介绍文章

1、Understanding Differential Privacy

Understanding Differential Privacy这篇文章主要简要地介绍了一下差分隐私保护的基本思想，即即使删去某个样本，总体分布不会受到影响。

里面引用了两个资料，一个是 **The Algorithmic Foundations of Differential Privacy**，这里面讲了一些差分隐私的算法基础，以及 **Model Inversion Attacks that Exploit Confidence Information and Basic Countermeasures**，他展示了在机器学习算法中，我们有可能通过训练结果还原得到原本真实数据集。

2、A Brief Introduction to Differential Privacy

A Brief Introduction to Differential Privacy这篇文章介绍了差分隐私的灵敏度和隐私预算的问题。

这里看灵敏度的公式

$$\Delta f = \max_{D_1, D_2} ||f(D_1) - f(D_2)||_1$$

这里面的`f`就是表示一个具体的公式了，按照文章中举的例子，如果只是投票的话，那么`f`的灵敏度一定是1，因为在相差一个数据的情况下，肯定是个数相差一，如果`f`是一个简单的将输入的个数四舍五入的方法的话，那么得到的结果最多会相差5.

这样一个简单的方法上，不会有太多的问题，但是要是复杂的函数的话，那么对于灵敏度计算是一个很麻烦的方法，文中指出**estimating sensitivities、improving on estimates of sensitivity、circumventing the calculation of sensitivity** 可以对灵敏度进行估计。

虽然在一次查询中，通过添加噪音来让对方无法确定某个数据是否在数据集中是可行的，但是随着查询的增多，噪音的平均效果就会变为0，这样对方经过多次查询得到的均值就仍然会暴露原始的数据信息。其原因就是查询所造成的隐私损失是累加的，多次查询就会导致隐私损失不断增加，隐私损失的不断增加就会导致数据添加的噪音基本失效，为此，我们往往会规定一个最大的隐私损失上限，若用户多次查询所造成的隐私损失大于该阈值，我们就认为添加噪音所添加的隐私保护方法失效，而该阈值就叫做隐私额度(privacy budget)。