

# Étude du problème MP-LWE

Sacha Ben-Arous, sous la direction d'Alice Pellet-Mary

8 Juin - 21 Juillet 2023

## Table des matières

|          |  |           |
|----------|--|-----------|
| <b>1</b> | <b>Introduction</b>                          | <b>2</b>  |
| <b>2</b> | <b>Préliminaires</b>                         | <b>2</b>  |
| 2.1      | Problème LWE et difficulté . . . . .         | 3         |
| 2.2      | Variantes structurées . . . . .              | 4         |
| <b>3</b> | <b>Étude de la réduction</b>                 | <b>5</b>  |
| 3.1      | Principe de la réduction . . . . .           | 5         |
| 3.2      | Effets géométriques . . . . .                | 7         |
| 3.2.1    | Évolution du volume . . . . .                | 7         |
| 3.2.2    | Évolution de la distance au réseau . . . . . | 10        |
| 3.3      | Heuristique gaussienne . . . . .             | 10        |
| <b>4</b> | <b>Schéma de chiffrement</b>                 | <b>12</b> |
| 4.1      | Preuve de correction . . . . .               | 12        |
|          | <b>Références</b>                            | <b>14</b> |

# 1 Introduction

Les réseaux euclidiens sont une construction algébrique permettant entre autres de définir des problèmes mathématiques dont la résolution algorithmique est conjecturée difficile, même pour des ordinateurs quantiques. Cela les rend donc particulièrement intéressants pour construire des protocoles sûrs en cryptographie post-quantique.

Deux exemples fondamentaux de problèmes sur les réseaux sont le *Small Integer Solutions problem* (SIS) introduit par Ajtai en 1996 [Ajt96], et le *Learning With Errors problem* (LWE), découvert par Regev en 2005 [Reg05].

Le problème LWE est privilégié dans la construction de schémas de chiffrement car il est facile d'en tirer des constructions cryptographiques. D'autre part il été prouvé [Reg05] que résoudre une instance aléatoire de LWE est aussi dur que résoudre la pire instance d'un problème supposé dur. On dit que LWE bénéficie d'une réduction *pire-cas moyen-cas*.

Cependant, si l'on utilise la version standard de LWE pour construire des protocoles, ces derniers auront une efficacité moyenne à cause d'opérations faisant intervenir de grandes matrices aléatoires. La variante *Polynomial Learning With Errors* (PLWE), proposée par Stehlé *et al.* [SSTX09], résout ce problème en utilisant des réseaux structurés : les calculs matriciels correspondent alors à des produits de polynômes, calculables plus rapidement. Cependant, ce gain d'efficacité se fait potentiellement au détriment de garanties de sécurité : les polynômes sont manipulés dans  $\mathbb{Z}_p[X]/f$  et la complexité de la variante est directement liée au  $f$  choisi.

Afin de se débarrasser de cette dépendance, Roşca *et al.* introduisent le *Middle-Product Learning With Errors problem* (MP-LWE) [RSSS17] dont l'intérêt est d'être aussi dur que des classes exponentiellement grandes de problèmes PLWE (dont on espère qu'elles contiennent au moins une instance difficile), tout en conservant l'efficacité des réseaux structurés.

Durant mon stage, j'ai ainsi travaillé sur la variante MP-LWE du problème de Regev, et plus particulièrement sur les effets de la réduction de PLWE vers MP-LWE proposée par [RSSS17]. Pour cela, j'ai étudié l'évolution des différents paramètres régissant la difficulté de ces problèmes (par exemple le volume des réseaux sous-jacents), dans le cadre d'une certaine heuristique. J'ai ensuite prouvé qu'avec grande probabilité, une version faible de cette heuristique est vérifiée dans le cadre des réseaux étudiés.

La section 2 du rapport introduit les définitions utilisées, ainsi que le thème du stage. À partir de la sous-section 3.2, tous les théorèmes, résultats empiriques et code constituent ma contribution (sauf mention du contraire). De plus, en étudiant [RSSS17], j'ai remarqué qu'une partie de la preuve de correction du schéma de chiffrement proposé était fautive. Ainsi, j'en donne une autre version dans la partie 4, avec des hypothèses renforcées.

## 2 Préliminaires

**Définition 2.1** Un *réseau euclidien* de  $\mathbb{R}^m$  est l'ensemble des combinaisons à coefficients entiers de vecteurs linéairement indépendants  $b_1, \dots, b_n$ , que l'on note :

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

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  $B := [b_1, \dots, b_n]$  la matrice dont les colonnes sont formées par les  $(b_i)_{1 \leq i \leq n}$ , on considérera de manière équivalente :

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

**Définition 2.2 (Notations)**

- On note  $\mathbb{Z}_q$  (resp.  $\mathbb{R}_q$ ) le quotient  $\mathbb{Z}/q\mathbb{Z}$  (resp.  $\mathbb{R}/q\mathbb{Z}$ ), et  $\|\cdot\|$  désigne la norme euclidienne.
- Si  $E$  est un ensemble fini, on note  $\mathcal{U}(E)$  la distribution uniforme sur cet ensemble.
- Pour  $n \in \mathbb{N}$ , on note  $\mathbb{K}^{<n}[X]$  l'ensemble des polynômes de degré strictement plus petit que  $n$ , à coefficients dans  $\mathbb{K}$ .
- Pour  $\sigma \in \mathbb{R}^+$ , on note  $\mathcal{N}(\sigma)$  la distribution gaussienne centrée de variance  $\sigma^2$ , ainsi que  $\lfloor \mathcal{N}(\sigma) \rfloor$  cette distribution arrondie à l'entier le plus proche.
- Pour  $\mathcal{D}$  une distribution de probabilité sur  $\mathbb{K}$  et  $n \in \mathbb{N}$ , on note  $\mathcal{D}^n[X]$  la distribution de probabilité sur  $\mathbb{K}^n[X]$  où chaque coefficient suit la loi  $\mathcal{D}$ .
- Si  $f$  et  $g$  sont des polynômes, on note  $g \bmod f$  le reste dans la division euclidienne de  $g$  par  $f$ .
- Pour  $f \in \mathbb{Z}^m[X]$ , on définit  $EF(f) := \max_{\substack{g \in \mathbb{Z}^{2m-1}[X] \\ g \neq 0}} \left( \frac{\|g \bmod f\|_\infty}{\|g\|_\infty} \right)$  le *facteur d'expansion* de  $f$ .
- Si  $(A_i)_{i \leq t}$  est une famille de matrices, on désigne par  $[A_{i \leq t}]$  la matrice par blocs qui correspond à l'empilement vertical des  $(A_i)_{i \leq t}$ .
- Pour  $A$  et  $B$  des matrices, on désigne par  $[A|B]$  la matrice dont les colonnes sont celles de  $A$ , puis celles de  $B$ .

