Université Paris 8 Année 2021–2022

M1 Mathématiques et applications, parcours ACC et CSSD

Cryptographie à clef publique – Devoir semaine 9

devoir du 08/04/2022
à rendre jusqu'au 22/04/2022

Exercice 1. Implantation du chiffrement NTRU.

Le but de cet exercice est d'implanter une version simple du système de chiffrement NTRU.

Pour cela, vous aurez besoin de manipuler des polynômes à coefficients dans $\mathbb{Z}_q := \mathbb{Z}/q\mathbb{Z}$. Comme il est assez long de programmer les opérations sur ces polynômes (mais c'est un bon exercice), deux solutions s'offrent à vous :

1. utiliser un logiciel de calcul formel, je vous conseille `sagemath` ou `magma`
2. utiliser le script `python` que je vous fournis ci-dessous :

   `https://www.math.univ-paris13.fr/~lavauzelle/teaching/2021-22/docs/CP/devoirs/DP/poly.py`

   Ce script ne se veut pas être une bibliothèque à part entière, mais il est suffisant pour programmer les fonctions de cet exercice.

   Pour importer le script, faire la commande suivante en début de fichier python :
   `from poly import *`

Décrivons le système de chiffrement NTRU. Pour cela, on considère $N \geq 2$ un entier, et p et q deux nombres premiers entre eux tels que $3 \leq p \ll q$. Pour simplifier, on supposera que p et q sont des nombres premiers.

On note $S_p = \{-\frac{p-1}{2}, -\frac{p-1}{2}+1 \ldots, \frac{p-1}{2}\}$ et $S_q = \{-\frac{q-1}{2}, -\frac{q-1}{2}+1 \ldots, \frac{q-1}{2}\}$. Lorsqu'on effectue une réduction modulo p, on suppose que les entiers sont alors écrits dans S_p.

Question 1.– Implanter une fonction `reduce(x, p)` qui prend en entrée un entier naturel x et un entier $p \geq 3$, et qui retourne la réduction de x modulo p écrite dans S_p.

Les algorithmes de génération de clefs publique/privée, de chiffrement et de déchiffrement sont donnés en dernière page du sujet.

Question 2.– Implanter `keygen(N, p, q)`, la fonction de génération des clefs NTRU.

Question 3.– Implanter `encrypt(M, H, N, p, q)`, la fonction de chiffrement NTRU, où M est le message à chiffrer et H est le polynôme définissant la clef publique.

Question 4.– Implanter `decrypt(Y, F, N, p, q)`, la fonction de déchiffrement NTRU, où Y est le chiffré et F est le polynôme définissant la clef privée.

Question 5.– Écrire un script de test qui vérifie que vos fonctions sont correctement implantées. Pour les valeurs de N, p et q, on prendra $N = 7$, $p = 3$ et $q = 101$ par exemple.

Le chiffrement NTRU étant probabiliste, il est parfois possible que le déchiffrement échoue et ne retourne pas le message initialement chiffré. On souhaite estimer cet probabilité d'échec en fonction des paramètres du système (N, p et q).

Question 6.– En tirant successivement des clefs et des messages aléatoires, estimer expérimentalement la probabilité d'échec du déchiffrement NTRU pour :

— $N = 20$, $p = 3$, $q = 101$,
— $N = 20$, $p = 3$, $q = 53$,
— $N = 20$, $p = 3$, $q = 21$.

Algorithme 1 : Génération des clefs

Entrée :

Sortie : une paire de clés publique/privée

1 Définir $U(X)$ et $V(X)$ deux polynômes de $\mathbb{Z}_q[X]/(X^N-1)$ dont les coefficients sont tirés uniformément dans S_p.

2 Calculer $F(X) = 1 + 3U(X)$ et $G(X) = 3V(X)$.

3 Si $F(X)$ n'est pas inversible mod $X^N - 1$, recommencer pour U et F les étapes 1. et 2.

4 Calculer $F(X)^{-1} \mod (X^N-1)$ et $H(X) = G(X)F(X)^{-1} \mod (X^N-1)$.

5 La clé publique est $H(X)$, la clé privée est $F(X)$.

Algorithme 2 : Chiffrement

Entrée : La clé publique $H(X) \in \mathbb{Z}_q[X]/(X^N-1)$, un message $M(X) \in \mathbb{Z}_q[X]/(X^N-1)$ dont tous les coefficients sont dans S_p.

Sortie : Un chiffré $Y(X) \in \mathbb{Z}_q[X]/(X^N-1)$

1 Calculer le polynôme $M(X) \in \mathbb{Z}_q[X]/(X^N-1)$ associé au message $\boldsymbol{m}$.

2 Tirer uniformément $R(X) \in \mathbb{Z}_q[X]/(X^N-1)$ dont tous les coefficients sont dans S_p.

3 Calculer et retourner $Y(X) = R(X)H(X) + M(X) \mod (X^N-1)$.

Algorithme 3 : Déchiffrement

Entrée : La clé privée $F(X) \in \mathbb{Z}_q[X]/(X^N-1)$, le chiffré $Y(X) \in \mathbb{Z}_q[X]/(X^N-1)$

Sortie : Un message $A(X)$

1 Calculer $A(X) = Y(X)F(X) \in \mathbb{Z}_q[X]/(X^N-1)$.

2 Retourner $A(X)$ avec ses coeffocients réduits modulo p et écrits dans S_p.