# 一种灵活且可验证的隐私保护联邦学习方案

## 摘要

随着深度学习的发展，人们越来越关注数据的安全性。联邦学习可以解决数据孤岛问题，但它也带来了更严重的数据隐私问题。此外，在多源数据协作过程中，整个联邦学习系统的效率通常不高。在本文中，我们介绍了一种称为FVFL的方案，该方案保证了本地数据的安全性和对合谋攻击的抵抗力，更重要的是，它可以很好地支持客户端灵活的参与联邦学习。我们采用Paillier加密和秘密共享来保证客户端的数据安全性和对合谋攻击的抵抗力。此外，我们的加密机制允许客户端灵活地参与联邦学习，加密算法的正确性不受客户端退出的影响。引入超递增序列来减少整个系统的通信开销，仿真结果表明结果显著;引入拉格朗日插值多项式和秘密共享实现验证机制，防止云中聚合结果的恶意伪造。验证机制确保客户端在云中获得真实可靠的聚合结果。此外，我们的验证机制允许客户端灵活地参与联邦学习，验证算法的正确性不受客户端退出的影响。实验结果表明，FVFL具有较高的精度和效率。

## 1.概述

随着人工智能技术的出现，大数据的处理和操作已经变得非常高效和简单，已广泛应用于人脸识别、在线医疗诊断和语音识别等[1]。准确的网络模型需要大量的数据，这些数据通常由不同的所有者保留。然而，数据通常包含敏感信息，数据所有者不能直接传输数据(GDPR)[3]，这导致了我们所说的数据孤岛问题，影响了人工智能技术的进一步发展。

联邦学习是解决数据安全问题的有效解决方案，它在本地保持数据，所有参与者都可以合作构建有效的全局网络模型。谭等人。 [2] 提出了联邦学习的具体概念，表明联邦学习是确保数据安全和解决数据孤岛问题的有效方法。Yang等人[3]根据客户端数据的特点，将联邦学习分为水平联邦学习(HFL)、垂直联邦学习(VFL)和联邦迁移学习(FTL)，这些方法几乎适用于所有类型的数据孤岛，保证数据隐私。

简单的联邦学习方法不足以完全保证数据的安全性，需要添加同态(HE)、差分隐私(DP)和安全多方计算(MPC)[4]、[5]、[6]等隐私计算来保证数据的安全性。Phong等人[7]指出，在联邦学习过程中，真实的用户数据可以通过共享梯度推导出来。研究[8]，[9]表明，通过使用攻击模式对生成网络使用攻击模式，可以通过联邦学习中共享参数来恢复客户端的数据。研究[10]表明，毒害攻击的方法使全局模型偏离，降低了模型的精度。因此，为了建立安全可靠的联邦学习系统，我们需要采用隐私计算技术。在[7]中采用同态加密，以确保梯度数据不会泄露，梯度安全聚合将在云中完成。Li等人[11]使用阈值Paillier方法对梯度数据进行加密，保证联邦学习中客户端的数据安全性，所有客户端都可以灵活地参与联邦学习系统。魏等人。 [12] 使用 DP 来确保梯度数据的隐私，并确保整个联邦学习系统在半诚实安全模型中的安全性。为了增强整个联邦学习系统的安全性，[13]和[14]中使用了同态加密和DP保护方法，使整个联邦学习系统更加安全和高效。最近的Reasearch[15]采用安全多方计算秘密共享方法，保证联邦学习中各个客户端的数据安全性。

隐私计算技术可以保证半诚实模型下数据的安全性，但不足以防止联邦学习系统中参与者的恶意攻击。使用 Beaver 三元组方法的研究 [16] 确保了客户端数据的隐私，并设计了一个额外的参数来衡量贡献，它考虑了具有不同数据质量的不同客户端 [17]。同态加密用于保证用户数据的安全性，并使用一些额外的评估策略来确保用户数据的可靠性[18]。DP技术用于保护用户数据的隐私，评估数据集用于评估用户数据，防止用户的恶意行为，保证联邦学习系统中用户数据的安全性和可信度[19]。零知识证明技术用于防止用户的恶意行为。在[20]中，为了解决联邦学习的公平性问题，防止搭便车客户端参与，利用区块链中的激励机制保证所有客户端的公平参与。参考文献[21]使用区块链技术来跟踪和审计客户端的数据，以防止客户端的恶意行为。

