Calcul d’index pour le problème du logarithme discret sur courbes elliptiques

Stage réalisé au sein de l'UCL Crypto Group <http://www.uclouvain.be/crypto/>, sous la direction de Christophe Petit <http://perso.uclouvain.be/christophe.petit/>.

Le problème du logarithme discret sur courbes elliptiques est un des problèmes les plus importants en cryptographie. Après vingt ans de cryptanalyse infructueuse, ce problème semble beaucoup plus difficile à résoudre que les deux autres problèmes très utilisés en cryptographie (le problème de la factorisation d’entiers et le problème du logarithme discret sur les corps finis). Récemment, la méthode du calcul d’index (qui a mené aux meilleurs algorithmes pour les deux autres problèmes) a pu progressivement être adaptée aux courbes elliptiques sur des corps de petite caractéristique.

Le stage fera le point sur les résultats récents de Diem, Faugère, Gaudry, Hodges, Joux, Perret, Petit, Renault, Semaev, Schlaffer, Vitse. Il proposera des variantes des attaques existantes et réalisera des implémentations en Magma.