Calcul de Groupes de Classes d'un Corps de Nombres et Applications à la Cryptologie

Alexandre Gélin
UPMC Paris 6

Dans un corps de nombres, deux structures particulières apparaissent naturellement : le groupe des unités et le groupe des idéaux (fractionnaires). Bien que ces deux groupes soient infinis, il existe des structures finies permettant de les représenter assez fidèlement. Pour le groupe des unités, il est de type fini, c'est-à-dire engendré par un nombre fini d'éléments. Pour le groupe des idéaux, il suffit de quotienter par le sous-groupe formé des idéaux principaux pour obtenir un groupe fini, le *groupe de classes*.

Après avoir rappelé les définitions et résultats importants sur les groupes de classes d'un corps de nombres, nous retracerons rapidement un historique des avancées dans le domaine, depuis Gauss jusqu'à aujourd'hui. De nos jours, les meilleurs algorithmes sont sous-exponentiels en la taille du discriminant du corps. La méthode générale repose, comme pour la factorisation ou le problème du logarithme discret, sur une méthode du calcul d'indice.

Enfin, nous terminerons cet exposé en regardant les applications des méthodes utilisées pour le calcul du groupe de classes d'un corps de nombres en cryptologie. En effet, nous pouvons adapter nos résultats afin de résoudre le *Principal Ideal Problem* : étant donné un idéal principal dans un corps de nombres, est-il possible d'en retrouver un générateur ? Certains cryptosystèmes complètement homomorphes se sont basés sur ce problème et nous nous sommes focalisés en particulier sur celui présenté par Smart et Vercauteren à PKC 2010. Nous décrirons l'attaque mise en place avec Thomas Espitau, Pierre-Alain Fouque, Paul Kirchner et Jean-FranÃ§ois Biasse et qui sera présentée à EuroCrypt 2017.