这里有很多工作来防止恶意行为来自客户端，但只有少量的工作是防止恶意行为来自云。为了进一步加强整个系统的安全性，保证中央服务器联邦学习聚合结果的真实性和可靠性，[22]使用计算开销巨大的双线性对方法构建聚合签名，以确保可以验证云聚合结果。[23]中使用了同态哈希认证方法，可以防止恶意攻击者从云端，保证用户能够获得可靠的聚合结果。[24]中使用了秘密共享的方法，客户端可以通过验证秘密值被正确聚合来说服云聚合结果为真可靠。参考文献[25]采用拉格朗日插值多项式来防止云中的恶意伪造。然而，[25]中的上述方法必须同时确保整个系统客户端在线，这使得整个系统不太实用。

在实践中，联邦学习客户端可能会出于各种原因退出。因此，整个系统必须具有很强的鲁棒性，以确保当客户端同时不在线时完成联邦学习过程。此外，对于具有聚合结果的可验证性联邦学习系统，聚合结果的可验证性不应受到少数客户端的影响。

在本文中，我们认为客户端是一个半诚实的威胁模型，即客户端遵循协议设置来执行。但是，服务器端可能存在恶意攻击者。我们考虑了上述威胁模型，并引入了一个名为FVFL的方案，该方案保证了本地数据的安全性和对合谋攻击的抵抗力，更重要的是，它可以很好地支持客户端灵活的参与联邦学习。我们采用 Paillier 加密和 Shamir 的秘密共享来保证客户端的数据安全；引入超递增序列来减少整个系统的通信开销；引入拉格朗日插值多项式和 Shamir 的秘密共享来实现验证机制，以防止恶意伪造聚合导致云。此外，我们的验证机制允许客户端灵活地参与联邦学习。总之，我们的贡献可以总结如下。

1)我们利用超递增序列对梯度数据进行编码。更重要的是，超增加序列显着降低了整个系统的通信开销。

2)设计了一种高效的隐私保护联邦学习加密机制，该机制抵抗合谋攻击，支持客户端退出。

3）我们设计了一种有效的隐私保护联邦学习验证机制，即使一些客户端同时退出，也可以顺利执行。

4)通过大量的仿真实验分析了FVFL的效用，证明了该方案具有较高的精度和效率，验证开销是可以接受的。

本文的其余部分组织如下。在第 II 节中，我们概述了 FVFL 的问题定义、威胁模型和目标。在第三节中，我们概述了联邦学习、Paillier加密、拉格朗日插值多项式和Shamir的秘密共享。在第 IV 节中，我们描述了我们的 FVFL 的细节。在第 V 节中，我们对 FVFL 的正确性、数据隐私和可验证性进行了一些分析。在第 VI 节中，我们进行了安全分析。在第七节中，我们进行了一系列实验来评估性能。最后，我们在第 VIII 节中给出了一些结论。

## 2.问题概述

### A.问题定义：

（在我们的方案中，有三个实体：1）可信权威（TA）； 2）客户端； 3）中央聚合服务器。TA将参数分发给客户端，客户端利用参数代码对梯度进行加密，服务器聚合模型参数。

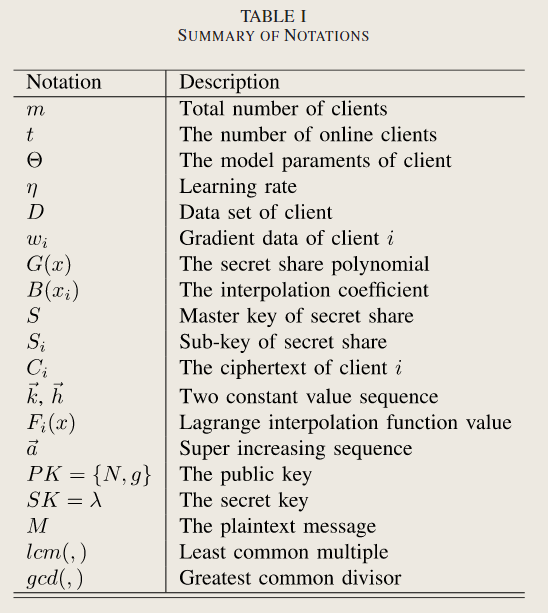
在这个模型中，应该考虑三个挑战。首先，每个客户端的梯度数据可能会损害本地数据的隐私，客户端应该能够确保本地数据安全和隐私。其次，服务器可能是无信任的。服务器的责任是接收和聚合梯度数据，并将真实可靠的聚合结果返回给每个客户端。但是，服务器可能会受到恶意攻击或为了节省计算资源的目的的影响，因此梯度聚合结果不可信。第三，在联邦学习过程中，由于各种原因，客户端可能会退出，联邦学习系统应该能够正常工作，但不受客户端退出的影响。

