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 $P(x)$

Bootstrapping Fonctionnel

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

- Étant donné une LUT $L = (f(0), f(1), \ldots, f(p-1))$ et un chiffré $[x]$ de vecteur $x \in \mathbb{Z}_p^w$

1. $T(X) \leftarrow Hermite(L)$ // Interpolation “nettoyante” en un polynôme en $X = e^{2\pi i x}$
2. $P(X) \leftarrow Chebyshev(x \mapsto e^{2\pi i x})$ // Interpolation “précise” de l’exponentielle complexe
3. $[e^{2\pi i x}] \leftarrow Evaluate(P(X), [x])$
4. $\uparrow Evaluate(T(X), [e^{2\pi i x}])$

Évaluation avec l’algorithme de Paterson-Stockmeyer