# Chiffrement homomorphe

## Ring Learning With Errors in TFHE

Soit $\mathscr{R}_q = \mathbb{Z}_q[X]/\langle X^N + 1 \rangle$ l'anneau des polynômes sur $\mathbb{Z}_q$ de degré inférieur à $N$

On défini le chiffre RLWE, à clé secrète $S \in \mathscr{R}_q$ avec $s_i \in \{0,1\}$ par:

$$Enc_S : \mathscr{R}_p \to \mathscr{R}_q \times \mathscr{R}_q$$
$$M \mapsto (A, A \cdot S + \Delta M + E)$$

$$Dec_S : \mathscr{R}_q \times \mathscr{R}_q \to \mathscr{R}_p$$
$$(A, B) \mapsto (B - A \cdot S)/\Delta$$

Où $A \in_R \mathscr{R}_{q'}$ $E \in_{\chi_\sigma} \mathscr{R}_q$ et $\Delta = \frac{p}{q}$

# Chiffrement homomorphe

## Boite à outils RevoLUT

ZAMA
TFHE-rs

**Blind Array Access**