Application de la méthode Clapoti aux courbes elliptiques ordinaires

Maxime Louvet*[1]

[1]Laboratoire de Mathématiques de Versailles – Université de Versailles Saint-Quentin-en-Yvelines, Université Paris-Saclay, Centre National de la Recherche Scientifique – France

Résumé

Les isogénies entre courbes elliptiques ordinaires peuvent être utilisées pour transférer le problème du logarithme discret (DLP) depuis une courbe donnée vers une courbe "faible", où le DLP est facile à résoudre. Celles entre courbes supersingulières sont utilisées pour construire des schémas de signature. En 2022, l'utilisation d'un critère de Kani de 1997, permettant de caractériser les isogénies non-triviales entre produits de deux courbes elliptiques, a permis d'exhiber une attaque dévastatrice sur sur l'un de ces schémas appelé SIDH. On s'intéresse aux applications de ces résultats au calcul d'isogénies entre courbes ordinaires.

Dans cette présentation, on se concentre sur la méthode Clapoti, qui est déjà utilisée pour accélérer le calcul d'isogénies dans les schémas de signatures récents basés sur les courbes supersingulières. Cependant même si cette méthode est énoncée en toute généralité, les prérequis nécessaires sont différents selon le cas supersingulier ou ordinaire. On expose les difficultés rencontrées pour mettre en place cette méthode dans le cas ordinaire, où l'anneau d'endomorphismes est facilement accessible mais où les points de grande torsion sont a priori définis sur des extensions du corps de base de degrés élevés. On donne une estimation de la complexité des procédures énoncées.

*Intervenant