# Chapter 5 隐私保护

沙之洲 2020012408

## 1 请从基本思想、隐私保护水平等角度分析比较差分隐私与匿名化的不同，并举例说明。

在基本思想上，匿名化通过隐藏用户身份和数据的对应关系来保护用户隐私，通常使用的方法是泛化、抑制、聚类、微聚集、分解、置换等等；差分隐私通过在数据的查询结果中添加噪声来保护个体隐私，最大程度上保留数据的统计意义，以降低数据可用性为代价保护个体隐私。

在隐私保护水平上，匿名化不能够完全保证隐私不被泄露，攻击者可以利用背景知识进行攻击，而差分隐私是具有严格隐私保护证明的隐私保护模型。

一个例子。假设一家医院的医疗数据库为用户提供统计查询服务。匿名化会采用抑制技术，对患者的姓名进行抑制，同时对患者的年龄和住址进行泛化，但是攻击者仍然有可能通过背景知识对匿名后的数据进行重新识别。差分隐私会在查询结果中加入一定的噪声，在保留统计信息的前提下，让攻击者无法知道某个具体的患者是否出现在查询结果当中。

## 2 同态加密中的半同态加密和全同态加密各指什么，各有何优缺点?

半同态加密指的是仅支持加法同态或者乘法同态的加密体制

全同态加密指的是支持加法同态和乘法同态，并且可以进行任意多次加法和乘法运算的加密体制

半同态加密的优点是简单易用，常见的半同态加密算法有 RSA，ElGamal 和 Paillier 算法。缺点是只能支持一种同态算法，不能进行复杂的运算。

全同态加密的优点是支持加法和乘法同态，并且可以进行任意次运算，加密算法的功能更强大。缺点是计算复杂度较高，加密算法更复杂，整体性能远低于半同态加密算法