网络空间安全导论 · Ch5

计01　容逸朗　2020010869

Q1.

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。

- 从基本思想的角度而言，两者的差别如下：
  - 差分隐私的基本思想是对数据集中的每个个体的隐私进行保护，而不保证数据集的整体性的隐私。
  - 具体来说，对于每个数据点，差分隐私会将其随机地加上一个噪音，使得外部攻击者无法确定该数据点是由哪个具体个体提供的。
  - 匿名化的基本思想是在确保数据公开可用的前提下，保护用户的敏感数据和个人身份之间的对应关系，从而保护用户的个人隐私。
  - 具体来说，匿名化通过去除个体的识别信息，如姓名、地址等来达到隐私保护的目的。
- 隐私保护水平：
  - 匿名化的隐私保护水平较弱。
  - 尽管匿名化可以保护个体的身份信息，但是在某些情况下，攻击者可以通过其他属性信息来推断出个体的身份。而且匿名化后的数据可能会失去一些有用的信息，这可能会影响数据的有效性和查询结果的可靠性。
  - 差分隐私有更强的隐私保护水平。
  - 它能够保护每个个体的隐私，并且保证查询结果是可信的。差分隐私可以提供严格的隐私保护证明，即使攻击者已经知道部分数据的情况下，也不能推断出任何一位个体的真实数据。
- 例子：假设有一份包含年龄和性别信息的数据集，其中包含了某些敏感信息是需要保护的。
  - 使用差分隐私方法，我们可以为每个数据点添加随机噪音。例如，对于一个年龄为 25 岁、性别为男性的数据点，我们可以将其年龄加上一个随机噪音，使得最终的年龄值不为 25 岁。这样，即使攻击者已经了解了所有其他数据点的信息，也无法确定这个数据点的真实年龄和性别信息。
  - 使用匿名化方法，我们可以去除个体的识别信息，如姓名等。例如，我们可以将所有数据点的姓名信息都替换为 “小明”。但是如果攻击者已经掌握了外部信息，如某个人的年龄、性别和地址等信息，就有可能通过这些外部信息来确定匿名化后的数据点的来源。

Q2.

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：** 允许在密文上执行一种特定的运算（通常是加法或乘法）但不能同时进行多种运算的方案。
  - 优点：计算速度较快；
  - 缺点：无法实现复杂的模型；
- **全同态加密：** 同时满足加同态和乘同态性质，可以进行任意多次加和乘运算的加密函数。
  - 优点：应用场景广泛，可以实现更加复杂的计算任务；
  - 缺点：计算速度较慢、实现难度较大。