École normale supérieure **2019-2020**
Département d'informatique

Introduction à la cryptologie
TD n° 11 : Apprendre avec des erreurs

Exercice 1 (Réductions de LWE)**.** On considère une distribution LWE de paramètre n, p, χ, c'est-à-dire la distribution LWE $(a, a \cdot s + e)$ où $a \leftarrow_\$ \mathbb{Z}_p^n$, $s \leftarrow_\$ \mathbb{Z}_p^n$, $e \leftarrow \chi$. Le problème LWE standard est de retrouver le secret s, étant donné un nombre illimité de samples de la distribution précédente. On considère quelques variantes de ce problème.

1. LWE non-uniforme : le but est de retrouver s avec des samples illimités $(a, a \cdot s + e)$ où $a \leftarrow_\$ \mathbb{Z}_p^n$, $s \leftarrow \sigma$, $e \leftarrow \chi$, où σ est une distribution quelconque (non nécessairement uniforme). Montrer que si on a un algorithme magique qui résout LWE standard, on sait résoudre LWE non-uniforme. La réciproque est-elle vraie ?
2. LWE avec secrets multiples : le but est de retrouver $S \in \mathbb{Z}_p^{n \times k}$ avec des samples illimités $(a, aS+e)$ où $a \leftarrow_\$ \mathbb{Z}_p^n$, $s \leftarrow_\$ \mathbb{Z}_p^{n \times k}$, $e \leftarrow \chi^k$. Montrer que si l'on sait résoudre LWE standard, on sait résoudre ce problème. La réciproque est-elle vraie ?
3. Échange secret-erreur : le but est de retrouver s avec des samples illimités $(a, a \cdot s + e)$ où $a \leftarrow_\$ \mathbb{Z}_p^n$, $s \leftarrow \chi^n$, $e \leftarrow \chi$. Montrer que si l'on sait résoudre ce problème, on sait résoudre LWE standard, et inversement.
   Indication : trouver une relation linéaire entre s et un vecteur de n termes d'erreur provenant de n samples distincts.

Exercice 2 (Chiffrement Dual-Regev)**.** Soient p un nombre premier, m, n deux entiers, et χ une distribution gaussienne sur $\mathbb{Z}_p$ d'écart type αp centrée en 0. On suppose que ces paramètres sont choisis de manière à ce que les propriétés suivantes soient vérifiées.

(a) La version décisionnelle de LWE avec paramètres $m+1, n, p, \chi$ est vraie, c'est-à-dire que les deux distributions suivantes sont indistinguables : la distribution LWE $(A, As+e)$ où $A \leftarrow \mathbb{Z}_p^{(m+1) \times n}$, $s \leftarrow_\$ \mathbb{Z}_p^n$, $e \leftarrow \chi^{m+1}$; et la distribution uniforme (A, b) où $A \leftarrow \mathbb{Z}_p^{(m+1) \times n}$, $b \leftarrow_\$ \mathbb{Z}_p^{m+1}$.

(b) Les deux distributions suivantes sont (statistiquement) indistinguables : la distribution $(A, x^T A)$ où $A \leftarrow \mathbb{Z}_p^{m \times n}$, $x \leftarrow_\$ \{0,1\}^m$; et la distribution uniforme (A, u^T) où $A \leftarrow \mathbb{Z}_p^{m \times n}$, $u \leftarrow_\$ \mathbb{Z}_p^n$.

(c) Pour tout $k \leq m+1$, si $x_1, \ldots, x_k$ sont tirés indépendamment avec χ, alors $|\sum x_i| < p/5$, sauf avec probabilité négligeable.

Considérons le chiffrement à clef publique suivante, avec paramètre public $A \leftarrow_\$ \mathbb{Z}_p^{m \times n}$.

- **Génération de clef :** clef secrète $x \leftarrow_\$ \{0,1\}^m$; clef publique $u = x^T A$. (Ici, u est un vecteur ligne, i.e. une matrice $\mathbb{Z}_p^{1 \times n}$.)
- **Chiffrement :** le chiffrement d'un bit $b \in \{0,1\}$ est $(\alpha, \beta) = (As + e, us + e' + b\lfloor p/2 \rfloor)$, où $s \leftarrow_\$ \mathbb{Z}_p^n$, $e \leftarrow \chi^m$, $e' \leftarrow \chi$.
- **Déchiffrement :** si $\beta - x^T \alpha$ est plus proche de 0 que de $\lfloor p/2 \rfloor$, alors le message déchiffré est 0 ; sinon c'est 1.

1. Montrer que le schéma de chiffrement est correct (le déchiffré d'un chiffré est le message d'origine, sauf avec probabilité négligeable).
2. Montrer que la distribution des chiffrés du message $b = 0$ est indistinguable de la distribution des chiffrés du message $b = 1$ (même avec connaissance des valeurs publiques A et u).
3. Montrer que le schéma cache les clefs de chiffrement : la distribution des chiffrés d'un message b avec une clef publique u est indistinguable de la distribution des chiffrés du même message b avec une clef publique u'.

4. Donner une manière d'étendre ce schéma pour chiffrer k bits dans un même message chiffré, en lui ajoutant seulement $k-1$ valeurs dans $\mathbb{Z}_p$.

Exercice 3 (Anonymité de la clef)**.** Nous souhaitons construire une schéma de chiffrement à clef publique qui cache la clef de chiffrement utilisée, afin de cacher l'idendité du destinataire. On dit que le chiffrement cache la clef s'il n'existe pas d'adversaire efficace qui gagne au jeu suivant : l'adversaire choisit un message et tire deux clefs publiques aléatoirement. Il reçoit ensuite le chiffrement de son message avec l'une des deux clefs publiques (choisie au hasard, uniformément), et doit deviner laquelle. On dit que l'adversaire gagne s'il devine correctement la clef utilisée avec une probabilité significativement meilleure que $1/2$ (correspondant à deviner au hasard).

1. Est-ce que RSA cache les clefs ?
2. Même question si on suppose (1) le message dont le chiffré est observé par l'adversaire est tiré uniformément, et l'adversaire n'en a pas connaissance (il voit seulement son chiffré) ; et (2) le module RSA est choisi uniformément parmi les entiers de B bits pour B suffisamment grand (pour simplifier, on oublie que le module doit être un produit de deux grands premiers).
3. Est-ce que le chiffrement ElGamal cache la clef ?