Apprentissage avec erreurs

Nécessité du bruit

- Clé privée: $s \xleftarrow{R} \mathbb{Z}_q^n$
- Clé publique: $(a_i, b_i = (a_i \cdot s)/q)_{i=1}^m$ avec $a_1, \ldots, a_m \xleftarrow{R} \mathbb{Z}_q^n$

$$\begin{pmatrix} a_{1,1} & \cdots & a_{1,n} \\ \vdots & & \vdots \\ a_{n,1} & \cdots & a_{n,n} \end{pmatrix} \times \begin{pmatrix} s_1 \\ \vdots \\ s_n \end{pmatrix} \equiv_q q \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix}$$

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