# 背景

通过联邦学习训练得到的模型和数据集集中在中心服务器上进行训练得到的模型相比效果相似，但是联邦学习存在隐私泄露的风险。在联邦学习的过程中有大量中间参数需要交换,有学者指出可以根据中间参数来推断已获取的信息是否来自某个特定的参与者。如果参与者是恶意的，参与训练的模型数据可能会被污染。即使在训练之初可以避免恶意参与者的存在，参与者也可能会导致数据信息的泄漏。

# Pailier算法

Paillier加密算法是一种著名的半同态加密方案，具有效率高、安全性证明完善的特点。当使用Paillier加密算法时，包括三个主要阶段：密钥生成、加密过程和解密过程。

## 密钥生成阶段：

1. 随机选择两个大素数 p 和 q，确保它们的长度相等，并满足条件： ，这确保了模数 和欧拉函数 。
2. 计算 和。
3. 随机选择 ，确保满足条件：，其中 。
4. 计算私钥参数 μ，使其满足 。

最终，公钥为 (N, g)，私钥为 。

## 加密过程：

1. 选择一个整数 m，其中 .
2. 选择一个随机整数r，其中 .
3. 计算密文 c，满足：

## 解密过程：

1. 计算
2. 计算
3. 计算明文 .

# 基于中国剩余定理（CRT）的优化算法

在Paillier加密算法中，中国剩余定理（CRT）被用于提高加密速度。以下是具体步骤：

1. **计算模逆：** 首先，计算两个质数 p 和 q 对应的模逆，即 和。这包括计算 和 ，它们是模 p和模 q下 p-1和 q-1 的逆元。然后，计算 以及 和 。
2. **随机选择 R：** 随机选择整数 R，确保它在模 n下属于乘法群 。
3. **模指数运算：** 计算 g的 R 次幂在模 p和模 q下的余数，即 、，以及 和 。
4. **中国剩余定理：** 利用CRT，将模n 上的 c 分解成两个部分，即 和。这两个部分分别满足 和。
5. **合并结果：** 利用模运算规则，将 和 结合得到 。这样，模指数运算的结果转化为了在 和 上的运算，提高了加密算法的效率。