Distributed Trust and Blockchains		Date:	*14-November-2019*
Instructor: *Sujit Prakash Gujar*		Scribes:	Bhavi Dhingra Shaily Mishra

Lecture 18: Differential Privary (contd.)

Contents

1 Recap

What is the likelihood that if x gives O output, y gives O output

$$\ln\left(\frac{Pr(M(x)=O)}{Pr(M(y)=O)}\right) \leq \epsilon$$

The LHS of the above inequality is termed as *Privacy Loss*.
The above condition holds for ϵ differential privacy.

1.1 Random Mechanism - 1

Toss a coin

- If H: respond x_i
- If T: toss coin again
  - If H: respond 1
  - If T: respond 0

$x = (x_1, ..., x_i, ..., x_n)$
$y = (\tilde{x}_1, ..., \tilde{x}_i, ..., \tilde{x}_n)$

$where, x_i, \tilde{x}_i \in \{0, 1\}$

$$\ln\left(\frac{Pr(\tilde{x}_i=1 \mid x_i=1)}{Pr(\tilde{x}_i=1 \mid x_i=0)}\right) = \ln\left(\frac{3/4}{1/4}\right) = \ln 3 \quad \leftarrow (\textbf{High Privacy Loss})$$

1.2 Random Mechanism - 2

$$\tilde{x}_i = \begin{cases} x_i & \text{with probability } \left(\frac{e^\epsilon}{e^\epsilon+1}\right) \\ \bar{x}_i & \text{with probability } \left(\frac{1}{e^\epsilon+1}\right) \end{cases}$$

$$\begin{aligned} \text{Privacy Loss} &= \ln\left(\frac{Pr(\tilde{x}_i=1 \mid x_i=1)}{Pr(\tilde{x}_i=1 \mid x_i=0)}\right) \\ &= \ln\left(\left(\frac{e^\epsilon}{e^\epsilon+1}\right) / \left(\frac{1}{e^\epsilon+1}\right)\right) \\ &= \ln\left(e^\epsilon\right) \\ &= \epsilon \quad \leftarrow (\textbf{Better Mechanism}) \end{aligned}$$

$\epsilon = 0$ implies complete randomness

2 General Mechanism

- Add noise to the answer such that,
  - Each answer doesn't leak too much info about the database
  - Noisy answer is close to the original answer
- Noise is added through the Laplace distribution which is similar to normal distribution. Primary difference is that Laplace distribution has a sharper peak.
- Laplacian mechanism works for any function with a real number as an output

$x = (x_1, \ldots, x_n)$
$y = (x_1, \ldots, x_n, x_{n+1})$

$where, x_i \in \{0, 1\}$

Query is mean query i.e. $\mu_x = \frac{1}{n}\sum_{i=1}^{n} x_i$

Output will be $\mu_x + noise$
$noise = Lap\left(\frac{1}{\epsilon n}\right)$, with $mean = 0$, and, $variance = \frac{1}{\epsilon n}$

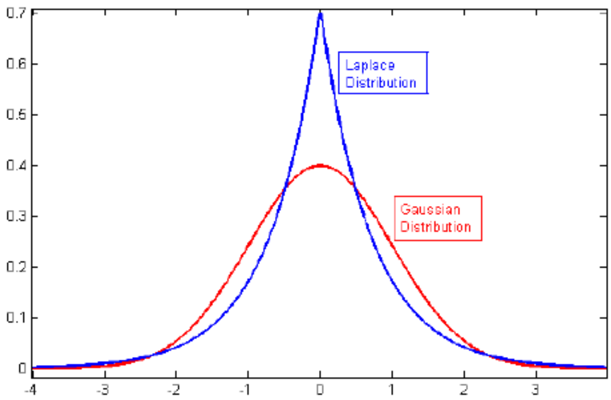

Figure 1: Laplace and Gaussian Distributions

$f(x|\mu, b) = \frac{1}{2b} e^{\frac{-|x-\mu|}{b}}$
where,
  $\mu : mean$
  $b : variance$

x y have different dimensions
So, we will use a new representation

x = (1's, 0's)
y = (1's, 0's)

x = (n-k, k) — $k \in [0, n]$

There are four possibilities for y
$y = (n-k-1, k)$
$\quad = (n-k+1, k)$
$\quad = (n-k, k-1)$
$\quad = (n-k, k+1)$

2.1 Calculating privacy loss when x = (n-k, k) and y = (n-k+1, k)

$PrivacyLoss = \ln\left(\frac{Pr(M(x)=z \mid x=(n-k,k))}{Pr(M(y)=z \mid y=(n-k+1,k))}\right)$
Output, $M(x) = z = \mu_x + noise$
$\quad \implies noise = z - \mu_x$

Noise is Lap$\left(\frac{1}{\epsilon n}\right)$, thus, $f\,(x|\mu, b) = \frac{\epsilon n}{2} e^{-|x-\mu|\epsilon n}$

$$
\begin{aligned}
\implies \text{Privacy Loss} &= \ln\left(\frac{\frac{\epsilon n}{2} e^{-|z-\mu_x|\epsilon n}}{\frac{\epsilon n}{2} e^{-|z-\mu_y|\epsilon n}}\right) \\
&= \ln e^{\epsilon n(|z-\mu_y|-|z-\mu_x|)} \\
&\leq \ln e^{\epsilon n|\mu_x-\mu_y|} \\
&\leq \epsilon n|\mu_x - \mu_y| \\
&\leq \epsilon
\end{aligned}
$$