**2.1 Problème LWE et difficulté**

**Définition 2.3 (Distribution LWE)** Soient  $q \geq 2$ ,  $m \geq 1$ ,  $\chi$  une distribution de probabilité sur  $\mathbb{R}$ . À partir de  $s \in \mathbb{Z}_q^m$ , on définit  $\mathcal{D}_{q,\chi,m}(s)$  la distribution sur  $\mathbb{Z}_q^m \times \mathbb{R}_q$  obtenue en choisissant  $a \leftarrow \mathcal{U}(\mathbb{Z}_q^m)$ ,  $e \leftarrow \chi$ , et qui renvoie  $(a, b) := (a, \langle a, s \rangle + e \bmod q)$ .

**Définition 2.4 (Problèmes LWE)** Soient  $q \geq 2$ ,  $m \geq 1$ ,  $\chi$ . On tire  $s \leftarrow \mathcal{U}(\mathbb{Z}_q^m)$ , et muni de la distribution  $\mathcal{D}_{q,\chi,m}(s)$  précédente, on peut alors définir deux problèmes :

- **LWE-Décisionnel** consiste à distinguer un nombre arbitraire d'échantillons de  $\mathcal{D}_{q,\chi,m}(s)$  et le même nombre d'échantillons de  $\mathcal{U}(\mathbb{Z}_q^m) \times \mathcal{U}(\mathbb{R}_q)$ .
- **LWE-Calculatoire** consiste à retrouver le secret  $s$  à partir d'un nombre fixé d'échantillons indépendants.

En notant  $A$  la matrice dont les lignes sont formées des  $(a_i)_{i \leq t}$ ,  $e := (e_i)_{i \leq t}$  et  $b := (b_i)_{i \leq t}$  ( $t$  représente le nombre d'échantillons), on a :  $b = As + e \bmod q$ .

**Définition 2.5** Dans un réseau  $\Lambda$ , on note  $\lambda_i := \inf\{r, \dim(\text{Vect}(\Lambda \cap \mathcal{B}(0, r))) = i\}$  le  $i$ -ème minimum du réseau. En particulier, on a  $\lambda_1 = \inf\{\|v\|, v \in \mathcal{L}(B) \setminus \{0\}\}$  qui est le plus court vecteur non nul du réseau.

Rq :  $\lambda_i$  s'interprète comme le rayon de la plus petite boule centrée à l'origine qui contient  $i$  vecteurs indépendants du réseau.

Le calcul effectif de ces minimums semble très dur : les meilleurs algorithmes polynomiaux connus calculant  $\lambda_1$  ont un facteur d'approximation exponentiel.

**Définition 2.6** On appelle volume d'un réseau  $\mathcal{L} = \mathcal{L}(B)$  la quantité  $\sqrt{\det(B^\top B)}$ . Elle ne dépend pas de la base choisie.

Le théorème suivant fournit une borne sur  $\lambda_1$  :

**Théorème 2.1 (Minkowski)** Dans un réseau  $\mathcal{L}$  de dimension  $n$ ,  $\lambda_1 \leq \sqrt{n} \cdot \text{vol}(\mathcal{L})^{\frac{1}{n}}$

On peut alors considérer le problème algorithmique suivant, qui apparait lors de l'étude des réseaux reliés aux protocoles utilisant LWE :

**Définition 2.7 (BDD)** Soit  $B$  une base d'un réseau de dimension  $n$ , et  $\gamma \geq 2$ . Une instance du problème *Bounded Distance Decoding* est un vecteur  $t \in \mathbb{R}^m$  de la forme  $t = x + e$ , où  $x \in \mathcal{L}(B)$  et  $\|e\| \leq \lambda_1/\gamma$ . Le problème consiste à retrouver  $x$  (ou  $e$ ) à partir de  $t$ .

En revenant au problème LWE-Calculatoire, on constate que ce dernier se réduit à une instance de BDD dans le réseau engendré par les colonnes de  $A$  (de dimension  $t \times m$ ) et  $q\text{Id}_t$  où  $t$  est le nombre d'échantillons.

En effet,  $b = As + e \bmod q$ , donc avec  $x := b - e \bmod q$  et  $e$  choisi petit par rapport à  $\lambda_1$ ,  $b = x + e$  est bien une instance de BDD.

On travaille alors dans  $\mathcal{L} := \{y \in \mathbb{Z}^t \mid \exists x \in \mathbb{Z}^m, y = Ax \bmod q\}$ , et on va montrer que  $\mathcal{L} = \{y \in \mathbb{Z}^t \mid \exists x \in \mathbb{Z}^{m+t}, y = [A|q\text{Id}_t] \cdot x\}$

Pour  $y \in \mathcal{L}$ , il existe  $x \in \mathbb{Z}^m$  tel que  $y = Ax \bmod q$ . Alors en notant  $k \in \mathbb{Z}^t$  le vecteur tel que  $y = Ax + k \cdot q\text{Id}_t$  et  $x' \in \mathbb{Z}^{m+t}$  dont les  $m$  premières composantes sont celles de  $x$ , et les autres celles de  $k$ , on a  $y = [A|q\text{Id}_t] \cdot x'$  qui est bien dans le second réseau.

Réciproquement, pour  $y$  dans le second réseau, il existe  $x \in \mathbb{R}^{m+t}$  tel que  $y = [A|q\text{Id}_t] \cdot x$ . Alors en notant  $x' \in \mathbb{Z}^m$  le vecteur constitué des  $m$  première composantes de  $x$ , et  $x'' \in \mathbb{R}^t$  le reste, on a que  $y = Ax' + q\text{Id}_t x''$ , donc  $y = Ax' \bmod q$ .

**Conjecture 2.1** Dans un réseau de dimension  $n$ , pour  $\gamma$  polynomial en  $n$ , le problème BDD est conjecturé exponentiellement (en  $n$ ) dur à résoudre, même sur des ordinateurs quantiques.

## 2.2 Variantes structurées

On considère la variante polynomiale du problème LWE :

**Définition 2.8 (Distribution PLWE)** Soient  $q \geq 2$ ,  $m > 0$ ,  $f$  polynôme de degré  $m$ ,  $\chi$  une distribution sur  $\mathbb{R}_q[X]/f$ . À partir de  $s \in \mathbb{Z}_q[X]/f$ , on définit la distribution  $P_{q,\chi}^{(f)}(s)$  sur  $\mathbb{Z}_q[X]/f \times \mathbb{R}_q[X]/f$  obtenue en tirant  $a \leftarrow \mathcal{U}(\mathbb{Z}_q[X]/f)$ ,  $e \leftarrow \chi$  et qui renvoie  $(a, b = a \cdot s + e)$ .

