des couplages pour l'étude des volcans d'isogénies et l'utilisation des isogénies pour l'implémentation efficace des couplages. Les volcans d'isogénies sont des graphes dont les nœuds sont des courbes elliptiques et les arrêts sont des isogénies entre les courbes. Les algorithmes permettant de parcourir ces graphes ont été donnés par Kohel (1996) et par Fouquet et Morain (2001). Néanmoins, à présent, il n'est pas possible de prédire, lorsqu'on veut faire un pas sur le volcan, la direction de ce pas. Supposons que la cardinalité de la courbe est connue. Étant donné un point d'ordre l sur la courbe, nous donnons une méthode de déterminer la direction de l'isogénie dont le noyau est engendré par ce point. Notre méthode, qui comprend seulement le calcul de quelques couplages, est très efficace et donne des algorithmes rapides pour le parcours des graphes d'isogénies. Dans la deuxième partie de cette thèse, nous nous sommes intéressés au calcul du couplage sur des courbes elliptiques en forme d'Edwards. En utilisant une isogénie de degré 4, nous avons donné les premières formules pour le calcul efficace des couplages sur les courbes d'Edwards.

Abstract :

Pairings were used in cryptography for the first time to transform the elliptic curve discrete logarithm problem into a discrete logarithm problem in the finite field. Later on, it was shown that pairings could be used to build cryptosystems. In this thesis we propose the use of pairings in the study of isogeny volcanoes and the use of isogenies for efficient implementation of pairings. Isogeny volcanoes are graphs whose vertices are elliptic curves and whose edges are l-isogenies. Algorithms allowing to travel on these graphs were developed by Kohel in his thesis (1996) and later on, by Fouquet and Morain (2001). However, up to now, no method was known, to predict, before taking a step on the volcano, the direction of this step. Given a point P of order l on the elliptic curve, we develop a method to decide whether the subgroup generated by P is the kernel of a horizontal isogeny, a descending or an ascending one. Our method, which consists mainly in the computation of a small number of pairings, is very efficient and gives, in most cases, simple algorithms, allowing to navigate on the volcano. The second part of this thesis focuses on the implementation of pairings on elliptic curves in Edwards form. Using an isogeny of degree 4 from the Edwards curve to an elliptic curve in Weierstrass form, we gave the first efficient implementation of Miller's algorithm on Edwards curves. Our method has performances similar to implementations of the same algorithm on the Weierstrass form of an elliptic curve.

INFORMATIONS COMPLÉMENTAIRES

Jean-Marc COUVEIGNES, *Professeur des Universités, à l'Université Toulouse 2* - Toulouse - Rapporteur

David KOHEL, *Professeur des Universités, à l'Université de la Méditerranée* - Institut de Mathématiques de Luminy - Marseille - Rapporteur

Antoine JOUX, *Professeur Associé, à l'Université de Versailles Saint-Quentin-en-Yvelines/*Laboratoire Parallélisme, Réseaux, Système, Modélisation (PRISM) - Versailles - Directeur de thèse

Louis GOUBIN, *Professeur des Universités, à l'Université de Versailles Saint-Quentin-en-Yvelines/*Laboratoire Parallélisme, Réseaux, Système, Modélisation (PRISM)- Versailles - Examinateur

Ariane MEZARD, *Professeure des Universités, à l'Université de Versailles Saint-Quentin-en-Yvelines/*Laboratoire de Mathématiques de Versailles (LMV) - Versailles - Examinateur

Tanja LANGE, *Professeure, à l'Université Technique d'Eindhoven (Pays-Bas)* - Examinateur

Benjamin SMITH, *Chargé de Recherche, à l'INRIA Saclay* - Laboratoire d'Informatique de l'Ecole Polytechnique - Palaiseau - Examinateur

Contact : dredval service FED : theses@uvsq.fr