Cryptanalyse — 4TCY902U
Responsable : G. Castagnos

Devoir surveillé — 7 novembre 2017

Durée 1h30
accès aux fonctions programmées en TP, aux énoncés des TP et à la fiche d'initiation à Sage autorisés, autres documents non autorisés
Les deux exercices sont indépendants.

1 Exercice théorique

Soit $n > 1$ un entier. Soit $B = (b_1, \dots, b_n)$ une famille de n vecteurs linéairement indépendants de $\mathbf{R}^n$, base d'un réseau L. Pour $i = 1, \dots, n$, on note $B^{(i)} = (b_1, \dots, b_{i-1}, 2b_i, b_{i+1}, \dots, b_n)$ et $L^{(i)}$ le réseau engendré par $B^{(i)}$.

(a) Soit $u \in L^{(i)}$, montrer que $u - b_i \in L$.

(b) Montrer que $b_i \notin L^{(i)}$.

(c) Soit $v \in L$ un vecteur atteignant le minimum du réseau L. Montrer qu'il existe $i \in \{1, \dots, n\}$ tel que $u := v + b_i \in L^{(i)}$.

(d) Supposons que l'on dispose d'un algorithme $\mathscr{A}$ qui étant donnés une base d'un réseau de dimension n, et un vecteur $t \in \mathbf{R}^n$ retourne un vecteur du réseau le plus proche de t. Déduire de ce qui précède un algorithme polynomial (en pseudo code) utilisant $\mathscr{A}$ qui, étant donné une base d'un réseau de dimension n, retourne un vecteur non nul le plus court de ce réseau. Autrement dit, établir une réduction polynomiale de SVP à CVP.

2 Exercice plutôt pratique

On considère le générateur de suite chiffrante suivant. On utilise un LFSR de longueur ℓ. L'état initial du LFSR noté K constitue la clef secrète. La rétroaction du LFSR est publique, on note P le polynôme de rétroaction et on suppose P primitif de degré ℓ.

Après avoir chargée la clef, on produit une suite chiffrante en répétant ceci :

1. Le LFSR est mis à jour **deux** fois, produisant deux bits a et b ;
2. Si $(a, b) = (1, 0)$, le bit de sortie du générateur est 0,
3. Si $(a, b) = (1, 1)$, le bit de sortie du générateur est 1,
4. Sinon si $(a, b) = (0, 0)$ ou $(a, b) = (0, 1)$, alors on ne sort rien.

Par exemple, avec le LFSR de longueur 3, de polynôme de rétroaction $P = 1 + X + X^3$ initialisé par $K = [0, 1, 1]$ la suite produite par le générateur est $1, 1, 0, 0, 1, 1, 0, 0, 1, 1 \ldots$

(a) Donner le code d'une fonction qui produit N bits par ce générateur. Elle doit prendre en entrée la clef secrète K et le polynôme de rétroaction P du LFSR et l'entier N. Donner les 10 premiers bits produits par le générateur avec : $\ell = 4, K = [0, 1, 0, 0]$, $P = 1 + X^3 + X^4$.

(b) Retour au cas général : montrer que $2^{\ell-1}$ est une période de la suite z construite par ce générateur (Indication : considérer $2(2^\ell - 1)$ bits de sortie du LFSR). De plus, montrer que z est équilibrée.

(c) On suppose ℓ pair et avoir accès à $N \geqslant \ell/2$ bits de suite chiffrante z produite par ce générateur. Proposer une attaque plus efficace que la recherche exhaustive visant à retrouver un état interne du LFSR produisant cette suite z.

(d) Implémenter cette attaque pour retrouver un état interne produisant la suite z_{22} produite par un LFSR de longueur 22 et de polynôme de rétroaction P_{22} donnés dans le fichier suivant : `https://www.math.u-bordeaux.fr/~gcastagn/22.sage`