Autour de la difficulté du problème "Learning With Errors"

Adeline Langlois

Équipe Aric du LIP, ENS Lyon

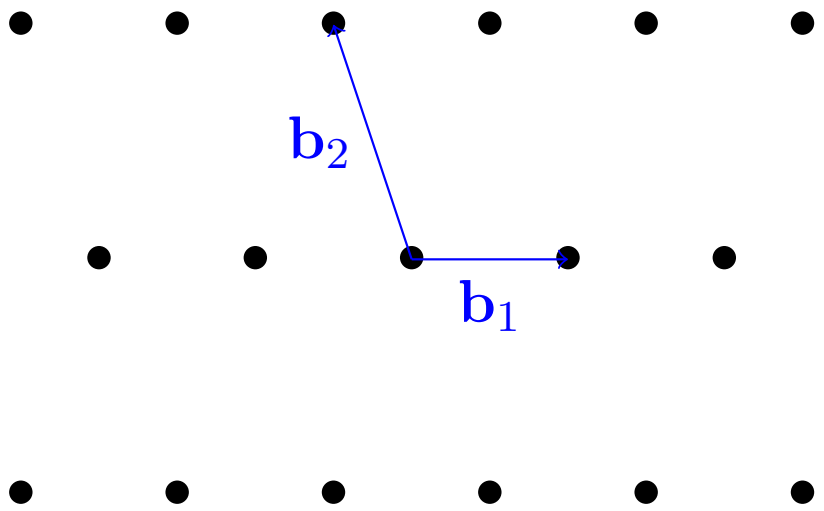
Travaux en commun et en cours avec D. Stehlé, Z. Brakerski, C. Peikert et O. Regev

12 octobre 2012

Résultats principaux

- Difficulté du problème LWE indépendamment de la forme arithmétique du module q.
- Difficulté du problème Ring-LWE indépendamment de la forme arithmétique du module q.
- **Conséquence** : Dequantumisation de la preuve de difficulté de LWE pour q polynomial.

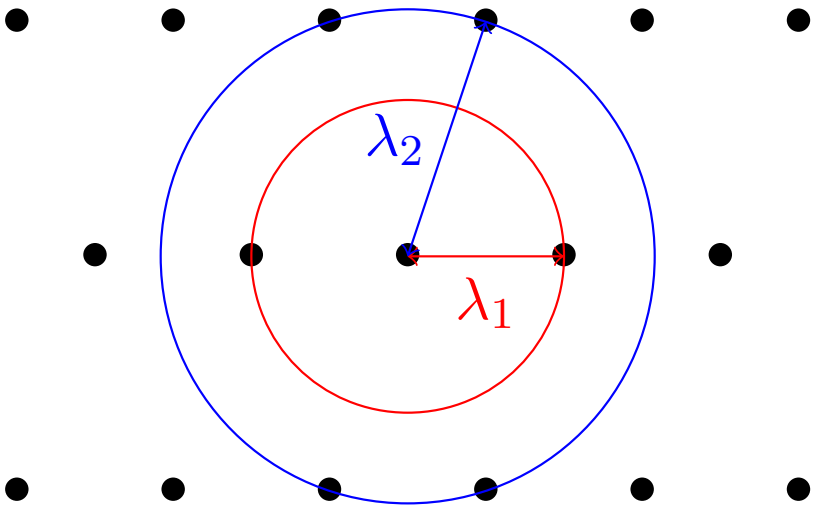
Réseaux euclidiens et problèmes sur les réseaux



Réseau euclidien

$\mathcal{L}(\mathbf{B}) = \{\sum_{i=1}^{n} a_i \mathbf{b}_i, a_i \in \mathbb{Z}\}$, avec $(\mathbf{b}_i)_{1 \leq i \leq n}$, vecteurs linéairement indépendants, est une base de $\mathcal{L}(\mathbf{B})$.

