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

Introduction à la cryptologie
TD n° 11 : Correction.

Exercice 1 (Réductions de LWE)**.**

1. Étant donnés des samples $(a, a \cdot s + e)$ où $s \leftarrow \sigma$, on transforme ces samples de la manière suivante : on tire $s' \leftarrow_{\$} \mathbb{Z}_p^n$, puis on remplace $(a, a \cdot s + e)$ par $(a, a \cdot (s + s') + e)$. Les nouveaux samples ainsi obtenus ont une distribution identique à LWE pour un secret uniforme, donc on peut appeler notre algorithme magique pour retrouver $s + s'$. En déduisant s' on retrouve s. La réciproque est fausse, par exemple en considérant la distribution σ où le secret s n'a qu'une valeur possible. Résoudre une telle instance est trivial, et ne peut donc pas impliquer la résolution LWE avec un secret uniforme (en supposant que celle-ci est non-triviale).
2. On observe que chaque sample LWE avec des secrets multiples $(a, aS+e)$ donne lieu à k samples LWE classiques avec k secrets indépendants. En résolvant chaque instance avec un appel séparé à notre algorithme qui résout LWE standard, on retrouve S. Réciproquement, si on a un algorithme qui sait résoudre LWE avec des secrets multiples, et qu'on a une instance de LWE classique, il suffit de lui ajouter $k-1$ instances avec des secrets de notre choix pour obtenir une instance de LWE avec des secrets multiples. En la résolvant, on retrouve tous les secrets, y compris celui de notre instance de départ. Dans toutes ces réductions, le point crucial à vérifier est que quand on réduit vers LWE classique ou une de ses variantes, on obtient bien une instance distribuée de manière identique à une instance légitime ; dans les cas considérés jusqu'ici, c'est à chaque fois immédiat, mais c'est le point important (sinon on ne peut pas en général argumenter que l'algorithme vers lequel on réduit va fonctionner correctement).
3. On met de côté n samples avec des valeurs a_i linéairement indépendantes (après avoir observé $n + t$ samples, la probabilité qu'ils ne soient pas générateurs de $\mathbb{Z}_p^n$ décroît exponentiellement avec t, donc on obtient n samples indépendants très rapidement). Soit A la matrice formée par ces samples, e le vecteur d'erreur correspondant. Sous forme matricielle, on a $(A, b = As + e)$, où a, b sont connus. On déduit la relation linéaire : $s = A^{-1}(b - e)$. On utilise cette relation pour substituer e à s dans les samples qui suivent. Plus précisément : étant donné un sample (a', b'), on a : $b' = \langle a' | s \rangle + e'$, où $\langle \cdot | \cdot \rangle$ dénote le produit scalaire. En substituant, on obtient : $b' - \langle (A^{-1})^T a' | b \rangle = -\langle (A^{-1})^T a' | e \rangle + e'$, où $(\cdot)^T$ désigne la transposition. Le sample $(\langle (A^{-1})^T a', b' - \langle (A^{-1})^T a' | b \rangle)$ est donc un sample LWE valide pour le secret e. Noter que $(A^{-1})^T a'$ est bien uniforme pour a' uniforme. La réciproque est vraie également à cause de la question 1.

Exercice 2 (Chiffrement Dual-Regev)**.**

1. Le déchiffré d'un chiffré est $\beta - x^T \alpha = e' + x^T e + b\lfloor p/2 \rfloor$. Le terme $e' + x^T e$ est une somme d'au plus $m + 1$ éléments tirés suivant χ, donc par la propriété (c), sauf avec probabilité négligeable, $|e' + x^T e| < p/5$. Il s'ensuite $|\beta - x^T \alpha - b\lfloor p/2 \rfloor| < p/5$, donc $\beta - x^T \alpha$ est plus proche de $b\lfloor p/2 \rfloor$ que de $(1 - b)\lfloor p/2 \rfloor$.
2. Soit $\overline{A}$ la matrice formée de A, en lui ajoutant une ligne en bas contenant u. Soit $\overline{e}$ le vecteur e, en lui ajoutant une coordonnée en bas contenant e'. Lorsque $b = 0$, en empilant les deux coordonnées du chiffré, on peut le représenter sous la forme $\overline{A}s + \overline{e}$. Ici, il y a deux observations à faire. La première, c'est que par l'hypothèse (b), u est indistinguable d'une matrice uniforme, même en connaissant A, donc $\overline{A}$ est indistinguable d'une valeur uniforme. Il s'ensuit que $\overline{A}s + \overline{e}$ est indistinguable de la partie droite d'un sample LWE distribué comme dans l'hypothèse (a) ; il est donc indistinguable d'une valeur uniforme même en connaissant $\overline{A}$, c'est-à-dire même en

connaissant A et u (on utilise ici une propriété de composition de l'indistinguabilité qu'on ne formalisera pas). Ainsi, le chiffré de $b = 0$ est indistinguable de valeurs uniformément aléatoires. Le chiffré de $b = 1$ est composé de la même manière, sauf que la dernière coordonnée est translatée de $b\lfloor p/2 \rfloor$. Comme le translaté d'une valeur uniforme par une constante est toujours uniforme, on a la même propriété que dans le cas précédent. On conclut que les chiffrés de $b = 0$ et $b = 1$ sont tous deux indistinguables de la distribution uniforme, en particulier ils sont indistinguables entre eux.

3. On a montré dans la question précédente que le chiffré d'un bit b est indistinguable d'une valeur uniforme, même en connaissant A et u. En particulier il est indistinguable d'une distribution qui ne dépend pas de u, ni de A, ni de b.
4. En s'inspirant de LWE avec des secrets multiples (la question 2 de l'exercice précédent), on utilise k valeurs $u_1, \ldots, u_k$, chacun construite comme u, c'est-à-dire $u_i = x_i^T A$ pour $x_i \leftarrow_\$ \{0,1\}^m$. Soit U la matrice formée par ces valeurs, un chiffré devient $(As + e, Us + e' + \lfloor p/2 \rfloor b_v$, où b_v est le vecteur formé des k bits à chiffrer.

Exercice 3 (Anonymité de la clef)**.**

1. Non, c'est un chiffrement déterministe. Il suffit donc de chiffrer le message avec une des clefs publiques et de comparer avec le chiffré qui nous intéresse pour confirmer si c'est la clef utilisée.
2. La réponse est encore non. Soit N_1 let plus petit des deux modules, et N_2 le plus grand. Comme les modules sont tirés uniformément parmi les entiers de B bits, on peut se convaincre facilement qu'avec une probabilité bornée inférieurement par une constante non nulle, $N_2 \geq 1.5 \cdot N_1$. Dans ce cas, un élément uniforme inférieur à N_2 a une probabilité au moins $1/3$ d'être supérieur à N_1. Or le chiffré d'un élément uniforme est un élément uniforme (on néglige le fait qu'il est inversible), donc un chiffré avec N_2 a une probabilité bornée inférieurement par une constante non nulle, et donc non-négligeable, de révéler que N_2 a été utilisé.
3. Oui. Soit x, g^x une paire clef privée/clef publique ElGamal. Un message chiffré avec cette clef est de la forme $(g^r, m \cdot g^{xr})$. On peut supprimer le message puisqu'on le suppose connu. Reconnaître si c'est cette clef publique qui a été utilisée dans le chiffrement du message revient à reconnaître si (g^x, g^r, g^{xr}) forme un triplet Diffie-Hellman. En supposant que Diffie-Hellman décisionnel est difficile dans le groupe (ce qu'on suppose de toute façon pour utiliser ElGamal), ce problème est difficile.