The Privacy of the Analyst and The Power of the State

Moni Naor
Weizmann Institute of Science

Joint work with Cynthia Dwork and Salil Vadhan
The Privacy of the Analyst

Loaded term: We use **Differential Privacy**

The Power of the State

How to maintain the privacy of the **queries**, not only the data

The issue of maintaining PFA arises only if there is coordination in noise – state. Show that this is necessary.
Lots of Data

Recent years: a lot of data is available to companies and government agencies

- Census data
- Huge databases collected by companies
  - Data deluge
- Public Surveillance Information
  - CCTV
  - RFIDs
- Social Networks

Data contains **personal** and **confidential** information
Social benefits from analyzing large collections of data

John Snow’s map
Cholera cases in London epidemic of 1854

Water Pump on Broad Street

Cholera cases
Social benefits from analyzing large collections of data

What about Privacy?

• Better Privacy Better Data

• Almost any usage of the data that is not carefully crafted will leak something about it
Privacy of Public Data Analysis

The holy grail:

Get utility of statistical analysis while protecting privacy of every individual participant

Ideally:

Privacy-preserving sanitization should allow reasonably accurate answers to meaningful information

Is it possible to phrase the goal in a meaningful and achievable manner?
Setting for the talk

Database → Curator/Sanitizer → Released data
Setting for the talk: Interactive case

Multiple queries, chosen adaptively
“Pure” Privacy Problem

- Difficult Even if
  - Curator is Angel
  - Data are in Vault

Nevertheless: tight connection to problems in cryptography

You can run but you can’t hide
Databases that Teach

• Database teaches that smoking causes cancer.
  – Smoker S’s insurance premiums rise.
  – This is true even if S not in database!

• Learning that smoking causes cancer is the whole point.
  – Smoker S enrolls in a smoking cessation program.

• **Differential privacy:** limit harms to the *teachings*, not participation
  – Outcome of any analysis is essentially equally likely, independent of whether any individual joins, or refrains from joining, the dataset.
Differential Privacy

Protect *individual* participants:

Dwork, McSherry, Nissim & Smith 2006
Differential Privacy

Sanitizer \( M \) gives \( \varepsilon \)-differential privacy if:

for all adjacent \( D_1 \) and \( D_2 \), and all \( A \in \text{range}(M) \):

\[
\Pr[M(D_1) \in A] \leq e^{\varepsilon} \Pr[M(D_2) \in A]
\]

Participation in the data set poses no additional risk
Example of Differential Privacy

\( X \) set of \((\text{name}, \text{tag} 2 \{0, 1\})\) tuples

One query: \# of participants with \text{tag}=1

Sanitizer: output \# of 1's + noise

- noise from \text{Laplace distribution} with parameter \(1/\varepsilon\)
- \(\Pr[\text{noise} = k-1] \approx e^\varepsilon \Pr[\text{noise}=k]\)
\((\varepsilon, \delta)\) - Differential Privacy

Sanitizer \(M\) gives \((\varepsilon, \delta)\) -differential privacy if:
for all adjacent \(D_1\) and \(D_2\), and all \(A \in \text{range}(M)\):
\[
\Pr[M(D_1) \in A] \leq e^{\varepsilon} \Pr[M(D_2) \in A] + \delta
\]

Typical setting \(\varepsilon = \frac{1}{10}\) and \(\delta\) negligible

This talk: \(\delta\) negligible
Differential Privacy

Hugely successful:
• Algorithms in many setting and for many tasks

Important Properties:
• Composability
  – Applying the sanitization several time yields a graceful degradation

• Robustness to side information
  – No need to specify exactly what the adversary knows
Counting Queries

Q is a set of predicates $q: U \mapsto \{0, 1\}$

Query: how many $x$ participants satisfy $q$?

