Cryptanalyse

Cours 11 - Cryptanalyse à l'Aide de Réseaux Euclidiens

Maxime Bombar

Mardi 19 Novembre

Introduction

Exemple avec RSA

```
sage: N, e, p, q, d = keyGen(2^150) # e=3
sage: message = Integer("lemotdepassepourajourdhuiestbarracuda
   ",base=35)
sage: c = message^e % N
```

Exemple avec RSA

```
sage: N, e, p, q, d = keyGen(2^150) # e=3

sage: message = Integer("lemotdepassepourajourdhuiestbarracuda
   ",base=35)
sage: c = message^e % N


## On peut peut-etre deviner le format du message?
sage: a = Integer("lemotdepassepourajourdhuiest000000000",
   base=35)
sage: X = Integer("xxxxxxxxx", base=35)
```

Exemple avec RSA

```
sage: message = Integer("lemotdepassepourajourdhuiestbarracuda
   ",base=35)
sage: c = message^e % N
sage: a = Integer("lemotdepassepourajourdhuiest000000000",
   base=35)
sage: X = Integer("xxxxxxxxx", base=35)

sage: M = matrix([[X^3, 3*X^2*a, 3*X*a^2, a^3-c], [0, N*X^2,
   0, 0], [0, 0, N*X, 0], [0, 0, 0, N]])
sage: B = M.LLL()
sage: Q = B[0][0]*x^3/X^3+B[0][1]*x^2/X^2+B[0][2]*x/X+B[0][3]
sage: print(Q.roots(ring=ZZ)[0][0].str(base=35))
barracuda
```

Quelle est Cette Diablerie ?

Théorème (Coppersmith, 1996)
On peut efficacement calculer jusqu'à une fraction $1/e$ d'un message chiffré par RSA avec exposant public e s'il on connaît le reste du texte clair.

```
sage: N.nbits() # Taille du chiffre
298
sage: Integer('barracuda', base=35).nbits()
45
sage: floor(N*(1/e))
99
```

Un Mot Clé

Réseau Euclidien

Flashback : Réseaux Euclidiens

Qu'est-ce qu'un Réseau ?

Définition : Un réseau est un ensemble de points dans un espace de dimension n ayant une structure périodique. On le munit du produit scalaire canonique $\langle \cdot, \cdot \rangle$.

Formellement : $\mathcal{L} \subset \mathbb{R}^n$ est un réseau si $\mathcal{L}$ est un sous-groupe **discret** de $\mathbb{R}^n$.

Dimension et Bases

Définition/Propriété : Tout réseau $\mathcal{L}$ est une combinaison linéaire entière d'une famille libre $(b_1, \ldots, b_d)$de $\mathbb{R}^n$:

$$\mathcal{L} \stackrel{\text{def}}{=} \Big\{ \sum_{i=1}^{d} \lambda_i b_i \mid \lambda_i \in \mathbb{Z} \Big\}.$$

L'entier d est appelé *dimension* ou *rang* du réseau $\mathcal{L}$. Si $d = n$ on dit que le réseau est de *rang plein*. En général, les b_i sont représentés en colonne dans une matrice $B \in \mathbb{R}^{n \times d}$. Pour une telle matrice, on note $\mathcal{L}(B) \stackrel{\text{def}}{=} B \cdot \mathbb{Z}^d$ le réseau associé.

Attention : Les bases ne sont pas uniques (mais d l'est)!

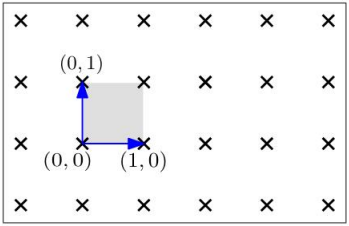
Sous-groupe Discret ?

Rappel : $\mathcal{L} \subset \mathbb{R}^n$ est discret si la topologie induite par $\mathbb{R}^n$ est discrète, *i.e.*, si tous les sous-ensembles de $\mathcal{L}$ sont ouverts. Ici, on a une distance (*e.g.*, euclidienne) $||\cdot||$. Cette définition se ramène donc à

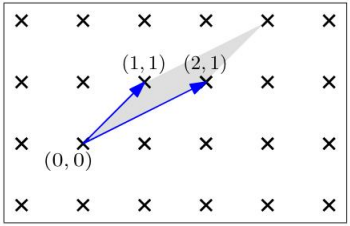
$$\exists \delta > 0 \text{ tel que } \forall x \neq y \in \mathcal{L}, \quad ||x - y|| > \delta$$

Propriété : Un sous-groupe de $\mathbb{R}^n$ non trivial est discret si et seulement si la quantité $\min_{x \neq y \in \mathcal{L}} ||x - y|| = \min_{x \in \mathcal{L} \setminus \{0\}} ||x||$ est bien définie, et strictement positive.

