# Differential Privacy

**Idea**

- Use randomization to protect privacy, but at the same time recover the distribution from population

## Randomness is Essential!

- Assume we have a non-trivial deterministic algorithm
- There exists a query and two databases $A$ and $B$ and yield different outputs
- Change one row of $A$ to $B$ each time, there must be a time when the output is changed by changing only one row. (A row corresponds to a person's profile)
- The value of that row can then be learnt from an adversary

## Notations

- Database $x$: collections of records from $X$
- Represent databases by their histograms: $x \in N^{|X|}$
- where $x_i$ denotes the number of elements in DB of type $i \in X$
- $\ell_1 : ||x - y||_1 = \sum_{i=1}^{|X|} |x_i - y_i|$
- so $||x||_1$ is the total size of the database and $||x - y||_1$ is the number of different records

## Definition

- A randomized algorithm $M$ with domain $N^{|X|}$ is $(\epsilon, \delta)$-differentially private
- if for all $S \subseteq Range(M)$ and for all $x, y \in N^{|X|}$ such that $||x - y||_1 \leq 1$:
$$\Pr[M(x) \in S] \leq e^{\epsilon} \Pr[M(y) \in S] + \delta \tag{1}$$
- **in other words, probability of generating any outcome is similar by changing 1 element**

## Properties

**Immunity to post-processing**

- $f \circ M$ is differentially private for any $f$
- *It suffices to prove for deterministic $f$. Then the proof is trivial based on the definition*

**Promises**

- Suppose the set of event $A$ and a utility function $u_i : A \to \mathbb{R}^*$
- Assume $f : Range(M) \to A$ determines the distribution of the future event
- We have

$$\mathbb{E}_{a \sim M(x)}[u_i(f(a)] \leq E_{a \sim M(y)}[u_i(f(a))] \tag{2}$$

- for any $||x - y||_1 \leq 1$.
- so one person influence little

## Mechanism

**Random coin toss**

**Laplace Mechanism**

- Given any function $f : N^{|X|} \to \mathbb{R}^k$, the Laplace mechanism is described as:

$$M_k(x, f, \epsilon) = f(x) + (Y_1, \ldots, Y_k) \tag{3}$$

- where $Y_i$ is drawn randomly from $Lap(\frac{\Delta f}{\epsilon})$
- $\Delta f = \max_{x,y \in N^{|X|}, ||x-y||_1 = 1} ||f(x) - f(y)||_1$
- $Lap(b) = \frac{1}{2b} e^{-\frac{|x|}{b}}$

**Theorem (Privacy)**

- Laplace Mechanism preserves $(\epsilon, 0)-$differential privacy

**Accuracy Guarantee**