Apprentissage avec erreurs

Nécessité du bruit

- Clé secrète: $s \xleftarrow{R} \mathbb{Z}_q^n$
- n cryptogrammes sans bruit: $(a_i, b_i = a_i \cdot s)_{i=1}^n$ avec $a_1, \ldots, a_n \xleftarrow{R} \mathbb{Z}_q^n$

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

$\Longrightarrow$ Élimination Gaussienne

Apprentissage avec erreurs

Schéma de chiffrement

- $p < q$ des puissances de deux et $\Delta = q/p$
- Clé secrète: $s \xleftarrow{R} \{0,1\}^n$
- Avec $a \xleftarrow{R} \mathbb{Z}_q^n$ appelé le masque et l'erreur $e \xleftarrow{\phi} \mathbb{Z}_q$

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

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

- On a $Dec_s(Enc_s(m)) = m$ tant que $e < \Delta$