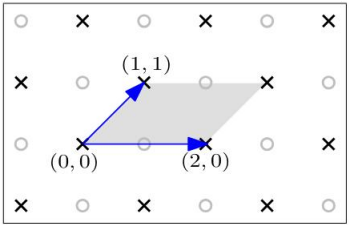
Exemples



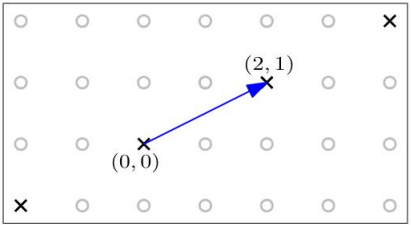
(a) A basis of $\mathbb{Z}^2$



(b) Another basis of $\mathbb{Z}^2$



(c) Not a basis of $\mathbb{Z}^2$



(d) Not a full-rank lattice

Pavé Fondamental

Définition : Soit $\mathcal{L}$ un réseau de $\mathbb{R}^n$, et soit B une base. On appelle *pavé fondamental* de B le parallélépiped

$$\mathcal{P}(B) \stackrel{\text{def}}{=} B \cdot [-1/2, 1/2).$$

Propriété : Soit B une base de $\mathcal{L}$. Alors tout vecteur $t \in \mathrm{Span}_{\mathcal{R}}(\mathcal{L})$ peut s'écrire de manière unique sous la forme $t = x + e$ avec $x \in \mathcal{L}$ et $e \in \mathcal{P}(B)$.

Déterminant et Matrices de Gram

Définition : Soit $\mathcal{L}$ un réseau et B. Le volume du pavé fondamental $\mathcal{P}(B)$ ne dépend pas du choix de B et est appelé **déterminant** de $\mathcal{L}$:

$$\det \mathcal{L} \overset{\text{def}}{=} \mathrm{Vol}(\mathcal{P}(B))$$

Soit B une base de $\mathcal{L}$. On note $G \overset{\text{def}}{=} BB^T = (\langle b_i, b_j \rangle_{1 \leqslant i,j \leqslant d})$ la *matrice de Gram* associée. Alors

$$\det \mathcal{L} = \sqrt{\det G}$$

La Borne de Minkowski

Rappel : L'élément $\lambda_1 \stackrel{\text{def}}{=} \min_{x \in \mathcal{L} \setminus \{0\}} ||x||$ est bien défini, et est strictement positif.

Théorème (Minkowski) On munit $\mathcal{L} \subset \mathbb{R}^n$ de la norme euclidienne $|| \cdot ||$. Alors

$$\gamma(\mathcal{L}) \stackrel{\text{def}}{=} \frac{\lambda_1}{\det \mathcal{L}^{1/n}} \leqslant \sqrt{\frac{2n}{\pi e}} + o(\sqrt{n}).$$

Exemples

- $\mathcal{L} = \mathbb{Z}^n$ a pour minimum $\lambda_1 = 1$ et possède $2n$ vecteurs minimaux. De plus, $\det \mathcal{L} = 1$ et $\gamma(\mathcal{L}) = 1$.
- Soit $B \stackrel{\text{def}}{=} \begin{pmatrix} -1 & 1 \\ 1 & 2 \end{pmatrix}$ et soit $\mathcal{L} = \mathcal{L}(B) \subset \mathbb{R}^2$ le réseau associé. On peut vérifier que $\lambda_1(\mathcal{L}) = \sqrt{2}$, atteint par $(-1, 1)$ et $(1, -1)$. Par ailleurs, $\det \mathcal{L} = 3$.

Dans l'exemple précédent, la base B est formée de vecteurs relativement courts. En particulier, un des vecteurs de base atteint λ_1. Une autre base est par exemple $B' \stackrel{\text{def}}{=} \begin{pmatrix} 1 & 2 \\ 0 & 3 \end{pmatrix}$ qui possède des vecteurs plus longs, et « moins orthogonaux »

Objectif : Représenter un cryptosystème comme un réseau euclidien dont les éléments secrets seraient des vecteurs courts $\longrightarrow$ Petites combinaisons linéaires entières.

Problème : Trouver des vecteurs très courts dans un réseau est un problème difficile SVP (*Shortest Vector Problem*).

Réduction de Réseaux

Mise en Bouche

Objectif : À partir d'une base B d'un réseau $\mathcal{L}(B)$, on cherche à trouver une base B' formée de vecteurs les plus courts possibles, et les plus orthogonaux possibles.

