Algorithme rho de pollard

TAFFOREAU Nicolas

7 février 2012

Table des matières

Chapitre 1

Rapel sur les courbes elliptique

définition Soit un un corp Fp (p premier) de caractéristique différente de 2 ou 3, soit a, b app Fp. Un courbe elliptique est définit par le point à l'infini et l'ensemble des points (x,y) tel que soit satifait l'equation suivante :

$$y^2 = x^3 + a * x + b.$$

Ces points forme un groupe abélien avec comme zero le point à l'infini et un loi de groupe. Soit P, Q app F, $P = (x_1, y_1)$, $Q = (x_2, y_2)$ alors $P + Q = (x_3, y_3)$ tel que

$$x_3 = \mu^2 - x_1 - x_2,\ y_3 = \mu(x_1 - x_3)$$
$$\mu = \frac{y_2 - y_1}{x_2 - x_1} \text{ si } P <> Q$$
$$\mu = \frac{3 * x_1^2 + a}{2 * y_1} \text{ si } P = Q$$

propriété importante pour les inverse pour la loi d'addition sur Fp. Si $P = (x_1, y_1)$ alors $-P = (x_1, -y_1)$. (sur Fq) ?

Chapitre 2

Algorithme rho de Pollard

L'algorithme rho de pollard est basé sur le paradoxe des anniversaire. Dans un groupe finit si on prend des éléments de façon aléatoire, il faut en moyenne tirer $\sqrt{n}$ éléments pour obtenir un élément que l'on à déjà tiré, ou n est le nombre d'élément de notre ensemble. Le nom de cette algorithme est dû à la forme que prend la suite aléatoire, on a d'abord un pré-cycle puis le cycle.

2.1 dans un groupe du type Fp

Dans un groupe du type Fp, Pollard a choisit comme fonction de tirage aléatoire un fonction qui ne tient compte que de l'élément précédent. $f(x) = x + Psix \in [0; p/3[$
$f(x) = x + xsix \in [p/3; 2p/3[$
$f(x) = x + Qsix \in [2p/3; p[$
Ici P est un generateur du groupe et Q est l'element dont on veut connaitre le logarithme en base P.

Algorithm 1 rho pollard

Entrées: p,P,Q
Sorties: x tel que $Q = P^x$

2.2 sur les courbe elliptique

2.3 algorithme de floyd

Chapitre 3

Negation map

3.1 methode general

sur une courbe elliptique sur Fp l'inverse de P = (x,y,z), simplifié à (x,y) est -P = (x,-y). le but de cette méthode est de reduire le groupe de moitier, donc de faire une recherche de log discret dans <P>/<H>. On obtient donc une relation du type $\pm[a]P \pm [b]Q = \pm[a']P \pm [b']Q$. Il nous suffit donc de retrouver exactement la relation avec les bon signe pour retrouver le logarithme discret.

3.2 cycle infructueux

apppartition très fréquente de cycle de taille 2 n'important pas d'information sur le log discret on les elimine donc en ......

Chapitre 4

nombre de groupe r

Chapitre 5

additive walk

point important : plus trop une marche alléatoire pour 3 groupes donc plus pour r groupes r $>$ 19.

Chapitre 6

endomorphisme

Chapitre 7

parrallelisation

pour parralelisé le log discret on definie une règle pour avoir des point remarquable (tel que ....) a chaque fois que l'on a après une marche un point remarquable on le transmet a un serveur central ainsi que les donné de départ quand on a deux intersection de point remarquable on a une collision.

Chapitre 8

bibliograpie