CS2080: Applied Privacy for Data Science
Introduction to Differential Privacy (cont.)

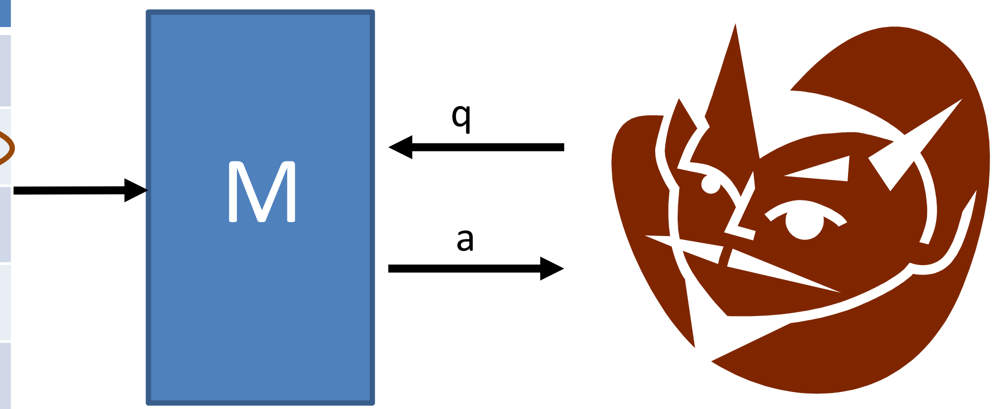
School of Engineering & Applied Sciences
Harvard University

February 12, 2025

DP for one query/release

[Dwork-McSherry-Nissim-Smith ’06]

Sex	Blood	⋯	HIV?
F	B	⋯	Y
F	A		Y
M	O	⋯	N
M	O	⋯	Y
F	A	⋯	N
M	B	⋯	Y



randomized mechanism

adversary

Def: M is ε-DP if for all x, x' differing on one row, and all q

$\forall$ sets T, $$\Pr[M(x,q) \in T] \leq e^{\varepsilon} \cdot \Pr[M(x',q) \in T]$$

(Probabilities are (only) over the randomness of M.)

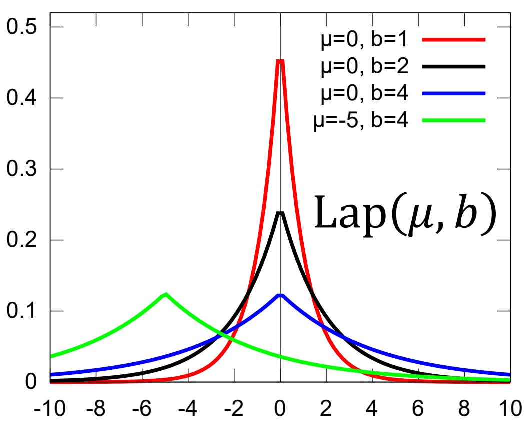
The Laplace Mechanism

[Dwork-McSherry-Nissim-Smith ’06]

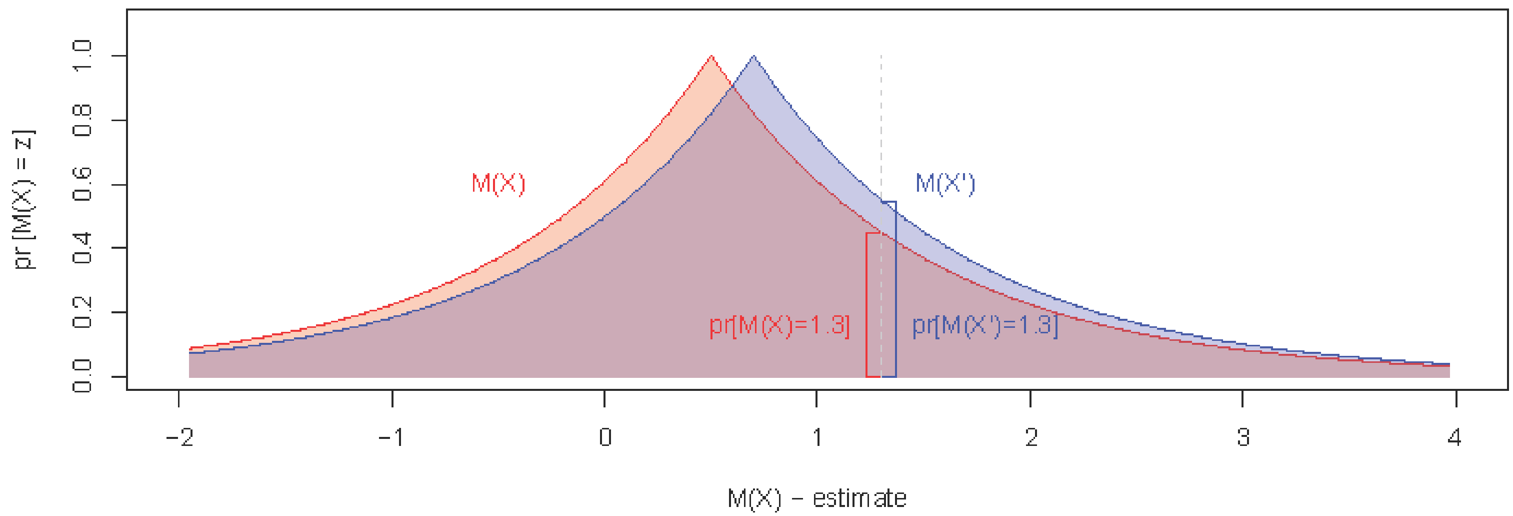
- Let $\mathcal{X}$ be a data universe, and $\mathcal{X}^n$ a space of datasets.
  - This is the Bounded DP setting: n known and public.
- For $x, x' \in \mathcal{X}^n$, write $x \sim x'$ if x and x' differ on ≤ 1 row.
- For a query $q : \mathcal{X}^n \to \mathbb{R}$, the global sensitivity is