Réseaux euclidiens et problèmes sur les réseaux



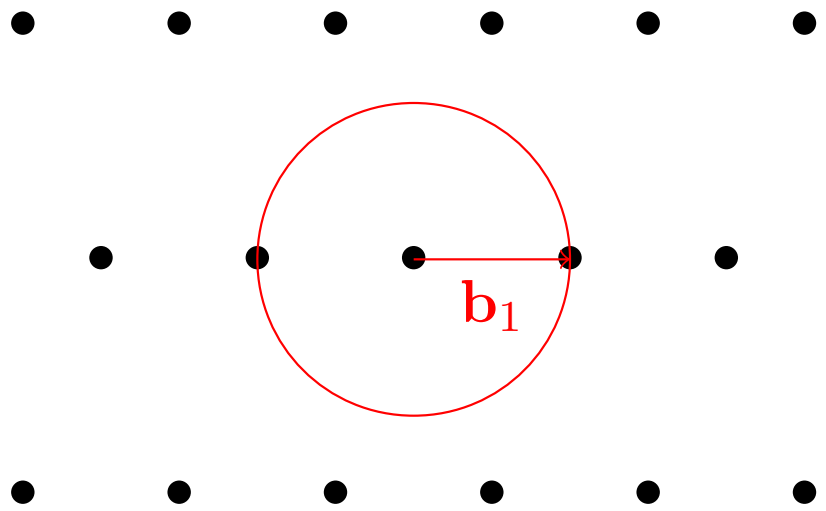
Définitions :

- 1er minimum
- 2nd minimum

Réseau euclidien

$\mathcal{L}(\mathbf{B}) = \{\sum_{i=1}^{n} a_i \mathbf{b}_i, a_i \in \mathbb{Z}\}$, avec $(\mathbf{b}_i)_{1 \leq i \leq n}$, vecteurs linéairement indépendants, est une base de $\mathcal{L}(\mathbf{B})$.

Réseaux euclidiens et problèmes sur les réseaux



Définitions :

- 1er minimum
- 2nd minimum

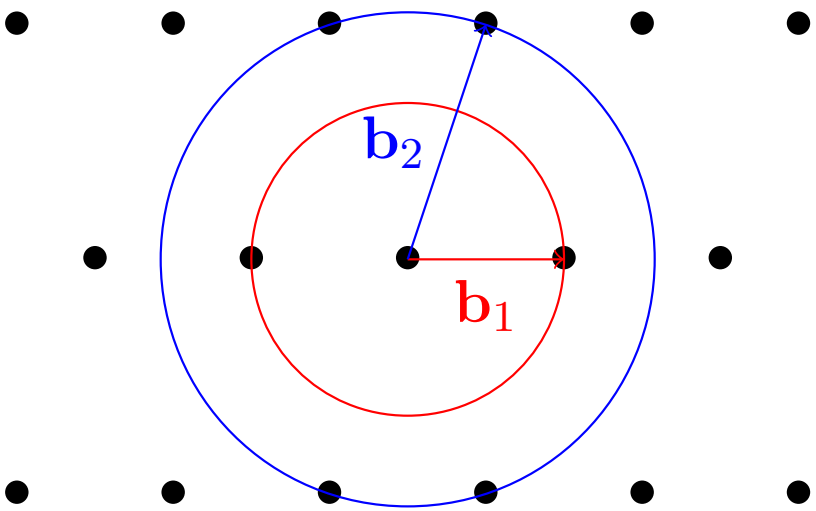
Problèmes :

- Shortest Vector Pb

Réseau euclidien

$\mathcal{L}(\mathbf{B}) = \{\sum_{i=1}^{n} a_i \mathbf{b}_i, a_i \in \mathbb{Z}\}$, avec $(\mathbf{b}_i)_{1 \leq i \leq n}$, vecteurs linéairement indépendants, est une base de $\mathcal{L}(\mathbf{B})$.

