Interpolation polynomiale

Méthode d'Hermite - analytique - FHE friendly

- Forme close donnée dans [AKP25] en fonction des puissances de $e^{2\pi i x}$

$$T(x) = a_0 + \sum_{k=1}^{p-1} \left(a_k \cdot e^{2\pi i k x} \right)$$

$$a_0 = \frac{1}{p} \sum_{l=0}^{p-1} f(l) \qquad\qquad a_k = \frac{2(p-k)}{p^2} \sum_{l=0}^{p-1} \left(f(l) \cdot e^{-2\pi k l i / p} \right)$$

- Nécessite une seule évaluation aveugle de $x \mapsto e^{2\pi i x}$

- Puisque $T(x) = P(e^{2\pi i x})$ pour $P(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_{p-1} x^{p-1}$

Re: 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