Ensuite, on définit un nouveau produit sur les polynômes, qui consiste à garder les  $d$  coefficients du milieu dans un produit de degré  $d + 2k - 1$  :

**Définition 2.9 (Middle-Product)** Soient  $d_a, d_b, d, k \in \mathbb{N}$  tels que  $d_a + d_b - 1 = d + 2k$ . Alors le *middle-product*  $\odot_d : \mathbb{R}^{<d_a}[X] \times \mathbb{R}^{<d_b}[X] \rightarrow \mathbb{R}^{<d}[X]$  est la fonction :

$$(a, b) \mapsto a \odot_d b = \left\lfloor \frac{(a \cdot b) \bmod x^{k+d}}{x^k} \right\rfloor$$

Concrètement, cela consiste à garder les  $d$ -termes du milieu dans le produit usuel.

On construit alors une distribution plus générale utilisant le produit précédent :

**Définition 2.10 (Distribution MP-LWE)** Soient  $n, d > 0$ ,  $q \geq 2$  et  $\chi$  une distribution sur  $\mathbb{R}_q^{<d}[X]$ . Pour  $s \in \mathbb{Z}_q^{<n+d-1}[X]$ , on définit la distribution  $\text{MP}_{q,n,d,\chi}(s)$  sur  $\mathbb{Z}_q^{<n}[X] \times \mathbb{R}_q^{<d}[X]$  obtenu en tirant  $a \leftarrow \mathcal{U}(\mathbb{Z}_q^{<n}[X])$ ,  $e \leftarrow \chi$  et qui renvoie  $(a, b = a \odot_d s + e)$ .

Les problèmes décisionnels  $\text{PLWE}_{q,\chi}^{(f)}(s)$  et  $\text{MP-LWE}_{q,n,d,\chi}(s)$  associés peuvent se définir ensuite de manière parfaitement analogue au cas  $\text{LWE}$  classique.

**Théorème 2.2 (Théorème 3.6 [RSSS17])** Soient  $n, d > 0$ ,  $q \geq 2$ , et  $\alpha \in (0, 1)$ . Pour  $S > 0$ , on note  $\mathcal{F}(S, d, n)$  les polynômes de  $\mathbb{Z}[X]$  unitaires, dont le coefficient constant est inversible dans  $\mathbb{Z}_q$ , de degré  $m$  vérifiant  $d \leq m \leq n$ , et tels que  $\text{EF}(f) \leq S$ . Il existe une réduction *ppt* depuis  $\text{PLWE}_{q,\mathcal{N}(\alpha q)^{<d}[X]}^{(f)}$  décisionnel pour tout  $f \in \mathcal{F}(S, d, n)$  vers  $\text{MP-LWE}_{q,n,d,\mathcal{N}(\alpha' q)^{<d}[X]}$  décisionnel, où  $\alpha' = \alpha d S$ .

Il s'agit du résultat principal de [RSSS17]. Durant mon stage, j'ai étudié comment la réduction explicitée dans la preuve du théorème agit géométriquement sur les réseaux sous-jacents aux problèmes de manière à ne pas en diminuer la complexité.

### 3 Étude de la réduction

Afin de manipuler les réseaux sous-jacents à ces variantes, il est nécessaire de définir les objets suivants :

**Définition 3.1** Soient  $f, a \in \mathbb{R}_q[X]$  de degré  $m$  et  $n$ , et  $d \in \mathbb{N}$

- On note  $\text{Rot}_f^d(a) \in \mathbb{R}^{d \times m}$  la matrice dont la  $i$ -ème ligne est constituée des coefficients de  $a \cdot x^{i-1} \bmod f$ . On écrira  $\text{Rot}_f(a)$  pour  $\text{Rot}_f^m(a)$
- On note  $\text{Toep}^{d,n}(a) \in \mathbb{R}^{d \times (n+d-1)}$  la matrice dont la  $i$ -ème ligne est constituée des coefficients de  $a \cdot x^{i-1}$ .
- On note  $M_f^d \in \mathbb{R}^{d \times m}$  la matrice dont l'entrée  $(i, j)$  est le coefficient constant de  $x^{i+j-2} \bmod f$ . On écrira  $M_f$  pour  $M_f^m$ .

Dans la suite, on notera de manière identique un polynôme et le vecteur de ses coefficients. De plus, pour un vecteur  $a$ , on notera  $\bar{a}$  ce vecteur renversé.

**Lemme 3.1** Soient  $d, k > 0$ , et  $a \in \mathbb{R}^{<k+1}[X]$ ,  $b \in \mathbb{R}^{<k+d}[X]$  et  $f \in \mathbb{R}[X]$  de degré  $m$ , alors :

- (1)  $\text{Rot}_f^d(a) = \text{Toep}^{d,k+1}(a) \cdot \text{Rot}_f^{k+d}(1)$
- (2)  $a \odot_d b = \overline{\text{Toep}^{d,k+1}(a)} \cdot \bar{b}$
- (3)  $\text{Rot}_f(a \cdot b) = \text{Rot}_f(a) \cdot \text{Rot}_f(b)$
- (4) Si  $\deg(a) < m$ ,  $\text{Rot}_f(a) \cdot (1, 0, \dots, 0)^\top = M_f \cdot a$

Les preuves sont fournies dans [RSSS17].

#### 3.1 Principe de la réduction

Cette section a pour but d'expliquer les grandes lignes de la preuve de [RSSS17] afin de poser le contexte de l'étude menée dans les parties suivantes.

Soient  $q \geq 2$ ,  $\alpha \in (0, 1)$ ,  $f$  polynôme vérifiant les hypothèses du Théorème 2.1, dont on gardera les notations.

À partir de  $s \in \mathbb{Z}_q[X]/f$ , on se donne initialement un nombre  $t$  d'échantillons  $(a_i, b_i)_{i \leq t}$  de  $\text{P}_{q,\mathcal{N}(\alpha q)^{<d}[X]}^{(f)}(s)$ .

Le but est de construire  $t$  échantillons  $(a'_i, b'_i)_{i \leq t}$  de  $\text{MP}_{q,n,d,\mathcal{N}(\alpha' q)^{<d}[X]}(s)$ .

Dans un premier temps, on va "prolonger" les  $a_i$  dans un espace de polynômes de plus grand degré. Ensuite grâce au Lemme 3.1 on passera du produit usuel dans l'espace quotient au middle-product. Il

faudra alors re-randomiser le secret, et éliminer la dernière dépendance en  $f$  dans la distribution de la nouvelle erreur.

Tout d'abord, on tire  $(r_i)_{i \leq t} \leftarrow \mathcal{U}(\mathbb{Z}_q^{<n-m}[X])$ , et on définit  $a'_i := a_i + f \cdot r_i \in \mathbb{Z}_q^{<n}[X]$ . On a alors que, les  $a_i$  et  $r_i$  étant uniformes, les  $a'_i$  le sont aussi. Moralement, on rajoute la partie des  $a_i$  qui a été oubliée en passant au quotient. La preuve formelle consitue le Lemme 2.1 de [Lyu16]. Elle se fait par récurrence, en utilisant de manière cruciale que  $f$  est unitaire.

