Université Paris 8 Année 2021–2022

M1 Mathématiques et applications, parcours ACC et CSSD

Cryptographie à clef publique – Feuille de TD 8

01/04/2022

Le corrigé de certains exercices sera disponible à l'adresse suivante :

`www.math.univ-paris13.fr/~lavauzelle/teaching/2021-22/clef-publique.html`

$(\star)$ exercice fondamental $(\star\star)$ pour s'entraîner $(\star\star\star)$ pour aller plus loin 💻 sur machine

---

Exercice 1. $(\star)$ Anneaux dans NTRU.

Soit $N \geq 1$ un entier. On note $\mathcal{R} = \mathbb{Z}[X]/(X^N - 1)$.

On définit

$$\begin{array}{rccc} \phi : & \mathcal{R} & \to & \mathbb{Z}^N \\ & A(X) = \sum_{i=0}^{N-1} a_i X^i & \mapsto & \boldsymbol{a} = (a_0, \ldots, a_{N-1}) \end{array}$$

et l'opération $\star : (\mathbb{Z}^N)^2 \to \mathbb{Z}^N$ comme $\boldsymbol{a} \star \boldsymbol{b} = \boldsymbol{c}$ où pour tout $i \in \{0, \ldots, N-1\}$

$$c_i = \sum_{j+k \equiv i \mod N} a_j b_k \,.$$

Question 1.– Démontrer que ϕ est un isomorphisme entre les anneaux $(\mathcal{R}, +, \cdot)$ et $(\mathbb{Z}^N, +, \star)$.

À un élément $\boldsymbol{a} \in \mathbb{Z}^N$, on associe également une matrice carrée de taille $N \times N$ sur $\mathbb{Z}$ de la manière suivante :

$$\boldsymbol{M}(\boldsymbol{a}) = \begin{pmatrix} a_0 & a_1 & & & a_{N-1} \\ a_{N-1} & a_0 & a_1 & & a_{N-2} \\ & & \ddots & & \\ a_1 & a_2 & & a_{N-1} & a_0 \end{pmatrix} .$$

On note $\mathcal{M}_N$ l'ensemble des matrices de cette forme.

Question 2.– Démontrer que $\boldsymbol{M} : \mathbb{Z}^N \to \mathcal{M}_N$ est également un isomorphisme d'anneaux.

Question 3.– Vérifier que $\boldsymbol{a}\,\boldsymbol{M}(\boldsymbol{b}) = \boldsymbol{a} \star \boldsymbol{b}$ pour tous $\boldsymbol{a}, \boldsymbol{b} \in \mathbb{Z}^N$ (écrits comme des vecteurs lignes).

Question 4.– En déduire deux méthodes pour déterminer si $\boldsymbol{a} \in \mathbb{Z}^N$ est inversible dans $(\mathbb{Z}^N, +, \star)$, et le cas échéant calculer son inverse. On donnera la complexité de ces méthodes en nombre d'opérations entières, en fonction de N.

Exercice 2. $(\star)$ Chiffrement NTRU sur un petit exemple.

On considère le cryptosystème NTRU comme présenté en cours. On pose $q = 31$, $p = 3$ et $N = 5$. Si les calculs sont jugés trop difficiles, on n'hésitera pas à s'aider d'un logiciel de calcul formel.

Question 1.– On considère l'algorithme de génération de clefs. Supposons que les polynômes $U(X) = X^4 + X^3 + X^2 + X$ et $V(X) = X^3 - X^2 + X + 1$ ont été tirés.

1. Calculer les polynômes F et G.
2. Le polynôme F est–il inversible dans $\mathcal{R}$? si oui, l'inverser.
3. En déduire la clé publique et la clé privée.

Question 2.– On considère l'algorithme de chiffrement. Chiffrer le message $(-1, 1, 0, 0, 0)$ avec la clé publique obtenue à la question précédente. On considèrera que le vecteur $\boldsymbol{r}$ tiré aléatoirement est $(-1, -1, -1, -1, 1)$.

Question 3.– On considère l'algorithme de déchiffrement. Déchiffrer le chiffré $7X^4 - 5X^3 + 13X^2 + X - 5$ à l'aide de la clé privée $F(X) = 3X^3 + 3X^2 - 2$.

Exercice 3. $(\star\star)$ Grandeurs pour le chiffrement NTRU.

On considère le cryptosystème NTRU, avec les paramètres N, p et q comme présentés en cours.

Question 1.–

1. Donner, en fonction de p et N, une majoration du nombre de choix possibles pour le polynôme $U(X)$.
2. En déduire une borne supérieure sur le nombre de clés privées. Puis, en fixant $p = 3$, déduire la valeur minimale de N afin d'obtenir une sécurité de 128 bits face à une attaque par recherche exhaustive.

Question 2.– Soit $\boldsymbol{u} \in \mathbb{Z}_q^N$, où les coefficients sont écrits dans $\{-\frac{q-1}{2}, \dots, \frac{q-1}{2}\}$.

1. Quelle est la valeur maximale de $\|\boldsymbol{u}\|_2$?
2. Si $\boldsymbol{u} \in \mathbb{Z}_q^N$ est uniforme, que vaut typiquement $\mathbb{E}(\|\boldsymbol{u}\|_2)$?

Question 3.– Soit $\boldsymbol{f}, \boldsymbol{h} \in \mathbb{Z}_q^N$ les vecteurs associés à $F(X)$ et $H(X)$ dans la génération des clefs.

1. Calculer une borne supérieure sur $\|\boldsymbol{f}\|_2$ en fonction de p et N.
2. Peut-on majorer $\|\boldsymbol{h}\|_2$ de manière similaire ?

Question 4.– Soit $\boldsymbol{r}, \boldsymbol{g} \in \mathbb{Z}_q^N$ les vecteurs associés à $R(X)$ et $G(X)$ dans le chiffrement et la génération des clefs.

1. En considérant que $\boldsymbol{r}$ et $\boldsymbol{g}$ ont chacun $N/3$ coordonnées nulles, et qu'ils sont formés d'éléments de $\{-\frac{p-1}{2}, \dots, \frac{p-1}{2}\}$, quelle est la valeur maximale peut atteindre un coefficient de $\boldsymbol{r} \star \boldsymbol{g}$?
2. Comparer avec la valeur de $q/2$ pour les choix $N = 401$, $q = 2048$ et $p = 3$.
3. Conclure sur la validité du chiffrement NTRU dans ce cas.