Université Paris 8 Année 2021–2022

M1 Mathématiques et applications, parcours ACC et CSSD

Cryptographie à clef publique – Devoir semaine 8

devoir du 01/04/2022
à rendre jusqu'au 08/04/2022

Exercice 1. Un schéma de signature générique.

Dans cet exercice, on s'intéresse à un schéma de signature générique, qui ne présuppose que l'utilisation d'une fonction à sens unique.

Soit E et E' deux ensembles finis et $f : E \to E'$ une fonction à sens unique. Le schéma de signature est défini pour un certain paramètre k.

Algorithme 1 : Génération des clefs

Entrée :
Sortie : une paire de clés publique/privée

1 Tirer uniformément $2k$ éléments aléatoires de E distincts, et les stocker dans une matrice de taille $(2 \times k)$:

$$\boldsymbol{A} = \begin{pmatrix} a_{0,1} & a_{0,1} & \dots & \dots & a_{0,k} \\ a_{1,1} & a_{1,2} & \dots & \dots & a_{1,k} \end{pmatrix} \in E^{2\times k}$$

2 Calculer la matrice $\boldsymbol{B}$ de taille $(2 \times k)$ sur E', constituée des $b_{i,j} = f(a_{i,j})$:

$$\boldsymbol{B} = \begin{pmatrix} f(a_{0,1}) & f(a_{0,1} & \dots & \dots & f(a_{0,k}) \\ f(a_{1,1}) & f(a_{1,2}) & \dots & \dots & f(a_{1,k}) \end{pmatrix} \in (E')^{2\times k}$$

3 La clé publique est $\boldsymbol{B}$, la clé privée est $\boldsymbol{A}$.

Algorithme 2 : Signature

Entrée : la clé privée $\boldsymbol{A}$, le message à signer $\boldsymbol{m} \in \{0,1\}^k$
Sortie : la signature $\boldsymbol{s}$

1 Pour tout $i \in \{1,\dots,k\}$, définir $s_i := a_{m_i,i}$.
2 Retourner la signature $\boldsymbol{s} = (s_1,\dots,s_k) \in E^k$

Algorithme 3 : Vérification

Entrée : la clé publique $\boldsymbol{B}$, la signature $\boldsymbol{s}$, le message à signer $\boldsymbol{m} \in \{0,1\}^k$
Sortie : un booléen `true/false`

1 Vérifier que $f(s_i) = B_{m_i,i}$ pour tout $i \in \{1,\dots,k\}$.

Question 1.– Expliquer pourquoi, si la fonction f n'est pas à sens unique, alors la signature n'est pas sûre.

Question 2.– Expliquer pourquoi la même paire de clés ne peut pas être utilisée pour signer deux messages.

Question 3.– A priori, le schéma semble construit de sorte que la longueur des messages, et le nombre de colonnes de la clé publique et de la clé privée sont égaux.

1. En quoi cela pose-t-il problème d'un point de vue pratique ?
2. Proposer une modification de la signature afin qu'elle puisse rester pratique pour n'importe quel message à signer.
3. En déduire (approximativement) la taille des clés de cette signature. Justifier.

Exercice 2. NTRU sans erreur de déchiffrement.

On a vu en cours que le chiffrement NTRU peut mener à des erreurs de déchiffrement. Pour simplifier, on se place toujours dans le cas où $p = 3$. On rappelle que l'on fixe également deux entiers $N \geq 1$ et $q \geq 2$, et que l'on note $\mathbb{Z}_q$ l'anneau des entiers modulo q.

Une contre-mesure consiste alors à fixer un entier $d \leq N/2$, et à tirer les polynômes U, V, R dans $\mathbb{Z}_q[X]/(X^N - 1)$, avec la contrainte que, parmi les coefficients de chacun de ces polynômes, exactement d d'entre eux sont égaux à 1, exactement d d'entre eux sont égaux à -1, et le reste est égal à 0.

On note maintenant $\mathcal{R}(d)$ le sous-ensemble de ces polynômes de $\mathbb{Z}_q[X]/(X^N - 1)$. Le système de chiffrement devient donc le suivant :

Algorithme 4 : Génération des clefs

Entrée :
Sortie : une paire de clés publique/privée

1 Tirer uniformément $U(X)$ et $V(X)$ deux polynômes dans $\mathcal{R}(d)$.
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 5 : Chiffrement

Entrée : La clé publique $H(X)$, le message $\boldsymbol{m} \in \{-1, 0, 1\}^N$.
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 $R(X) \in \mathcal{R}(d)$.
3 Calculer et retourner $Y(X) = R(X)H(X) + M(X)$.

Algorithme 6 : Déchiffrement

Entrée : La clé privée $H(X)$, le chiffré $Y(X) \in \mathbb{Z}_q[X]/(X^N - 1)$
Sortie : Un message $\boldsymbol{a} \in \{-1, 0, 1\}^N$

1 Calculer $A(X) = Y(X)F(X) \in \mathbb{Z}_q[X]/(X^N - 1)$.
2 Retourner la liste $\boldsymbol{a}$ des coefficients de $A(X)$, réduits modulo 3, et écrits dans $\{-1, 0, 1\}$

Question 1.– Donner le pseudo-code d'un algorithme qui permet le tirage aléatoire de $U(X)$ avec les contraintes définies plus haut. On précisera sa complexité en fonction de d et/ou de N.

Question 2.– Quelle est, en valeur absolue, la valeur maximale que peut atteindre un coefficient de $A(X)$, dans l'algorithme de déchiffrement ?

Question 3.– En déduire une contrainte simple reliant d et q qui permet de s'assurer que, dans ce contexte, le déchiffrement est valide avec probabilité 1.

Question 4.– Démontrer qu'avec cette modification, le chiffrement NTRU n'est pas indistiguable de l'aléa. Pour cela, on pourra s'intéresser à l'évaluation en 1 des polynômes engagés dans le cryptosystème.