Utilisation de réseaux en cryptographie

Quentin Deschamps

Automne 2020 *M2 SRI, ISFA*

Introduction et définition

Ajout de bruit : le problème LWE

- One time pad
- Learning with errors
- Exercice
- Un schéma d'encryption avec LWE

Contexte

- Protocole basés sur RSA non résistants au quantique.

Contexte

- Protocole basés sur RSA non résistants au quantique.
- On cherche un autre problème sur lequel baser des protocoles.

Réseau euclidien

Définition

Un réseau Λ de $\mathbb{R}^n$ est un sous-groupe discret de $\mathbb{R}^n$ pour l'addition, tel que le sous-espace vectoriel engendré par Λ soit égal à $\mathbb{R}^n$.

Réseau euclidien

Définition

Un réseau Λ de $\mathbb{R}^n$ est un sous-groupe discret de $\mathbb{R}^n$ pour l'addition, tel que le sous-espace vectoriel engendré par Λ soit égal à $\mathbb{R}^n$.

Exemple

L'ensemble $\mathbb{Z}^2$ des points à coordonnées entières de $\mathbb{R}^2$ est un réseau de $\mathbb{R}^2$

Représentation d'un réseau

La façon usuelle de représenter un réseau Λ est de donner une base de ce réseau : un ensemble de vecteurs v_i tel que Λ soit l'ensemble des combinaisons linéaires **entières** des v_i.

Représentation d'un réseau

La façon usuelle de représenter un réseau Λ est de donner une base de ce réseau : un ensemble de vecteurs v_i tel que Λ soit l'ensemble des combinaisons linéaires **entières** des v_i.

Définition

Une base d'un réseau Λ de $\mathbb{R}^n$ est un ensemble de vecteurs v_i tel que tout élément de Λ s'écrit d'une unique façon comme une combinaison entière des v_i.

Propriétés

- Si $n \geq 2$ un réseau de $\mathbb{R}^n$ possède une infinité de bases.
- Toutes les bases ont cardinal n.

Propriétés

- Si $n \geq 2$ un réseau de $\mathbb{R}^n$ possède une infinité de bases.
- Toutes les bases ont cardinal n.
- Exercice : preuve ?

Plus court vecteur

Problème

Étant donné un réseau Λ quel vecteur possède la norme euclidienne la plus faible ?

Plus court vecteur

Problème SVP : Shortest vector problem

Étant donné un réseau Λ quel vecteur possède la norme euclidienne la plus faible ?

Exemple

$v_1 = (8, -3) \quad v_2 = (-6, 2)$
$3v_1 + 4v_2 = (0, 1)$

Plus court vecteur

Problème

Étant donné un réseau Λ quel vecteur possède la norme euclidienne la plus faible ?

Exemple

$v_1 = (8, -3) \quad v_2 = (-6, 2)$
$3v_1 + 4v_2 = (0, 1)$

Remarque : Il n'y a pas un unique plus court vecteur.

Plus court vecteur

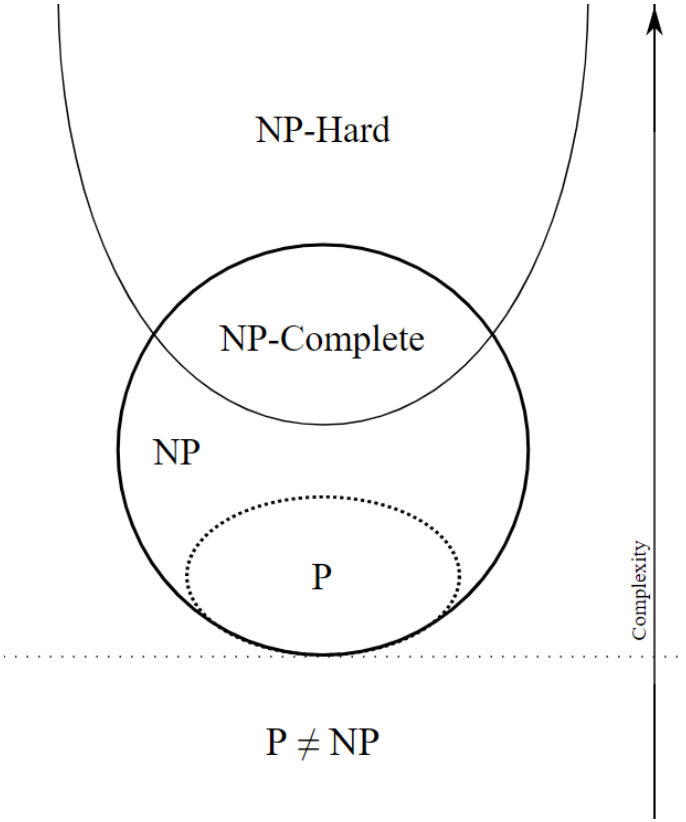
Problème

Étant donné un réseau Λ quel vecteur possède la norme euclidienne la plus faible ?

