CS 599: Formal Methods in Security and Privacy
Differential Privacy

Marco Gaboardi
gaboardi@bu.edu

Alley Stoughton
stough@bu.edu
Releasing the mean of Some Data

\[
\text{Mean}(d : \text{private data}) : \text{public real}
\]

\[
i := 0;
\]

\[
s := 0;
\]

\[
\text{while } (i < \text{size}(d))
\]

\[
s := s + d[i]
\]

\[
i := i + 1;
\]

\[
\text{return } (s/i)
\]
Releasing the mean of Some Data

\textbf{Mean}(d : \text{private data}) : \text{public real}
\begin{align*}
i &:= 0; \\
s &:= 0; \\
\text{while } (i < \text{size}(d)) &\quad \text{do} \\
\quad s &:= s + d[i] \\
\quad i &:= i + 1; \\
\text{return } (s/i)
\end{align*}
Privacy-preserving data analysis?

We want to release some information to a data analyst and protect the privacy of the individuals contributing their data.
Privacy-preserving data analysis?

We want to release some information to a data analyst and protect the privacy of the individuals contributing their data.

Differential Privacy: the idea

A. Haeberlen

3 USENIX Security (August 12, 2011)

Private data

N(flue, >1955)?

826±10

N(brain tumor, 05-22-1955)?

3 ±700

Noise

Differential Privacy:

Ensuring that the presence/absence of an individual has a negligible statistical effect on the query's result.

Trade-off between utility and privacy

q1

q2

…

qk
Differential Privacy: motivation

A. Haeberlen

Motivation: Protecting privacy

USENIX Security (August 12, 2011)

I know Bob is born 05-22-1955 in Philadelphia...

A first approach: anonymization.

Using different correlated anonymized data sets one can learn private data.
Fundamental Law of Information Reconstruction

The release of too many overly accurate statistics permits reconstruction attacks.
Reconstruction attack

Differential Privacy:
Ensuring that the presence/absence of an individual has a negligible statistical effect on the query's result.

Trade-off between utility and privacy.

Motivation: Protecting privacy.

A first approach: anonymization.

Using different correlated anonymized data sets one can learn private data.

To anonymize data:

- Add noise
- Apply anonymization techniques

By adding noise, we can make it difficult for an attacker to reconstruct the original data.

Attacker
Reconstruction attack
Reconstruction attack

Differential Privacy: the idea

Promising approach: Differential privacy

Differential Privacy: ensuring that the presence/absence of an individual has a negligible statistical effect on the query's result.

Trade-off between utility and privacy.

Differential Privacy: motivation

Motivation: Protecting privacy

Data

I know Bob is born 05-22-1955 in Philadelphia…

A first approach: anonymization.

Using different correlated anonymized data sets one can learn private data.

Reconstruction attack

Attacker
Reconstruction attack

Differential Privacy: the idea

Promising approach: Differential privacy

USENIX Security (August 12, 2011)

Private data

\[ N(\text{flu}, 1955) ? \]
\[ 826 \pm 10 \]

\[ N(\text{brain tumor}, 05-22-1955) ? \]
\[ 3 \pm 700 \]

Noise

Differential Privacy: Ensuring that the presence/absence of an individual has a negligible statistical effect on the query's result.

Trade-off between utility and privacy.

Differential Privacy: motivation

USENIX Security (August 12, 2011)

Motivation: Protecting privacy

\[ D \]
\[ q_1 \]
\[ q_2 \]
\[ \ldots \]
\[ q_k \]

Attacker

I know Bob is born 05-22-1955 in Philadelphia…

A first approach: anonymization.

Using different correlated anonymized data sets one can learn private data.

Reconstruction attack

\[ q_1 \]
\[ q_2 \]
\[ \ldots \]
\[ q_k \]

Attacker

\[ D \]
Differential Privacy: ensuring that the presence/absence of an individual has a negligible statistical effect on the query's result.

Reconstruction attack

D → Noise → q1 → q2 → ... → qk → D'
Reconstruction attack

We say that the attacker wins if

$$d(D, D') \sim 0$$
Reconstruction attack

We say that the attacker wins if

$$d(D, D') \sim 0$$

In this class case we can use Hamming distance
Privacy vs Utility
Quantitative notions of Privacy

- The impossibility results discussed above suggest a quantitative notion of privacy,
- a notion where the privacy loss depends on the number of queries that are allowed,
- and on the accuracy with which we answer them.
Differential privacy: understanding the mathematical and computational meaning of this trade-off.

[Dwork, McSherry, Nissim, Smith, TCC06]
Privacy-preserving data analysis?

- The analyst knows no more about me after the analysis than what she knew before the analysis.
Privacy-preserving data analysis?

- The analyst knows no more about me after the analysis than what she knew before the analysis.
Privacy-preserving data analysis?

- The analyst knows no more about me after the analysis than what she knew before the analysis.

