Session 7

Differential privacy

Reminder

A function (mechanism) F satisfies differential privacy if for all neighboring x, x', and all possible outputs S,

$$\frac{P\Big(F(x) = S\Big)}{P\Big(F(x') = S\Big)} \leq e^{\epsilon}$$

Reminder: Laplace Mechanism

For a function f with sensitivity s, define the Laplace mechanism

$$F(x) = f(x) + \text{Laplace}\left(\frac{s}{\epsilon}\right)$$

Reminder: Sensitivity

A function $f : \mathcal{D} \to \mathbb{R}$ has global sensitivity

$$\mathrm{GS}\, f = \max_{x, x'; d(x, x') = 1} |f(x) - f(x')| ,$$

where if x' is constructed from x by adding or removing one row, then $d(x, x') = 1$.

Reminder: Exponential Mechanism

We have

1. Set $\mathcal{R}$ of possible outputs
2. Scoring function $u : \mathcal{D} \times \mathcal{R} \to \mathbb{R}$ with sensitivity Δu
3. Output $r \in \mathcal{R}$ with probability

$$\propto \exp\left(\frac{\epsilon\, u(x, r)}{2\Delta u}\right)$$