### B.威胁模型和目标

我们将FVFL中的威胁模型定义如下。我们相信 TA 安全可靠，不会受到任何恶意攻击。我们假设联邦学习系统中的客户端是诚实和好奇的，这意味着客户端将遵循协议设置，但由于各种原因，客户端可能是离线的。我们假设服务器端可能存在恶意行为。服务器可能会恶意伪造聚合结果，或者尝试破坏一些客户端形成串通攻击来窃取其他客户端的机密数据。因此，我们的FVFL模型的目标是保证客户端的局部梯度安全性，客户端能够判断云聚合结果的可靠性，整个系统能够抵抗一些客户端之间的串通攻击。整个系统支持客户灵活参与。

## 3.预备知识

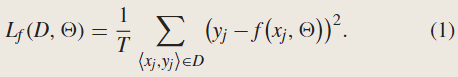
在这一部分中，我们将介绍联邦学习、Paillier同态加密、拉格朗日插值和Shamir的秘密共享，然后基于上述基本概念构建一个灵活且可验证的隐私保护联邦学习系统。本文中使用的数学符号总结在表 I 中。



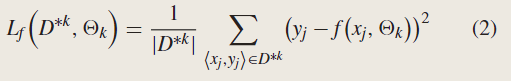
### A.联邦学习

（1）深度学习：一般来说，深度学习模型由输入层、隐藏层和输出层三层组成。我们可以将深度学习模型描述为函数 f (x, θ) = y，其中 x 表示用户输入，θ 是模型参数，y 是函数 f 的输出与参数θ。

（2）随机梯度下降算法SGD：对于梯度下降（GD），不失一般性，有 T 对训练数据 (x, y)，数据集为 D = {(xj, yj), j =1, 2,。, T}，基于上述数据集，损失函数可以描述为：



与GD不同的是，在第k次迭代中，SGD将随机选择一个子集D \* k而不是整个数据集D。损失函数可以描述为



根据上述损失函数，在第k次迭代中，梯度将是：

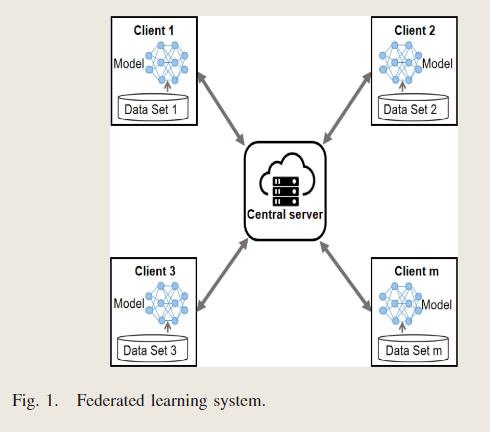


然后，我们可以更新模型参数如下：

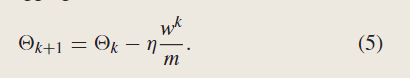


其中 η 是客户端的学习率。

（3）联邦聚合：如图1所示，联邦学习可以桥接各种组织来训练全局模型，存在一个中央服务器，它聚合数据所有者发送的参数。



在联邦学习的第 k 次迭代期间，客户端 i 计算梯度 wk i ，中央服务器聚合 m 个客户端梯度以获得 wk = ∑i=mi=1 wk i ，然后将聚合结果发送给每个客户端。每个客户端通过聚合结果更新本地模型：



### B.Paillier加密

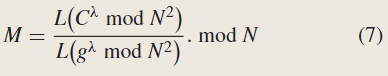
Paillier加密系统实现了同态加密，广泛应用于现有工作。特定的 Paillier 加密系统由三个算法组成。

