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

Weina Wang, Lei Ying, and Junshan Zhang

DIFFERENTIAL PRIVACY
- A mechanism satisfies $\epsilon$-differential privacy if for any neighboring $x, x'$ and any $y$
  \[ p_{Y|X}(y | x) \leq e^\epsilon p_{Y|X}(y | x'). \]
- Indistinguishability between pairwise likelihoods.
- Limited additional information leakage.
- The privacy–distortion problem under differential privacy (PD-DP):
  \[
  \min_{p_{X|Y}, p_Y} \sum_{x \in D^n} \sum_{y \in D^n} p_X(x)p_{Y|X}(y | x)d(x, y)
  \]
  subject to \( p_{Y|X}(y | x) \leq e^\epsilon p_{Y|X}(y | x'), \)
  \( \forall x, x' \in D^n: x \sim x', \forall y \in D^n, \)
  \( p_{Y|X} \) is valid.

Optimal Solution:
\[
p_{X|Y}(y | x) = \frac{e^{-\epsilon d(x, y)}}{(1 + (|1| - 1)e^{-\epsilon})^n}.
\]

Main Result 1:
\[
\epsilon^* (D) - \epsilon x \leq \epsilon^*_D (D) \leq \epsilon^*_1 (D)
\]

IDENTIFIABILITY
- A mechanism satisfies $\epsilon$-identifiability if for any neighboring $x, x'$ and any $y$
  \[ p_{X|Y}(x | y) \leq e^\epsilon p_{X|Y}(x' | y). \]
- Indistinguishability between pairwise posteriors.
- Absolute guarantee.
- The privacy–distortion problem under identifiability (PD-I):
  \[
  \min_{p_{X|Y}, p_Y} \sum_{x \in D^n} \sum_{y \in D^n} p_X(x)p_{Y|X}(y | x)d(x, y)
  \]
  subject to \( p_{Y|X}(y | x) \leq e^\epsilon p_{Y|X}(y' | x | y), \)
  \( \forall x, x' \in D^n: x \sim x', \forall y \in D^n, \)
  \( p_{X|Y}, p_Y \) are valid, consistent with $p_X$.

Main Result 2:
Given a distortion requirement, the optimal mechanisms are the same.

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

Privacy–Distortion Tradeoff
\[
\epsilon^* (D) = \inf \{ \epsilon : \epsilon\text{-privacy level is achievable with } \mathbb{E}[d(X, Y)] \leq D \},
\]
where $d$ is the Hamming distance.

MUTUAL-INFO PRIVACY
- A mechanism satisfies $\epsilon$-mutual-information privacy if $I(X; Y) \leq \epsilon$.
- Average guarantee.
- The privacy–distortion problem under mutual-information privacy (PD-MIP):
  \[
  \min_{p_{X|Y}, p_Y} I(X; Y)
  \]
  subject to \( \sum_{x \in D^n} \sum_{y \in D^n} p_X(x)p_{Y|X}(y | x)d(x, y) \leq D, \)
  \( p_{Y|X} \) is valid.
- Rate–distortion function.