Transformations autorisées : Les opérations suivantes sur une base B ne changent pas le réseau engendré :

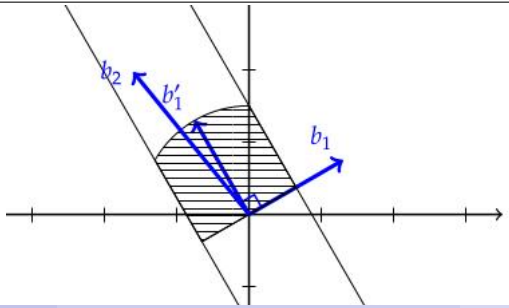
- Changement d'un signe : $B_i \to -B_i$.
- Échange de deux vecteur : $(B_i, B_j) \to (B_j, B_i)$
- Translation **entière** : $B_i \to B_i + k \cdot B_j$ avec $k \in \mathbb{Z}$ et $j \neq i$.

Cas de la Dimension 2 - Réduction de Gauss-Lagrange

Définition : Une base (b_1, b_2) d'un réseau $\mathcal{L} \subset \mathbb{R}^2$ est dite réduite si :

- $||b_1|| \leqslant ||b_2||$
- Si (b_1, b_1') est une base orthogonale directe de $\mathbb{R}^2$ alors

$$b_2 \in \left\{ t_1 b_1 + t_2 b_1' \;\middle|\; t_1, t_2 \in \mathbb{R}, |t_1| \leqslant \frac{1}{2}, t_2 > 0 \right\}.$$



Réduction de Gauss-Lagrange

Algorithme 1 : Algorithme de Réduction de Gauss-Lagrange

Entrées : (b_1, b_2) une base de $\mathcal{L}$

Output : (b_1', b_2') une base réduite.

répéter

Échanger $b_1 \leftarrow b_2$;

$b_2 \leftarrow b_2 - \left\lfloor \frac{\langle b_1, b_2 \rangle}{||b_2||^2} \right\rceil \cdot b_1$ // Minimise $||b_2 - \lambda \cdot b_1||^2$

;

jusqu'à $||b_1|| \leqslant ||b_2||$;

retourner (b_1, b_2).

Vidéo par Alice Pellet-Mary

https://apelletm.pages.math.cnrs.fr/page-perso/documents/presentations/LLL.mp4

Exemple

Appliquons l'algorithme de réduction à $M \overset{\text{def}}{=} \begin{pmatrix} 6 & 10 \\ 1 & 3 \end{pmatrix}$.

Rappel : Orthonormalisation de Gram-Schmidt

Soit $(b_1, \ldots, b_d)$ une famille libre de d vecteurs de $\mathbb{R}^n$. On pose

$$\begin{cases} b_1^\star &= b_1 \\ b_i^\star &= b_i - \sum_{j=1}^{i-1} \mu_{i,j} b_j^\star \text{ avec } \mu_{i,j} = \dfrac{\langle b_i, b_j^\star \rangle}{||b_j^\star||^2} \text{ pour } 1 \leqslant j < i, 2 \leqslant i \leqslant d. \end{cases}$$

Dimension Supérieure

Définition : Une base B d'un réseau $\mathcal{L}$ satisfait la **condition de taille** si les coefficients de son orthonormalisation de Gram-Schmidt satisfont

$$|\mu_{i,j}| \leqslant \frac{1}{2} \; \forall 1 \leqslant j < i \leqslant d.$$

Définition : Une base B d'un réseau est dite **LLL-réduite** si elle vérifie la condition de taille, et si son orthonormalisée vérifie la condition de Lovász

$$\left(\frac{3}{4} - \mu_{i,i-1}^2\right) ||b_{i-1}^\star||^2 \leqslant ||b_i^\star||^2, \; \forall 2 \leqslant i \leqslant d.$$

Algorithme LLL

Réduction en Dimension n : L'idée est de choisir une paire de vecteurs de base, de les réduire avec Gauss-Lagrange, puis d'en choisir une autre. Cependant, il faut que l'algorithme termine en temps raisonnable. C'est dû à la condition de Lovász.

L'algorithme LLL retourne une base LLL-réduite à partir d'une base $(b_1, \ldots, b_d)$ d'un réseau $\mathcal{L} \subset \mathbb{R}^n$ en temps $O(d^5 n \log^3(\max ||b_i||))$.

LLL permet de trouver $x \in \mathcal{L}$ tel que

$$\lambda_1 \leqslant ||x|| \leqslant 2^n \cdot \lambda_1$$

en temps polynomial.