Projet FHE BPCE × Paris Digital Lab
Inversion d'un premier système de chiffrement

Ethan Bandasack, Mathis Bottinelli, Malo Leroy

Avril 2025

- S : clé secrète
- ei, j : bruit aléatoire pour la i^{e} ligne du dataset pour le j^{e} chiffrement
- m_i : i^{e} ligne du dataset en clair
- $c_{i,j}$: i^{e} ligne du dataset chiffré pour le j^{e} chiffrement
- σ : écart-type

$$\left.\begin{array}{rl} S \times e_{1,1} + m_1 &= c_{1,1} \\ & \vdots \\ S \times e_{n,1} + m_n &= c_{n,1} \\ \vdots & \\ S \times e_{1,N} + m_1 &= c_{1,N} \\ & \vdots \\ S \times e_{n,N} + m_n &= c_{n,N} \end{array}\right\} \quad \left.\begin{array}{c} S \times e_1 + m = c_1 \\ \vdots \\ S \times e_N + m = c_N \end{array}\right\} \quad S\sigma(e) = \sigma(c)$$

Figure 1: Chiffrement de $n = 31037$ lignes (`"rwa"`) $N = 4000$ fois avec $e_{i,j}$ tirés uniformément entre -100 et 99

Notons qu'il est d'autant plus facile d'inverser le système avec une loi d'espérance non nulle.

Les systèmes de chiffrement actuels sont basés sur le problème LWE, qui est rendu difficile par l'ajout d'un bruit gaussien qui rompt la linéarité.