CS573 Data Privacy and Security

Differential Privacy – Real World Deployments

Li Xiong
Applying Differential Privacy

• Real world deployments of differential privacy

– OnTheMap  
– RAPPOR  
– Chrome
The maps above show LODES data in New York City in the OnTheMap application. The map on the left shows employment by census block in Lower Manhattan (in dense urban areas one census block is often equivalent to one city block). Large, dark dots have more employment than small, light dots. The map on the right shows the residential patterns of the same workers (those employed in Lower Manhattan). Workers employed in Lower Manhattan live throughout New York City as well as in New Jersey and other areas of New York state.
Why privacy is needed?

US Code: Title 13 CENSUS

It is against the law to make any publication whereby the data furnished by any particular establishment or individual under this title can be identified.

Violating the statutory confidentiality pledge can result in fines of up to $250,000 and potential imprisonment for up to five years.
Synthetic Data and US Census

• U.S. Census Bureau uses synthetic data to share data from Survey of Income and Program Participation, American Community Survey, Longitudinal Business Database and OnTheMap

• Only OnTheMap has formal privacy guarantee.

[HMKGAV15] proposed differentially private algorithms to release the rest of the attributes.
Applying Differential Privacy

- Real world deployments of differential privacy
  - OnTheMap
  - RAPPOR
  - Chrome

Module 4
Tutorial: Differential Privacy in the Wild
A dilemma

• Cloud services want to protect their users, clients and the service itself from abuse.

• Need to monitor statistics of, for instance, browser configurations.
  – Did a large number of users have their home page redirected to a malicious page in the last few hours?

• But users do not want to give up their data
Problem

What are the frequent unexpected Chrome homepage domains?

⇒ To learn malicious software that change Chrome setting without users’ consent

finance.com

fashion.com

weirdstuff.com

[Erlingsson et al CCS’14]
Why privacy is needed?

Liability (for server)
Storing unperturbed sensitive data makes server accountable (breaches, subpoenas, privacy policy violations)
**Randomized Response** (a.k.a. local randomization)

<table>
<thead>
<tr>
<th>D</th>
<th>Disease (Y/N)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Y</td>
<td></td>
</tr>
<tr>
<td>Y</td>
<td></td>
</tr>
<tr>
<td>N</td>
<td></td>
</tr>
<tr>
<td>Y</td>
<td></td>
</tr>
<tr>
<td>N</td>
<td></td>
</tr>
<tr>
<td>N</td>
<td></td>
</tr>
</tbody>
</table>

With probability $p$, 
Report true value

With probability $1-p$, 
Report flipped value

<table>
<thead>
<tr>
<th>O</th>
<th>Disease (Y/N)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Y</td>
<td></td>
</tr>
<tr>
<td>N</td>
<td></td>
</tr>
<tr>
<td>N</td>
<td></td>
</tr>
<tr>
<td>N</td>
<td></td>
</tr>
<tr>
<td>Y</td>
<td></td>
</tr>
<tr>
<td>N</td>
<td></td>
</tr>
</tbody>
</table>
Differential Privacy Analysis

• Consider 2 databases $D, D'$ (of size $M$) that differ in the $j^{th}$ value
  
  $- D[j] \neq D'[j]$. But, $D[i] = D'[i]$, for all $i \neq j$

• Consider some output $O$

\[
\frac{P(D \rightarrow O)}{P(D' \rightarrow O)} \leq e^\varepsilon \iff \frac{1}{1 + e^\varepsilon} < p < \frac{e^\varepsilon}{1 + e^\varepsilon}
\]
Utility Analysis

• Suppose \( n_1 \) out of \( n \) people replied “yes”, and rest said “no”

• What is the best estimate for \( \pi = \text{fraction of people with disease} = Y \)?

\[
\hat{\pi} = \frac{n_1/n - (1-p)}{2p-1}
\]

• \( E(\hat{\pi}) = \pi \)

• \( \text{Var}(\hat{\pi}) = \frac{\pi(1-\pi)}{n} + \frac{1}{n(16(p-0.5)^2 - 0.25)} \)

  Sampling  Variance due to coin flips
Using Randomized Response

• Using Randomized Response
  – Each bit collects 0 or 1 for a predicate value

• Challenges:
  – Arbitrarily large strings
  – Longitudinal attack (repeated responses over time)

• Rappor solution:
  – Use bloom filter
  – Use two levels of randomized response: permanent, instantaneous
Client Input Perturbation

• Step 1: Compression: use $h$ hash functions to hash input string to $k$-bit vector (Bloom Filter)

Why Bloom filter step?
Simple randomized response does not scale to large domains (such as the set of all home page URLs)
Bloom filter

