Privacy-preserving Release of Statistics: Differential Privacy

Anupam Datta
CMU

Fall 2014
Privacy-Preserving Statistics: Non-Interactive Setting

Goals:
- Accurate statistics (low noise)
- Preserve individual privacy (what does that mean?)

Database $D$ maintained by trusted curator
- Census data
- Health data
- Network data
- ...

Analyst

Sanitized Database $D'$

Add noise, sample, generalize, suppress
Privacy-Preserving Statistics: Interactive Setting

Goals:
• Accurate statistics (low noise)
• Preserve individual privacy (what does that mean?)
Classical Intuition for Privacy

• “If the release of statistics $S$ makes it possible to determine the value [of private information] more accurately than is possible without access to $S$, a disclosure has taken place.”  [Dalenius 1977]
  – Privacy means that anything that can be learned about a respondent from the statistical database can be learned without access to the database

• Similar to semantic security of encryption
Impossibility Result [Dwork, Naor 2006]

- **Result**: For reasonable “breach”, if sanitized database contains information about database, then some adversary breaks this definition.

- **Example**
  - Terry Gross is two inches shorter than the average Lithuanian woman.
  - DB allows computing average height of a Lithuanian woman.
  - This DB breaks Terry Gross’s privacy according to this definition... **even if her record is not in the database!**
Very Informal Proof Sketch

• Suppose DB is uniformly random
• “Breach” is predicting a predicate g(DB)
• Adversary’s background knowledge:
  \[ r, H(r ; \text{San(DB)}) \oplus g(DB) \]
  where H is a suitable hash function, r=H(DB)
• By itself, does not leak anything about DB
• Together with San(DB), reveals g(DB)
Differential Privacy: Idea

Released statistic is about the same if any individual’s record is removed from the database.

[Dwork, McSherry, Nissim, Smith 2006]
An Information Flow Idea

Changing input databases in a specific way changes output statistic by a small amount.
Not Absolute Confidentiality

Does not guarantee that Terry Gross’s height won’t be learned by the adversary
Differential Privacy: Definition

Randomized sanitization function $\kappa$ has $\varepsilon$-differential privacy if for all data sets $D_1$ and $D_2$ differing by at most one element and all subsets $S$ of the range of $\kappa$, $\Pr[\kappa(D_1) \in S] \leq e^\varepsilon \Pr[\kappa(D_2) \in S]$

Answer to query # individuals with salary > $30K is in range [100, 110] with approximately the same probability in $D_1$ and $D_2$
Achieving Differential Privacy: Interactive Setting

How much and what type of noise should be added?

User

Tell me $f(D)$

$f(D)+\text{noise}$

Database $D$

$x_1$

$\ldots$

$x_n$
Example: Noise Addition

- Say we want to release a summary $f(x) \in \mathbb{R}^p$
  - e.g., proportion of diabetics: $x_i \in \{0, 1\}$, $f(x) = \frac{1}{n} \sum x_i$
- Simple approach: add noise to $f(x)$
  - How much noise is needed?
- Intuition: $f(x)$ can be released accurately when $f$ is insensitive to individual entries $x_1, x_2, \ldots, x_n$
Global Sensitivity

\[ A(x) = f(x) + \text{noise} \]

- **Global Sensitivity:**
  \[ GS_f = \max_{\text{neighbors } x, x'} \| f(x) - f(x') \|_1 \]

  ➤ Example: \[ GS_{\text{proportion}} = \frac{1}{n} \]
Exercise

• Function $f$: # individuals with salary > $30K
• Global Sensitivity of $f = \ ?$

• Answer: 1
Background on Probability Theory
(see Oct 11, 2013 recitation)
Continuous Probability Distributions

• Probability density function (PDF), $f_X$

$$\Pr[a \leq X \leq b] = \int_a^b f_X(x) \, dx.$$

• Example distributions
  – Normal, exponential, Gaussian, Laplace
Laplace Distribution

PDF = \( \frac{1}{2b} \exp \left( -\frac{|x - \mu|}{b} \right) \)

Mean = \( \mu \)

Variance = \( 2b^2 \)

Laplace Distribution

➢ Laplace distribution Lap(λ) has density

\[ h(y) \propto e^{-|y|/\lambda} \]

