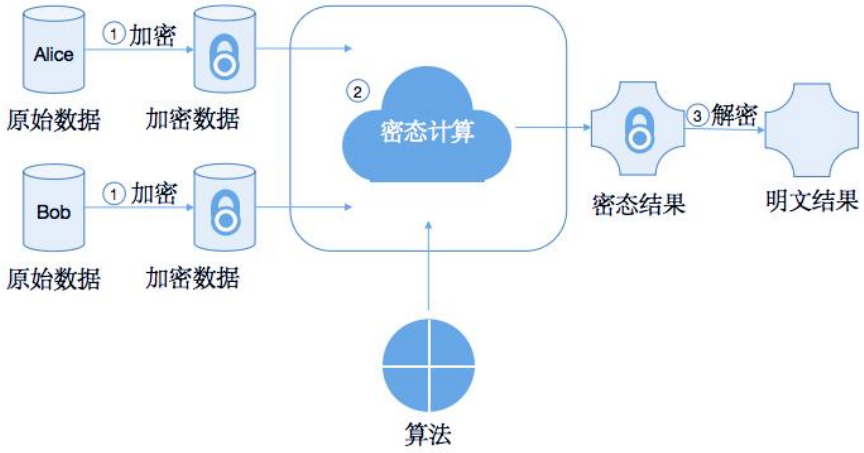
同态加密
Homomorphic Encryption

同态加密是在 1978 年由 Ron Rivest 等提出，是一种基于数学难题的计算复杂性理论的密码学技术。同态加密的主要思想是对经过同态加密的数据进行某种方法计算得到一个输出，将这一输出进行解密,其结果与用同种方法计算未加密的原始数据得到的输出结果一致。



同态加密具有加法同态性和乘法同态性，可利用加法和乘法构造任意的计算方法对密文运算。根据同态性质可分为：

(1) 部分同态加密(Partially Homomorphic Encryption - PHE)方案：是指具有单一的加法同态性或乘法同态性，例如：RSA 算法、Elgamal 算法和 Paillier 算法等。

(2) 有限层次全同态加密(Leveled Fully Homomorphic Encryption - LFHE 或 SomeWhat Homomorphic Encryption - SWHE)方案：是指支持对密文进行有限次数的同态加法和同态乘法，例如：BGV12 方案、GSW13 方案和 CKKS17 方案等。

(3) 全同态加密(Fully Homomorphic Encryption - FHE)方案：支持对密文进行无限次数的加法同态和乘法同态，即任何类型的计算，例如 GSW、BFV、CKKS、TFHE 等。

随着近年来国内外对数据安全和隐私保护的需求越来越高，同态加密技术不断优化和突破，开始走向商用阶段，在云计算和隐私计算等场景中被逐步应用。同态加密实现密文间的多种计算功能，即先计算后解密得到的结果可以等价于先解密后计算结果，这个特性对于保护敏感数据跨域计算过程的安全具有重要意义。同态加密可适用于金融、医疗、政务等跨机构间的联合查询、联合统计、联合建模、联合预测等多种落地场景。同态加密应用过程可单独使用进行集中式代理计算、分布式的多方联合统计等，也可应用于联邦学习、隐匿查询、安全求交等技术方案作为一个底层支撑密码学技术组件，满足更广泛的多样性应用需求，扩展到更大更复杂的实际业务场景范围。