# 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同，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。在联邦学习系统中，如果参与者是恶意的，那么在训练过程中，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加密算法是一种最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。包括密钥生成、加密过程、解密过程三个阶段。

## 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 .

# 算法改进

在算法加密的过程中，输入为 ，输出为 c。为了提高算法的加密速度，可以利用中国剩余定理的空间特性对数据进行预处理，将在 下的模指数运算转化到 和 上，从而提升 Paillier 算法的效率。

具体步骤如下：

1. **计算模逆：** 计算 和的模逆 和 ，其中 然后令, ,
2. **随机选择 R：** 随机选取一个整数 R，使得 .
3. **计算模指数运算：** 计算 , , , ,
4. **中国剩余定理：** 利用中国剩余定理公式计算 和 分别等于 和 ，其中 ,
5. **合并结果：** 根据模运算的规则 得到