Ensuite, en utilisant le Lemme 3.1 et la définition des  $(b_i)_{i \leq t}$ , on a

$$\text{Rot}_f(b_i) = \text{Rot}_f(a_i) \cdot \text{Rot}_f(s) + \text{Rot}_f(e_i)$$

Ce qui donne, en conservant la première colonne (i.e en multipliant par  $(1, 0, \dots, 0)^\top$ ) et les  $d$  premières lignes :

$$\begin{aligned} M_f^d \cdot b_i &= \text{Rot}_f^d(a_i) \cdot M_f^d \cdot s + M_f^d \cdot e_i \\ &= \text{Rot}_f^d(a'_i) \cdot M_f^d \cdot s + M_f^d \cdot e_i \\ &= \text{Toep}^{d,n}(a'_i) \cdot \text{Rot}_f^{d+n-1}(1) \cdot M_f^d \cdot s + M_f^d \cdot e_i \\ \overline{b'_i} &= \text{Toep}^{d,n}(a'_i) \cdot \overline{s'} + \overline{e'_i} \end{aligned}$$

$$\text{où on a noté } \begin{cases} b'_i = \overline{M_f^d \cdot b_i} \\ s' = \overline{\text{Rot}_f^{d+n-1}(1) \cdot M_f^d \cdot s} \\ e'_i = \overline{M_f^d \cdot e_i} \end{cases}$$

Alors on a, toujours en utilisant le Lemme 3.1, que  $b'_i = a'_i \odot_d s' + e'_i$

On a de plus que, en notant  $J \in \mathbb{R}^{d \times d}$  la matrice qui a des 1 sur son anti-diagonale et des 0 ailleurs, la nouvelle distribution de l'erreur est  $J \cdot M_f^d \cdot \mathcal{N}(\alpha q)^{<d}[X]$ . Pour obtenir à nouveau une gaussienne, il suffit alors de majorer les valeurs singulières de la nouvelle distribution, et de choisir le majorant comme variance de la nouvelle gaussienne. Or dans notre cas, on a clairement  $\|J\| = 1$  et  $\|M_f\| \leq d\text{EF}(f) \leq dS$ , d'où  $\alpha' = \alpha dS$  convient, comme annoncé dans le Théorème 2.1.

Ensuite, on constate que le nouveau secret est encore fortement lié au secret de l'ancien réseau. Pour régler ce problème, on prend  $s'' \leftarrow \mathcal{U}(\mathbb{Z}_q^{n+d-1}[X])$  et en sortie, on ajoute à chaque  $(a'_i, b'_i)$  le couple  $(0, a'_i \odot_d s'')$ , de manière à re-randomiser le secret, i.e : le nouveau secret  $\tilde{s} = s' + s''$  est maintenant uniforme dans le nouveau réseau.

Finalement, comme on réduit d'une variante décisionnelle vers une autre, il faut vérifier que si les échantillons sont uniformes au départ, alors ils le sont encore à l'arrivée. Or, si  $b_i$  est uniformément distribué, alors  $b'_i$  l'est aussi car  $M_f$  est inversible modulo  $q$ . Cette dernière affirmation repose sur l'hypothèse que le coefficient constant  $f_0$  de  $f$  est inversible modulo  $q$  car :

$$M_f = \begin{bmatrix} 1 & 0 & \dots & 0 \\ 0 & 0 & \dots & -f_0 \\ \vdots & \vdots & \ddots & * \\ 0 & -f_0 & * & * \end{bmatrix}$$

### 3.2 Effets géométriques

À partir de maintenant, et pour toute la suite du rapport, les théorèmes et résultats empiriques présentés sont issus de mon stage (sauf mention du contraire). Ma contribution consiste à quantifier l'évolution des paramètres régissant la difficulté des instances BDD sous-jacentes aux variantes étudiées lors de la réduction de [RSSS17] précédemment détaillée.

Comme on a pu le voir dans la définition du problème BDD, la difficulté d'une instance  $x$  dans un réseau  $\mathcal{L}$  est d'une part exponentielle en la dimension du réseau, et d'autre part, elle est reliée au facteur  $\gamma$ , que l'on peut écrire  $\gamma = \frac{\lambda_1}{\text{dist}(x, \mathcal{L})}$ . Plus  $\gamma$  est petit, plus l'instance est difficile, et inversement.

**Remarque 3.1 (Heuristique gaussienne)** Dans un réseau aléatoire, l'heuristique gaussienne donne une estimation de  $\lambda_1$  :

$$\lambda_1 \simeq \sqrt{\frac{n}{2\pi e}} \text{vol}(\mathcal{L})^{\frac{1}{n}}$$

On admet pour l'instant que nos réseaux structurés suivent cette heuristique, et on étudiera la pertinence de cette hypothèse dans un second temps. Cela nous permet d'avoir une estimation de  $\lambda_1$ , et donc du facteur  $\gamma$  associé à l'instance  $x$  de BDD étudiée :  $\gamma \simeq \frac{\sqrt{n} \text{vol}(\mathcal{L})^{\frac{1}{n}}}{\text{dist}(x, \mathcal{L})}$ .

Ainsi, les deux caractéristiques des réseaux permettant d'estimer la complexité du problème BDD associé sont leur volume, et la distance au point choisi. Dans ce qui suit, on se propose donc d'étudier ces deux quantités dans le cadre de la réduction précédemment présentée.

#### 3.2.1 Évolution du volume

Afin d'étudier les effets de cette réduction, on remarque que 3 réseaux distincts apparaissent, et on se propose donc d'en étudier les propriétés :

- Le réseau initial  $\mathcal{L}_0 = \{y \in \mathbb{Z}^{tm} \mid \exists x \in \mathbb{Z}^m, y = [\text{Rot}_f(a_i)_{i \leq t}] \cdot x \bmod q\}$
- Le réseau intermédiaire  $\mathcal{L}_1 = \{y \in \mathbb{Z}^{td} \mid \exists x \in \mathbb{Z}^d, y = [\text{Rot}_f^d(a_i)_{i \leq t}] \cdot x \bmod q\}$  qui correspond au projeté en dimension  $dt$  du réseau initial  $\mathcal{L}_0$
- Le réseau final  $\mathcal{L}_2 = \{y \in \mathbb{Z}^{td} \mid \exists x \in \mathbb{Z}^{n+d-1}, y = [\text{Toep}^{d,n}(a'_i)_{i \leq t}] \cdot x \bmod q\}$

Comme démontré en préliminaires, on a que  $\mathcal{L}_0$  est engendré par les colonnes de la matrice  $[[\text{Rot}_f(a_i)_{i \leq t}] \mid q\text{Id}_t]$ . En particulier, son sous-espace vectoriel engendré est égal à l'espace entier (ou encore son rang est égal à la dimension ambiante), on dit que c'est un réseau de *rang plein*. De plus, ce réseau contient les  $(0, \dots, q, \dots, 0)^\top$ , dans ce cas il est dit *q-aire*.

