Étude du problème MP-LWE

Sacha Ben-Arous

31 Août 2023

ENS Paris-Saclay

Plan

Introduction aux réseaux

Définition

Un **réseau euclidien** de $\mathbb{R}^m$ est l'ensemble des combinaisons à coefficients entiers de vecteurs linéairements indépendants $b_1, \ldots, b_n$, que l'on note :

$$\mathcal{L}(b_1, \ldots, b_n) := \left\{ \sum_{i=1}^{n} x_i b_i, x_i \in \mathbb{Z} \right\}$$

Définition

Un **réseau euclidien** de $\mathbb{R}^m$ est l'ensemble des combinaisons à coefficients entiers de vecteurs linéairements indépendants $b_1, \ldots, b_n$, que l'on note :

$$\mathcal{L}(b_1, \ldots, b_n) := \left\{ \sum_{i=1}^{n} x_i b_i, x_i \in \mathbb{Z} \right\}$$

Le réseau est alors de *dimension* n, et la famille des $(b_i)_{1 \leq i \leq n}$ est appelée **base** de ce réseau.

Définition

Un **réseau euclidien** de $\mathbb{R}^m$ est l'ensemble des combinaisons à coefficients entiers de vecteurs linéairements indépendants $b_1, \ldots, b_n$, que l'on note :

$$\mathcal{L}(b_1, \ldots, b_n) := \left\{ \sum_{i=1}^{n} x_i b_i, x_i \in \mathbb{Z} \right\}$$

Le réseau est alors de *dimension* n, et la famille des $(b_i)_{1 \leq i \leq n}$ est appelée **base** de ce réseau.

En notant $B := [b_1, \ldots, b_n]$, on considérera de manière équivalente :

$$\mathcal{L}(B) := \{Bx, x \in \mathbb{Z}^n\}$$

Exemples

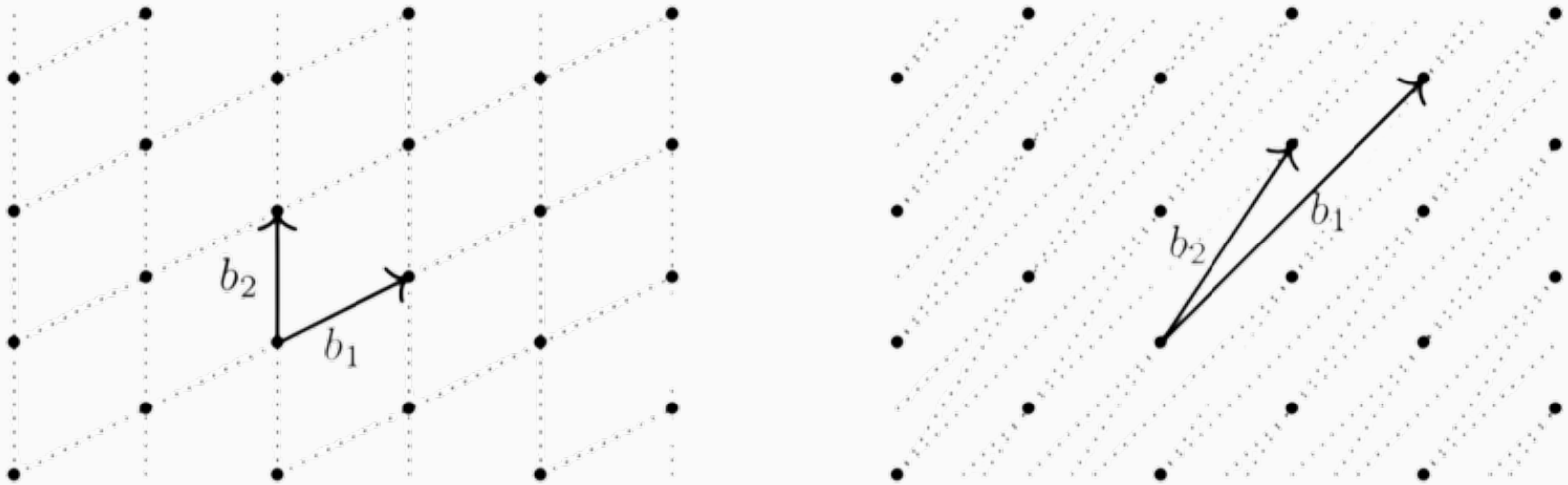

Figure 1 – Exemple de réseau [Kat23]

Learning With Errors

Learning With Errors Problem :

On fixe des entiers n et t, un nombre premier q et une distribution de bruit $\mathcal{N}(\sigma)$. On tire un secret $s \hookleftarrow \mathcal{U}(\mathbb{Z}_q^n)$.

