On the Relation Between Differential Privacy, Identifiability and Mutual-Information Privacy

Weina Wang, Lei Ying, and Junshan Zhang

ASU Arizona State University

Differential Privacy

- A mechanism satisfies ϵ-differential privacy if for any neighboring x, x' and any y

$$p_{Y|X}(y \mid x) \le e^{\epsilon} p_{Y|X}(y \mid x').$$

  - Indistinguishability between pairwise likelihoods.
  - Limited additional information leakage.
- The privacy–distortion problem under differential privacy (PD-DP):

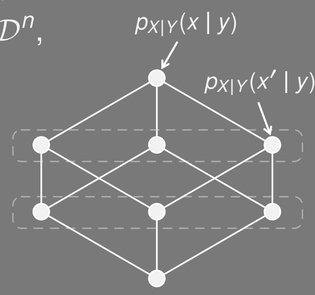
$$\min_{p_{Y|X}} \quad \sum_{x\in\mathcal{D}^n}\sum_{y\in\mathcal{D}^n} p_X(x)p_{Y|X}(y \mid x)d(x,y)$$

$$\text{subject to} \quad p_{Y|X}(y \mid x) \le e^{\epsilon_d} p_{Y|X}(y \mid x'),$$
$$\forall x, x' \in \mathcal{D}^n : x \sim x', \forall y \in \mathcal{D}^n,$$
$$p_{Y|X} \text{ is valid.}$$

Relaxed to the same problem:

$$\min_{p_{X|Y},\, p_Y} \quad \sum_{x\in\mathcal{D}^n}\sum_{y\in\mathcal{D}^n} p_Y(y)p_{X|Y}(x \mid y)d(x,y)$$

$$\text{subject to} \quad p_{X|Y}(x \mid y) \le e^{\epsilon} p_{X|Y}(x' \mid y),$$
$$\forall x, x' \in \mathcal{D}^n : x \sim x', \forall y \in \mathcal{D}^n,$$
$$p_{X|Y},\ p_Y \text{ are valid.}$$



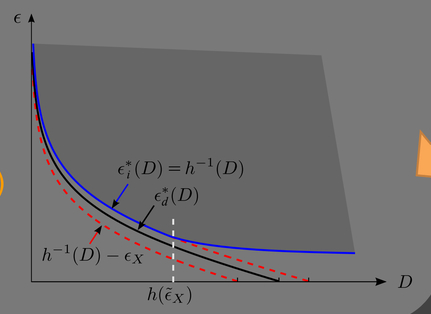
Optimal Solution:

$$p_{X|Y}(x \mid y) = \frac{e^{-\epsilon d(x,y)}}{\left(1 + (|\mathcal{D}| - 1)e^{-\epsilon}\right)^n}$$

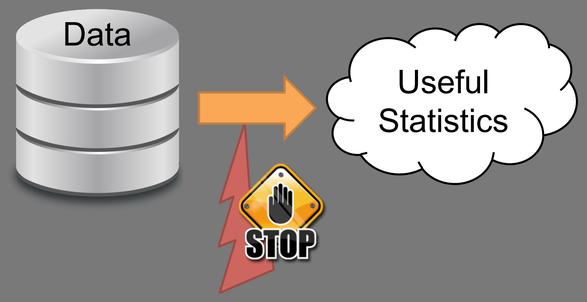
$$D^*(\epsilon) = h(\epsilon) \triangleq \frac{n}{1 + \frac{e^{\epsilon}}{|\mathcal{D}|-1}}$$

Main Result 1:

$$\epsilon_i^*(D) - \epsilon_X \le \epsilon_d^*(D) \le \epsilon_i^*(D)$$



Privacy-Preserving Data Analysis



Synthetic Database Releasing

- X, Y : $\mathcal{D}^n$-valued random variables; $X \sim p_X$.
- Neighbors on $\mathcal{D}^n$: $x \sim x'$ if x and x' differ on one entry.

Privacy–Distortion Tradeoff

$\epsilon^*(D) = \inf\{\epsilon : \epsilon\text{-privacy level is achievable with } \mathbb{E}[d(X,Y)] \le D\}$,

where d is the Hamming distance.

Identifiability

- A mechanism satisfies ϵ-identifiability if for any neighboring x, x' and any y

$$p_{X|Y}(x \mid y) \le e^{\epsilon} p_{X|Y}(x' \mid y).$$

  - Indistinguishability between pairwise posteriors.
  - Absolute guarantee.
- The privacy–distortion problem under identifiability (PD-I):

$$\min_{p_{X|Y},\, p_Y} \quad \sum_{x\in\mathcal{D}^n}\sum_{y\in\mathcal{D}^n} p_Y(y)p_{X|Y}(x \mid y)d(x,y)$$

$$\text{subject to} \quad p_{X|Y}(x \mid y) \le e^{\epsilon_i} p_{X|Y}(x' \mid y),$$
$$\forall x, x' \in \mathcal{D}^n : x \sim x', \forall y \in \mathcal{D}^n,$$
$$p_{X|Y},\ p_Y \text{ are valid, consistent with } p_X.$$

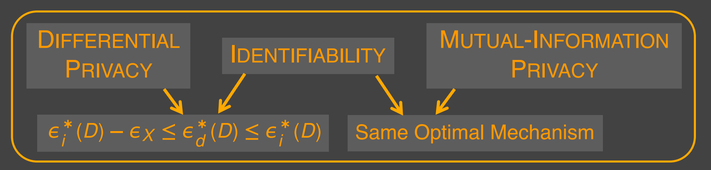
Mutual-Information Privacy

- A mechanism satisfies ϵ-mutual-information privacy if $I(X;Y) \le \epsilon$.
  - Average guarantee.
- The privacy–distortion problem under mutual-information privacy (PD-MIP):

$$\min_{p_{Y|X}} \quad I(X;Y)$$

$$\text{subject to} \quad \sum_{x\in\mathcal{D}^n}\sum_{y\in\mathcal{D}^n} p_X(x)p_{Y|X}(y \mid x)d(x,y) \le D,$$
$$p_{Y|X} \text{ is valid.}$$

  - Rate–distortion function.



Main Result 2:

Given a distortion requirement, the optimal mechanisms are the same.