Réseaux euclidiens et problèmes sur les réseaux



Définitions :

- 1er minimum
- 2nd minimum

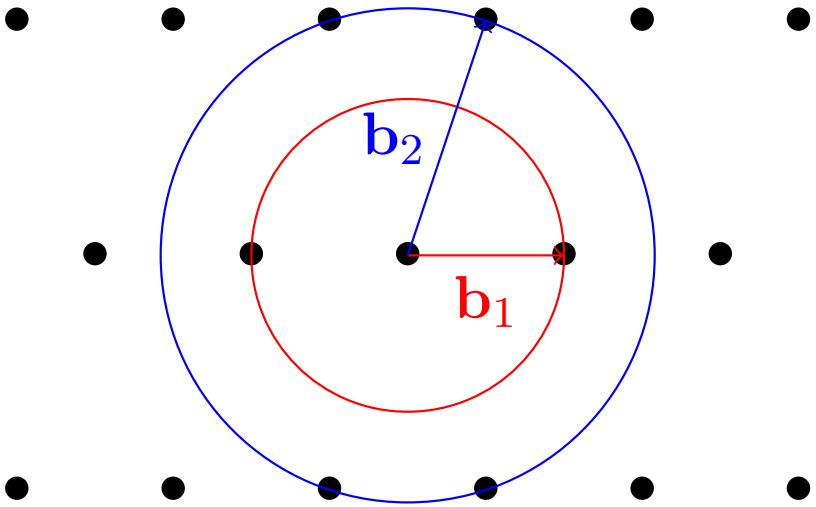
Problèmes :

- Shortest Vector Pb
- Shortest Independent Vectors Pb

Réseau euclidien

$\mathcal{L}(\mathbf{B}) = \{\sum_{i=1}^{n} a_i \mathbf{b}_i, a_i \in \mathbb{Z}\}$, avec $(\mathbf{b}_i)_{1 \leq i \leq n}$, vecteurs linéairement indépendants, est une base de $\mathcal{L}(\mathbf{B})$.

Réseaux euclidiens et problèmes sur les réseaux



Définitions :

- 1er minimum
- 2nd minimum

Problèmes :

- Shortest Vector Pb
- Shortest Independent Vectors Pb
- Facteur d'approximation : γ

Conjecture

Les problèmes d'approximation dans les réseaux avec des γ polynomiaux sont des problèmes exponentiellement difficiles.

Cryptographie reposant sur les réseaux

Intérêts

- Simplicité
- Efficacité potentielle
- Preuves de sécurité
- Cryptographie post-quantique
- Gentry 2009 : chiffrement totalement homomorphe

Contexte

- $\mathbb{Z}_q = \mathbb{Z}/q\mathbb{Z}$,

Distribution Gaussienne

Pour tout $\alpha > 0$ et $\mathbf{x} \in \mathbb{Z}^n$, on définit la distribution Gaussienne :

$$\nu_\alpha(\mathbf{x}) = \frac{1}{\alpha^n} \cdot e^{-\pi \|\frac{\mathbf{x}}{\alpha}\|^2}.$$

Propriété : $e \sim \nu_\alpha \Rightarrow e$ petit.