（1）密钥生成：密钥生成中心设置安全参数K0，然后选择一个安全模量N = pq，其中p和q是满足p = q的高阶大素数。TA 选择生成器数 g ∈ Z∗N2 ，满足 gcd(L(gλ mod N2)，N) = 1, gcd(.) 表示最大公约数，L(x) = X − 1/N，λ = lcm(p -1, q − 1), lcm(.) 表示最不常见的多重。Paillier加密方案的公钥为PK = {N, g}，私钥为SK = λ。

（2）加密：给定一个消息 M ∈ ZN ，选择一个随机数 r ∈ Z∗N ，则密码 C 可以计算为



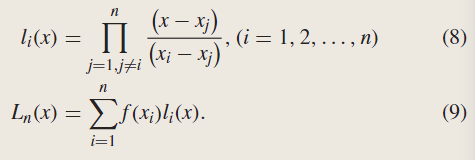
（3）解密：给定密码 C，对应的消息 M 可以恢复为



值得注意的是，Paillier加密系统可证明对所选明文攻击是安全的。

### C.拉格朗日插值

给定 n 个点，拉格朗日插值方法可以通过这 n 个点找到 n-1 阶的唯一多项式。下面简要介绍拉格朗日插值。给定 n 个不同的插值点 xi，{i = 1, 2,。, n}，以及相应的数字 f (xi), 函数 f ，有一个唯一的 n 度公式。然后，n次多项式Ln(x)可以写成拉格朗日形式:Ln(x) =∑n i=1 f (xi)l i(x)。通过上述拉格朗日插值公式，我们可以得出结论，对于n次多项式函数，选择它的任何n个点可以恢复函数表达式。

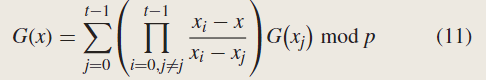


### D.沙米尔秘密共享

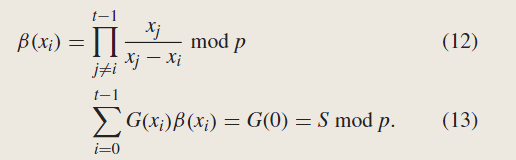
秘密共享方案是一种将秘密分成n个片段的方案，并用不同的有效成员分发这些片段。如果对手捕获系统中的成员，他只能获得一部分秘密。只有当对手至少获得t条秘密时，他才能得到整个秘密。通常采用Shamir的秘密共享技术来实现这一结果。可信方选择一个多项式来分割秘密。