Théorème

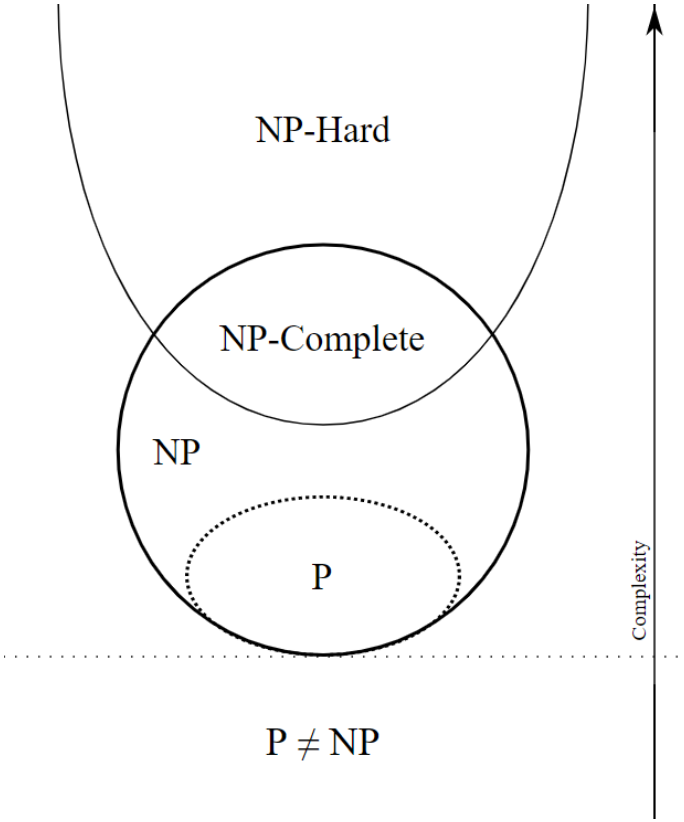
Le problème de trouver un plus court vecteur dans un réseau est NP-difficile.

Parenthèse sur la complexité



- RSA : NP-complet
- SVP : NP-hard

Parenthèse sur la complexité



- RSA : NP-complet
- SVP : NP-hard

- Question : où se trouve le problème du logarithme discret ?

Complexité de SVP

Résultat

Pour un réseau de dimension n, les meilleurs algorithmes connus pour résoudre SVP ont un temps d'exécution en $2^{\omega(n)}$.

Complexité de SVP

Résultat

Pour un réseau de dimension n, les meilleurs algorithmes connus pour résoudre SVP ont un temps d'exécution en $2^{\omega(n)}$.

- Pour que SVP soit difficile il faut manipuler des réseaux "grands".
- Importance de maîtriser les coûts lors des calculs.

Introduction et définition

Ajout de bruit : le problème LWE

One time pad

Learning with errors

Exercice

Un schéma d'encryption avec LWE

Masque de Véran

- Codage d'un message m de longueur l.

Masque de Véran

- Codage d'un message m de longueur l.
- Générer une chaîne aléatoire de caractère de longueur l : $r \xleftarrow{\$} \{0,1\}^r$

Masque de Véran

- Codage d'un message m de longueur l.
- Générer une chaîne aléatoire de caractère de longueur l : $r \xleftarrow{\$} \{0,1\}^r$
- Sommer (ou exclusif les deux chaînes)

Masque de Véran

- Codage d'un message m de longueur l.
- Générer une chaîne aléatoire de caractère de longueur l : $r \xleftarrow{\$} \{0,1\}^r$
- Sommer (ou exclusif les deux chaînes)
- Clef secrète : r, message codé $c = r \oplus m$

Masque de Véran

- Codage d'un message m de longueur l.
- Générer une chaîne aléatoire de caractère de longueur l : $r \xleftarrow{\$} \{0,1\}^r$
- Sommer (ou exclusif les deux chaînes)
- Clef secrète : r, message codé $c = r \oplus m$
- Déchiffrement $m = c \oplus r$

Masque de Véran

- Codage d'un message m de longueur l.
- Générer une chaîne aléatoire de caractère de longueur l : $r \xleftarrow{\$} \{0,1\}^r$
- Sommer (ou exclusif les deux chaînes)
- Clef secrète : r, message codé $c = r \oplus m$
- Déchiffrement $m = c \oplus r$

Théorème

Le masque de Véran achève une sécurité parfaite si r est parfaitement aléatoire.

Limitations

- Clef secrète de même longueur que le message.
- Impossible d'utiliser deux fois la même clef.
- Aléatoire parfait : difficile à créer.

Limitations

- Clef secrète de même longueur que le message.
- Impossible d'utiliser deux fois la même clef.
- Aléatoire parfait : difficile à créer.

C'est un idéal que l'on cherche à approcher.

Principe

- Idée : difficile de distinguer du véritable aléatoire d'une information + un bruit.

Problème mathématique

Problème

Soit **s** un vecteur. Connaissant des produits scalaires $< a, s >$, avec a connu est-il possible de retrouver s ?