➢ Changing one point translates curve

Change of notation from previous slide:

\[ x \rightarrow y \quad \mu \rightarrow 0 \]
\[ b \rightarrow \lambda \]
Achieving Differential Privacy
Laplace Mechanism

\[ A(x) = f(x) + \text{noise} \]

- Global Sensitivity: 
  \[ GS_f = \max_{\text{neighbors } x, x'} \| f(x) - f(x') \|_1 \]

- Example: 
  \[ GS_{\text{proportion}} = \frac{1}{n} \]

Theorem: If \( A(x) = f(x) + \text{Lap} \left( \frac{GS_f}{\epsilon} \right) \), then \( A \) is \( \epsilon \)-differentially private.
Laplace Mechanism: Proof Idea

**Theorem:** If $A(x) = f(x) + \text{Lap}\left(\frac{\text{GS}_f}{\epsilon}\right)$, then $A$ is $\epsilon$-differentially private.

Laplace distribution $\text{Lap}(\lambda)$ has density $h(y) \propto e^{-\frac{||y||_1}{\lambda}}$

Sliding property of $\text{Lap}\left(\frac{\text{GS}_f}{\epsilon}\right)$: $\frac{h(y)}{h(y+\delta)} \leq e^{\epsilon \frac{||\delta||}{\text{GS}_f}}$ for all $y, \delta$

**Proof idea:**
- $A(x)$: blue curve
- $A(x')$: red curve
- $\delta = f(x) - f(x') \leq \text{GS}_f$
Example: Noise Addition

- **Example: proportion of diabetics**
  - $GS_{proportion} = \frac{1}{n}$
  - Release $A(x) = \text{proportion} \pm \frac{1}{\epsilon n}$

- **Is this a lot?**
  - If $x$ is a random sample from a large underlying population, then sampling noise $\approx \frac{1}{\sqrt{n}}$
  - $A(x)$ “as good as” real proportion
Using Global Sensitivity

• Many natural functions have low global sensitivity
  – Histogram, covariance matrix, strongly convex optimization problems
Composition Theorem

• If \( A_1 \) is \( \varepsilon_1 \)-differentially private and \( A_2 \) is \( \varepsilon_2 \)-differentially private and they use independent random coins then \( \langle A_1, A_2 \rangle \) is \( (\varepsilon_1 + \varepsilon_2) \)-differentially private

• Repeated querying degrades privacy; degradation is quantifiable
Applications

- Netflix data set [McSherry, Mironov 2009; MSR]
  - Accuracy of differentially private recommendations (wrt one movie rating) comparable to baseline set by Netflix

- Network trace data sets [McSherry, Mahajan 2010; MSR]

<table>
<thead>
<tr>
<th>Packet-level analyses</th>
<th>High accuracy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Packet size and port dist.</td>
<td>strong privacy</td>
</tr>
<tr>
<td>Worm fingerprinting [27]</td>
<td>weak privacy</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Flow-level analyses</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Common flow properties [30]</td>
<td>strong privacy</td>
</tr>
<tr>
<td>Stepping stone detection [33]</td>
<td>medium privacy</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Graph-level analyses</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Anomaly detection [13]</td>
<td>strong privacy</td>
</tr>
<tr>
<td>Passive topology mapping [9]</td>
<td>weak privacy</td>
</tr>
</tbody>
</table>
Challenge: High Sensitivity

• Approach: Add noise proportional to sensitivity to preserve $\varepsilon$-differential privacy

• Improvements:
  – Smooth sensitivity [Nissim, Raskhodnikova, Smith 2007; BGU-PSU]
  – Restricted sensitivity [Blocki, Blum, Datta, Sheffet 2013; CMU]
Challenge: Identifying an Individual’s Information

• Information about an individual may not be just in their own record

  – Example: In a social network, information about node A also in node B *influenced* by A, for example, because A may have caused a link between B and C
Differential Privacy: Summary

• An approach to releasing privacy-preserving statistics
• A rigorous privacy guarantee
  – Significant activity in theoretical CS community
• Several applications to real data sets
  – Recommendation systems, network trace data,
• Some challenges
  – High sensitivity, identifying individual’s information, repeated querying