**Lemme 3.2** Si  $a_1$  est inversible dans  $\mathbb{Z}_q[X]/f$ , alors  $\mathcal{L}_0$  est engendré par

$$\left[ \begin{array}{c|ccc} \text{Id}_m & 0 & \cdots & 0 \\ \text{Rot}_f(a_2) \cdot \text{Rot}_f(a_1)^{-1} & q & \cdots & 0 \\ \vdots & & \ddots & \vdots \\ \text{Rot}_f(a_t) \cdot \text{Rot}_f(a_1)^{-1} & 0 & \cdots & q \end{array} \right]$$

**Preuve :**

Pour alléger les notations, on pose  $A_i := \text{Rot}_f(a_i)$  et  $A := [\text{Rot}_f(a_i)_{i \leq t}]$ . Premièrement, si  $a_1$  est inversible modulo  $f$ , alors  $A_1$  est inversible. En effet, on a  $\text{Rot}_f(a_1) \cdot \text{Rot}_f(a_1^{-1}) = \text{Rot}_f(a_1 \cdot a_1^{-1}) =$

$\text{Rot}_f(1) = \text{Id}_m$ , d'où  $\text{Rot}_f(a_1)^{-1} = \text{Rot}_f(a_1^{-1})$ . On peut alors remarquer que :

Si  $y \in \mathcal{L}_0$ , alors il existe  $x$  tel que  $y = Ax \bmod q$ , donc en notant  $x' := \text{Rot}_f(a_1) \cdot x$ , on a  $y = A \cdot \text{Rot}_f(a_1)^{-1} \cdot x' \bmod q$ , d'où

$$\left[ \begin{array}{c} \text{Id}_m \\ \text{Rot}_f(a_2) \cdot \text{Rot}_f(a_1)^{-1} \\ \vdots \\ \text{Rot}_f(a_t) \cdot \text{Rot}_f(a_1)^{-1} \end{array} \right] \quad \left| \quad \begin{array}{c} q \cdot \text{Id} \end{array} \right]$$

engendrer  $\mathcal{L}_0$ . Alors, des combinaisons linéaires des colonnes du bloc de gauche permettent de retirer les  $m$  premières colonnes du bloc de droite (ces dernières étant engendrées par les autres colonnes de la matrice). Finalement, on a bien que les vecteurs voulus engendrent  $\mathcal{L}_0$ . □

**Théorème 3.1** Si l'un des  $a_i$  est inversible dans  $\mathbb{Z}_q[X]/f$ , alors  $\text{vol}(\mathcal{L}_0) = q^{m(t-1)}$

**Preuve :**

On commence par remarquer que quitte à permuter les  $a_i$ , la forme précédente est valable dès qu'au moins l'un d'entre eux est inversible modulo  $f$ . Il suffit alors de dire que les colonnes de la matrice constituée sont linéairement indépendantes pour obtenir une base du réseau. Or cette matrice est triangulaire inférieure à termes diagonaux non nuls, donc ses colonnes sont libres, et de plus son déterminant vaut le produit des termes diagonaux, ce qui achève la preuve. □

On aimerait pouvoir utiliser la même preuve dans le cas des réseaux  $\mathcal{L}_1$  et  $\mathcal{L}_2$ , cependant cela n'est pas possible car les matrices composant le bloc de gauche sont rectangulaires, donc n'admettent pas d'inverse. On peut cependant justifier que cette colonne est de rang plein, ce qui permettra d'obtenir un résultat sur le volume analogue à celui qui précède.

**Théorème 3.2** Supposons  $q$  premier, alors :

- Avec une probabilité  $\geq 1 - (\frac{m}{q})^{\lfloor t/\lceil \frac{m}{d} \rceil \rfloor}$ , on a que  $\text{vol}(\mathcal{L}_1) = q^{td-m}$ .
- Avec une probabilité  $\geq 1 - (\frac{n+d-1}{q})^{\lfloor t/\lceil \frac{n+d-1}{d} \rceil \rfloor}$ , on a que  $\text{vol}(\mathcal{L}_2) = q^{td-(n+d-1)}$ .

Si on utilise les ordres de grandeurs proposés dans le schéma de chiffrement de [RSSS17], on a :

$$\mathbb{P}(\text{vol}(\mathcal{L}_2) = q^{td-(n+d-1)}) \geq 1 - \left( \frac{1}{n^{\frac{3}{2}} \sqrt{\log n}} \right)^{\log n}$$

**Preuve :** Les deux cas étant analogues, on se contente de la preuve pour  $\mathcal{L}_2$ . Il suffit de montrer qu'avec bonne probabilité,  $A := [\text{Toep}^{d,n}(a'_i)_{i \leq t}]$  est de rang plein.

On commence par rappeler de lemme de Schwartz-Zippel : pour un polynôme multivarié non nul de degré  $n$ , à coefficients dans  $\mathbb{Z}/p\mathbb{Z}$  où  $p$  est premier, la probabilité d'annuler ce polynôme en choisissant les variables uniformément est au plus  $\frac{n}{p}$ .

On considère donc la matrice carrée constituée des  $n+d-1$  premières lignes de  $A$ , que l'on note  $A_1$ . Le déterminant de cette sous-matrice est un polynôme à plusieurs variables, de degré  $n+d-1$ , dont les variables sont choisies uniformément dans  $\mathbb{Z}_q$ . Ce polynôme est non nul, par exemple on peut choisir



$a_{\lceil \frac{n+d-1}{d} \rceil} = 1$ ,  $a_1 = x^d$ ,  $a_2 = x^{2d}$ , ... et alors  $A_1$  est une matrice de permutation, donc  $\det(A_1) = 1 \neq 0$ . Alors, d'après le lemme,  $q$  étant premier, on a que :

$$\mathbb{P}[\det(A_1) = 0] \leq \frac{n+d-1}{q}$$

On peut ensuite répéter ce processus pour les sous-matrices suivantes. Cependant, afin de conserver l'indépendance, il faut faire attention à ne pas reprendre une Toeplitz déjà utilisée. Ainsi,  $A_k$  sera la sous matrice carré commençant à la  $(k-1)d\lceil \frac{n+d-1}{d} \rceil$ -ème ligne. Au total, on pourra donc avoir au moins  $\lfloor t/\lceil \frac{n+d-1}{d} \rceil \rfloor$  sous matrices carrés dont les entrées sont mutuellement indépendantes. Alors :

$$\begin{aligned} \mathbb{P}(\text{rg}(A) < n+d-1) &\leq \mathbb{P}\left(\bigcap_{k \leq \lfloor t/\lceil \frac{n+d-1}{d} \rceil \rfloor} \det A_k = 0\right) \\ &= \mathbb{P}[\det(A_1) = 0]^{\lfloor t/\lceil \frac{n+d-1}{d} \rceil \rfloor} \\ &= \left(\frac{n+d-1}{q}\right)^{\lfloor t/\lceil \frac{n+d-1}{d} \rceil \rfloor} \end{aligned}$$

Ce qui donne bien l'inégalité voulue. On peut alors procéder aux mêmes inversions et opérations sur les colonnes que dans le cas de  $\mathcal{L}_0$ , pour obtenir de manière analogue la valeur du volume.  $\square$

On précise que cette borne est loin d'être optimale. En effet, les résultats expérimentaux laissent penser que la probabilité d'être de rang plein pour nos matrices structurées est en fait la même que pour des matrices où les coefficients sont choisis uniformément (dans ce cas on a une formule exacte).

