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 $\mathcal{M} : \mathcal{X}^{(\mathbb{N})} \to \mathcal{T}$ est (ε, δ)-*differentially private* si

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

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

Définition 1.3: *Longueur*
Soit $x \in \mathcal{X}^{(\mathbb{N})}$ et $f : \mathcal{X}^{(\mathbb{N})} \to \mathcal{T}$. La longueur est le nombre minimum de valeurs à modifier dans x pour obtenir x' tel que $f(x') = t$.

$$\mathrm{len}_f(x,t) = \inf_{x' \in \mathcal{X}^{(\mathbb{N})}} \{||x-x'||_1 \mid f(x') = t\}$$

Définition 1.4: *Mécanisme de sensibilité inverse*
Soit $f : \mathcal{X}^{(\mathbb{N})} \to \mathcal{T}$. Pour une mesure μ sur $\mathcal{T}$, on définit le mécanisme aléatoire $M(x)$ par sa fonction de densité

$$t \mapsto \frac{\exp(-\mathrm{len}_f(x,t)\varepsilon/2)}{\int_{\mathcal{T}} \exp(-\mathrm{len}_f(x,s)\varepsilon/2)\mathrm{d}\mu(s)}$$