Differential Privacy: the idea of ensuring that the presence/absence of an individual has a negligible statistical effect on the query's result. This balances utility and privacy, allowing for data analysis without compromising individual privacy.
Privacy-preserving data analysis?

Prior Knowledge

~

Posterior Knowledge
Privacy-preserving data analysis?
Privacy-preserving data analysis?

**Question:** What is the problem with this requirement?
Privacy-preserving data analysis?

If nothing can be learned about an individual, then nothing at all can be learned at all!

[DworkNaor10]
Privacy-preserving data analysis?

• The analyst learn *almost the same* about me after the analysis as what she would have learnt if I *didn’t contribute my data.*
Privacy-preserving data analysis?

• The analyst learn almost the same about me after the analysis as what she would have learnt if I didn’t contribute my data.
Privacy-preserving data analysis?

- The analyst learn almost the same about me after the analysis as what she would have learnt if I didn’t contribute my data.

Differential Privacy: the idea of ensuring that the presence/absence of an individual has a negligible statistical effect on the query's result. There's a trade-off between utility and privacy.

\[ q_1 \quad q_2 \quad \ldots \quad q_k \]
Privacy-preserving data analysis?

- The analyst learn almost the same about me after the analysis as what she would have learnt if I didn’t contribute my data.

Differential Privacy: the idea of ensuring that the presence/absence of an individual has a negligible statistical effect on the query’s result.

Trade-off between utility and privacy.
Privacy-preserving data analysis?

- The analyst learn **almost the same** about me after the analysis as what she would have learnt if I didn’t contribute my data.

Differential Privacy: the idea

A. Haeberlen

USENIX Security (August 12, 2011)

Private data

N(flue, >1955)?

826±10

N(brain tumor, 05-22-1955)?

3 ±700

Differential Privacy:

Ensuring that the presence/absence of an individual has a negligible statistical effect on the query’s result.

Trade-off between utility and privacy.

q1

q2

…

qk
Adjacent databases

• We can formalize the concept of contributing my data or not in terms of a notion of distance between datasets.

• Given two datasets \( D, D' \in DB \), their distance is defined as:

\[
D \Delta D' = |\{ k \leq n \mid D(k) \neq D'(k) \}|
\]

• We will call two datasets adjacent when \( D \Delta D' = 1 \) and we will write \( D \sim D' \).
Privacy Loss

In general we can think about the following quantity as the **privacy loss** incurred by observing $r$ on the databases $b$ and $b'$.

$$\text{L}_{b,b'}(r) = \log \left( \frac{\text{Pr}[Q(b)=r]}{\text{Pr}[Q(b')=r]} \right)$$
(ε,δ)-Differential Privacy

**Definition**

Given ε,δ ≥ 0, a probabilistic query Q: X^n → R is (ε,δ)-differentially private iff for all adjacent database b_1, b_2 and for every S ⊆ R:

\[ \Pr[Q(b_1) \in S] \leq \exp(\varepsilon) \Pr[Q(b_2) \in S] + \delta \]
Differential Privacy

$Q : \text{db} \Rightarrow \mathbb{R}$ probabilistic

$Q(b \cup \{x\})$

$Q(b \cup \{y\})$
Differential Privacy

\[ d(Q(b \cup \{x\}), Q(b \cup \{y\})) \leq \varepsilon \quad \text{with probability } 1 - \delta \]
\[(\varepsilon, \delta)\text{-Differential Privacy}\]

\[
\left| \log \frac{\Pr[Q(b_1)=r]}{\Pr[Q(b_2)=r]} \right| \leq \varepsilon
\]

with probability \(1-\delta\)
(ε, δ)-indistinguishability

Statistical distance:

\[ \Delta(\mu_1, \mu_2) = \max_{E \subseteq A} | \mu_1(E) - \mu_2(E) | = \delta \]

can be seen as a notion of δ-indistinguishability.

We say that two distributions \( \mu_1, \mu_2 \in D(A) \), are at δ-indistinguishable if:

\[ \Delta(\mu_1, \mu_2) \leq \delta \]
(ε,δ)-indistinguishability

We can define a ε-skewed version of statistical distance. We call this notion ε-distance.

\[ \Delta_\varepsilon(\mu_1, \mu_2) = \sup_{E \subseteq A} \max(\mu_1(E) - e^{\varepsilon}\mu_2(E), \mu_2(E) - e^{\varepsilon}\mu_1(E), 0) \]

