Apprentissage avec erreurs

Reformulation

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

$$\begin{pmatrix} a_{1,1} & \ldots & a_{1,n} \\ \vdots & & \vdots \\ a_{n,1} & \ldots & a_{n,n} \end{pmatrix} \times \begin{pmatrix} s_1 \\ \vdots \\ s_n \end{pmatrix} + \begin{pmatrix} e_1 \\ \vdots \\ e_n \end{pmatrix} \equiv_q \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix}$$

- A priori $\exp(n)$ systèmes d'équations à résoudre

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 $a_1, \ldots, a_n \xleftarrow{R} \mathbb{Z}_q^n$

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

$\Longrightarrow$ Élimination Gaussienne