- Approximate set membership problem
- Generalized hashtable
- k-bit vector, h hash functions, each function hashes an element to one of the bits
- Tradeoff space with false positive (no false negative)
Permanent RR

• Step 2: Permanent randomized response $B \rightarrow B'$
  - With user tunable probability parameter $f$
  - $B'$ is memorized and will be used for all future reports

\[ B'_i = \begin{cases} 
1, & \text{with probability } \frac{1}{2} f \\
0, & \text{with probability } \frac{1}{2} f \\
B_i, & \text{with probability } 1 - f 
\end{cases} \]
Instantaneous RR

• Step 4: Instantaneous randomized response $B' \rightarrow S$
  – Flip bit value 1 with probability $1-q$
  – Flip bit value 0 with probability $1-p$
Instantaneous RR

- **Step 4:** Instantaneous randomized response $B' \rightarrow S$
  - Flip bit value 1 with probability $1-q$
  - Flip bit value 0 with probability $p$

$$P(S_i = 1) = \begin{cases} q, & \text{if } B'_i = 1. \\ p, & \text{if } B'_i = 0. \end{cases}$$
**Instantaneous RR**

- **Step 4:** Instantaneous randomized response $B' \rightarrow S$
  - Flip bit value 1 with probability $1-q$
  - Flip bit value 0 with probability $1-p$

---

**Why randomize two times?**

- Chrome collects information each day
- Want perturbed values to look different on different days to avoid linking
Server Report Decoding

- Estimates bit frequency from reports $\tilde{f}(D)$
- Use cohorts (groups of users)
Differential Privacy of RAPPOR

• Permanent randomized response
• Instantaneous randomized response
• Assume no temporal correlations
  – Extreme example: report age by days
Parameter Selection (Exercise)

• Recall RR for a single bit
  — RR satisfies $\varepsilon$-DP if reporting flipped value with probability $1 - p$, where $\frac{1}{1+e^\varepsilon} \leq p \leq \frac{e^\varepsilon}{1+e^\varepsilon}$

• Question 1: if Permanent RR flips each bit in the $k$-bit bloom filter with probability $1-p$, which parameter affects the final privacy budget?
  1. # of hash functions: $h$
  2. bit vector size: $k$
  3. Both 1 and 2
  4. None of the above
Parameter Selection (Exercise)

- **Answer:** # of hash functions: $h$
  - Remove a client’s input, the maximum changes to the true bit frequency is $h$. 

RAPPOR Demo

http://google.github.io/rappor/examples/report.html

Simulation Input

- Number of clients: 100,000
- Total values reported / obfuscated: 700,000
- Unique values reported / obfuscated: 50

RAPPORT Parameters

- \( k \): Size of Bloom filter in bits, 16
- \( h \): Hash functions in Bloom filter, 2
- \( m \): Number of Cohorts, 64
- \( p \): Probability \( p \), 0.5
- \( q \): Probability \( q \), 0.75
- \( f \): Probability \( f \), 0.5
Utility: Parameter Selection

- $h$ affects the utility most compared to other parameters.
Other Real World Deployments

- Differentially private password Frequency lists [Blocki et al. NDSS ‘16]
  - release a corpus of 50 password frequency lists representing approximately 70 million Yahoo! users
  - varies from 8 to 0.002
- Human Mobility [Mir et al. Big Data ’13]
  - synthetic data to estimate commute patterns from call detail records collected by AT&T
  - 1 billion records ~ 250,000 phones
- Apple will use DP [Greenberg. Wired Magazine ’16]
  - in iOS 10 to collect data to improve QuickType and emoji suggestions, Spotlight deep link suggestions, and Lookup Hints in Notes
  - in macOS Sierra to improve autocorrect suggestions and Lookup Hints
Summary

• A few real deployments of differential privacy
  – All generate synthetic data
  – Some use local perturbation to avoid trusting the collector
  – No real implementations of online query answering

• Challenges in implementing DP
  – Covert channels can violate privacy

• Need to understand requirements of end-to-end data mining workflows for better adoption of differential privacy.
References


D. J. Mir; S. Isaacman; R. Caceres; M. Martonosi; R. N. Wright, “DP-WHERE: Differentially private modeling of human mobility”, Big Data 2013

F. McSherry, “PINQ: Privacy Integrated Queries”, SIGMOD 2009


J. Reed, B. Pierce, M. Gaboardi, “Distance makes types grow stronger: A calculus for differential privacy”, ICFP 2010


A. Smith, "Privacy-preserving statistical estimation with optimal convergence rates", STOC 2011

I. Mironov, “On significance of the least significant bits for differential privacy ppt”, CCS 2012