Rappels CKKS

Chiffrement complètement homomorphe approximatif

- Encodage de vecteurs complexes $a, b \in \mathbb{C}^n$ en polynômes $R_p = \mathbb{Z}_p[X]/(X^N + 1)$
  - Identifiant la multiplication polynomiale au produit de Hadamard (terme à terme)
- Chiffrement RLWE par masquage et bruitage
  - Combinaisons linéaires pour $c \in \mathbb{C}$ "gratuites"
  - Multiplications chiffrées coûteuses

$\Longrightarrow$ Évaluation (SIMD) de polynôme $P(x)$ sur un chiffré

$$E(a) + cE(b) = E(a + cb)$$

$$E(a) \times E(b) = E(a \odot b)$$

$$P(E(a)) = E(P(a))$$

Bootstrapping Fonctionnel

Motivation

- Les opérations sur les chiffrés accumulent du bruit
  - On chiffre $1 \in \mathbb{Z}$ comme par exemple $[1.2]$ (bruité) et calcule $x \mapsto x^4$ en aveugle
  - $[1.2] \times [1.2] = [1.44]$ puis $[1.44] \times [1.44] = [2.0736]$
- Quand on déchiffre, on retrouve 2 alors qu'on aurait voulu retrouver 1
- **Bootstrapping**: On veut réduire le bruit entre les opérations
- **Fonctionnel**: Et évaluer au passage des fonctions non-linéaires