Niveau : 1 **Jaune**

Le problème du logarithme discret dans Z/pZ (p premier)

1 Le problème du logarithme discret

Soit G un **groupe cyclique** d'ordre n que nous noterons multiplicativement. Soit α un générateur du groupe G. Ainsi tout élément x du groupe G s'écrit d'une unique façon sous la forme :

$$x = \alpha^k$$

avec $0 \leq k \leq n-1$. L'exposant k est appelé le logarithme discret de l'élément x de G.

Le **problème du logarithme discret (DLP)** est de trouver k lorsqu'on se donne x. Bien entendu ce problème n'a de sens que si on dit sous quelle forme sont représentés les éléments x du groupe G. Pour certains groupes représentés de manière naturelle le problème du logarithme discret est difficile, c'est-à-dire qu'on ne connaît aucun algorithme réalisable en pratique pour des tailles grandes (disons à l'heure actuelle 1024 bits et plus). Le groupe multiplicatif $\mathbb{Z}/p\mathbb{Z}^*$ est de ceux là.

2 Le cas des entiers modulo p

Quand on représente les éléments de $\mathbb{Z}/p\mathbb{Z}^*$ de manière naturelle comme des entiers de l'intervalle $\{1, \cdots, p-1\}$, le problème du logarithme discret est difficile, mais pas autant que dans un groupe générique. On connaît des **algorithmes sous-exponentiels** pour le résoudre. Ceci a des conséquences sur la taille du groupe à utiliser de manière à ce que le problème du logarithme discret soit infaisable. Le nombre premier p doit avoir au minimum 1024 bits, ce qui assure à peu près la même sécurité qu'un **groupe générique** d'ordre ayant 160 bits. Rappelons qu'un groupe générique pour le problème du logarithme discret est un groupe pour lequel on ne connaît pas d'algorithme spécifique à ce groupe pour résoudre le problème du logarithme discret, et donc pour lequel les seuls algorithmes disponibles sont les algorithmes qui marchent pour tous les groupes, par exemple l'algorithme "pas de géant, pas de bébé", et qui sont jusqu'à présent exponentiels.

3 Autres groupes

3.1 Groupe multiplicatif d'un corps fini

Le groupe multiplicatif d'un corps fini général est aussi un groupe cyclique. Le cas de $\mathbb{Z}/p\mathbb{Z}^*$ en est évidemment un cas particulier. Le cas général souffre hélas du même défaut que le cas particulier : il existe des algorithmes sous-exponentiels pour résoudre le problème du logarithme discret.

3.2 Sous-groupe d'ordre premier q de $\mathbb{Z}/p\mathbb{Z}^*$

Si q est un nombre premier qui divise $p-1$, le sous groupe cyclique d'ordre q de $\mathbb{Z}/p\mathbb{Z}^*$ est intéressant car il se comporte comme un groupe générique. Il faut bien comprendre que les éléments de ce sous-

groupe s'écrivent naturellement dans le groupe $\mathbb{Z}/p\mathbb{Z}^*$, comme des nombres compris entre 1 et $p-1$. On dispose donc de deux méthodes pour résoudre le problème du logarithme discret dans ce sous-groupe : soit utiliser un algorithme générique dans le sous-groupe d'ordre q, soit utiliser un algorithme particulier (sous-exponentiel) dans le groupe $\mathbb{Z}/p\mathbb{Z}^*$. On a donc tout intérêt à adapter les tailles de p et de q pour que ces deux méthodes soient à peu près du même ordre de difficulté : par exemple 1024 bits pour p et 160 bits pour q. L'avantage qu'on peut y trouver est de diminuer la taille des exposants à utiliser (si on travaille dans un groupe d'ordre q, les exposants sont compris entre 0 et $q-1$). En revanche on ne gagne rien sur la taille des éléments puisque ils s'écrivent naturellement comme des éléments de $\mathbb{Z}/p\mathbb{Z}^*$. Il existe d'autres avantages sur le plan des preuves de sécurité qu'on ne peut détailler ici.

3.3 Groupe des points d'une courbe elliptique

Le groupe des points d'une courbe elliptique est, sauf cas particuliers de certaines courbes, est un groupe intéressant en cryptographie dans la mesure où on ne connaît aucun algorithme sous-exponentiel pour son problème du logarithme discret. L'avantage ici esst double : on utilise non seulement des exposants plus petits (ou des multiplicateurs car ces groupes sont habituellement notés additivement),mais des représentations des éléments qui sont aussi naturellement plus courtes.

4 Problèmes proches du problème du logarithme discret

La méthode d'échange de clé de Difie-Hellman repose sur la difficulté du problème du logarithme discret. Rappelons que dans cette méthode un groupe cyclique public G est fixé ainsi qu'un générateur public α de ce groupe. Deux interlocuteurs A et B vont construire une clé commune K. Pour cela A tire au sort un entier n plus petit que l'ordre de G, de même B tire au sort un entier m. L'interlocuteur A calcule α^n et le transmet à B. L'interlocuteur B fait de même, il calcule α^m et le transmet à A. Maintenant A calcule $(\alpha^m)^n$ tandis que B calcule $(\alpha^n)^m$, ils obtiennent tous les deux la même clé secrète $K = \alpha^{mn}$. (En pratique, on adapte la taille de la clé K en appliquant une fonction de compression publique à α^{mn}). On voit bien entendu, que si on savait résoudre facilement le problème du logarithme discret ce système n'aurait aucune sécurité. En regardant de plus près, on peut exhiber un problème plus précis sur lequel repose la sécurité de cet échange. Étant donnés les deux nombres $x = \alpha^n$ et $y = \alpha^m$ calculer le nombre $z = \alpha^{mn}$. Ce problème est appelé le **problème calculatoire de Diffie-Hellman (CDH)**. Il est clair que ce problème est réductible au problème du logarithme discret. En revanche on ne sait pas si le problème du logarithme discret est en général réductible au problème calculatoire de Diffie-Hellman. Il n'y a actuellement aucun exemple de groupe où le problème CDH aurait une solution simple alors qu'on ne connaitrait aucun algorithme polynomial pour DLP.
On peut définir aussi le problème décisionnel de Diffie-Hellman (DDH) qui à partir de trois nombres $x = \alpha^n$, $y = \alpha^m$ et z doit répondre par oui ou non à la question : le nombre z est-il égal à α^{mn}. Il est clait que le problème DDH est réductible au problème CDH. Et ici on a des exemples de groupes où le problème DDH est facile, alors qu'on ne connaît aucun algorithme polynomial pour résoudre CDH dans ces groupes.

Auteur : Ainigmatias Cruptos
Diffusé par l'Association ACrypTA