# 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

# Bootstrapping Fonctionnel

## Algorithme pour évaluer en aveugle $f : \mathbb{Z}_p \to \mathbb{Z}_p$ et réduire le bruit

- Étant donné une description de fonction $f(x)$ quelconque et un chiffré $[x]$ de vecteur $x \in \mathbb{Z}_p^w$
- On veut produire un chiffré $[f(x)]$ avec un bruit réduit

1. On interpole $f(x)$ en un polynôme “nettoyant” $P(x)$
   - Calcul en clair “gratuit”
2. On évalue $P(x)$ sur notre chiffré
   - Coût en temps et bruit dépend du degré de $P(x)$