Learning With Errors

Learning With Errors Problem :

On fixe des entiers n et t, un nombre premier q et une distribution de bruit $\mathcal{N}(\sigma)$. On tire un secret $s \hookleftarrow \mathcal{U}(\mathbb{Z}_q^n)$.

Le problème est le suivant : à partir de t échantillons

$$(a_i, b_i) := (a_i, \langle a_i, s \rangle + e_i \bmod q)$$

où $a_i \hookleftarrow \mathcal{U}(\mathbb{Z}_p^n)$ et $e_i \hookleftarrow \mathcal{N}(\sigma)$, on souhaite retrouver le secret s.

Learning With Errors

Learning With Errors Problem :

On fixe des entiers n et t, un nombre premier q et une distribution de bruit $\mathcal{N}(\sigma)$. On tire un secret $s \hookleftarrow \mathcal{U}(\mathbb{Z}_q^n)$.

Le problème est le suivant : à partir de t échantillons

$$(a_i, b_i) := (a_i, \langle a_i, s \rangle + e_i \bmod q)$$

où $a_i \hookleftarrow \mathcal{U}(\mathbb{Z}_p^n)$ et $e_i \hookleftarrow \mathcal{N}(\sigma)$, on souhaite retrouver le secret s.

Rq : Sans bruit, le problème est facile à résoudre.

Lien avec les réseaux

Cela revient à chercher le point le plus proche de $A \cdot s + e$ dans le réseau engendré par

$$A' := \left[\begin{array}{c|ccc} & q & \cdots & 0 \\ A & \vdots & \ddots & \vdots \\ & 0 & \cdots & q \end{array}\right] \in \mathbb{Z}^{t \times (n+t)}$$

Difficulté de LWE

- La difficulté est relié au facteur $\gamma = \frac{\lambda_1}{\|e\|}$

Difficulté de LWE

- La difficulté est relié au facteur $\gamma = \frac{\lambda_1}{\|e\|}$
- Plus γ est petit, plus le problème est dur

Difficulté de LWE

- La difficulté est relié au facteur $\gamma = \frac{\lambda_1}{\|e\|}$
- Plus γ est petit, plus le problème est dur
- Si $\gamma = poly(n)$, ce problème est conjecturé exponentiellement dur à résoudre, même sur un ordinateur quantique

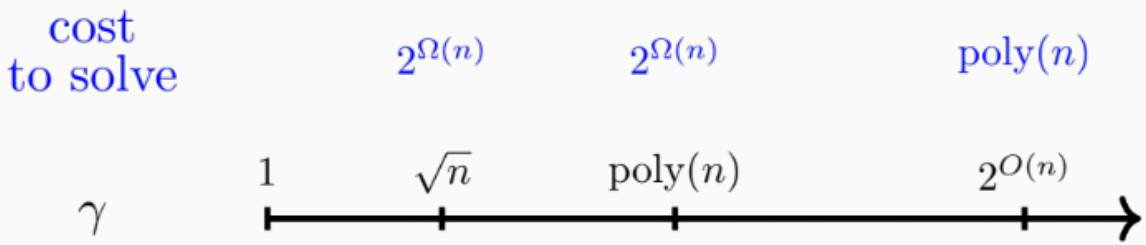

Figure 2 – Lien difficulté/gamma [Kat23]

Variantes structurées

Problème : LWE tel quel est peu efficace à cause des grandes matrices aléatoires.

Variantes structurées

Problème : LWE tel quel est peu efficace à cause des grandes matrices aléatoires.

Solution : Rajouter de la structure : polynômes (Stehlé *et al.* [SSTX09])

Illustration

Concrètement, cela consiste à représenter matriciellement le produit de polynômes, et donc à mettre des blocs structurés dans A

