Chapter 5 隐私保护

赵晨阳 2020012363

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。

1.1 基本思想

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、抑制等技术，将原始数据进行修改和变形，以避免对用户隐私的直接披露。

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，使得相差一条记录的数据集的输出难以区分，以降低数据可用性为代价保护个体隐私。差分隐私保证了在有限的噪声幅度内，任何人的隐私都不会被泄露。

1.2 隐私保护水平

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，从而还原出原始数据，暴露用户的隐私信息。而差分隐私是具有严格隐私保护证明的隐私保护模型，它通过引入噪声，使得隐私信息不可逆转，提供了更高的隐私保护水平。

1.3 举例说明

（教材上的例子）某医院想要共享患者的医疗数据，以便于研究疾病的治疗方法。匿名化方法是对患者的年龄进行泛化，将具体年龄转化为年龄段，抑制敏感信息。差分隐私方法是在查询结果中添加一定程度的噪声，使得数据的输出不再完全准确，但是保证了患者的个人隐私不会被泄露。

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?

同态加密是一种加密技术，可以在密文状态下对数据进行计算，从而保护数据隐私。具体而言，它支持对于密文直接进行运算，可以将密文上的运算映射到明文上，实现了非数据拥有方对加密数据的直接操作，在满足了用户对数据的处理需求的同时，又保护了用户隐私。

同态加密可以分为半同态加密和全同态加密两种形式。

半同态加密又称为部分同态加密，是仅支持加法同态或者乘法同态的加密机制。常见的半同态加密算法有 RSA、Paillier 等。

全同态加密允许对密文进行任意次数的加法和乘法操作，因此可以进行更加复杂的计算。常见的全同态加密算法有 Gentry 的基于理想格的全同态加密方案。

半同态加密的优点是计算速度快，加解密效率高，但缺点是只能进行一次特定计算，因此适用范围有限。全同态加密的优点是可以进行任意次数的计算，具有更广泛的适用范围，但缺点是计算复杂度高，加解密效率较低，且实现难度较大。