Le Rubik’s cube pour les cryptographes

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/>.

Il est bien connu que l'ensemble des configurations du Rubik's cube forme un groupe fini qui peut être engendré par les 6 permutations élémentaires. Ce casse-tête bien connu est réputé difficile, mais certainement pas au sens cryptographique du terme. Il existe en effet des algorithmes très efficaces pour résoudre le Rubik's cube, le record du monde pour un être humain étant de seulement 7,08 secondes.

La sécurité d'un très grand nombre de protocoles cryptographiques utilisés quotidiennement, comme le RSA, repose sur l'hypothèse que certains problèmes mathématiques sont très difficiles à résoudre, même avec l'aide d'ordinateurs très puissants. Les problèmes les plus célèbres utilisés en cryptographie sont la factorisation entière (utilisée dans le cas du RSA) et le logarithme discret, mais d'autres problèmes moins connus ont également été proposés, et pourraient (qui sait?) peut-être les remplacer un jour.

Ce mémoire s'intéresse aux problèmes de représentation et de factorisation dans des groupes finis non commutatifs. Le problème de représentation est le suivant: étant donné un groupe fini G et un ensemble d'élements s_i appartenant à G qui génèrent le groupe, trouver une combinaison des éléments s_i qui se ramène à l'élément neutre du groupe. Le problème de factorisation est un peu plus général: on reçoit en plus un élément quelconque du groupe, et on doit trouver une combinaison des éléments s_i qui se ramène à cet élément.

Pour fixer les idées, on peut reprendre l'exemple du Rubik’s cube. Dans ce cas, le groupe G est l'ensemble des permutations possibles du cube. L'élément neutre correspond à la configuration de base. Si les éléments s_i choisis sont les permutations élémentaires (les 6 rotations d'un quart de tour), alors on sait que le problème de représentation est facile à résoudre. Le problème de factorisation est beaucoup moins étudié (et ne fait pas encore partie des épreuves des championnats du monde!) mais n'est probablement pas beaucoup plus compliqué.

Pour revenir à la cryptographie, plusieurs fonctions de hachage (une des primitives les plus utilisées en cryptographie) ont été proposées, dont la sécurité repose sur la difficulté de résoudre les problèmes de représentation et de factorisation dans des groupes de matrices 2*2 à coefficients dans un corps fini. Dans ce cas, le problème de représentation sera le suivant: on reçoit deux matrices A et B qui génèrent le groupe, et il faut trouver un produit de ces matrices (le plus petit possible) qui donne la matrice identité. Plusieurs des schémas proposés ont été cassés, complètement ou en partie, mais d'autres schémas continuent de défier la communauté scientifique.

Le stage fera le point sur les attaques connues, proposera des améliorations ou extensions, et implémentera les résultats en Magma.