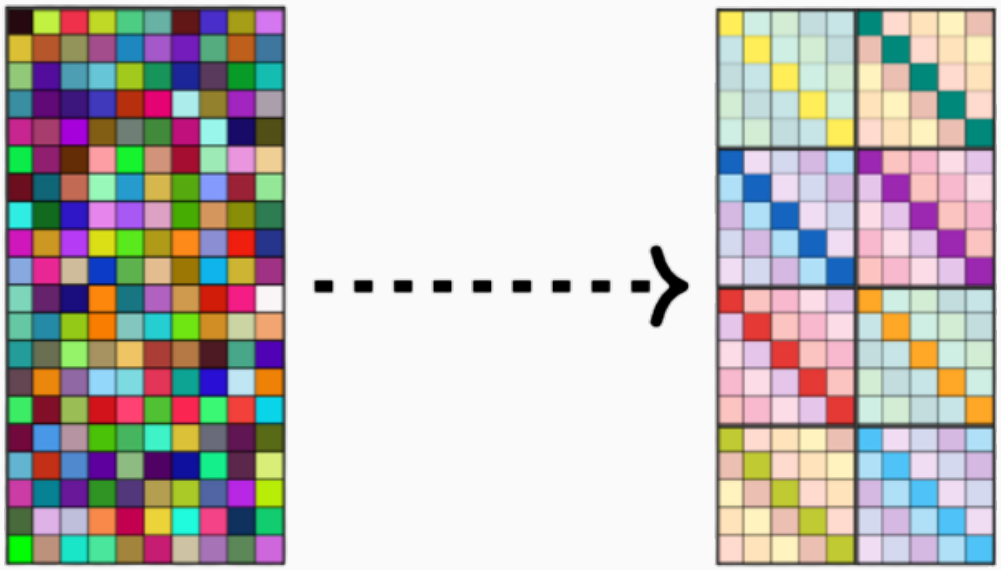

Figure 3 – Représentation de la structure d'un réseau [Kat23]

Variantes structurées

Défaut : nouveau paramètre $f \in \mathbb{Z}_q^m[X]$ qui régit la complexité.

Ex : $x^n + 1$ et $x^n - 1$

Variantes structurées

Défaut : nouveau paramètre $f \in \mathbb{Z}_q^m[X]$ qui régit la complexité.

Ex : $x^n + 1$ et $x^n - 1$

Roșca *et al.* [RSSS17] introduisent une nouvelle variante structurée, et y réduisent des classes exponentiellement grandes de problèmes P-LWE.

Étude de la réduction

Objectif

- Comprendre le fonctionnement de la réduction, et son impact sur les paramètres de difficulté.

Objectif

- Comprendre le fonctionnement de la réduction, et son impact sur les paramètres de difficulté.

- Établir des propriétés sur le nouveau réseau d'arrivée

Représentation matricielle de la réduction

On défini $\text{Rot}_f(a)$ pour qu'elle vérifie $\text{Rot}_f(a) \cdot b = (a \times b \mod f)$

Représentation matricielle de la réduction

On défini $\mathrm{Rot}_f(a)$ pour qu'elle vérifie $\mathrm{Rot}_f(a) \cdot b = (a \times b \mod f)$

Ex : Si $f = x^4 + 1$ et $a = \sum_{0 \leq i < 4} a_i x^i$, alors :

$$\mathrm{Rot}_f(a) = \begin{pmatrix} a_0 & a_1 & a_2 & a_3 \\ -a_3 & a_0 & a_1 & a_2 \\ -a_2 & -a_3 & a_0 & a_1 \\ -a_1 & -a_2 & -a_3 & a_0 \end{pmatrix}$$

Représentation matricielle de la réduction

De même pour $\mathrm{Toep}_d(a)$, choisie pour avoir $\mathrm{Toep}_d(a) \cdot b = (a \odot_d b)$

Représentation matricielle de la réduction

De même pour $\mathsf{Toep}_d(a)$, choisie pour avoir $\mathsf{Toep}_d(a) \cdot b = (a \odot_d b)$

Ex : Si $d = 3$ et $a = \sum_{0 \leq i < 4} a_i x^i$, alors :

$$\mathsf{Toep}(a) = \begin{pmatrix} a_0 & a_1 & a_2 & a_3 & 0 & 0 & 0 \\ 0 & a_0 & a_1 & a_2 & a_3 & 0 & 0 \\ 0 & 0 & a_0 & a_1 & a_2 & a_3 & 0 \\ 0 & 0 & 0 & a_0 & a_1 & a_2 & a_3 \end{pmatrix}$$

Représentation matricielle de la réduction

$$\text{La réduction va donc de } A_1 = \begin{bmatrix} \mathsf{Rot}_f(a_1) \\ \vdots \\ \mathsf{Rot}_f(a_t) \end{bmatrix} \text{ vers } A_2 = \begin{bmatrix} \mathsf{Toep}_d(a_1) \\ \vdots \\ \mathsf{Toep}_d(a_t) \end{bmatrix}$$

Heuristique gausienne

Volume d'un réseau $\mathcal{L}(B) := \sqrt{\det(B^\top B)}$.

