DATA SECURITY AND PRIVACY

Introduction to Differential Privacy
• Differential Privacy: From Theory to Practice
  • Chapter 2: A Primer on Differential Privacy
Differential Privacy [Dwork et al. 2006]

- Definition: A mechanism $A$ satisfies $\varepsilon$-Differential Privacy if and only if
  - for any neighboring datasets $D$ and $D'$
  - and any possible transcript $t \in \text{Range}(A)$,
    \[
    \Pr[A(D)=t] \leq e^{\varepsilon} \Pr[A(D')=t]
    \]
  - For relational datasets, typically, datasets are said to be neighboring if they differ by a single record.

- Intuition:
  - Privacy is not violated if one’s information is not included in the input dataset
  - Output does not overly depend on any single record
Given a function \( f : D \rightarrow \mathbb{R}^d \) over an arbitrary domain \( D \), the **sensitivity** of \( f \) is
\[
S(f) = \max_{A,B \text{ where } A \Delta B = 1} \| f(A) - f(B) \|_1
\]

**Examples:**
1. **Count:** for \( f(D) = |D| \), \( S(f) = 1 \).
2. **Sum:** for \( f(D) = \Sigma d_i \), where \( d_i \in [0, \Lambda] \), \( S(f) = \Lambda \).

**Laplace Mechanism:** Calibrating noise to sensitivity

[DMNS’06]

Given a function \( f : D \rightarrow \mathbb{R}^d \) over an arbitrary domain \( D \), the computation
\[
M(X) = f(X) + \text{Laplace}(S(f)/\epsilon)^d
\]

provides \( \epsilon \)-differential privacy.

**Examples:**
1. **NoisyCount(D)** = \( |D| + \text{Laplace}(1/\epsilon) \).
2. **NoisySum(D)** = \( \Sigma d_i + \text{Laplace}(\Lambda/\epsilon) \).

\[
\Pr[M(A) \in S] \leq \Pr[M(B) \in S] \times \exp(\epsilon).
\]
Example of Laplace Mechanism

- Consider an example table of $N=23,450$ records with schema to the right?
- How many tuples are from IN?
  - True count: 546
- Answer while satisfying $\varepsilon_1$-DP: $546 + \text{Lap}(\Delta/\varepsilon_1)$
  - $\Delta = 1$
- How many people have score above 23?
- How many .....?

<table>
<thead>
<tr>
<th>Name</th>
<th>Score</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alice</td>
<td>20</td>
<td>CA</td>
</tr>
<tr>
<td>Bob</td>
<td>23</td>
<td>CA</td>
</tr>
<tr>
<td>Carl</td>
<td>25</td>
<td>IN</td>
</tr>
<tr>
<td>David</td>
<td>18</td>
<td>NY</td>
</tr>
<tr>
<td>.......</td>
<td>.......</td>
<td>.....</td>
</tr>
<tr>
<td>Frank</td>
<td>20</td>
<td>TX</td>
</tr>
<tr>
<td>Jane</td>
<td>14</td>
<td>IN</td>
</tr>
</tbody>
</table>
In general, counting queries can be answered relatively accurately

- Since one tuple affects the result by at most 1
- A small amount of noise (following the Laplace distribution) can be added to achieve DP
Suppose we are interested only in the score distribution, then we want to publish the histogram to the right.

- Add \( \text{Lap}(\Delta/\varepsilon) \) to each of the cell
- What is the sensitivity \( \Delta \)?
• In unbounded DP, D has one more record than D’
  • $\Delta$(histogram) = 1
• In bounded DP, D and D’ have the same number of records, and only one of them differ
  • $\Delta$(histogram) = 2
**Exponential Mechanism [MT’07]**

Let $q: \mathcal{D} \times \mathbb{R} \to \mathbb{R}$ be a query function that, given a database $d \in \mathcal{D}^n$, assigns a score to each outcome $r \in \mathbb{R}$.

Then the exponential mechanism $M$, defined by

$$M(d, q) = \{\text{return } r \text{ with probability } \propto \exp(\varepsilon q(d, r)/2S(q))\},$$

maintains $\varepsilon$-differential privacy.

**Reminder:**

$$S(q) = \max_{A, B \text{ where } A \Delta B = 1} \|q(A) - q(B)\|$$

**Motivation:**

$$\Pr(r) \propto \exp\left(\varepsilon \frac{q(d, r)}{2S(q)}\right)$$

Impact of changing a single record is within ±1

**Example - Private vote what to order for lunch:**

<table>
<thead>
<tr>
<th>Option</th>
<th>Score (votes)</th>
<th>Sensitivity=1</th>
<th>Sampling Probability ε=0</th>
<th>Sampling Probability ε=0.1</th>
<th>Sampling Probability ε=1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pizza</td>
<td>27</td>
<td>0.25</td>
<td>0.4</td>
<td>0.88</td>
<td></td>
</tr>
<tr>
<td>Salad</td>
<td>23</td>
<td>0.25</td>
<td>0.33</td>
<td>0.12</td>
<td></td>
</tr>
<tr>
<td>Hamburger</td>
<td>9</td>
<td>0.25</td>
<td>0.16</td>
<td>$10^{-4}$</td>
<td></td>
</tr>
<tr>
<td>Pie</td>
<td>0</td>
<td>0.25</td>
<td>0.11</td>
<td>$10^{-6}$</td>
<td></td>
</tr>
</tbody>
</table>
What is the median score?

- Define $q(D, x) = -|\# \text{ of students with score higher than } x - \# \text{ of students with score lower than } x|$

- What is the sensitivity?

  - I.e., what is $\max(|q(D, x) - q(D', x)|)$?
Properties of DP

- Sequential Composability
  - If $A_1$ satisfies $\varepsilon_1$-DP, and $A_2$ satisfies $\varepsilon_2$-DP, then outputting both $A_1$ and $A_2$ satisfies $(\varepsilon_1 + \varepsilon_2)$-DP

- Parallel Composability
  - If $D$ is divided into two parts, applying $A_1$ and $A_2$ on the two parts satisfy $(\max(\varepsilon_1, \varepsilon_2))$-DP

- Post-processing Invariance
  - If $A_1$ satisfies $\varepsilon_1$-DP, then $A_2(A_1(\cdot))$ satisfies $\varepsilon_1$-DP for any $A_2$
When designing a multiple-step algorithm for $\varepsilon$-DP, one needs to divide $\varepsilon$ into portions so that each step consumes some
Some queries are hard to answer

- E.g., max, since it can be greatly affected by a single tuple
Four Settings of Satisfying DP

- Local setting
  - Do not trust server, perturb data before sending to server

- Interactive setting
  - Answer queries as they come, not knowing what the rest of the queries are

- Single workload
  - Learn a few parameters

- Non-interactive publishing
  - Able to answer a broad range of queries
Limitation of Interactive Setting

- Answering each query consumes some privacy budget
- After answering a pre-determined number of queries, one exhausts the privacy budget, and cannot answer any question anymore
- Problem especially intractable when dealing with multiple users of data
Design a mechanism $A$, such that given $D$, one publishes $T=A(D)$.

Requirements

- Privacy friendly
  - Preventing adversaries from learning (individual) information from $O=A(D)$ and $A$
- Useful (fidelity-preserving)
  - Allow data users (researchers) to learn (aggregated) information from $O=A(D)$ and $A$