其中 S 是主键。根据上述方程，给定xi，我们可以得到G(xi)， Si ={xi,G(xi)}是对应的子密钥共享。多项式 G(x) 也可以表示如下：



当 x = 0 时，G(x) = S，我们利用 β(xi) 表示拉格朗日插值系数。所以主密钥 S 可以表示如下：



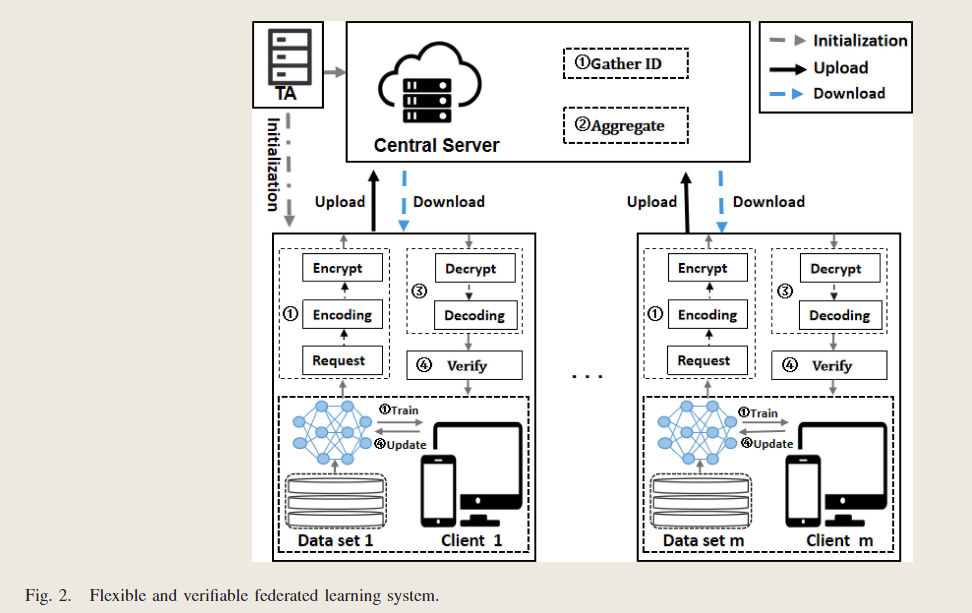
在拉格朗日插值多项式的帮助下，我们可以很容易地恢复主密钥 S。

## 4.解决方案

本节首先概述FVFL，然后详细介绍其程序。

### A.概述

如图2所示，该系统由TA、客户端和中央聚合服务器组成:：

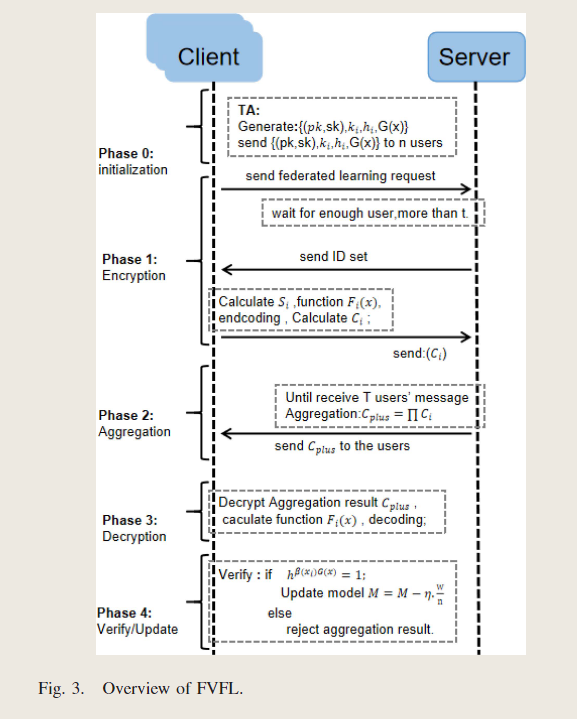


1) TA: TA初始化神经网络模型，生成键和参数，并将它们分发给客户端。

2）客户端：我们的方案由 m 个客户端组成，每个客户端都有自己的数据集。在联邦学习过程中，系统允许客户端在不同的时间在线。特别是，在验证聚合结果的正确性时，所有客户端不需要参与结果的聚合，但仍然可以验证结果的正确性。

3)中央聚合服务器:在每一轮联邦学习中，中央服务器聚合上传的密文，然后将聚合结果分发给每个客户端。在我们的系统中，我们认为中央服务器是恶意的。它可能会尝试通过接收到的梯度窃取客户端的隐私信息，更糟糕的是，伪造聚合的结果发送给客户端。

如图 3 所示，FVFL 包括四个阶段：1）初始化阶段； 2）客户端训练模型和加密； 3）中央服务器聚合； 4）客户端解密和更新本地模型。



阶段 0（初始化）：TA 初始化整个系统并将一些参数分发给客户端。客户端使用这些参数对数据进行加密。

阶段 1（客户端训练模型）：客户端根据本地数据集训练模型，然后对计算的梯度进行编码和加密并将它们上传到云端以完成聚合更新。

阶段 2（中央服务器聚合）：中央服务器聚合接收到的参数并将它们返回给每个客户端。

阶段3（更新本地模型）：客户端接收来自云的聚合结果、解密和解码聚合结果，客户端验证聚合结果的可靠性，然后恢复特定的聚合结果并更新本地模型。

### B.初始化阶段

在我们的 FVFL 框架中，TA 需要生成和分发以下参数。

1)以安全参数K0为输入，输出Paillier加密系统{N, g, p, q}的参数，我们设置公钥PK = {N, g}，私有秘密λ = lcm(p−1,q−1)，私钥SK = {λ, p, q}。TA 将 {PK, SK} 分发给所有客户端。PK和SK分别用于加密和解密梯度数据。

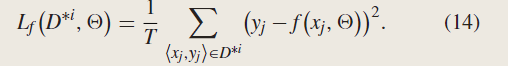
2) TA 需要生成一个超递增的序列 a, a = (a1, a2,., a+1)，其中 a+1∑ni=1 ai。TA 计算编码参数 gi =ga i , i = 1,。, n + 1。 TA 选择随机数 r∗ ∈ Z∗N 并计算 f1 = r∗q mod N2。根据 g 计算 f2 = gq mod N2 ，TA 发送 {f1, f2, a, g1, g2,。, gn+1} 到所有客户端。f1 将用于加密梯度数据，f2 将用于验证聚合结果。{a, g1, g2,., gn+1} 将用于对梯度数据进行编码和解码。