$$\Delta q = \mathrm{GS}_q = \max_{x \sim x'} |q(x) - q(x')|.$$

- The Laplace distribution with scale b, $\mathrm{Lap}(b)$:
  - Has density function $f(y) = e^{-|y|/b}/2b$.
  - Mean 0, standard deviation $\sqrt{2} \cdot b$.



Theorem: $M(x, q) = q(x) + \mathrm{Lap}(\Delta q/\varepsilon)$ is ε-DP.



Two Laplace distributions, for two adjacent datasets x and x'. The definition of ϵ-differential privacy requires the ratio of $M(x)/M(x')$ is not greater than e^{ϵ} for all points along the x-axis. Thus for any realized output z (for example here, $z = 1.3$) we can not determine that x or x' were more likely to have produced z.

Calculating Global Sensitivity

1. $\mathcal{X} = \{0,1\}, q(x) = \sum_{i=1}^{n} x_i, \Delta q = \mathbf{1}$

2. $\mathcal{X} = \mathbb{R}, \ q(x) = \sum_{i=1}^{n} x_i, \Delta q = \infty$

3. $\mathcal{X} = [0,1], \ q(x) = \text{mean}(x_1, x_2, \dots, x_n), \Delta q = \mathbf{1/n}$

4. $\mathcal{X} = [0,1], \ q(x) = \text{median}(x_1, x_2, \dots, x_n), \Delta q = \begin{cases} \mathbf{1 \text{ if } n \text{ odd}} \\ \mathbf{1/2 \text{ if } n \text{ even}} \end{cases}$

5. $\mathcal{X} = [0,1], \ q(x) = \text{variance}(x_1, x_2, \dots, x_n), \Delta q = \mathbf{1/n - 1/n^2}$

Q: for which of these queries is the Laplace Mechanism “useful”?

A: 1, 3, 5

Properties of the Definition

- Suffices to check pointwise: M is ε-DP if and only if
  $\forall x \sim x' \; \forall q \; \forall y \; \Pr[M(x,q)=y] \leq e^{\varepsilon} \cdot \Pr[M(x',q)=y]$.

- Preserved under post-processing: If M is ε-DP and f is any function, then $M'(x,q) = f(M(x,q))$ is ε-DP.

- (Basic) composition: If M_i is ε_i-DP for $i = 1, \ldots, k$, then
  $$M'\big(x,(q_1,\ldots,q_k)\big) = (M_1(x,q_1),\ldots,M_k(x,q_k))$$
  is $(\varepsilon_1 + \cdots + \varepsilon_k)$-DP
  - Use independent randomness for the k queries
  - Holds even if q_i's are chosen adaptively

Interpreting the Definition

- Whatever an adversary learns about me, it could have learned from everyone else's data.

- Mechanism cannot leak "individual-specific" information.

- Above interpretations hold regardless of adversary's auxiliary information or computational power.

- Protection against MIAs: let $X = (X_1, \ldots, X_n)$ be a r.v. distributed on $\mathcal{X}^n$ and $X_{-i} = (X_1, \ldots, X_{i-1}, \perp, X_{i+1}, \ldots, X_n)$ be X with Alice's data removed. Then for every MIA A,

$$\underbrace{\Pr\left[A\left(M(X)\right) = \text{"In"}\right]}_{\text{TPR on } X} \leq e^{\varepsilon} \cdot \underbrace{\Pr\left[A\left(M(X_{-i})\right) = \text{"In"}\right]}_{\text{FPR on } X_{-i}}$$

Varying the Data Domain and Privacy Unit

- Unbounded DP (n not publicly known):
  - Datasets: multisets x from a data universe $\mathcal{X}$
    - Can represent as histogram $h_x: \mathcal{X} \to \mathbb{N}$, $h_x(i) =$ # copies of i
  - Adjacency: $x \sim x'$ if $|x \Delta x'| \leq 1$ (add/remove 1 record)
    - Equivalently $\sum_{i \in \mathcal{X}} |h_x(i) - h_{x'}(i)| \leq 1$

- Social Networks:
  - Datasets: graphs G
  - Adjacency: $G \sim G'$ if
    - differ by ≤ 1 edge (edge privacy), OR
    - differ by ≤ 1 node and incident edges (node privacy)

    Q: which is better for privacy?

Real Numbers Aren't

[Mironov `12]

- Digital computers don't manipulate actual real-numbers
  - Floating-point implementations of the Laplace Mechanism can have $M(x,q)$ and $M(x',q)$ disjoint $\rightarrow$ privacy violation!

- Solutions:
  - Round outputs of M to a discrete number (with care).
  - Or use the Geometric Mechanism:
    - Ensure that $q(x)$ is always an integer multiple of γ.
    - Define $M(x,q)$=$q(x) + \gamma \cdot \mathrm{Geo}(\Delta q / \gamma\varepsilon)$,
      where $\Pr[\mathrm{Geo}(b) = k] \propto \exp(-|k|/b)$ for $k \in \mathbb{Z}$.