PDS, 10.11.21

$M : \mathcal{X}^n \longrightarrow \mathcal{Y}$

Two neighboring datasets X^n, $\bar{X}^n$ differ in at most one entry.

Def: M is ε-d.p. iff
$\forall Y \subseteq \mathcal{Y}$, $\forall X^n \sim \bar{X}^n$:

$$\frac{P[M(X^n) \in Y]}{P[M(\bar{X}^n) \in Y]} \leq e^{\varepsilon}$$

Remarks

- ε privacy parameter, smaller ε is more private

  $0.1 \leq \varepsilon \leq 5$

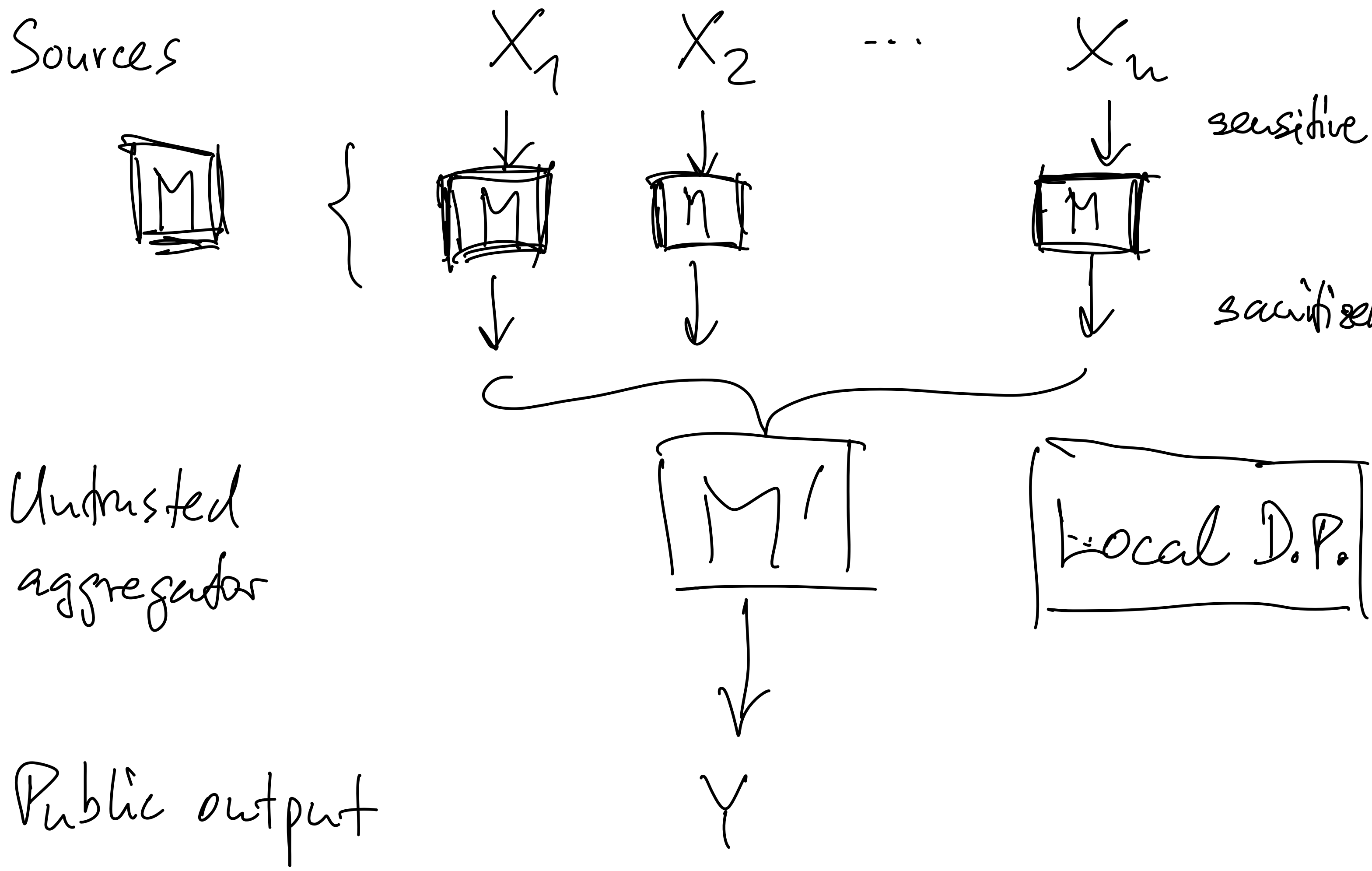
- One entry in dataset affects

every output at most by a factor of e^{ε}

- M must be randomized
- D.P. is symmetric in X and $\bar{X}$
- Why e^{ε}? Additive privacy measure, because $e^{\varepsilon_1} \cdot e^{\varepsilon_2} = e^{\varepsilon_1 + \varepsilon_2}$

How can this be implemented?

Sources/persons	$\underbrace{X_1 \quad X_2 \quad \cdots \quad X_n}$	
(sensitive)	$\downarrow$	
Trusted aggregator	$X^n \rightarrow \boxed{M}$	Global D.P. Central D.P.
(sanitized)	$\downarrow$	
Public output	Y	



Randomized Response is D.P.

$$X_i \in \{0,1\}$$

$$Y_i = \begin{cases} X_i & \text{w/ prob. } \alpha \\ R_i & \text{w/ prob. } 1-\alpha \end{cases}$$

where $R_i \xleftarrow{R} \{0,1\}$

Then, for any y^n, for $X^n \sim \bar{X}^n$: $\dfrac{P[M(X^n) = y^n]}{P[M(\bar{X}^n) = y^n]} =$

for $Y^n = M(X^n)$, $\bar{Y}^n = M(\bar{X}^n)$: $\quad \dfrac{\prod_i P[Y_i = y_i]}{\prod_i P[\bar{Y}_i = y_i]} =$

Suppose X^n and $\bar{X}^n$ differ in pos. j: $\quad \dfrac{P[Y_j = y_j]}{P[\bar{Y}_j = y_j]} = \%$