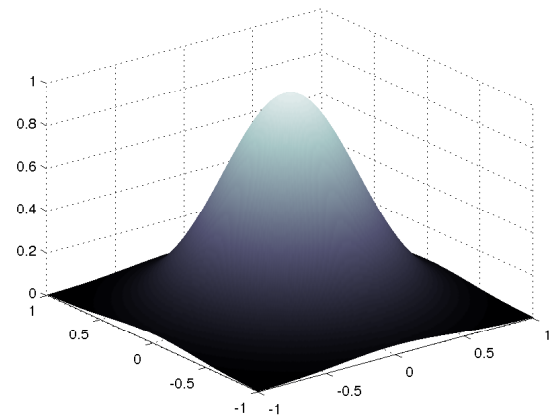


FIGURE: Gaussienne continue

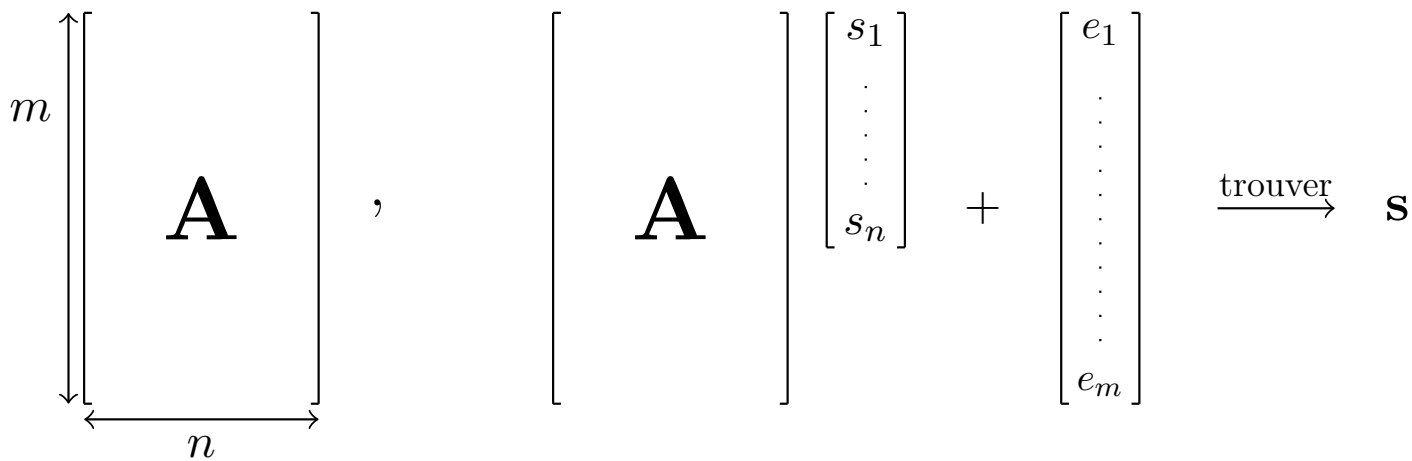
Learning With Errors [Regev05] :

$\mathrm{LWE}_{q,\alpha}$ version calculatoire

Trouver $\mathbf{s} \in \mathbb{Z}_q^n$, étant donné $\mathbf{A} \in \mathbb{Z}_q^{m \times n}$ et $\mathbf{b} = \mathbf{A}\mathbf{s} + \mathbf{e}\ [q]$, où $\mathbf{e}$ est Gaussien.

$\mathrm{LWE}_{q,\alpha}$ version décisionnelle

Distinguer entre $(\mathbf{A}, \mathbf{b})$ uniforme et $(\mathbf{A}, \mathbf{A}\mathbf{s} + \mathbf{e} \bmod q)$, où $\mathbf{A} \leftarrow U(\mathbb{Z}_q^{m \times n})$, $\mathbf{s} \leftarrow U(\mathbb{Z}_q^n)$ est secret, et $\mathbf{e}$ est Gaussien.



Exemple chiffrement à clé publique [Regev 2005]

- **Paramètres** : $n, m, q \in \mathbb{Z}$, $\alpha \in \mathbb{R}$,
- **Clés** : $\text{sk} = \mathbf{s} \hookleftarrow U(\mathbb{Z}_q^n)$,
  soient $\mathbf{A} \hookleftarrow U(\mathbb{Z}_q^{m \times n})$ et $e \hookleftarrow \nu_\alpha^m$, $\text{pk} = (\mathbf{A}, \mathbf{b})$ avec $\mathbf{b} = \mathbf{As} + \mathbf{e}$ $[q]$.
- **Chiffrement** $(M \in \{0,1\})$ **:** Choisir $\mathbf{r} \hookleftarrow U(\{0,1\}^m)$,

$$\mathbf{u}^T = \overbrace{r_1 \quad \cdots \quad r_m}^{} \begin{bmatrix} & & \\ & \mathbf{A} & \\ & & \end{bmatrix}, \; v = \overbrace{r_1 \quad \cdots \quad r_m}^{} \begin{bmatrix} b_1 \\ \vdots \\ b_m \end{bmatrix} + \lfloor q/2 \rceil \cdot M$$

Exemple chiffrement à clé publique [Regev 2005]

