同学们，老师早上好

今天和大家分享的主题是一种灵活且可验证的隐私保护联邦学习方案FVFL

整个报告分为四个部分，分别是报告概述，预备知识，主要贡献，及结论与思考。

什么是联邦学习呢，其实就是一种分布式机器学习方法，旨在保护数据隐私情况下进行模型训练。这种分布式的学习方法必然涉及到传输过程中如何保护数据隐私，如何确保训练正确执行，如何确保模型纯净等等问题，也就是老生常谈的模型安全问题。如梯度的隐私泄露，投毒攻击，拜占庭攻击等。本文就是在这样的研究背景下提出了一种确保客户端隐私且可验证的高效联邦学习方案。

具体的应用场景如以往的联邦学习框架一样，包含中央服务器与客户端。

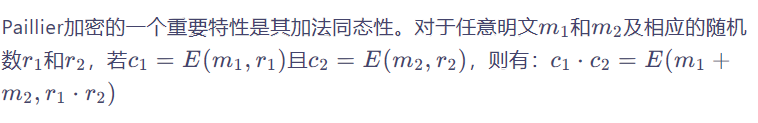
本文在参考了其他论文后，发现了前辈们的工作存在以下不足之处，叙述ppt

针对这些不足之处，本文做出了以下贡献，叙述ppt。

在正式描述FVFL方案前，让我们先来了解一下预备知识。

首先就是基础理论知识，我们稍作概述大家了解即可，细节有兴趣的话可以自己下来找原论文看看。

Paillier同态加密，一种基于复合剩余类问题和数论中的难度假设设计的公钥加密算法，具备加法同态特性。而在本文中，利用到的就正是这个重要的特性，加法同态性。什么是加法同态性？简单来说就是



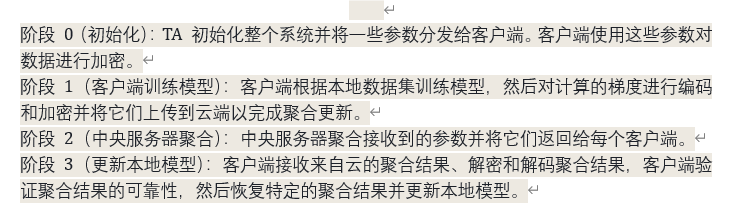
第二个需要了解的就是Shamir的秘密共享算法，也就是老师师兄师姐们常说的t of n门限算法。通过它我们可以在n个参与者之间安全地分发和重建秘密。在本文中是实现客户端灵活退出的重要算法。

最后一个是拉格朗日插值多项式，一种通过给定的一组点来构造一个多项式的方法，该多项式在这些点上的值与给定的值相等。在客户端编码时，通过拉格朗日插值多项式算法对私钥和数据编码，以保证客户端后续验证子密钥是否正确聚合，从而确定梯度是否正确聚合。

了解完基础理论后，来看一看本文的应用场景，设计三方，安全可靠的可信授权第三方TA，诚实和好奇的客户端，可能恶意的服务器端

介绍完我们的预备知识，接下来介绍本文的主要贡献，首先就是FVFL方案的概览。

主要有四个阶段，如图所示，



看起来本文的方案既简单又明了吧，实际上与其他方案相比，算法复杂度上确有较大的优化。

如表所示，本文主要比较了先进的四种方案，这几种方案的算法复杂度都处于一个o（MN）的量级，一旦客户端多起来，那么开销是成倍的增长的。而本文的方案则是降低了常用的加解密，聚合，验证等算法，使得这几个算法与数据维度相独立，降低算法的计算开销。通过使用超递增序列来编码数据，将计算开销集中在数据的编码解码中，在实验中，本文的这种方法可以显著的降低计算开销，并且获得一个可以接受的验证开销，这正是本文方案的改进之处。

对于一个安全方案来说，没有安全性分析可不行，不然谁相信你这个是安全的方案呢。所以最后来概括一下本文的安全性分析。

首先，我们定义三个定理如ppt所示。对于定理1，考虑这样的情况来证明。

客户端的梯度由超递增序列编码，由共享私钥屏蔽，由 Paillier 加密以生成密文，然后通过公共通道传输到云服务器。公共通道中可能存在攻击者A窃取传输的密文数据。然而，由于Paillier加密算法在语义上是安全的，满足IND-CPA安全定义，即使攻击者A拦截密文消息，他也无法恢复与明文相关的任何信息。

对于定理2，当模型训练器接收来自云的密文聚合结果时，Shamir 的秘密共享协议确保至少有 t 个客户端参与联邦学习，以便客户端可以成功地解密聚合结果。客户端进一步使用拉格朗日插值和Shammir的秘密共享来验证云聚合结果，以防止云伪造数据。由于聚合结果是通过Paillier同态算法的同态运算得到的，聚合结果仍然是Paillier加密得到的密文数据，而Paillier算法显然是满足IND-CPA（选择明文攻击）安全的。即使攻击者A拦截聚合的密文消息，他也无法恢复与清晰文本相关的任何信息，从而攻击者成功划分密文数据的概率可以忽略不计。

除此之外，在聚合阶段，若服务器不正确执行聚合算法，那么为了虚假聚合结果，云必须让至少 t 个客户端合谋以获得它们共享的子密钥，而这在实践中很难实现。因此，聚合结果满足定理2。

对于定理3，为了解码超递增的序列编码是一个背包问题，这个问题是NP困难的，在多项式时间内没有解，因而服务器无法获得特定的数据。然而本文使用Paillier加密方案进一步加密客户端数据，并且该加密方案满足语义安全性和IND-CPA安全定义。这样即使攻击者A拦截密文消息，他也无法恢复与明文相关的任何信息。因此，证明了定理 3。

非常感谢各位老师同学听我瞎讲，最后总结一下本文的主要内容与对我们研究工作的思考。

究其根本本文是通过结合不同的隐私保护技术，实现了一种高效的联邦学习模型，换句话说就是把好的东西组合到一起，然后发现效果还不错，这对我们以后的研究工作也有一定的启示，是不是把不同的东西结合到一起有奇效呢？我们是不是也可以在这样的思路指引下去做一下综合研究。