$$P[Y_j = 0] = \alpha P_{X_j}(0) + (1-\alpha)\frac{1}{2}$$

$$= \frac{1}{2} + \alpha\left(P_{X_j}(0) - \frac{1}{2}\right) \leq \frac{1}{2} + \frac{\alpha}{2}$$

$$\ldots \geq \frac{1}{2} - \frac{\alpha}{2}$$

$$\% \leq \frac{\frac{1}{2} + \frac{\alpha}{2}}{\frac{1}{2} - \frac{\alpha}{2}} = \frac{1+\alpha}{1-\alpha}$$

$(1 + x \approx e^x)$ $\quad \approx e^{2\alpha}$

Randomized response is approx. 2α-d.p.

6.3) Laplace mechanism

- How should noise be generated?

Here: $M: \mathcal{X}^n \to \mathcal{Y}^k$

(mostly consider $k=1$, $\mathcal{Y}=\mathbb{R}$)

$f: \mathcal{X}^n \to \mathbb{R}$: a arbitrary query function

$N \in \mathbb{R}$: r.v., noise

$$M(X^n) = f(X^n) + N$$

How to choose N?

- N should have mean 0
- For neighboring X^n and $\overline{X}^n$, let

$$\Delta = |f(X^n) - f(\overline{X}^n)|$$

- For D.P., it must hold

$$\frac{P[N = y]}{P[N = y + \Delta]} \leq e^{\varepsilon}$$

- What is the max. Δ for two neighboring X^n and $\overline{X}^n$?

<u>Def:</u> The <u>ℓ_1-sensitivity</u> of a query function $f : X^n \longrightarrow \mathbb{R}^k$ is

$$\Delta^{(f)} = \max_{\substack{X^n, \overline{X}^n \\ \text{s.t. } X^n \sim \overline{X}^n}} \| f(X^n) - f(\overline{X}^n) \|_1 .$$

<u>Ex.</u> $X^n = \{0,1\}^n$

$$f(X^n) = \frac{1}{n} \sum_i X_i$$

$$\Rightarrow \Delta^{(f)} \leq \frac{1}{n}$$

N should ensure that changing the output by at most Δ, changes the prob. ratio by at most e^{ε}.