- **Clés :** $\mathrm{sk} = \mathbf{s} \hookleftarrow U(\mathbb{Z}_q^n)$,
  soient $\mathbf{A} \hookleftarrow U(\mathbb{Z}_q^{m\times n})$ et $e \hookleftarrow \nu_\alpha^m$, $\mathrm{pk} = (\mathbf{A}, \mathbf{b})$ avec $\mathbf{b} = \mathbf{As} + \mathbf{e}\ [q]$.
- **Chiffrement** $(M \in \{0,1\})$ **:** Choisir $\mathbf{r} \hookleftarrow U(\{0,1\}^m)$,

$$\mathbf{u}^T = \overbrace{r_1 \ \cdots\cdots \ r_m}\begin{bmatrix} & \\ & \mathbf{A} \\ & \end{bmatrix},\ v = \overbrace{r_1 \ \cdots\cdots \ r_m}\begin{bmatrix} b_1 \\ \vdots \\ b_m \end{bmatrix} + \lfloor q/2 \rceil \cdot M$$

- **Déchiffrement** de $(\mathbf{u}, v)$: calcul de $v - \mathbf{u}^T\mathbf{s}$:

$$\underbrace{\overbrace{r_1 \ \cdots\cdots \ r_m}\left[\begin{bmatrix} & \\ & \mathbf{A} \\ & \end{bmatrix}\begin{bmatrix} s_1 \\ \vdots \\ s_n \end{bmatrix} + \begin{bmatrix} e_1 \\ \vdots \\ e_m \end{bmatrix}\right] + \lfloor q/2 \rceil \cdot M}_{v} - \underbrace{\overbrace{r_1 \ \cdots\cdots \ r_m}\begin{bmatrix} & \\ & \mathbf{A} \\ & \end{bmatrix}\begin{bmatrix} s_1 \\ \vdots \\ s_n \end{bmatrix}}_{\mathbf{u}^T\mathbf{s}} = \text{small} + \lfloor q/2 \rceil \cdot M$$

Si proche de 0 : renvoyer 0, si proche de $\lfloor q/2 \rfloor$: renvoyer 1.

Exemple chiffrement à clé publique [Regev 2005]

- **Clés :** $\mathrm{sk} = \mathbf{s} \hookleftarrow U(\mathbb{Z}_q^n)$,
  soient $\mathbf{A} \hookleftarrow U(\mathbb{Z}_q^{m\times n})$ et $e \hookleftarrow \nu_\alpha^m$, $\mathrm{pk} = (\mathbf{A}, \mathbf{b})$ avec $\mathbf{b} = \mathbf{As} + \mathbf{e}\ [q]$.

- **Chiffrement** $(M \in \{0,1\})$ **:** Choisir $\mathbf{r} \hookleftarrow U(\{0,1\}^m)$,

$$\mathbf{u}^T = \overbrace{r_1 \ \cdots\cdots \ r_m}\begin{bmatrix} & \\ & \mathbf{A} \\ & \end{bmatrix},\ v = \overbrace{r_1 \ \cdots\cdots \ r_m}\begin{bmatrix} b_1 \\ \vdots \\ b_m \end{bmatrix} + \lfloor q/2 \rceil \cdot M$$

- **Déchiffrement** de $(\mathbf{u}, v)$: calcul de $v - \mathbf{u}^T\mathbf{s}$:

$$\underbrace{\overbrace{r_1 \ \cdots\cdots \ r_m}\left[\begin{bmatrix} & \\ & \mathbf{A} \\ & \end{bmatrix}\begin{bmatrix} s_1 \\ \vdots \\ s_n \end{bmatrix} + \begin{bmatrix} e_1 \\ \vdots \\ e_m \end{bmatrix}\right] + \lfloor q/2 \rceil \cdot M}_{v} - \underbrace{\overbrace{r_1 \ \cdots\cdots \ r_m}\begin{bmatrix} & \\ & \mathbf{A} \\ & \end{bmatrix}\begin{bmatrix} s_1 \\ \vdots \\ s_n \end{bmatrix}}_{\mathbf{u}^T\mathbf{s}} = \text{small} + \lfloor q/2 \rceil \cdot M$$

LWE difficile $\Rightarrow$ ce chiffrement résiste aux attaques à clair choisi.

