

1. Définitions

Définition 1.1: *Bases de donnée voisines*

On dit que deux bases de données x et y sont voisines et on note $\|x - y\|_1 \leq 1$ si elles diffèrent sur au plus une entrée ie la distance de HAMMING qui les sépare et majorée par 1.

Définition 1.2: *Differential privacy*

On dit qu'un mécanisme aléatoire $\mathcal{M} : \mathcal{X}^{\mathbb{N}} \rightarrow \mathcal{T}$ est (ε, δ) -differentially private si

$$\forall \mathcal{S} \subset \mathcal{T} \quad \forall x, y \in \mathcal{X}^{\mathbb{N}} \quad \|x - y\|_1 \leq 1 \quad \Rightarrow \quad \mathbb{P}(\mathcal{M}(x) \in \mathcal{S}) \leq \exp(\varepsilon) \mathbb{P}(\mathcal{M}(y) \in \mathcal{S}) + \delta$$

De plus, si $\delta = 0$, on dit que \mathcal{M} est ε -differentially private.