

Bootstrapping Fonctionnel

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

- Étant donné une LUT $L = (f(0), f(1), \dots, f(p - 1))$ et un chiffré $[x]$ de vecteur $x \in \mathbb{Z}_p^w$
1. $T(X) \leftarrow \text{Hermite}(L)$ // Interpolation “nettoyante” en un polynôme en $X = e^{2\pi i x}$
 2. $P(X) \leftarrow \text{Chebyshev}(x \mapsto e^{2\pi i x})$ // Interpolation “précise” de l’exponentielle complexe
 3. $[e^{2\pi i x}] \leftarrow \text{Evaluate}(P(X), [x])$
 4. $\uparrow \text{Evaluate}(T(X), [e^{2\pi i x}])$
- Évaluation avec l’algorithme de Paterson-Stockmeyer

[PS73] Évaluation de polynôme
Paterson-Stockmeyer