$$\Leftrightarrow \frac{P[N = y]}{P[N = y + \Delta]} \leq e^{\varepsilon}$$

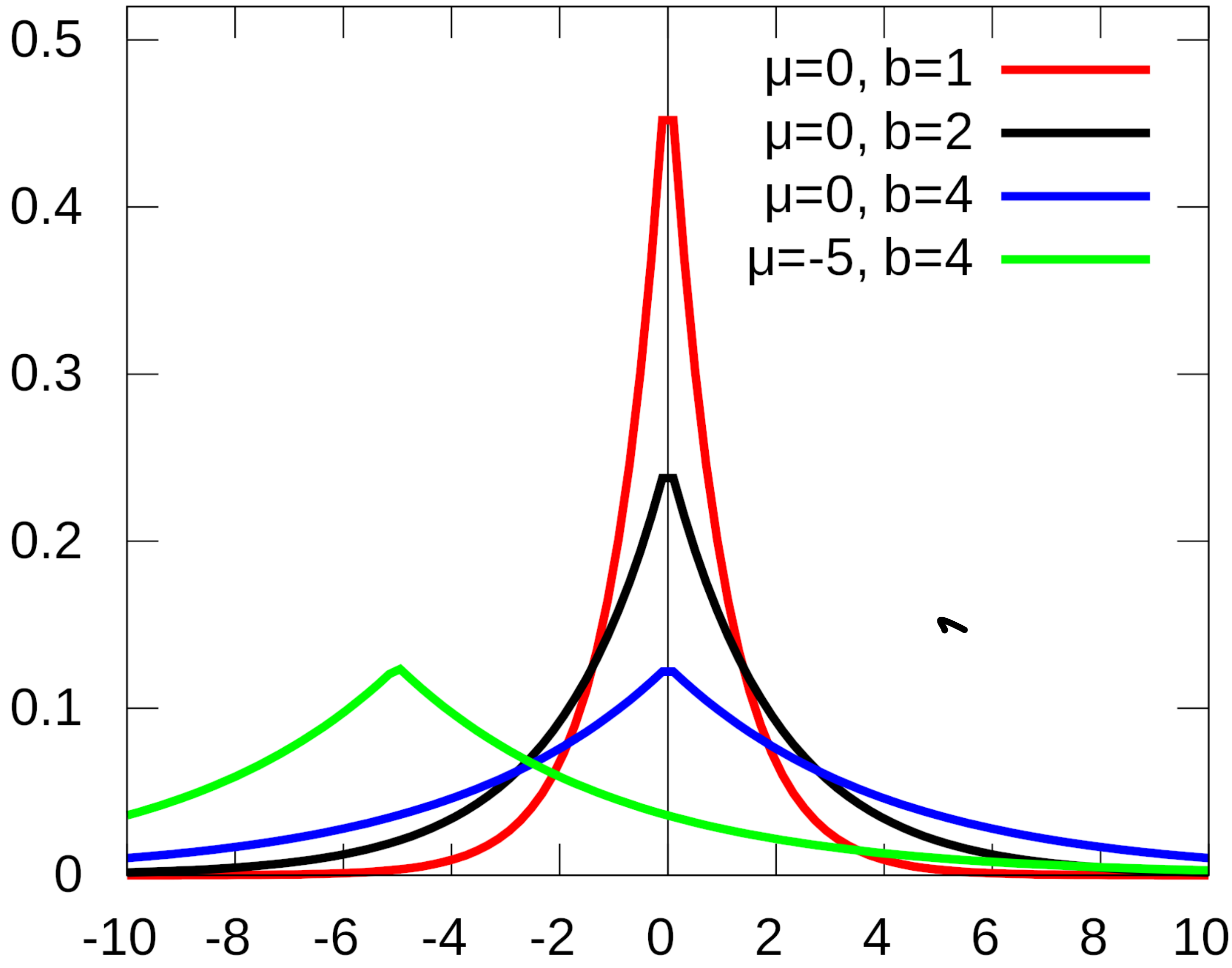
Def: A r.v. $X \in \mathbb{R}$ with p.d.f.

$$p(x) = \frac{1}{2b} \cdot e^{-\frac{|x|}{b}}$$

has Laplace distr. with param. b.