Relaxed accuracy:
answer query within $\alpha$ additive error w.h.p

Not so bad: some error anyway inherent in statistical analysis
Laplacian Mechanism for Counting Queries

Given query $q$:
1. Compute true answer $q(x)$
2. Output $q(x) + \text{Lap}\left(\frac{1}{\varepsilon}\right)$

- Handle $t$ online queries by adding $\text{Lap}(1/\varepsilon)$ independently
  - Privacy loss $o\left(\frac{t}{\varepsilon}\right)$
  - Can do better with $(\varepsilon, \delta)$-DP - $O\left(\frac{\sqrt{t}}{\varepsilon}\right)$

Need $t$ which is $o(n)$ ($\delta = 0$) and $o(n^2)$

Question: Can we handle number of queries $\ll n$?
Key Insight: Use **Coordinated Noise**

Starting from Blum-Ligget-Roth 2008:

- If noise is added in with careful coordination, rather than independently, can answer **hugely** many queries.

Wave of results showing:

- Differential Privacy for **every** set $Q$ of counting queries.
- Error is $\tilde{O}(n^{1/2} \log|Q|)$.

- Even in the interactive case - Roth & Roughgarden
- Private Multiplicative Weights Algorithm – Hardt and Rothblum
The PMW Algorithm

Maintain a distribution \( d \) on universe \( U \)

Initialize with \( d \)

Repeat

- Set \( a = R(q) \) - Lap(\( \mu \))

  - Repeat while no progress
    - Test: \( |q(D) \hat{a}| \leq \hat{t} \)
      - Output \( q(D) \).
    - Else (update): Output \( \hat{a} \)

Multiplicative Weights

- Powerful tool in algorithms design
- Learn a Probability Distribution iteratively
- In each round:
  - either current distribution is good
  - Or get a lot of information on distribution
- Update distribution

This is the state. Is completely public!

Algorithm fails if more than \( k \) updates
Overview: Privacy Analysis

For the query family $Q = \{0,1\}^U$ for $(\beta, \delta, \varepsilon)$ and $\dagger$ the PMW mechanism is

- $(\varepsilon, \delta)$ – differentially private
- $(\alpha, \beta)$ accurate for up to $\dagger$ queries where
  $$\alpha = \tilde{O}(1/(\varepsilon n)^{1/2})$$

- State = Distribution is privacy preserving for individuals (but not for queries)

Log dependency on $|U|$, $\delta$, $\beta$ and $\dagger$
Is coordination necessary?

The PMW Algorithm (and its predecessors) maintains state between queries

• Is this essential?

State may (and does!) leak information about other queries

• Can independent servers with no coordination provide the answers?
  – Efficiency
Privacy for the Analyst

• Data analysts may desire confidentiality for the questions they ask
  – Fear of embarrassment,
  – Persecution
  – Leakage to competitors
  – Law enforcement: indicate to the criminals about the investigation.
Privacy for the Analyst

Allowing carrying out research in privately: well-recognized principle of a free society

• Council of the American Library Association

``strongly recommends that the responsible officers of each library...

Advise all librarians and library employees that such records shall not be made available to any agency of state, federal, or local government except pursuant to such process, order or subpoena"
Results I: Statefulness is essential for handling very large numbers of queries

- A stateless differentially private algorithm cannot answer more than $\Omega(n^2)$ counting queries
  - where $n$ is the number of rows in the database.
  - bound is tight up to polylog factors.
  - exponential gap between the number of queries that can be answered by stateless and stateful mechanisms.

- Proof relies on “list-decoding”
Results I: Statefulness is essential for handling very large numbers of queries

Result can be interpreted as

- it is impossible to have **perfect privacy** for the data analysts, if we have differential privacy for the dataset.

Can also be interpreted as

- A negative result about **distributing the work** of answering queries among servers while maintaining differential privacy. Either:
  - Servers must share information about queries being asked or
  - Can only answer a small number of queries.
Results II: Privacy for the Analysts

If we want privacy for both the data subjects and the data analysts:

• Must look at stateful algorithms,

• Settle for less than perfect privacy for the data analysts
  – Something like differential privacy for the analysts

• Assume every analyst is assigned an ID,
  – ID is given to the mechanism along with every query made by that analyst
Results II: Privacy for the Analysts

Construct a stateful mechanism that:

• Is differentially private for the data subjects
• Can answer up to an exponential number of counting queries
• Provides analyst privacy:
  – view of any **one analyst** has approximately the same distribution regardless of what other queries are asked by **all of the other analysts**.