Rq : ne dépend pas de B

Heuristique gausienne

Volume d'un réseau $\mathcal{L}(B) := \sqrt{\det(B^\top B)}$.

Rq : ne dépend pas de B

Heuristique gaussienne :

$$|\{\text{points du réseau de norme} \leq R\}| \simeq \frac{V_n(R)}{\text{vol}(L)} = \frac{R^n V_n(1)}{\text{vol}(L)}$$

En particulier $\lambda_1 \simeq \sqrt{n} \cdot \text{vol}(L)^{\frac{1}{n}}$

Volumes

Théorème : Avec probabilité $\geq 1 - \frac{1}{q^{mt}}$ on a $\text{vol}(\mathcal{L}_1) = q^{m(t-1)}$

Volumes

Théorème : Avec probabilité $\geq 1 - \frac{1}{q^{mt}}$ on a $\text{vol}(\mathcal{L}_1) = q^{m(t-1)}$

Théorème : Avec une probabilité $\geq 1 - \left(\frac{n+d-1}{q}\right)^{\lfloor t/\lceil \frac{n+d-1}{d} \rceil \rfloor}$, on a que $\text{vol}(\mathcal{L}_2) = q^{td-(n+d-1)}$

Volumes

Théorème : Avec probabilité $\geq 1 - \frac{1}{q^{mt}}$ on a $\mathrm{vol}(\mathcal{L}_1) = q^{m(t-1)}$

Théorème : Avec une probabilité $\geq 1 - \left(\frac{n+d-1}{q}\right)^{\lfloor t/\lceil \frac{n+d-1}{d} \rceil \rfloor}$, on a que $\mathrm{vol}(\mathcal{L}_2) = q^{td-(n+d-1)}$

À retenir : $\frac{\mathrm{vol}(\mathcal{L}_1)^{\frac{1}{tm}}}{\mathrm{vol}(\mathcal{L}_2)^{\frac{1}{td}}} = q^{\frac{n}{td}}$, et $td \simeq n$ donc le volume change peu

Idée de preuve

- Il suffit d'avoir que A_1 et A_2 sont de rang plein

Idée de preuve

- Il suffit d'avoir que A_1 et A_2 sont de rang plein
- Pour A_1 : utiliser $\mathsf{Rot}_f(a)^{-1} = \mathsf{Rot}_f(a^{-1})$

Idée de preuve

- Il suffit d'avoir que A_1 et A_2 sont de rang plein
- Pour A_1 : utiliser $\mathrm{Rot}_f(a)^{-1} = \mathrm{Rot}_f(a^{-1})$
- Pour A_2 : plus dur car bloc pas carrés, il faut les rassembler. Ma preuve n'utilise pas la structure Toeplitz, et la borne est non optimale.

Résultats expérimentaux

$n = 22$, $d = 11, t = 3$, et $q = n^\beta \log n$ où on fait varier β. En pratique n est beaucoup plus grand, et dans le schéma $\beta = 2.5$. En faisant 10^6 tests, on obtient les résultats suivants :

	Probabilité empirique	Probabilité pour les matrices uniformes	Borne inférieure obtenue dans le théorème 3.2
$\beta = 0.75$ $q = 37$	0.998603	0.99924	0.135135
$\beta = 1$ $q = 71$	0.999629	0.999798	0.549295
$\beta = 1.5$ $q = 331$	0.999979	0.999990	0.903323

Erreurs

- $\mathbb{E}(\|e_1\|^2) = tm(\alpha q)^2$
- $\mathbb{E}(\|e_2\|^2) = td(\alpha dSq)^2$

car $\sigma_2 = (\alpha dS)\sigma_1$. Voir rapport pour détails.

