FHE - CKKS in a Nutshell

Ethan Bandasack

Mars 2025

1 Notation

1.1 Général

- $\log = \log_2$
- $\mathbb{Z} \cap]-q/2, q/2] \sim \mathbb{Z}_q$
- $x \leftarrow D \equiv x \sim \mathcal{U}(D)$
- λ : security parameter

1.2 Polynômes

- $M \in \mathbb{N}$: polynomial modulus, `poly_modulus_degree`
- $N = \phi(M) \quad (= 2^M)$
- $\Phi_M(X) = X^{\phi(M)} + 1$
- $\mathcal{R} = \mathbb{Z}[X]/(\Phi_M(X))$
- $p_1, \ldots, p_L \equiv 1 \ [2N] \in \mathcal{P}$: coefficient modulus, `coeff_modulus`
- $\mathcal{R}_q = \mathcal{R}/q\mathcal{R} = \mathbb{Z}_q[X]/(\Phi_M(X))$
- $t \in \mathbb{N}$: plaintext modulus, `plain_modulus`
- $\mathcal{S} = \mathbb{R}[X]/(\Phi_M(X))$
- $\mathbb{Z}_M^* = \{x \in \mathbb{Z}_M \mid \gcd(x, M) = 1\}$
- $\sigma : \begin{cases} \mathbb{Q}[X](\Phi_M(X)) & \to \mathbb{C}_N \\ a & \mapsto (a(\zeta_M^i))_{i \in \mathbb{Z}_M^*} = (a(\mathrm{e}^{2i\pi/M}))_{i \in \mathbb{Z}_M^*} \end{cases}$
- $\| \ a \ \|_\infty^{\text{can}} = \|\sigma(a)\|_\infty$
- c_M : constante d'anneau de $\mathcal{S}$
- CRT : matrice de Vandermonde sur $\zeta_{M\, i \in \mathbb{Z}_M^*}^i$
- $\| \ (u_{ij})_{0 \le i,j < N} \ \|_\infty = \max_{0 \le i < N} \left(\sum_{0 \le j < N} |u_{ij}| \right)$
- $\mathbb{H} = \{\mathbf{z} = (z_j)_{j \in \mathbb{Z}_M^*} \in \mathbb{C}_N \ z_j = \overline{z_{-j}}, \forall j \in \mathbb{Z}_M^*\}$
- $\mathbb{H} = U\mathbb{R}^N, U = \frac{1}{\sqrt{2}} \begin{pmatrix} I_{N/2} & \mathrm{i}J_{N/2} \\ J_{N/2} & -\mathrm{i}I_{N/2} \end{pmatrix}$

- $\forall r > 0, \rho_r : \begin{cases} \mathbb{H} & \to]0,1] \\ \mathbf{z} & \mapsto \exp(-\pi \parallel \mathbf{z} \parallel_2^2 \ / \ r^2) \end{cases}$
- $\Gamma_r = \frac{\rho_r}{r^{-N}}$
- $\forall \mathbf{r} \in (\mathbb{R}^+)^N, \Gamma_{\mathbf{r}} = U\mathbf{z} \in \mathbb{H}$, $\mathbf{z} \sim \Gamma_{r_i}^N$
- $\Psi_{\mathbf{r}} = \mathrm{CRT}_M^{-1} U\mathbf{z} \in \mathbb{Q}[X]/(\Phi_M(X)) \otimes \mathbb{R}$, $\mathbf{z} \sim \Gamma_{r_i}^N$
- $\mathcal{R}^\vee = \frac{1}{\phi(M)}\mathcal{R}$??
- $\mathcal{R}_q^\vee = \frac{1}{\phi(M)}\mathcal{R}_q$??
- $\chi = \lfloor \Psi_{\mathbf{r}} \rceil_{\mathcal{R}^\vee}$

2 Clés

- $A_{N,q,\chi}(s)$: distribution RLWE $(a, a \cdot s + e) \in \mathcal{R}_q \times \mathcal{R}_q^\vee, (a, e) \longleftarrow \mathcal{R}_q \times \chi$.