Proposition d'exposé aux JNCF 2019: Échange de clés à base de graphes d'isogénies CM sur un corps fini

Jean Kieffer (LFANT, Institut de mathématiques de Bordeaux)

20 décembre 2018

Résumé

Le but de l'exposé est de présenter un protocole d'échange de clés à partir de graphes d'isogénies entre courbes elliptiques sur un corps fini ([1] et [2]).

Les échanges de clés classiques (par exemple Diffie–Hellman dans un corps fini ou sur une courbe elliptique) sont cassés en présence d'un ordinateur quantique. Un des intérêts principaux de la cryptographie à base d'isogénies est de proposer des protocoles, dits post-quantiques, qui résistent également à ce nouveau type d'adversaire. La construction présentée est fondée sur une action de groupe fournie par la multiplication complexe (CM) : le groupe de classe d'un ordre quadratique imaginaire agit sur un ensemble de courbes elliptiques, et calculer l'action de « petits » générateurs revient à calculer des isogénies entre ces courbes.

L'efficacité du protocole dépend alors de celle du calcul d'isogénies. La méthode générale consiste à utiliser des équations modulaires, mais utiliser des points de torsion rationnels sur la courbe est plus efficace. Cela conduit à prendre des courbes elliptiques supersingulières pour pouvoir contrôler leur nombre de points : on atteint alors des performances crédibles en pratique.

Références

[1] Luca De Feo, Jean Kieffer, Benjamin Smith. Towards practical key exchange from ordinary isogeny graphs. In T. Peyrin and S. Galbraith (eds), Advances in Cryptology – ASIACRYPT 2018 (Springer)

[2] Wouter Castryck, Tanja Lange, Chloe Martindale, Lorenz Panny, Joost Renes. CSIDH : An Efficient Post-Quantum Commutative Group Action. In T. Peyrin and S. Galbraith (eds), Advances in Cryptology – ASIACRYPT 2018 (Springer)