Heuristique gaussienne

Théorème (Minkowski) : $\lambda_1 \leq \sqrt{n} \cdot \mathrm{vol}(\mathcal{L})^{\frac{1}{n}}$

Heuristique gaussienne

Théorème (Minkowski) : $\lambda_1 \leq \sqrt{n} \cdot \mathrm{vol}(\mathcal{L})^{\frac{1}{n}}$

Théorème : Si $d = \frac{n}{2}$ et $t \geq 4$ alors, avec probabilité $\geq 1 - \frac{1}{2^{td-1}q^{t-3}}$, on a :

$$\lambda_1^{\infty}(\mathcal{L}_2) \geq \frac{1}{2q}\mathrm{vol}(\mathcal{L}_2)^{\frac{1}{dt}}$$

Heuristique gaussienne

Théorème (Minkowski) : $\lambda_1 \leq \sqrt{n} \cdot \text{vol}(\mathcal{L})^{\frac{1}{n}}$

Théorème : Si $d = \frac{n}{2}$ et $t \geq 4$ alors, avec probabilité $\geq 1 - \frac{1}{2^{td-1}q^{t-3}}$, on a :

$$\lambda_1^{\infty}(\mathcal{L}_2) \geq \frac{1}{2q}\text{vol}(\mathcal{L}_2)^{\frac{1}{dt}}$$

Rq : Le résultat est en norme infinie, et est trop faible par rapport à ce qui attendu.

Schéma de chiffrement

Théorème [RSS17] : Si $\alpha \leq \frac{1}{16\sqrt{tk\lambda}}$ et $16t(k+1) \leq q$, alors pour tout $\mu \in \{0,1\}^{<d}[X]$, avec probabilité $\geq 1 - 2^{-\Omega(\lambda)}$ sur `(sk,pk)` $\hookleftarrow$ `KeyGen`, on a `Decrypt(sk,Encrypt(pk,mu)) = mu`

Preuve incorrecte, j'en donne une nouvelle version, avec des hypothèses renforcées.

Schéma de chiffrement

Théorème [RSS17] : Si $\alpha \leq \frac{1}{16\sqrt{tk\lambda}}$ et $16t(k+1) \leq q$, alors pour tout $\mu \in \{0,1\}^{<d}[X]$, avec probabilité $\geq 1 - 2^{-\Omega(\lambda)}$ sur `(sk,pk)` $\hookleftarrow$ `KeyGen`, on a `Decrypt(sk,Encrypt(pk,mu)) = mu`

Preuve incorrecte, j'en donne une nouvelle version, avec des hypothèses renforcées.

Théorème : Si $\alpha \leq \frac{1}{16(k+1)t\sqrt{\lambda}}$ et $8td(k+1) \leq qd \leq e^{\lambda}$, alors pour tout $\mu \in \{0,1\}^{<d}[X]$, avec probabilité $\geq 1 - 2^{-\Omega(\lambda)}$ sur `(sk,pk)` $\hookleftarrow$ `KeyGen`, on a `Decrypt(sk,Encrypt(pk,mu)) = mu`

Schéma de chiffrement

Théorème [RSS17] : Si $\alpha \leq \frac{1}{16\sqrt{tk\lambda}}$ et $16t(k+1) \leq q$, alors pour tout $\mu \in \{0,1\}^{<d}[X]$, avec probabilité $\geq 1 - 2^{-\Omega(\lambda)}$ sur `(sk,pk)` $\hookleftarrow$ `KeyGen`, on a `Decrypt(sk,Encrypt(pk,mu)) = mu`

Preuve incorrecte, j'en donne une nouvelle version, avec des hypothèses renforcées.

Théorème : Si $\alpha \leq \frac{1}{16(k+1)t\sqrt{\lambda}}$ et $8td(k+1) \leq qd \leq e^{\lambda}$, alors pour tout $\mu \in \{0,1\}^{<d}[X]$, avec probabilité $\geq 1 - 2^{-\Omega(\lambda)}$ sur `(sk,pk)` $\hookleftarrow$ `KeyGen`, on a `Decrypt(sk,Encrypt(pk,mu)) = mu`

Rq : La modification est essentiellement au niveau de α, que l'on a diminué. Cela a pour effet de réduire la variance de l'erreur gaussienne appliquée sur le message, ce qui le rend plus simple à déchiffrer, et facilite donc la preuve.

Conclusion

- MP-LWE gagne sur le plan algébrique tout en conservant la difficulté algorithmique
- Résultat sur l'heuristique gaussienne à améliorer
- Étudier l'influence de la structure sur le rang des réseaux

Références

[Kat23] Katharina Boudgoust, “Hardness Assumptions in Lattice-Based Cryptography”

RSSS17] Miruna Roșca , Amin Sakzad, Damien Stehlé et Ron Steinfeld “Middle-Product Learning With Errors”

SSTX09] Damien Stehlé, Ron Steinfeld, Keisuke Tanaka et Keita Xagawa “Efficient public key encryption based on ideal lattices”