Dénombrons les matrices de rang plein de taille  $m \times n$  (dans notre cas on aurait  $n+d-1$  colonnes et  $dt$  lignes) à coefficients dans  $\mathbb{Z}/p\mathbb{Z}$  où  $p$  est premier. On suppose sans perte de généralité que  $m \geq n$ , alors : la première colonne doit être non nulle, il y a donc  $p^m - 1$  choix, la seconde ne doit pas être dans l'espace engendré par la première, il y a donc  $p^m - p$  choix, etc ... Finalement, on a  $\prod_{0 \leq i < n} (p^m - p^i)$

matrices de rang plein. La probabilité d'en obtenir une en choisissant uniformément les coefficients vaut donc :  $\frac{1}{p^{mn}} \prod_{0 \leq i < n} (p^m - p^i) = \prod_{0 \leq i < n} (1 - \frac{1}{p^{m-i}})$ .

Pour les calculs expérimentaux, j'ai utilisé les ordres de grandeur proposés dans [RSSS17], i.e :  $t \simeq \log(n)$ ,  $d = \frac{n}{2}$ , et  $n = 22$ , ce qui donne  $d = 11, t = 3$ . En pratique,  $n$  serait pris beaucoup plus grand. J'ai de plus diminué  $p$ , qui sera pris premier, de l'ordre de  $n^\beta \log n$  où on fait varier  $\beta$ , afin d'avoir un nombre significatif de matrices de rang non plein (dans le schéma,  $\beta = 2.5$ ). En faisant  $10^6$  tests, on obtient alors les résultats suivants :

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

Le code utilisé pour produire ces résultats est disponible ici, au tag “rapport”.

Pour conclure cette partie, on observe que  $\text{vol}(\mathcal{L}_0)^{1/tm} = q^{1-\frac{1}{t}} > q^{1-\frac{1}{t}-\frac{n}{t}} = \text{vol}(\mathcal{L}_2)^{1/dt}$ . Ainsi, la réduction diminue le volume normalisé du réseau initial d'un facteur  $q^{n/t}$ , ce qui a pour effet d'augmenter la complexité des instances de BDD sous-jacentes.

### 3.2.2 Évolution de la distance au réseau

Dans le cas de LWE, la distance au réseau de l'instance de BDD est exactement égale à la norme du vecteur d'erreur  $e$ . On note  $e_0$  (resp.  $e_1$ ) (resp.  $e_2$ ) la variable aléatoire qui représente le vecteur d'erreur tiré dans  $\mathcal{L}_0$  (resp.  $\mathcal{L}_1$ ) (resp.  $\mathcal{L}_2$ ). Le vecteur  $e_0$  est l'erreur initiale de PLWE,  $e_1$  est la projection de  $e_0$  en dimension  $dt$ , et  $e_2$  est le vecteur d'erreur final dans la réduction, i.e après re-randomisation pour suivre une gaussienne de paramètre  $\sigma' = \alpha'q$ .

#### Théorème 3.3 (Erreur moyenne)

- $\mathbb{E}(\|e_0\|^2) = tm(\alpha q)^2$
- $\mathbb{E}(\|e_1\|^2) = td(\alpha q)^2$
- $\mathbb{E}(\|e_2\|^2) = td(\alpha d S q)^2$

#### Preuve :

On utilise la norme euclidienne, donc le carré de la norme d'un vecteur est égal à la somme des carrés de ses composantes. De plus le moment d'ordre deux d'une gaussienne centrée est égal à sa variance  $\sigma^2$ , ce qui donne les résultats voulus par linéarité de l'espérance.  $\square$

Comme dans la partie précédente, on constate que la réduction augmente la difficulté de BDD, car elle augmente la distance moyenne, et réduit donc le facteur  $\gamma$ .

### 3.3 Heuristique gaussienne

On va maintenant tenter de montrer la validité de l'utilisation de l'heuristique gaussienne dans notre cas. La borne de Minkowski fournissant une borne supérieure sur  $\lambda_1$ , il suffit d'obtenir une borne inférieure qui soit du même ordre. Ici, on obtiendra une borne plus faible, d'un facteur  $1/q$ .

On rappelle la notation  $A = [\text{Toep}^{d,n}(a_i)_{i \leq t}]$ , où les  $(a_i)_{i \leq t}$  sont des variables aléatoires.

Le théorème suivant fournit une borne sur  $\lambda_1^\infty$ , i.e le plus court vecteur non nul du réseau pour la norme infinie (on utilisait jusqu'ici la norme euclidienne). Comme on sait que  $\lambda_1 \geq \lambda_1^\infty$ , cela fournit aussi une borne dans le cas de la norme 2, mais on perd potentiellement un facteur  $\sqrt{n}$  car on s'attend généralement à avoir  $\lambda_1 \simeq \sqrt{n} \lambda_1^\infty$ .

**Théorème 3.4** Si  $q$  est premier,  $d = \frac{n}{2}$  et  $t \geq 4$  alors, avec probabilité  $\geq 1 - \frac{1}{2^{td-1}q^{t-3}}$  sur  $A$ , on a

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

#### Preuve :

Soit  $B > 0$  :

$$\begin{aligned} \mathbb{P}_A(\lambda_1^\infty(\mathcal{L}_2) \leq B) &= \mathbb{P}_A\left(\bigcup_{y \in \mathbb{Z}^{dt}} \{0 < \|y\|_\infty \leq B \wedge y \in \mathcal{L}_2\}\right) \\ &\leq \sum_{\substack{y \in \mathbb{Z}^{dt} \\ 0 < \|y\|_\infty \leq B}} \mathbb{P}_A(y \in \mathcal{L}_2) \end{aligned}$$

$$\mathbb{P}_A(\lambda_1^\infty(\mathcal{L}_2) \leq B) \leq \sum_{x \in \mathbb{Z}_q^{n+d-1}} \sum_{\substack{y \in \mathbb{Z}^{dt} \\ 0 < \|y\|_\infty \leq B}} \mathbb{P}_A(y = A \cdot x)$$