Since, $\mu_y = \frac{n\mu_x+1}{n+1}$ $\leftarrow$ (this will change according to which y we are selecting)
$\implies |\mu_x - \mu_y| \leq \frac{1}{n+1}$

Thus,
$\epsilon \to 0$: high privacy, low utility
$\epsilon \to \infty$: low privacy, high utility

2.2 Risk (Error)

$Risk = \mathbb{E}\,(\text{true answer - noisy answer})^2$
We know that, noisy answer = true answer + noise

$$
\begin{aligned}
\implies Risk &= \mathbb{E}\,(\text{noise})^2 \\
&= Var\left(Lap\left(\tfrac{1}{\epsilon n}\right)\right) \\
&= \frac{1}{\epsilon^2 n^2} \qquad \left(\epsilon < \tfrac{1}{n}\right)
\end{aligned}
$$

3 Query output is not a real no.

When query output is a real no., we use *Laplace Mechanism*.
What if it's not a real no.?

$f : Z_+^{|X|} \to \mathbb{R}^k$ (k dimensional output)

$M(x) = f(x) + (y_1, y_2, ..., y_k)$

We add Laplace noise for each dimension.

$y_i = Lap\left(\frac{\alpha}{\epsilon}\right)$ (What will α be?)

$$
\begin{aligned}
PrivacyLoss &= \ln\left(\frac{Pr(M(x) = z \mid x)}{Pr(M(y) = z \mid y)}\right) \\
&= \ln\left(\frac{\prod_{i=1}^{k} Pr(y_i = z_i - (f(x))_i)}{\prod_{i=1}^{k} Pr(y_i = z_i - (f(y))_i)}\right) \\
&= \ln\left(\frac{\prod_{i=1}^{k} \frac{\epsilon}{2\alpha} e^{\left(\frac{-|z_i - f(x)_i \mid \epsilon}{\alpha}\right)}}{\prod_{i=1}^{k} \frac{\epsilon}{2\alpha} e^{\left(\frac{-|z_i - f(y)_i \mid \epsilon}{\alpha}\right)}}\right) \\
&\leq \ln \prod_{i=1}^{k} e^{\frac{\epsilon |f(x)_i - f(y)_i|}{\alpha}} \\
&= \ln e^{\frac{\epsilon ||f(x) - f(y)||_1}{\alpha}}
\end{aligned}
$$

For this to be ϵ - differential private:
$\alpha = ||f(x) - f(y)||_1$

Since, we don't know $||f(x) - f(y)||_1$, we take the maximum possible:

$\Delta f = sup\ ||f(x) - f(y)||_1$ (L_1 sensitivity of f)

thus, $\alpha = \Delta f$

$$
\begin{aligned}
PrivacyLoss &= \ln e^{\frac{\epsilon\ ||f(x)\ -\ f(y)||}{\Delta f}} \\
&\leq \epsilon
\end{aligned}
$$

4 Sensitivity

For $f : D -> R^k$, the sensitivity of f is

$$\Delta f = max_{\mathrm{D_1 D_2}} \left\|(f(D_1) - f(D_2))\right\|_1 \tag{1}$$

For all D_1 , D_2 differing in atmost one element.
The sensitivity is represented as Δf and the query is represented as function f
The sensitivity of query helps us understand how much an individual's data influences the calculations and consequently the amount of noise that needs to be added
The sensitivty of f is normally small and consequently in most scenarios, the DP alogirthm doesn't need to add much noise.
Large Sensitivity when the value of ϵ is fixed serves as a warning that more noise needs to be added to mask the data

5 $(\epsilon\ \delta)$ differential privacy

- When $\epsilon << 1$

$$P_r(M(x) \in E) \leq e^{\epsilon} P_r(M(y) \in E) \tag{2}$$

is similiar to

$$P_r(M(x) \in E) \leq (1+\epsilon) P_r(M(y) \in E) \tag{3}$$

For very small x i.e. x<<1

$$e^x \equiv 1 + x$$

- $\forall E \subset S$, $\forall x, y$ s.t.
$\|(x-y)\|_1$

$$P_r(M(x) \in E) \leq e^{\epsilon} P_r(M(y) \in E) + \delta \tag{4}$$

  - we don't use δ unless we can guarantee that $\delta < \frac{1}{n}$
  - $(\epsilon, 0)$ we always achieve ϵ - differential privacy
  - (ϵ, δ), we can achieve ϵ-differential privacy with probability $\frac{1}{1-\delta}$

- Instead of Laplace noise, we add guassian noise (0,σ^2) , where $\sigma = \frac{\Delta_2 f \sqrt{c \ln(\frac{1}{\delta})}}{\epsilon}$, where $\Delta_2 f$ is L_2 sensitivity

$$\delta_2 = \sup_{\|(x-y)\|_1} \|(f(x) - f(y))\|_2$$

and

$$c^2 \geq 2 \ln(\frac{1.25}{\delta})$$

then it is (ϵ, δ) differential private

- Risk (in 2013) : $\mathcal{O}(\frac{d}{\epsilon n})$ where d is the no. of bits in each row.
On average : $\tilde{\mathcal{O}}(\frac{d}{\epsilon n})$
Currently the risk is (2016) : $\mathcal{O}(\frac{\sqrt{d \ln \frac{1}{\delta}}}{\epsilon n})$

References

[1] https://www.cis.upenn.edu/~aaroth/Papers/privacybook.pdf

[2] https://medium.com/georgian-impact-blog/a-brief-introduction-to-differential-privac

[3] http://sigmod2017.org/wp-content/uploads/2017/03/04-Differential-Privacy-in-the-wild-1.pdf