Session 3

Exercice 1 (Un exemple de Kyber).
Rappelons le chiffrement Kyber :

- KeyGen().
  - **Clé secrète.** $\mathsf{sk} = \mathbf{s} \in_R S_{\eta_1}^k$ tirée aléatoirement.
  - **Clé publique.** $\mathsf{pk} = (\mathbf{A}, \mathbf{t}) \in_R R_q^{k\times k} \times R_q^k$ tirées aléatoirement pour $\mathbf{A}$ et $\mathbf{t} = \mathbf{As} + \mathbf{e}$ avec $\mathbf{e} \in_R S_{\eta_2}^k$.
- Enc(pk, m). Pour chiffrer $\mathsf{m} \in \{0,1\}^n$, il faut transformer ce message en un polynôme binaire $m \in R_q$. Une fois la clé publique obtenue $\mathsf{pk} = (\mathbf{A}, \mathbf{t})$, tirer aléatoirement $\mathbf{r} \in_R S_{\eta_1}^k$, $\mathbf{e}_1 \in_R S_{\eta_2}^k$ et $e_2 \in_R S_{\eta_2}$, et calculer $\mathbf{u} = \mathbf{A^t r} + \mathbf{e}_1$ et $v = \mathbf{t^t r} + e_2 + \lfloor \frac{q}{2} \rfloor m$ et renvoyer $c = (\mathbf{u}, v) \in R_q^k \times R_q$ où $m \in R_q$.
- Dec(sk, c). Pour déchiffrer $c = (\mathbf{u}, v)$, $m = \mathrm{Round}_q(v - \mathbf{s^t u})$ avec $\mathsf{sk} = \mathbf{s}$.

Soit $q = 137, n = 4, k = 2, \eta_1 = 2$ et $\eta_2 = 2$. Soit
$\mathbf{A} = \begin{pmatrix} 21 + 57X + 78X^2 + 43X^3 & 126 + 122X + 19X^2 + 125X^3 \\ 111 + 9X + 63X^2 + 33X^3 & 105 + 61X + 71X^2 + 64X^3 \end{pmatrix}$,
$\mathbf{s} = \begin{pmatrix} 1 + 2X - X^2 + 2X^3 \\ -X + 2X^3 \end{pmatrix}$ et $\mathbf{e} = \begin{pmatrix} 1 - X^2 + X^3 \\ -X + X^2 \end{pmatrix}$.

1. Calculer la clé publique $(\mathbf{A}, \mathbf{t})$?
2. Chiffrer le message $\mathsf{m} = 0111$, représenté par le polynôme $X + X^2 + X^3$, avec $\mathbf{r} = \begin{pmatrix} -2 + 2X + X^2 - X^3 \\ -1 + X + X^2 \end{pmatrix}$, $\mathbf{e}_1 = \begin{pmatrix} 1 - 2X^2 + X^3 \\ -1 + 2X - 2X^2 + X^3 \end{pmatrix}$ et la valeur $e_2 = 2 + 2X - X^2 + X^3$, pour obtenir le chiffré $(\mathbf{u}, v)$?
3. Vérifier que le déchiffrement permet de retrouver le message m.

Exercice 2 (Arora-Ge).
Si $\mathbf{e} \in [-1, 1]^m$ avec m le nombre d'échantillons LWE, et si $m \geq n^3$, alors il est possible de résoudre LWE. Les équations sont de la forme $\langle \mathbf{a}_i, \mathbf{s} \rangle + e_i = b_i$ où $\mathbf{a}_i$ sont les lignes de la matrice $\mathbf{A}$, e_i et b_i les coordonnées correspondantes de $\mathbf{e}$ et $\mathbf{b}$. Le vecteur secret est $\mathbf{s} \in \mathbb{Z}_q^n$.

