Apprentissage avec erreurs

Schéma de signature 💀

- Soit le schéma de chiffrement à clé publique de Regev

$$\Pi_E = (Gen, Enc_{pk}, Dec_{sk})$$

- On définit le schéma de signature suivant:

$$\Pi_S = \begin{cases} Gen'(1^n) & = (sk, pk) \leftarrow Gen(1^n) \\ Sign_{sk}(m) & = (m, Dec_{sk}(m)) \\ Vrfy_{pk}(m, \sigma) & = m \stackrel{?}{=} Enc_{sk}(\sigma) \end{cases}$$

Just kidding

Apprentissage avec erreurs

Généralisation aux anneaux

- Rappel chiffrement d'un scalaire
- Avec $a \xleftarrow{R} \mathbb{Z}_q^n$ appelé le masque et l'erreur $e \xleftarrow{\chi} \mathbb{Z}_q$

$$Enc_s\colon \mathbb{Z}_p \to (\mathbb{Z}_q^n \times \mathbb{Z}_q) \qquad Dec_s\colon (\mathbb{Z}_q^n \times \mathbb{Z}_q) \to \mathbb{Z}_p$$

$$Enc_s(m) = (a, a \cdot s + \Delta m + e) \quad Dec_s(a, b) = (b - a \cdot s)/\Delta$$