(一)同态加密

1. 技术概述

同态加密是指对其加密数据进行处理得到一个输出，将此输出进 行解密,其结果与用同一方法处理未加密原始数据得到的结果一致。同态加密可以用以下的举例来说明:Alice 买到了一大块金子，

她想让工人把这块金子打造成一个项链。但是工人在打造的过程中有可能会偷金子,Alice 可以通过以下这种方法让工人加工金子又不能偷走金子。

Alice 将金子锁在一个密闭的盒子里面,这个盒子安装了一个手 套。工人可以带着这个手套，对盒子内部的金子进行处理。但是盒子 是锁着的,所以工人不仅拿不到金块,连处理过程中掉下的任何金子 都拿不到。加工完成后。Alice 拿回这个盒子，把锁打开，就得到了 金子。

这里面的对应关系如下,盒子:加密算法;盒子上的锁:用户密钥;将金块放在盒子里面并且用锁锁上:将数据用同态加密方案进行 加密;加工:应用同态特性,在无法取得数据的条件下直接对加密结 果进行处理;开锁:对结果进行解密，直接得到处理后的结果。

与普通加密算法只关注数据存储安全不同,同态加密算法关注的是数据处理安全，提供对加密数据进行加法和乘法处理的功能。使用同态

加密算法，不持有私钥的用户也可以对加密数据进行处理，处理过程不会泄露任何原始数据信息。同时，持有私钥的用户对处理过的数据进行解密后，可得到正确的处理结果。

同态加密算法从功能上可分为部分同态算法和全同态算法。所谓部分同态是指支持加法同态或者乘法同态或者两者都支持但是操作次数受限。而全同态算法则可简单理解为能不受限制地同时支持加法和乘法操作，从而完成各种加密后的运算(如加减乘除、多项式求值、指数、对数、三角函数等)。

利用同态加密，可以委托不信任的第三方对数据进行处理，而不泄露信息。因此，同态加密在云计算、电子商务、物联网等领域有重要应用。

2. 适用场景

同态加密在数据流通领域，包括数据共享和数据交易过程中，具有广阔应用前景。

如前文所述，在数据共享过程中需要对敏感数据进行脱敏处理，保证其不被泄露。同时，敏感信息本身具有分析和应用价值，若全部脱敏，将无法发挥其数据价值。同态加密技术为敏感数据隐私保护提供了一种新的解决思路，将数据中的敏感信息进行同态加密，但不影响其可操作性。

在数据流通场景中，数据需求方事先无法获知数据使用效果，因此无法评判数据价格的合理性。因此，在数据交易前，数据需求方可用部分加密数据进行计算，验证其可操作性及业务相关性，以此为基础，确定需求数据价格的合理性。

3. 技术方案

考虑数据流通过程中的委托计算场景。使用同态加密技术的委托计算场景涉及两类角色，数据持有方和数据处理方，其技术方案示意图 3.1 所示：

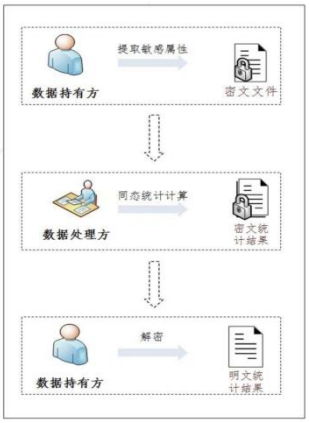

图 3.1 同态加密技术方案示意图

数据持有方拥有原始数据，并选择需要保护的敏感属性。在本地生成公私钥对后，使用生成的用户公钥，同态加密原始数据中的敏感属性，得到密文文件。之后数据持有方将密文文件发送给数据处理方，数据处理方对密文文件进行同态操作，在明文数据信息不可知的情况下，生成密文统计结果，此结果和明文状态直接加密得到的处理结果一致。数据处理方得到密文统计结果后，将其返回给数据持有方。数据

持有方接收到处理后的密文统计结果，使用用户私钥解密，获取明文统计结果。

4. 技术发展趋势

目前单一的支持加法同态操作或者乘法同态操作的同态加密算法设计相对简单，比如 Paillier 算法，ElGamal 算法等，这类算法在一些相对简单的数据分析场景中已足够支撑需求。但是从数据流通角度来看，数据处理的方式和场景将会越来越复杂，单一的加法同态或者乘法同态将无法满足要求。全同态算法将为数据加密操作提供完备的解决方案。然而全同态加密算法目前只是在理论层面论证可行性，其核心算法和性能问题尚未得到突破，当前存在密钥制作时间长以及制成的密钥过大等困难，工业界及密码学界仍在这一块进行积极的探索。