Résultats existants

- **Regev 05** : réduction **quantique** de SIVP à LWE pour q premier et polynomial.
- **Peikert 09** : réduction **classique** de SIVP à LWE pour q exponentiel et produit de petits facteurs connus.

$\Rightarrow$ **Contraintes sur** q

Pourquoi enlever ces contraintes ?

Problème ouvert depuis Regev en 2005.

Obtenir une réduction **classique** pour q polynomial.

Notre résultat

Résultat

Soient $n \geq 1$, $p, q \geq 2$, $\alpha, \beta > 0$ et $\mathbf{s}_{max}$ une borne sur la norme du secret, tels que :

$$\beta \geq \widetilde{\Omega}\left(\sqrt{\alpha^2 + \frac{\mathbf{s}_{max}^2}{\min(p^2, q^2)}}\right) \text{ et } \alpha q \geq \widetilde{\Omega}(\sqrt{1}),$$

alors il existe une réduction de $\mathrm{LWE}_{q,\alpha}$ à $\mathrm{LWE}_{p,\beta}$.

Conséquence

Il existe une réduction quantique de SIVP à LWE pour tout q.

Aperçu de la preuve : "modulus switching"

Principe : Transformer un échantillon de $\mathrm{LWE}_{q,\alpha}$ en un échantillon de $\mathrm{LWE}_{p,\beta}$:

- Discrétiser la distribution et réduire la taille de $\mathbf{s}$.
- Transformer $\mathbf{A} \hookleftarrow U(\mathbb{Z}_q^{m\times n})$ en $\mathbf{A}' \hookleftarrow U(\mathbb{Z}_p^{m\times n})$.
- $\mathbf{b} = \mathbf{A}\mathbf{s} + \mathbf{e} = \mathbf{A}'\mathbf{s} + (\mathbf{A}' - \mathbf{A})\mathbf{s} + \mathbf{e}$.
- Nouvelle erreur : $\mathbf{e}' = (\mathbf{A}' - \mathbf{A})\mathbf{s} + \mathbf{e}$.

Conséquence : "Dé-quantumisation"

On note $\mathrm{SIVP}_{\mathrm{dim},\gamma}$ et $\mathrm{LWE}^{\text{distribution du secret}}_{\mathrm{dim},q,\alpha}$.

Suite de réductions :

$$\mathrm{SIVP}_{\sqrt{n},n^{\omega(1)}} \underbrace{\leqslant}_{1} \mathrm{LWE}^{U(\mathbb{Z}_q^n)}_{\sqrt{n},2^n,n^{-\omega(1)}} \underbrace{\leqslant}_{2} \mathrm{LWE}^{U(\{0,1\}^n)}_{n,2^n,\frac{1}{poly(n)}} \underbrace{\leqslant}_{3} \mathrm{LWE}^{U(\mathbb{Z}_q^n)}_{n,poly(n),\frac{1}{poly(n)}}$$

1. **Peikert 2009**
2. **Goldwasser Kalai Peikert Vaikuntanathan 2010**
3. **Notre résultat**

Conclusion et travaux en cours

Résultat

- Une réduction de $\mathrm{LWE}_{q,\alpha}$ à $\mathrm{LWE}_{p,\beta}$.
- "Dé-quantumisation" de la preuve de difficulté de LWE.
- Difficulté de R-LWE pour tout modulo q (quantique !).

Conclusion et travaux en cours

Résultat

- Une réduction de $\mathrm{LWE}_{q,\alpha}$ à $\mathrm{LWE}_{p,\beta}$.
- "Dé-quantumisation" de la preuve de difficulté de LWE.
- Difficulté de R-LWE pour tout modulo q (quantique !).

Et ensuite ?

- "Dé-quantumisation" pour RLWE ?
- Est-ce que le module q est vraiment indispensable ?
- Difficulté de RLWE sous SIVP pour des réseaux arbitraires (non idéaux).