差分隐私顾名思义就是用来防范差分攻击的。

差分攻击：利用差值，得到某一些数据，是很好用来攻击聚合保护方式的。

差分隐私需要做到的就是使得攻击者的知识不会因为这些新样本的出现而发生变化。

对查询的结果加入噪声，使得攻击者无法辨别某一样本是否在数据集中

     对于传统机器学习,根据经验风险最小化得到的最优模型往往与决策边界附近的某些训练样本密切相关(如SVM 中的支持向量)。若这些样本的集合被增加、删除或修改,将会导致模型完全改变,在这种情况下,训练样本的信息将很 容易被推测出来