Problème mathématique

Problème

Soit **s** un vecteur. Connaissant des produits scalaires $< a, s >$, avec a connu est-il possible de retrouver s ?

En utilisant un pivot de Gauss, on peut retrouver s en temps polynomial.

Problème mathématique

Problème

Soit $\mathbf{s}$ un vecteur. Connaissant des produits scalaires $< a, s > + e$, avec a connu et un bruit aléatoire e est-il possible de retrouver s ?

Problème mathématique

Problème

Soit $\mathbf{s}$ un vecteur. Connaissant des produits scalaires $< a, s > + e$, avec a connu et un bruit aléatoire e est-il possible de retrouver s ?

Théorème

Si e est bien choisi, ce problème est aussi difficile que le problème du plus court vecteur.

Formalisme

Distribution de e : Gaussienne discrète

$$D_{\mathbb{Z},\sigma,c}(x) = \frac{\exp(-\pi(x-c)^2/\sigma^2)}{\sum_{k\in\mathbb{Z}} \exp(-\pi(k-c)^2/\sigma^2)}$$

Soient les entiers $n \geq 1$, $q \geq 2$, un paramètre réel $\alpha \in [0,1]$, et un vecteur $\mathrm{s} \in \mathbb{Z}_q^n$. La distribution LWE $D_{n,q,\alpha}(\mathrm{s})$ est définie sur $\mathbb{Z}_q^n \times \mathbb{Z}_q$ de la manière suivante :

- On échantillonne le « terme d'erreur » $e \leftarrow D_{\mathbb{Z},\alpha\cdot q,0}$
- On échantillonne uniformément $\mathrm{a} \leftarrow U(\mathbb{Z}_q^n)$
- On retourne le couple $(\mathrm{a}, \langle \mathrm{a}, \mathrm{s}\rangle + e \bmod q)$

Hypothèse cryptographique

Problème Recherche LWE

Étant donnés des valeurs distribuées selon $D_{n,q,\alpha}(\mathbf{s})$ retrouver $\mathbf{s}$.

Hypothèse cryptographique

Problème Recherche LWE

Étant donnés des valeurs distribuées selon $D_{n,q,\alpha}(s)$ retrouver $\mathbf{s}$.

Problème Décision LWE

Si $s \in \mathbb{Z}_q^n$ est tiré uniformément au hasard, distinguer la distribution $D_{n,q,\alpha}(s)$ de la distribution uniforme sur $Z_q^n \times \mathbb{Z}_q$.

Définitions et notations

Comment créer un générateur pseudo-aléatoire à partir de LWE ?

- $l < k \in \mathbb{N}$
- $n < m \in \mathbb{N} \quad q = 2^k \quad B = 2^l$
- $\mathbf{A} \xleftarrow{\$} \mathcal{U}(\mathbb{Z}_q^{m \times n})$
- $\mathbf{e} \xleftarrow{\$} \mathcal{U}([\frac{-B}{2}, \frac{B}{2}]^m)$
- $D_{LWE,\mathbf{A}} = (\mathbf{A}, \mathbf{A}.s + e \mod q)$ pour $\mathbf{s} \xleftarrow{\$} \mathcal{U}(\mathbb{Z}_q^n)$

Hypothèse : il est difficile de distinguer $D_{LWE,\mathbf{A}}$ d'une distribution uniforme. On cherche à prouver que $G_A(s, e) = A.s + e \mod q$ peut être utilisé comme un générateur aléatoire.

Questions

- Supposant que l, k, n, m sont tels que LWE est difficile, monter que G_A est un générateur pseudo-aléatoire.
- Quel est l'agrandissement du générateur ? (le rapport entre la taille de l'entrée et la taille de la sortie)
- Cas spéciaux : $B = 0$? $k = l$?

Schéma

Même notation que précédemment :

- $l < k \in \mathbb{N}$
- $n < m \in \mathbb{N} \quad q = 2^k \quad B = 2^l$
- $\mathbf{A} \xleftarrow{\$} \mathcal{U}(\mathbb{Z}_q^{m \times n})$
- $\mathbf{e} \xleftarrow{\$} \mathcal{U}([\frac{-B}{2}, \frac{B}{2}]^m)$

Fonctions du schéma :

- KeyGen : $\mathbf{s} \xleftarrow{\$} \mathcal{U}(\mathbb{Z}_q^n)$
- $\mathrm{Enc}(m) = As + e + \frac{q}{2}m \mod q$
- $\mathrm{Dec}(c, s)$: calculer $\mathbf{v} = c - As$. Pour chaque élément v_i du vecteur $\mathbf{v}$ renvoyer 0 si $\frac{-q}{4} \leq v_i \leq \frac{q}{4}$ et 1 sinon.

Questions

- Prouver que le schéma est correct.
- Prouver que sous l'hypothèse LWE, ce schéma est sécurisé.
- Combien de bits sont nécessaires pour envoyer 1 bit d'information avec ce schéma ?