Event occurs with the same probability up to a
• $1+\varepsilon$ multiplicative factor
• negligible $\delta$ additive factor
Stateless Mechanism

Initial coordination Information

Call $M : 2^U \times Q \mapsto R$ a stateless query release mechanism
Known Stateless Mechanisms

- Independent noise
- Randomized Response

The mechanism generates a fictitious database \( \hat{x} \) that is weakly correlated with the original database \( x \),

- For all \( w \in U \setminus x \) we have \( \Pr[w \in \hat{x}] = \frac{1}{2} \)
- For all \( w \in x \) we have \( \Pr[w \in \hat{x}] = \frac{1}{2} + \varepsilon \)

- To answer query \( q \): answer with the right expectation

Expected error \( o(1) \) provided that \( |U| = o(n^2) \).

answer every query \( q \) according to them.

- Expected error \( o(1) \) for non adaptive queries
- provides only \((O, \tilde{O}(\text{polylog}n/n))\) Differential Privacy
Why Coordination is Necessary

• Being stateless implies* \( \frac{1}{4} \) the responses can be thought as a **fixed** function

• Will show that can generate correlated responses with a function of an unknown individual \( \xi \)
  – The dictator function
  – Inner product

• Proof relies on the list-decoding properties of
  – “long code”
  – Goldreich Levin
Totally informed reidentification game

1. Let $\mathbf{x}$ be a uniformly random subset of $\mathbf{U}$ of size $n$.
2. Let $\xi$ be a uniformly random element of $\mathbf{x}$.
3. Feed the set $\xi^c = \mathbf{x} \setminus \{\xi\}$ to $A$, who then outputs a query sequence $q^{(1)}, q^{(2)}, \ldots, q^{(t)}$.
4. $A$ obtains responses $y= (y^{(1)}, y^{(2)}, \ldots, y^{(t)})$ from $M$.
5. $A$ then outputs a probability distribution $p$ on $\mathbf{U}$.

• $A$'s payoff is (by definition) $p(\xi)^{1/2}$.
  - The expectation $E[p(\xi)^{1/2}]$ is over all the randomness in the game.
Differentially Privacy and Reidentification

Proposition: If $\mathcal{M} : 2^U \times Q \mapsto R$ is an $(\varepsilon, \delta)$-differential privacy query release mechanism, then:

• for every adversary $A$, the expected payoff in the totally informed reidentification game is at most

$$e^{\varepsilon} \cdot \frac{1}{(U-n+1)^{1/2}} + \delta$$
Theorem: State is Essential

Let $\mathcal{M} : 2^U \times Q \mapsto R$ be a stateless query release mechanism that has expected error at most $1 - \gamma$ and supports $t \geq cn^2 \log |U|$ queries.

- Then there is an adversary, running in time $\text{poly}(n, t, |U|)$ that achieves payoff $\gamma/n$ in the totally informed reidentification game.
- In particular, if $\gamma = \Omega(1)$, $|U| = \omega(n^2)$, $\varepsilon = O(1)$, and $\delta = o(1/n)$, then $\mathcal{M}$ cannot be $(\varepsilon, \delta)$-differential privacy.
State is Essential: the queries

\( A(\xi^c) \):

