A Brief Introduction To Differential Privacy

LI Xiaofeng

HKUST(GZ)

2025-03-19

Outline

Outline

Outline

The differential privacy algorithm is very important in protecting the data privacy of individuals. The algorithm is used in data analysis, machine learning, and statistics.

- DP-SGD: Adding noises to the gradient while training the model
- US used differential privacy to protect the 2020 census data [1].

[1] Differential Privacy and Applications, IEEE Digital Privacy

Outline

2.1 Scenario

- A company want to analyze the incomes of the employees and publish many features about the data.
- The attacker could infer such sensitive data of **individual** from the published data.

I know your salary level!

Attacker

That’s my sensitive data!

Victim

Outline

3.1 Preliminary Concepts

To obtain such a mechanism, we need to define the following mathmatical concepts:

Query: A query is a function that takes a dataset as input and returns a real number, denoted by $f : \boldsymbol{X} \mapsto \mathbb{R}$

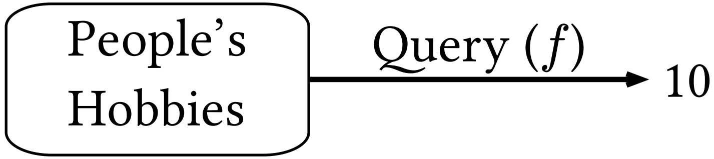

Figure 1: The query function.

3.1 Preliminary Concepts

Classical Probability distribution:

- Laplace Distribution: $f(x) = \frac{1}{2b}\exp\left(-\frac{|x-\mu|}{b}\right)$,where b is the scale parameter and μ is the mean.
- Gaussian Distribution

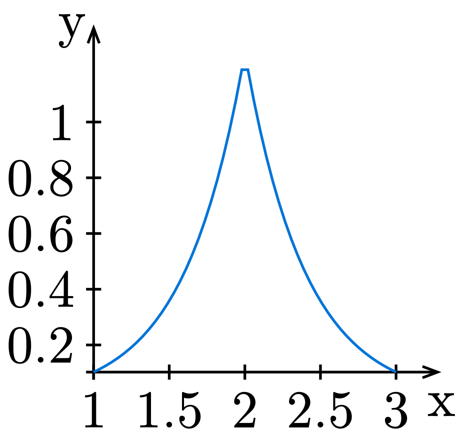

Figure 2: The PDF of Laplace Distribution.

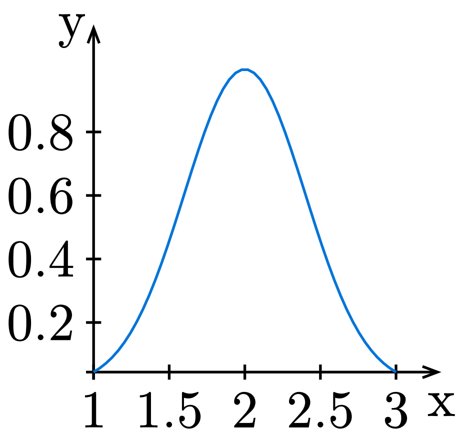

Figure 3: The PDF of Gaussian Distribution.

3.1 Preliminary Concepts

- Randomized Algorithm: For specific inputs, the output is not deterministic while it may follow a probability distribution.

  Example: $A(\boldsymbol{D}) = f(\boldsymbol{D}) + x$, where $x \sim \mathcal{N}(0, 1)$ and f is the query function

- Adjacent Datasets: Two datasets are adjacent if they differ by only one element. We could see it as two datasets, one containing a specific individual while another does not.

3.2 Definition

Now we could define a simple differential privacy algo. as follows:

A randomized algorithm $A : \boldsymbol{D} \mapsto \mathbb{R}$ satisfies ε-indistinguishable if for two adjacent dataset $\boldsymbol{D}$ and $\boldsymbol{D}'$ and any output O we have

$$\Pr\{A(\boldsymbol{D}) = O\} \le e^{\varepsilon} \Pr\{A(\boldsymbol{D}') = O\}$$

$$\left|\log\left(\frac{\Pr\{A(\boldsymbol{D}) = O\}}{\Pr\{A(\boldsymbol{D}') = O\}}\right)\right| \le \varepsilon$$

where ε is called the privacy budget or leakage [2].

[2] Calibrating Noise to Sensitivity in Private Data Analysis, Dwork and McSherry and Nissim and others

3.2 Definition

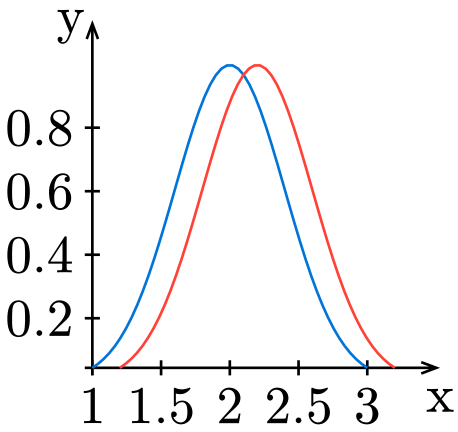

Figure 4: The PDF of two adjacent datasets.

For any two **adjacent datasets**, the **output** of the randomized algorithm should be **similar**.

Outline

4.1 Procedure

Procedure

1. Define the query function f. f is used to analyze the dataset and return the result.
2. Compute the sensitivity Δf of the query function. The sensitivity of the query function is the maximum change in the output between any two adjacent datasets.
3. Calculate the scale parameter b of the laplace mechanism: $b = \frac{\Delta f}{\varepsilon}$
4. Add noise to the query function: $A(\boldsymbol{D}) = f(\boldsymbol{D}) + \mathrm{Laplace}(0, b)$

Let's see an easy example...

4.2 Example

Dataset $\boldsymbol{D} \in \mathbb{R}^{100}$. The element d in D values between $[0, 120]$.

1. We define the query function as the mean of the datas, that is: $f(\boldsymbol{D}) = \frac{\sum \boldsymbol{D}}{100}$.
2. The sensity of f is $\Delta f = \frac{120}{100} = 1.2$
3. We set the privacy budget $\varepsilon = 0.1$, so the scale parameter $b = \frac{1.2}{0.1} = 12$.
4. A differential privacy algorithm could be obtained by $A(D) = f(D) + \text{Laplace}(0, 12)$.

Outline

5.1 Contrast

Advantages

- The ability to defend against new attacks [3].

  We assume the attackers have maximum knowledge about the dataset, and the differential privacy algorithm could still protect the data privacy.

- Balance between privacy and utility [3].

Drawback

- Hard to determine the perfect privacy budget [1].
- Reconstruction the noise model [1].

[1] Differential Privacy and Applications, IEEE Digital Privacy
[3] 差分隐私保护及其应用, 熊平 and 朱天清 and 王晓峰 and others

Outline

6.1 Code

Please check the python demo in the following link:
Python-Demo-4-Algorithm

Bibliography

Bibliography

[1] "Differential Privacy and Applications." [Online]. Available: https://digitalprivacy.ieee.org/publications/topics/differential-privacy-and-applications

[2] C. Dwork, F. McSherry, K. Nissim, and A. Smith, "Calibrating noise to sensitivity in private data analysis," in *Theory of Cryptography: Third Theory of Cryptography Conference, TCC 2006, New York, NY, USA, March 4-7, 2006. Proceedings 3*, 2006, pp. 265–284.

[3] 熊平, 朱天清, 王晓峰, and others, "差分隐私保护及其应用," 计算机学报, vol. 37, no. 1, pp. 101–122, 2014.