Sujet de stage M2 recherche

Petit logarithme discret

Laurent Imbert

LIRMM, CNRS, Université Montpellier 2

Laurent.Imbert@lirmm.fr

Soit G un groupe cyclique d'ordre n (noté multiplicativement) et soit g un générateur de G. Alors tout élément x de G peut s'écrire sous la forme $x = g^k$. Un tel entier k est appelé **logarithme discret** de x en base g.

Pour certains groupes, le logarithme discret est difficile à calculer. Cette propriété est très exploitée en cryptographie asymétrique. Un des groupes les plus simples sur lequel le logarithme discret est difficile à calculer est le groupe multiplicatif d'un corps fini à p éléments, où p est un nombre premier, c.-à.-d. l'ensemble des entiers $\{1, \ldots, p-1\}$ muni de la multiplication modulo p.

Le sujet de ce stage consiste à étudier les algorithmes permettant de calculer le logarithme discret sur $\mathbb{Z}/p\mathbb{Z}$ et à imaginer des optimisations lorsque le nombre premier p est "petit" (au plus 64 bits) ou possède une forme particulière. La programmation optimisée de ces algorithmes et une comparaison avec des implémentations disponible sera demandée.

Compétences requises : bases d'algèbre, programmation C/C++.