- Choose \( k \) \( \tilde{A} \{0, 1, ..., n\} \)
- Choose \( q_0: \xi^c \to \{-1,1\} \) such that
  - \( q_0(w) = 1 \) for exactly \( k \) elements \( w \in \xi^c \)
  - \( q_0(w) = -1 \) for remaining \( n-k-1 \) elements \( w \in \xi^c \)
- For \( j = 1, 2, ..., \dagger \)
  - Select \( q_1(j): U \setminus \xi^c \to \{-1,1\} \) uniformly at random,
  - (b) Let \( q^{(j)} = (q_0, q_1^{(j)}) \)
  
  the \textit{predicate} that is \( q_0 \) on \( w \in \xi^c \) and is \( q_1^{(j)} \) on \( w \in U \setminus \xi^c \)
- Output the queries \( (q^{(1)}, q^{(2)}, ..., q^{(\dagger)}) \) – Non adaptively

Switch from \( \{0,1\} \) to \( \{-1,1\} \)

Used in all queries
State Is Essential: The reconstruction

- The responses to \((q^{(1)}, q^{(2)}, ..., q^{(t)})\) are \((y^{(1)}, y^{(2)}, ..., y^{(t)})\)

Adversary computes \(c(w)\) for each \(w \in \mathcal{U} \setminus \xi^c\)

\[
c(w) = \frac{1}{t} \cdot \sum_{j=1}^{t} q_0(w) y^{(j)}
\]

- Outputs (any) probability distribution that assigns each element \(w \in \mathcal{U} \setminus \xi^c\) probability (at least)

\[
p(w) = \max \{c(w) - \gamma/(2n), 0\}
\]

If \(\sum_w p(w) > 1\) then fail
...State Is Essential: The reconstruction

• Fix $x = (\xi, \xi^c)$, $k$ and $q_0$.

• Now the expectation of $c(w)$ is the correlation between the function $g : \{\pm 1\}^U \setminus \xi^c \mapsto [-1,1]$

$$g(q_1) = E_j[M^{(j)}(x, (q_o, q_1))]$$

and the dictator function $\chi_w$ which maps $q_1$ to $q_1(w)$

$$E[c(w)] = hg, \chi_w i = E_{q_1}[g(q_0) \chi_w(q_0)]$$

• Setting $p(w) = \max\{c(w) - \gamma/2n, 0\}^2$

  - assign positive probability to all $w$ s. t. $g$ has significant correlation $\chi_w$. 
• Completely uncorrelated with $\chi_w$ for $w \neq \xi$
• Completely correlated with $\chi_w$ for $w = \xi$

For a reasonably accurate noisy mechanism $M$:
• the responses must be on the correlated with (most) elements in the database, and independent of (most) elements outside of the database.
...State Is Essential: The reconstruction

Claim: $E[p(\xi)^{1/2}] \geq \frac{\gamma}{2n}$

Claim: with probability at least $1 - \frac{\gamma}{4n}$ we have

$$\sum_w p(w) \cdot 1$$

Therefore the expected payoff of $A$ is at least

$$E[p(\xi)^{1/2}] - Pr[\sum_w p(w) \geq 1] \geq \frac{\gamma}{2n} - \frac{\gamma}{4n}$$

which is $\Omega(\frac{\gamma}{n})$
Smaller Error Case

If the error is smaller than adversary needs to know less about the database to succeed:

- In case the expected error is a relatively small $\alpha$ (instead of being close to 1), can modify $A$ where it only knows $n' = (\alpha + \gamma)n$ rows
  - The adversary succeeds with probability $\Omega(\gamma/n'^2)$
Stateful Mechanisms with IDs

For a

- data universe $U$
- a query family $Q = \{q : 2^U \rightarrow R\}$ and
- an ID space $I$,

a **stateful query mechanism with analyst IDs**

$$M : 2^U \times Q \times I \times S \rightarrow R \times S,$$

is a randomized function taking a database $x \times 2^U$, a query $q \in Q$, an analyst id $i \in I$, and a state $s \in S$ and outputs an answer $y \in R$ and a new state $s'$. 