$X \sim Lap(b)$

$Var[X] = 2b^2$



Def: The <u>Laplace mechanism</u> for $M: \mathcal{X}^n \to \mathbb{R}^k$ and query function $f: \mathcal{X}^n \to \mathbb{R}^k$ is

$$M(X^n) = f(X^n) + [N_1, \ldots, N_k]$$

where $N_j \sim \mathrm{Lap}\left(\frac{\Delta}{\varepsilon}\right)$ are indep. r.v., Δ is sensitivity of f.

Ex. Again $f(X^n) = \frac{1}{n} \sum_i X_i$,

we output

$$Y = M(X^n) = f(X^n) + \underbrace{\mathrm{Lap}\left(\frac{1}{\varepsilon \cdot n}\right)}_{N}$$

because $\Delta = \frac{1}{n}$

$$E[Y] = E[f(X^n)]$$

$$\mathrm{Var}[N] = \frac{2}{\varepsilon^2 n^2} \quad \ldots$$

Thm: The Laplace mechanism for k-dim. queries and $\varepsilon > 0$ is ε-differentially private.

Pf: Let X^n and $\bar{X}^n$ s.t. $X^n \sim \bar{X}^n$.

Define

$p_X(y^k)$ and $p_{\bar{X}}(y^k)$ are p.d.f. of $M(X^n)$ and $M(\bar{X}^n)$, resp.

$$\frac{p_X(y^k)}{p_{\bar{X}}(y^k)} = \frac{\prod_j e^{-\varepsilon \frac{|f(X)_j - y_j|}{\Delta}}}{\prod_j e^{-\varepsilon \frac{|f(\bar{X})_j - y_j|}{\Delta}}}$$

$$= \prod_j e^{-\frac{\varepsilon}{\Delta}\left(\underbrace{|f(X)_j - y_j| - |f(\bar{X})_j - y_j|}_{|f(X_j) - f(\bar{X}_j)|}\right)}$$

$$\leq \prod_j e^{-\frac{\varepsilon}{\Delta}|f(\bar{X})_j - f(X_j)|}$$

$$= e^{\sum_j \frac{\varepsilon}{\Delta} \| f(X)_j - f(\bar{X})_j \|}$$

$$= e^{\frac{\varepsilon}{\Delta} \underbrace{\| f(X) - f(\tilde{X}) \|_1}}$$

by def. of Δ

$$\leq e^{\frac{\varepsilon}{\Delta} \cdot \Delta}$$

$$= e^{\varepsilon}.$$

<u>Ex.</u> Counting queries: How many values we $x \in \mathcal{X}$ have some property?

$$X_i \in \{0, 1\}, \quad f(X^n) = \sum_i X_i$$

$$\Delta = 1$$

ε-d.p. version of counting statistic is

$$f(X^n) + \mathrm{Lap}\left(\tfrac{1}{\varepsilon}\right).$$

Ex. Histogram:

$$f : \mathcal{X}^n \to \mathbb{N}^k$$

$$f(X^n) = [H_1, \dots, H_k]$$

where H_j counts number of $x \in \mathcal{X}^n$ with some property.

ℓ_1 - sensitivity of $f(\cdot)$?

2 because changing from one bin to another

$$Y = f(X^n) + [N_1, \dots, N_k]$$

where $N_j \sim \mathrm{Lap}\left(\frac{2}{\varepsilon}\right) \dots$

output

$$Y = [Y_1, \dots, Y_k]$$

is a εd.p. histogram.

6.4 Properties of D. P.

a) Postprocessing preserves D. P.

$M : \mathcal{X}^n \to \mathcal{Y}$

Postprocessing alg. $A : \mathcal{Y} \to \mathcal{Z}$

any randomized function

Thm: If M is ε-d.p. then $A \circ M$ is also ε-d.p.

Pf: For any $z \in \mathcal{Z}$

$$P[A(M(X^n)) = z]$$

$$= \sum_{y \in \mathcal{Y}} \underbrace{P[M(X^n) = y]} \cdot P[A(y) = z]$$

(by ε-d.p.) $$\leq \sum_{y \in \mathcal{Y}} e^{\varepsilon} P[M(\bar{X}^n) = y] \cdot P[A(y) = z]$$

$$= e^{\varepsilon} \cdot P[A(M(\bar{X}^n)) = z] .$$

Next week: Guest talk by Prof. Mathias Humbert (UNIL) on privacy and machine learning.