Alors, pour  $y \in \mathbb{Z}^{dt}$  et  $1 \leq i \leq t$ , en notant  $y_i$  le vecteur constitué des coordonnées  $(i-1)d+1$  à  $id$  de  $y$ , on a :

$$\mathbb{P}_A(\lambda_1^\infty(\mathcal{L}_2) \leq B) \leq \sum_{x \in \mathbb{Z}_q^{n+d-1}} \sum_{\substack{y \in \mathbb{Z}^{dt} \\ 0 < \|y\|_\infty \leq B}} \prod_{i=1}^t \mathbb{P}_{a_i}(y_i = \text{Toep}^{d,n}(a_i) \cdot x)$$

Car les  $(a_i)_{i \leq t}$  sont mutuellement indépendants. Ensuite, on observe que, pour  $a \in \mathbb{Z}^{<n}[X]$  et  $x \in \mathbb{Z}_q^{n+d-1}$ , on a :

$$\text{Toep}^{d,n}(a) \cdot x = \begin{pmatrix} a_0 & \cdots & a_{n-1} & 0 & \cdots & 0 \\ 0 & a_0 & \cdots & a_{n-1} & 0 & \vdots \\ \vdots & 0 & \ddots & & \ddots & 0 \\ 0 & \cdots & 0 & a_0 & \cdots & a_{n-1} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_{n+d-1} \end{pmatrix} = \begin{pmatrix} x_1 & x_2 & \cdots & x_n \\ x_2 & x_3 & \cdots & x_{n+1} \\ \vdots & \cdots & \cdots & \vdots \\ x_d & \cdots & \cdots & x_{n+d-1} \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_{n-1} \end{pmatrix}$$

En notant  $\text{Ps}(x)$  la matrice de dimensions  $d \times n$  du membre de droite, on remarque que cette dernière est constante sur ses antidiagonales, i.e :  $i+j = r+s \Rightarrow \text{Ps}(x)_{i,j} = \text{Ps}(x)_{r,s}$ . Elle est dite *persymétrique*. En injectant cette égalité dans le calcul, on obtient :

$$\mathbb{P}_A(\lambda_1^\infty(\mathcal{L}_2) \leq B) \leq \sum_{x \in \mathbb{Z}_q^{n+d-1}} \sum_{\substack{y \in \mathbb{Z}^{dt} \\ 0 < \|y\|_\infty \leq B}} \prod_{i=1}^t \mathbb{P}_{a_i}(y_i = \text{Ps}(x) \cdot a_i)$$

Alors,  $a_i$  étant uniforme, on a :

$$\mathbb{P}_{a_i}(y_i = \text{Ps}(x) \cdot a_i) \leq \frac{q^{\dim(\ker \text{Ps}(x))}}{q^n} = \frac{1}{q^{\text{rg}(\text{Ps}(x))}}$$

Ainsi, en distinguant les  $x \in \mathbb{Z}_q^{n+d-1}$  suivant le rang de  $\text{Ps}(x)$ , on a :

$$\begin{aligned} \mathbb{P}_A(\lambda_1^\infty(\mathcal{L}_2) \leq B) &\leq \sum_{r=1}^d \sum_{\substack{x \in \mathbb{Z}_q^{n+d-1} \\ \text{rg}(\text{Ps}(x))=r}} \sum_{\substack{y \in \mathbb{Z}^{dt} \\ 0 < \|y\|_\infty \leq B}} \frac{1}{q^{rt}} \\ &\leq \sum_{r=1}^d \sum_{\substack{x \in \mathbb{Z}_q^{n+d-1} \\ \text{rg}(\text{Ps}(x))=r}} \frac{(2B+1)^{dt}}{q^{rt}} \end{aligned}$$

La somme sur  $r$  commence à 1, car si le rang de  $\text{Ps}(x)$  est nul, alors  $y$  l'est aussi, or on ne considère que des vecteurs non nuls.

Il faut maintenant dénombrer les  $x \in \mathbb{Z}_q^{n+d-1}$  tels que  $\text{rg}(\text{Ps}(x)) = r$ . Pour cela, on utilise un résultat

de Daykin [Day60] : pour  $p$  premier, le nombre de matrices persymétriques de dimensions  $m \times n$ , à

$$\text{coefficients dans } \mathbb{Z}/p\mathbb{Z} \text{ et de rang } r \text{ vaut : } \begin{cases} 1 & \text{si } r = 0 \\ p^{2(r-1)}(p^2 - 1) & \text{si } 1 \leq r < \min(m, n) \\ p^{2(r-1)}(p^{|m-n|+1} - 1) & \text{si } r = \min(m, n) \\ 0 & \text{sinon} \end{cases}$$

Dans notre cas, les dimensions sont  $d$  et  $n$ , et avec les valeurs utilisées dans [RSSS17], on a  $d = \frac{n}{2}$ . En particulier,  $2(d-1) + n - d + 1 \leq 3d$ . On majore donc, pour  $r$  quelconque, le cardinal de l'ensemble de ces matrices de rang  $r$  par  $q^{3r}$ . Alors :

$$\mathbb{P}_A(\lambda_1^\infty(\mathcal{L}_2) \leq B) \leq \sum_{r=1}^d q^{3r} \frac{(2B+1)^{dt}}{q^{rt}} = \frac{(2B+1)^{dt}}{q^{t-3}} \frac{1 - q^{d(3-t)}}{1 - q^{3-t}} \leq (2B+1)^{dt} \frac{1}{q^{t-3} - 1} \leq \frac{2(2B+1)^{dt}}{q^{t-3}}$$

En choisissant  $B = \frac{1}{4q} \text{vol}(\mathcal{L}_2)^{\frac{1}{td}} - \frac{1}{2}$ , on obtient finalement :

$$\mathbb{P}_A(\lambda_1^\infty(\mathcal{L}_2) \leq \frac{1}{4q} \text{vol}(\mathcal{L}_2)^{\frac{1}{td}} - \frac{1}{2}) \leq \frac{2}{q^{t-3}} \frac{\text{vol}(\mathcal{L}_2)}{(2q)^{td}} \leq \frac{2}{q^{t-3}} \frac{q^{td}}{(2q)^{td}} \leq \frac{1}{2^{td-1} q^{t-3}}$$

□

Cette preuve est inspirée de celle de Stehlé *et al.* [SS13] dans le cas PLWE pour des polynômes cyclotomiques. J'ai de même codé des simulations numériques pour observer ce résultat, elles sont disponibles ici.

