CKKS

Chiffrement homomorphe approximatif CKKS

Ring Learning With Errors (RLWE)

- On note $\mathscr{R} = \mathbb{Z}_q[X]/(X^N + 1)$ les polynômes de degré N à coefficients entiers modulo q
- Le chiffrement d'un message $m \in \mathscr{R}$ sous la clé $s \in \mathscr{R}$ avec aléas $a, e \xleftarrow{\$} \mathscr{R}$ est

$$Enc_s(m) = (-as + m + e, a) \in \mathscr{R}^2$$
$$Dec_s(b, a) = b + as = m + e \approx m$$