1. Montrer que l'équation $\langle \mathbf{a}_i, \mathbf{s} \rangle + e_i = b_i$ s'écrit sous la forme : $\prod_{e_i \in \{-1,0,1\}} (\langle \mathbf{a}_i, \mathbf{s} \rangle + e_i - b_i) = 0$.
2. Montrer que cette équation est un polynôme de degré 3 en les inconnues de $\mathbf{s} = (s_1, \ldots, s_n)$.
3. Montrer qu'il y a n^3 monômes de la forme $s_i s_j s_k$?
4. Résoudre un système polynomial est difficile et la technique de *relinéarisation* consiste à introduire de nouvelles variables s_{ijk} pour $s_i s_j s_k$ et à réécrire le système avec ces nouvelles variables. Montrer comment résoudre ce système si $m \geq n^3$.
5. Quelle est alors la complexité de l'algorithme d'Arora-Ge dans ce cas ?

Exercice 3 (Exemple signature Dilithium).
Rappelons la signature Dilithium :

- KeyGen().
  - Tirer aléatoirement $\xi \in_R \{0,1\}^{256}$ et calculer $(\rho, \rho', K) = H(\xi, 1024)$, où $\rho \in \{0,1\}^{256}$, $\rho' \in \{0,1\}^{512}$ et $K \in \{0,1\}^{256}$. Calculer
    $\mathbf{A} = \mathsf{ExpandA}(\rho) \in R_q^{k\times \ell}$, et $(\mathbf{s}_1, \mathbf{s}_2) = \mathsf{ExpandS}(\rho') \in S_\eta^\ell \times S_\eta^k$.
    Le vecteur publique $\mathbf{t} = \mathbf{As}_1 + \mathbf{s}_2 \in R_q^k$ et $tr = H(\rho \| \mathbf{t}, 2\lambda)$.

– **Clé de signature.** $\mathsf{sk} = (\rho, K, tr, \mathbf{s}_1, \mathbf{s}_2)$.
– **Clé de vérification.** $\mathsf{pk} = (\rho, \mathbf{t})$.

- $\underline{\mathsf{Sign}(\mathsf{sk}, \mathsf{m})}$. Pour signer le message $\mathsf{m} \in \{0,1\}^*$ avec la clé secrète sk : Calculer $\mathbf{A} = \overline{\mathsf{ExpandA}(\rho)}$, puis $\mu = H(tr \| \mathsf{m}, 512)$. Puis, calculer la chaîne binaire $\rho'' = H(K \| \text{rnd} \| \mu, 512)$ avec $\text{rnd} = 0^{256}$ pour une signature *déterministe* et $\text{rnd} \in_R \{0,1\}^{256}$ si randomisée.

  $\kappa \leftarrow 0$ et $Found \leftarrow false$
  while $Found = false$ **do**
    $\mathbf{y} = \mathsf{ExpandMask}(\rho'', \kappa) \in \tilde{S}^{\ell}_{\gamma_1}$
    $\mathbf{w} = \mathbf{A}\mathbf{y}$ et $\mathbf{w}_1 = \mathsf{HighBits}(\mathbf{w}, 2\gamma_2)$
    $\tilde{c} = H(\mu \| \mathbf{w}_1, 2\lambda)$
    $c = \mathsf{SampleInBall}(\tilde{c})$ et $\mathbf{z} = \mathbf{y} + c\mathbf{s}_1$
    $r_0 = \mathsf{LowBits}(\mathbf{w} - c\mathbf{s}_2, 2\gamma_2)$
    if $\|\mathbf{z}\|_\infty < \gamma_1 - \beta$ et $\|\mathbf{r}_0\|_\infty < \gamma_2 - \beta$ **then**
      $Found \leftarrow true$
    end if
    $\kappa \leftarrow \kappa + \ell$
  end while

  Renvoyer la signature $\sigma = (\tilde{c}, \mathbf{z}, \sigma, \mathsf{m})$.