## 4 Schéma de chiffrement

### 4.1 Preuve de correction

On rappelle le théorème de [RSSS17] :

#### **Théorème 4.1 (Lemme 4.1 [RSSS17])**

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  $(\text{sk}, \text{pk}) \leftarrow \text{KeyGen}$ , on a  $\text{Decrypt}(\text{sk}, \text{Encrypt}(\text{pk}, \mu)) = \mu$

Au cours de la preuve, une majoration incorrecte est utilisée, et on se propose donc d'en donner une autre version, avec des hypothèses renforcées.

**Théorème 4.2** 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  $(\text{sk}, \text{pk}) \leftarrow \text{KeyGen}$ , on a  $\text{Decrypt}(\text{sk}, \text{Encrypt}(\text{pk}, \mu)) = \mu$

Rq : La modification est essentiellement au niveau de  $\alpha$ , 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.

#### **Preuve :**

On se contente de reprendre la seconde moitié de la preuve, là où survient l'erreur, et on rappelle donc le contexte :

$s \leftarrow \mathcal{U}(\mathbb{Z}^{<n+d+k-1}[X])$ , pour  $i \leq t$  on a  $a_i \leftarrow \mathcal{U}(\mathbb{Z}^{<n}[X])$ ;  $e_i \leftarrow [\mathcal{N}(\alpha q)] [X]^{<k+d}$  et finalement  $r_i \leftarrow \mathcal{U}(\{0, 1\}^{<k+1}[X])$ . On note  $e_i(j)$  le  $j$ -ème coefficient de  $e_i$ . Le but est d'avoir avec bonne probabilité que :

$$\|\mu + 2 \sum_{i \leq t} r_i \odot_d e_i\|_\infty < q/2$$

où  $\mu \in \{0, 1\}^{<d}[X]$  est le message à chiffrer.

On commence par donner une borne classique sur la distribution gaussienne :

$$\begin{aligned} \mathbb{P}_{X \leftarrow \mathcal{N}(\sigma)}(|X| \geq M) &= \frac{2}{\sigma\sqrt{2\pi}} \int_M^\infty e^{-\frac{t^2}{2\sigma^2}} dt \\ &\leq \frac{2}{\sigma\sqrt{2\pi}} \int_M^\infty \frac{t}{M} e^{-\frac{t^2}{2\sigma^2}} dt \\ &\leq \frac{2\sigma}{M\sqrt{2\pi}} [-e^{-\frac{t^2}{2\sigma^2}}]_M^\infty \\ &\leq \frac{2\sigma}{M\sqrt{2\pi}} e^{-\frac{M^2}{2\sigma^2}} \end{aligned}$$

De plus, si on note  $E := \max_{i,j} |e_i(j)|$ , on a que :

$$\begin{aligned} |(r_i \odot_d e_i)(l)| &= |(r_i \times e_i)(l+k)| \\ &= \left| \sum_{j=0}^{k+l} r_i(j) e_i(k+l-j) \right| \\ &\leq (k+1)E \end{aligned}$$

Car les  $r_i$  étants de degré au plus  $k$ , il y a au plus  $k+1$  termes non nuls dans la somme.

Donc  $|(\sum_{i \leq t} r_i \odot_d e_i)(l)| \leq t(k+1)E$ .

Alors, on obtient que :

$$\begin{aligned} \mathbb{P}(\|\mu + 2 \sum_{i \leq t} r_i \odot_d e_i\|_\infty \geq q/2) &\leq \mathbb{P}(1 + 2E \geq \frac{q}{2t(k+1)}) \\ &\leq \mathbb{P}(\bigcup_{i,j} \{|e_i(j)| \geq \frac{q}{4t(k+1)} - \frac{1}{2}\}) \\ &\leq (k+d)t \mathbb{P}_{X \leftarrow \mathcal{N}(\alpha q)}(|X| \geq \frac{q}{4t(k+1)} - 1) \\ &\leq \frac{8t^2(k+1)(k+d)\alpha q}{q - 6t(k+1)} e^{-\frac{1}{2(\alpha q)^2} (\frac{q}{4t(k+1)} - 1)^2} \end{aligned}$$

En appliquant les hypothèses sur les paramètres de sécurité, on obtient l'inégalité suivante sur l'exposant :

$$\frac{1}{2(\alpha q)^2} \left( \frac{q}{4t(k+1)} - 1 \right)^2 \geq \frac{16^2 \lambda t^2 (k+1)^2}{2q^2} \left( \frac{q}{4t(k+1)} - 1 \right)^2 \geq \frac{\lambda}{2} \left( 4 - \frac{16t(k+1)}{q} \right)^2 \geq 2\lambda$$

On majore de même le facteur pré-exponentiel :

$$\frac{8t^2(k+1)(k+d)\alpha q}{q - 6t(k+1)} \leq \frac{8t^2(k+1)(k+d)\alpha q}{2t(k+1)} \leq 4t(k+d)q \frac{1}{16(k+1)t\sqrt{\lambda}} \leq \frac{(k+d)q}{4(k+1)\sqrt{\lambda}} \leq \frac{qd}{4\sqrt{\lambda}}$$

Finalement on obtient la borne voulue :

$$\begin{aligned}
 \mathbb{P}(\|\mu + 2 \sum_{i \leq t} r_i \odot_d e_i\|_\infty \geq q/2) &\leq \frac{qd}{4\sqrt{\lambda}} e^{-2\lambda} \\
 &\leq e^{-\lambda - \log(4\sqrt{\lambda})} \\
 &\leq 2^{-\Omega(\lambda)}
 \end{aligned}$$

□

## Références

- [Day60] David DAYKIN. “Distribution of Bordered Persymmetric Matrices in a Finite Field”. In : *Journal für die reine und angewandte Mathematik* 203 (1960), p. 47-54.
- [Ajt96] Miklós AJTAI. “Generating hard instances of lattice problems”. In : *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing* (1996).
- [Reg05] Oded REGEV. “On lattices, learning with errors, random linear codes, and cryptography”. In : *Journal of the ACM* 56 (2005), p. 1-40.
- [SSTX09] Damien STEHLÉ, Ron STEINFELD, Keisuke TANAKA et Keita XAGAWA. “Efficient public key encryption based on ideal lattices”. In : *International Conference on the Theory and Application of Cryptology and Information Security* (2009), p. 617-635.
- [SS13] Damien STEHLÉ et Ron STEINFELD. “Making NTRUEncrypt and NTRUSign as Secure as Standard Worst-Case Problems over Ideal Lattices”. In : (2013).
- [Lyu16] Vadim LYUBASHEVSKY. “Digital signatures based on the hardness of ideal lattice problems in all rings”. In : *International Conference on the Theory and Application of Cryptology and Information Security* (2016), p. 196-214.
- [RSSS17] Miruna ROȘCA, Amin SAKZAD, Damien STEHLÉ et Ron STEINFELD. “Middle-Product Learning With Errors”. In : *Annual International Cryptology Conference* (2017), p. 283-297.