intended to be an approximation of $q(x)$
Accuracy for Stateful Mechanisms

A stateful query mechanism with analyst IDs

\[ M : 2^U \triangleleft Q \triangleleft I \triangleleft S \mapsto R \triangleleft S, \]

is \((\alpha, \beta)\) accurate for \(t\) queries if for every database

\(x \in 2 \times 2^U\) and every randomized adversary \(A\) that

• adaptively queries \(M\) with queries \(q^{(1)}, q^{(2)}, \ldots, q^{(t)}\)
• and receives responses \(y=(y^{(1)}, y^{(2)}, \ldots, y^{(t)})\),

with probability at least \(1-\beta\) all the responses differ from the true answer by at most \(\alpha\)
**Analyst Privacy for Stateful Mechanisms**

\( M \) provides \((\varepsilon, \delta)\)-many-to-one analyst privacy if for every database \( x \in 2^{2^U} \), \( id \in 2^I \), and every two "honest" query strategies \( H_0 \) and \( H_1 \), for every adversary \( A \) that issues queries under \( id \), the view of \( A \) are \((\varepsilon, \delta)\)-indistinguishable whether \( H = H_0 \) or \( H = H_1 \):

- \( A \) and \( H \) interact with \( M \) where \( A \) determines when \( H \) gets to make queries and how many
  - but does not see the queries made or the responses that can issue queries with any ID other than \( id \).
Theorem: Analyst Privacy is Achievable for Stateful Mechanisms

For the query family $Q = \{0,1\}^U$ for $(\beta, \delta, \epsilon, \epsilon')$ and $t$ there is a stateful query mechanism with analyst IDs that is

- $(\epsilon, \delta)$–differentially private
- $(\epsilon', \beta)$ many-to-one analyst privacy
- $(\alpha, \beta)$ accurate for up to $t$ queries where

$$\alpha = \tilde{O}(1/(\epsilon n)^{1/4} (\epsilon')^{1/2})$$

Log dependency on $|U|$, $\delta$, $\beta$ and $t$
Two Level Approach

**In charge of privacy of the data**

PMW\textsubscript{inner}

**In charge of privacy of the analysts**

PMW\textsubscript{outer}

Outer layer

ID=1

ID=2

ID=3

Inner layer
Two Level Approach

Algorithm utilizes a single, long-lived, inner instantiation of the PMW algorithm, $PMW_{inner}$

- provides privacy for the data subjects over all the queries posed by all the analysts.
- rely on the differential privacy properties of PMW not on any specific characteristics

For each analyst id we spawn an `outer` instantiation of PMW, denoted $PMW_{id}$

- The outer $PMW_{id}$ algorithms do not access the database directly, only through $PMW_{inner}$. 
Security of the Two Level Approach

Combine the **accuracy** properties of PMW\textsubscript{inner} with the **privacy** properties of PMW\textsubscript{id}.

- Regardless of the other questions, PMW\textsubscript{inner} responds to PMW\textsubscript{id} with answers that are within $\pm \alpha$ of what the `bare’ database would have provided – except with probability at most $\beta$.
- We show that the **output** distribution of PMW\textsubscript{id} is approximately the same had it accessed the database directly.

True for any stateful oracle that provides $\pm \alpha$ accuracy.
Future Directions: Collusion

Mechanism PFA does not resist collusion among analysts
– privacy for the data is completely protected by the inner PMW.
– Some sort of recursion can help with this, but the deterioration in accuracy is devastating after about $\log \log n$ levels - protection only against very small coalitions.
– Can this be improved? Might cryptographic techniques help?
Future Directions: Error Complexity

• Is it the case that analyst-private differentially private algorithms have larger errors than vanilla differentially private algorithms?

• Our two-level scheme (PFA) yields accuracy that is quadratically worse than a single instantiation of PMW.
  – PMW can answer counting queries to within $\tilde{O}(1/n^{1/2})$
  – PFA can answer counting queries to within $\tilde{O}(1/n^{1/4})$
Future Directions: Analyst-Oblivious Algorithms

- Is there an analyst-private algorithm in which the curator can remain **oblivious** of the sources of the queries?
- Communication / Query Tradeoff:
- Other types of queries