- $\underline{\mathsf{Verif}(\mathsf{pk}, s)}$. Pour vérifier la signature $\sigma = (c, \mathbf{z})$ sur le message m avec la clé publique $(\rho, \mathbf{t})$:

  if $\|\mathbf{z}\|_\infty \geq \gamma_1 - \beta$ **then**
    Rejeter
  else
    $\mathbf{A} = \mathsf{ExpandA}(\rho)$
    $tr = H(\rho \| \mathbf{t}, 512)$ et $\mu = H(tr \| \mathsf{m}, 512)$
    $c = \mathsf{SampleInBall}(\tilde{c})$
    $\mathbf{w'}_1 = \mathsf{HighBits}(\mathbf{A}\mathbf{z} - c\mathbf{t}, 2\gamma_2)$
    if $\tilde{c} \neq H(\mu \| \mathbf{w'}_1, 2\lambda)$ **then**
      Rejeter
    end if
    return Accepte
  end if

Définition de $\mathsf{HighBits}_q$ et $\mathsf{LowBits}_q$: La fonction $\mathsf{Decompose}_q(r, \alpha)$ fonctionne de la manière suivante pour $r \in [0, q-1]$ et α paire tel que $q - 1 = m\alpha$. La sortie est (r_0, r_1) telle que $r = r_1\alpha + r_0$ avec $-\frac{\alpha}{2} < r_0 \leq \frac{\alpha}{2}$ et $0 \leq r_1 \leq m$. Les fonctions $\mathsf{HighBits}_q$ et $\mathsf{LowBits}_q$ sont définies par $r_1 = \mathsf{HighBits}_q(r, \alpha)$ et $r_0 = \mathsf{LowBits}_q(r, \alpha)$.

Soit $q = 16\ 417$, $\frac{q-1}{2} = 8\ 208$, $n = 4$, $R_q = \mathbb{Z}_{16417}[X]/(X^4 + 1)$, $(k, \ell) = (3, 2)$, $\eta = 10$, $\gamma_1 = 1024$, $\tau = 4$, $\beta = \tau\eta = 40$, et $\gamma_2 = \frac{q-1}{32} = 513$, $\alpha = 2\gamma_2 = 1\ 026$, $m = 16$ et $\gamma_1 - \beta = 984$ et $\gamma_2 - \beta = 473$. Soit

$$\mathbf{A} = \begin{pmatrix} 15\ 196 + 7\ 926X + 8\ 057X^2 + 13\ 612X^3 & 14\ 303 + 5X + 12\ 257X^2 + 2\ 347X^3 \\ 9\ 765 + 10\ 436X + 10\ 983X^2 + 5\ 860X^3 & 5\ 393 + 311X + 5\ 144X^2 + 10\ 841X^3 \\ 11\ 868 + 7\ 995X + 10\ 716X^2 + 3\ 121X^3 & 9\ 390 + 2\ 055X + 6\ 505X^2 + 2\ 440X^3 \end{pmatrix}$$

$$\mathbf{s}_1 \bmod q = \begin{pmatrix} 2 + 5X - 10X^2 - 5X^3 \\ 2 + 3X - 4X^2 - 4X^3 \end{pmatrix}, \ \mathbf{s}_2 \bmod q = \begin{pmatrix} -8 + 3X + 4X^2 + 4X^3 \\ 8 + 10X + X^2 + 8X^3 \\ -3 - 8X + 6X^2 + 6X^3 \end{pmatrix}.$$

1. Calculer la clé publique $\mathbf{t} = \mathbf{A}\mathbf{s}_1 + \mathsf{s}_2$?

2. Pour signer le message m, Alice tire
   $\mathbf{y} \bmod q = \begin{pmatrix} 707 - 155X + 357X^2 - 822X^3 \\ 474 - 566X - 869X^2 - 542X^3 \end{pmatrix}$, et $\gamma_1 = 1024$, calculer $\mathbf{w} = \mathbf{A}\mathbf{y}$ et $\mathbf{w}_1 = \mathsf{HighBits}(\mathbf{w}, 2\gamma_2)$, avec $2\gamma_2 = 1026$?
   Si $\tilde{c} = H(\mu, \mathbf{w}_1)$ et $c = \mathsf{SampleInBall}(\tilde{\mathsf{c}})$ et $c \bmod q = -1 - X + X^2 - X^3$, calculer $\mathbf{z}$ et la signature $\sigma = (\tilde{c}, \mathbf{z})$?
3. Enfin, vérifier si la signature est acceptée par le vérifieur ?