We say that two distributions \( \mu_1, \mu_2 \in \mathcal{D}(A) \), are at (ε,δ)-indistinguishable if:

\[ \Delta_\varepsilon(\mu_1, \mu_2) \leq \delta \]
c is **differentially private** if and only if for every $m_1 \sim m_2$ (extending the notion of adjacency to memories):

$$\{c\}_{m_1} = \mu_1 \text{ and } \{c\}_{m_2} = \mu_2 \text{ implies } \Delta_\varepsilon(\mu_1, \mu_2) \leq \delta$$
Releasing the mean of Some Data

\[
\text{Mean}(d : \text{private data}) : \text{public real}
\]
\[
i := 0;
\]
\[
s := 0;
\]
\[
\text{while } (i < \text{size}(d))
\]
\[	\quad s := s + d[i]
\]
\[	\quad i := i + 1;
\]
\[
\text{return } (s/i)
\]
Adding Noise

**Question:** What is a good way to add noise to the output of a statistical query to achieve $(\varepsilon,0)$-DP?
Adding Noise

**Question:** What is a good way to add noise to the output of a statistical query to achieve \((\varepsilon,0)\)-DP?

**Intuitive answer:** it should depend on \(\varepsilon\) or the accuracy we want to achieve, and on the scale that a change of an individual can have on the output.
Global Sensitivity

\[ GS_q = \max \{ |q(D) - q(D')| \text{ s.t. } D \sim D' \} \]
Global Sensitivity

$$\text{GS}_q = \max \{ | q(D) - q(D') | \text{ s.t. } D \sim D' \}$$
Global Sensitivity

\[ GS_q = \max \{ | q(D) - q(D') | \text{ s.t. } D \sim D' \} \]
Global Sensitivity

\[ GS_q = \max \{ | q(D) - q(D') | \text{ s.t. } D \sim D' \} \]
Laplace Distribution

\[ \text{Lap}(b, \mu)(X) = \frac{1}{2b} \exp \left( - \frac{|\mu - X|}{b} \right) \]

- The variance of the Laplace distribution is \( \sigma^2 = 2b^2 \).
- The Laplace distribution centered in 0 has the symmetric shape of two exponential distributions with symmetry axis in 0. The parameter \( b \) describes how "concentrated" the distribution is, see Figure 1.1 for two examples.

To ensure a bound on the privacy loss we need to calibrate the additive noise to the possible influence that a single individual can have on the result of the numeric query. This influence is captured by the notion of global sensitivity.

**Definition 1.8 (Global sensitivity).**

\[ \text{Global sensitivity} \] of a function \( q: \mathbb{R}^n \rightarrow \mathbb{R} \) is:

\[ \text{Global sensitivity} = \max_{\Delta D} \left| q(D) - q(D') \right| \]

Intuitively, smaller the global sensitivity of a function is and less impact a single individual has on the result of the function. So, when the global sensitivity is small we can add less noise to provide the same protection. This is the intuition behind the Laplace mechanism.

We use the notation \( \exp(c) \) for \( e^c \) for making the formulas easier to read.

Following the literature on differential privacy we use here the term "mechanism", there this is used as a synonym of algorithm, program, etc. It doesn't have any other special meaning.

\( b \) regulates the skewness of the curve,
Releasing privately the mean of Some Data

```
Mean(d : private data) : public real
    i:=0;
    s:=0;
    while (i<size(d))
        s:=s + d[i]
        i:=i+1;
    z:=$ Laplace(sens/eps,0)
    z:= (s/i)+z
    return z
```
Laplace Mechanism

Lap(d : priv data)(f: data -> real)
   (e:real) : pub real
   z:=\text{Laplace}(GS_f/e,0)
   z:= f(d)+z
   return z
Laplace Mechanism

\[
\text{Lap}(d : \text{priv data})(f: \text{data} \rightarrow \text{real}) (e: \text{real}) : \text{pub real}
\]
\[
z := \text{Laplace}(G_{S_f}/e, 0)
\]
\[
z := f(d) + z
\]
\[
\text{return } z
\]

It turns out that we could also write it as:

\[
\text{Lap}(d : \text{priv data})(f: \text{data} \rightarrow \text{real}) (e: \text{real}) : \text{pub real}
\]
\[
z := \text{Laplace}(G_{S_f}/e, f(d))
\]
\[
\text{return } z
\]
Theorem (Privacy of the Laplace Mechanism)
The Laplace mechanism is \((\varepsilon,0)\)-differentially private.

**Proof:** Intuitively

Figure 1.2 gives a graphical intuition of the privacy proof. If we assume that \(q\) is \(c\)-sensitive and we consider \(q(D)\) and \(q(D')\) we know that they differ for at most \(c\). By adding to both of them noise according to the Laplace distribution with scale \(\theta\) we obtain two distributions whose means are at most at distance \(c\), and whose shape is given by the Laplace distribution, as depicted in Figure 1.2. Notice that the scale of the two distribution is independent from their mean and it is equal for both of them. Two such Laplace distributions have the property that for each point \(z\) the ratio of their pdf evaluated in \(z\) lies in the interval \([e^{-\varepsilon},e^{\varepsilon}]\).
Laplace Mechanism

**Question:** How accurate is the answer that we get from the Laplace Mechanism?