« EXPLORATIONS DANS LES GRAPHES D'ISOGÉNIES » PAR LUCA DE FEO

Discipline : Informatique

Le vendredi 14 décembre 2018 à 15h
L'Université Versailles Saint-Quentin-en-Yvelines
Amphithéâtre B
UFR des Sciences
Batiment Fermat
45 avenue des Etats-Unis
78000 Versailles

Résumé :
Motivés par les applications récentes des graphes d'isogénies en cryptographie, nous allons faire une revue des problèmes liés aux isogénies de courbes elliptiques définies sur les corps finis, et de leur calcul. Les graphes d'isogénies se classent en deux familles : à multiplication complexe (CM) et supersinguliers. Les graphes CM jouissent d'une riche structure, liée à la théorie des ordres d'un corps quadratique imaginaire. Nous expliquons comment cette théorie donne des algorithmes pratiques pour se déplacer "verticalement" dans les graphes, en suivant le treillis des ordres quadratiques.
Cependant, "pratique" n'implique pas "simple". Afin d'implanter efficacement nos algorithmes, nous allons devoir étudier les méthodes connues pour calculer dans la clôture algébrique d'un corps fini. De façon remarquable, les isogénies vont aussi se révéler utiles pour ces algorithmes, leur calcul devenant ainsi à la fois un fin et un moyen.
Enfin, nous allons passer en revue les applications des graphes d'isogénies aux échanges de clefs cryptographiques. Les graphes CM offrent une généralisation naturelle de l'échange classique de Diffie–Hellman, un fait qui avait déjà été reconnu il y a vingt

ans, et qui a été récemment remis au goût du jour. La structure des graphes supersinguliers, d'un autre côté, est reliée aux ordres maximaux d'une algèbre de quaternions, et est plus compliquée à manier algorithmiquement; seulement récemment ces graphes ont été proposés comme une base pour la cryptographie. Dans les deux cas, la sécurité des protocoles cryptographiques est basée sur la difficulté de se déplacer "horizontalement" dans les graphes d'isogénies. Nous allons donc conclure notre étude avec une revue des algorithmes, à la fois classiques et quantiques, pour résoudre ces problèmes.

Abstract:
Motivated by the recent applications of isogeny graphs in cryptography, we review topics related to isogenies of elliptic curves defined over finite fields, and their computations. Isogeny graphs come in two families: complex multiplication (CM) and supersingular. CM graphs enjoy a rich structure, related to the theory of the orders of an imaginary quadratic field. We explain how this theory yields practical algorithms to move "vertically" in the graphs, along the lattice of quadratic orders. However, "practical" does not imply "easy". In order to efficiently implement our algorithms, we shall review the available methods to compute in the algebraic closure of a finite field. Interestingly, isogenies will also turn out to be useful for these algorithms, their computation thus becoming both a goal and a tool. Finally, we will review the application of isogeny graphs to cryptographic key exchange. CM graphs will offer a natural generalization of the classical Diffie–Hellman key exchange, a fact already recognized twenty years ago, and recently revamped. The structure of supersingular graphs, on the other hand, is related to the maximal orders of a quaternion algebra, and is harder to handle algorithmically; only recently these graphs have been proposed as a foundation for cryptography. In both cases, the security of the cryptographic protocols is based on the difficulty of moving "horizontally" in the isogeny graphs. We shall thus conclude our study with a review of the known algorithms, both classical and quantum, to solve these problems.

INFORMATIONS COMPLÉMENTAIRES

Monsieur Andreas ENGE - Directeur de Recherches, INRIA Bordeaux, France - Rapporteur
Monsieur Florian HESS – Professeur des Universités, Université d’Oldenburg, Allemagne - Rapporteur
Monsieur David KOHEL - Professeur des Universités, Université Aix-Marseille, France - Rapporteur
Monsieur Paulo BARRETO – Maitre de conférences HDR, University of Washington

Tacoma, Etats-Unis - Examinateur
Monsieur Jean-Marc COUVEIGNES - Professeur des Universités, Université de Bordeaux, France - Examinateur
Madame Annick VALIBOUZE - Professeur des Universités, Université Pierre et Marie Curie, France - Examinatrice
Monsieur Louis GOUBIN - Professeur des Universités, Université de Versailles Saint-Quentin-en-Yvelines, France - Tuteur

Contact : DSR - Service FED : theses@uvsq.fr