Distributed Trust and Blockchains		Date:	*November 11th, 2019*
Instructor: *Sujit Prakash Gujar*		Scribes:	Anurag Jain, Raviteja Vinjam

Lecture 17: Exploring Mechanisms for Differential Privacy

1 Recap

1. A randomized algorithm is defined as $\mathbf{M} : \mathbb{Z}_+^X \to \triangle(S)$ where $X = \{t_1, t_2, .., t_k\}$
   $x \in (x_1, x_2, \ldots, x_k)$ and each x_i represents number of entries of type t_i
2. **ϵ-Differential Privacy:** $\mathbf{M}$ is said to provide ϵ-differential privacy if $\forall x, y$ such that $\|x - y\|_1 = 1$ (where $\|x - y\| = \sum_{i=1}^{k} |x_i - y_i|$ represents the L1-Norm) then,
   $Pr[M(x) \in E] \leq e^{\varepsilon} Pr[M(y) \in E]$

2 Quantifying Privacy

ϵ can be considered as a measure of privacy loss, $\varepsilon \geq \ln\left(\frac{Pr[M(x)=0]}{Pr[M(y)=0]}\right)$

2.1 Coin Toss Example

Let $x_i = \begin{cases} 1 & \text{if a certain property is true} \\ 0 & \text{otherwise.} \end{cases}$
and an algorithm $\mathbf{M}$ defined as follows:

- Flip a coin
- If the output was 'Tails' then output x_i, otherwise
- Flip the coin again and output 1 if 'Heads' and 0 if tails

$$\frac{Pr\left(\frac{\tilde{x_i}=1}{x_i=1}\right)}{Pr\left(\frac{\tilde{x_i}=1}{x_i=0}\right)} = \frac{\frac{1}{2}+\frac{1}{4}}{\frac{1}{4}} = \frac{3}{4} = 3$$

$\varepsilon = \ln 3$

2.2 A Mechanism for Arbitrary ϵ-Differential Privacy

$$\tilde{x_i} = \begin{cases} X_i \text{ with probability } \dfrac{e^{\varepsilon}}{e^{\varepsilon}+1} \\ \bar{X_i} \text{with probability } \dfrac{1}{e^{\varepsilon}+1} \end{cases} \tag{1}$$

3 Some Results on Differential Privacy

Theorem 1. *Let $f : S \mapsto S'$ be a mapping on the output of ϵ-differentially private mechanism $\mathbf{M}$, then $f(\mathbf{M})$ is also ϵ-differentially private*

Proof Intuition *Given :*

$$Pr[f \circ M(x) \, \epsilon \, E] \leq e^{\varepsilon} Pr[M(y) \, \epsilon \, E]$$
$$and \; E_2 = \{x \, \epsilon \, S \mid f(x) \, \epsilon \, E_1\}$$

(Refer figure 1)

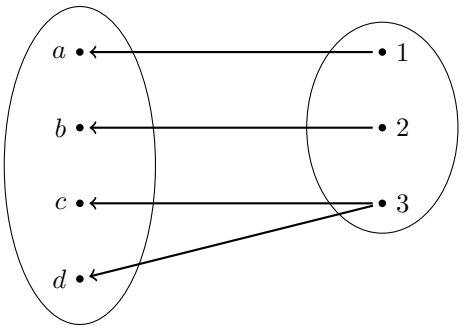

Figure 1: Mapping diagram of inverse relation f^{-1}

$$\begin{aligned} & Pr[f \circ M(x) \, \epsilon \, E_1] = Pr[M(x) \, \epsilon \, E_2] \\ \implies & Pr[f \circ M(x) \, \epsilon \, E_1] \leq e^{\varepsilon} Pr[M(y) \, \epsilon \, E_2] \\ \implies & Pr[f \circ M(x) \, \epsilon \, E_1] \leq e^{\varepsilon} Pr[f \circ M(y) \, \epsilon \, E_1] \end{aligned}$$

Theorem 2. *Any ϵ-differentially private mechanism is $k\epsilon$ group differentially private for a group of size k*
Proof left as an excercise for the reader

4 Advantages of Differential Privacy

1. Mitigates linkage attacks by providing protection against re-identification
2. Quantification of privacy loss, we can choose an ε suitably by analysing the tradeoff between accuracy and privacy. This is an important parameter to tune as people will not share their data unless their reward by doing so is more than the expected penalty from privacy loss.
3. Composition does not increase privacy loss. This provides guarantee against all possible techniques available to the adversary.
4. Provides Group Privacy in a similar manner.

5 A Mechanism for Summary Statistics

Consider a Mean Query

$$\mu = \frac{\sum_{i=1}^{n} x_i}{n}$$

consider a function Noise(z) the additive noise introduced by our mechanism.

$$\tilde{\mu} = \mu + \text{Noise}(z)$$

5.1 Laplacian Noise

For ease of analysis let us consider our Noise as Laplacian Noise with mean 0 and variance $\frac{1}{\varepsilon n}$. Recall that a random variable has a Laplace(μ, b) distribution if its probability density function is

$$f(x \mid \mu, b) = \frac{1}{2b} \exp\left(-\frac{|x-\mu|}{b}\right)$$

$$= \frac{1}{2b} \begin{cases} \exp\left(-\frac{\mu - x}{b}\right) & \text{if } x < \mu \\ \exp\left(-\frac{x-\mu}{b}\right) & \text{if } x \geq \mu \end{cases}$$

Where μ is a location parameter and $b > 0$, which is sometimes referred to as the diversity, is a scale parameter. [Wikipedia contributors, 2019]

References

[Wikipedia contributors, 2019] Wikipedia contributors (2019). Laplace distribution — Wikipedia, the free encyclopedia. [Online; accessed 17-November-2019].