3) TA 生成两个常数序列 k =(k1, k2,., kn+1) 和 h = (h1, h2,., hn+1)。这两个常数序列将用作插值来处理客户端梯度。

4) 根据私有秘密 p，TA 根据系统参数 p 选择随机数 r，使得 r &lt; p。TA构造两个具有不同系数的Shamir秘密共享多项式G1(x)和G2(x)，选择两个Shamir秘密共享多项式的模量为p，则p−r和r分别为Shamir秘密共享算法中共享的主密钥，通过运行Shamir的秘密共享算法生成2m个子密钥对，主密钥对记为S i1 = {(xi, G1(xi))， i = 1,2，…，, m}，主密钥 p - r 的子密钥对表示为 S i2 = {(xi, G2(xi))，i = 1, 2,。, m}，其中 {xi, i = 1, 2,., m} 是 m 个不同的随机值，{G1(xi)，i = 1, 2,。, m} 是从多项式 G1(x) 输入 xi 获得的值，{G2(xi)，i = 1, 2,。, m} 是从多项式 G2(x) 输入 xi 获得的值。然后，TA 将 {S i1, S i2} 分发给客户端 i，并将 {x1, x2,., xm} 到所有客户端。{S i1, S i2} 将用于对梯度数据进行加密并抵抗合谋攻击。{x1, x2,., xm} 将用于恢复主密钥。

### C.客户端训练模型阶段

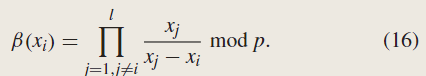
在这个阶段，每个客户端基于本地数据集 D = {(xj, yj), j = 1, 2, 训练自己的模型。, T}，基于上述数据集，每个客户端采用 SGD 获得梯度。客户端随机选择子集D∗计算损失函数



客户端i执行SGD来计算私有梯度wi



梯度向量是一个 n 维向量，描述为 wi = (wi1, wi2,., win)。其次，客户端 i 将联邦学习请求发送给云端，将相应的 ID 发送给云端。当云等待从客户端接收到超过 t 的请求时，云收集所有在线客户端的 ID，并返回每个客户端 ID 集。客户端根据服务器返回的id包从{x1, x2，…中选择对应的xi。, xm} 并计算



客户端 i 进一步计算子键 Si，如下所示。



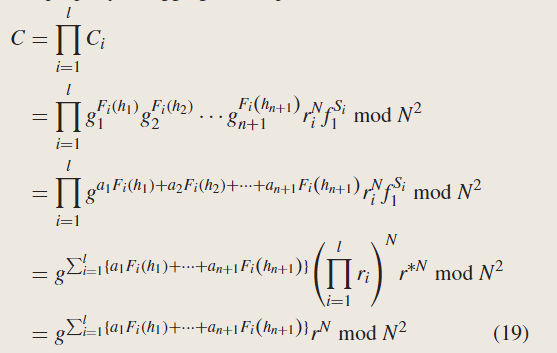
最后，为了保证客户端数据的安全性，减少通信开销，客户端用TA分布的参数加密和包梯度数据。首先，客户端使用常数序列 k = {k1, k2,., kn+1} 插值私有梯度数据 wi = {wi1,., win} 和共享子密钥 Si，则客户端输入常数序列 h = {h1, h2,., hn+1} 到函数 Fi(x) 来计算相应的函数值 Fi(hi)，然后客户端 i 使用加密参数 {g1, g2,., gn+1, f1, N} 由 TA 和子密钥 Si 分布，以加密值{Fi(h1), Fi(h2)。, Fi(hn+1)}



在客户端i得到加密值Ci后，客户端将加密数据上传到云服务器，等待云完成联邦学习的聚合更新。

### D.聚合阶段

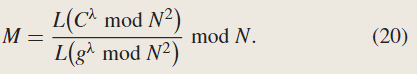
在聚合服务器接收来自所有客户端的密文后，服务器利用加性同态属性将密码聚合为



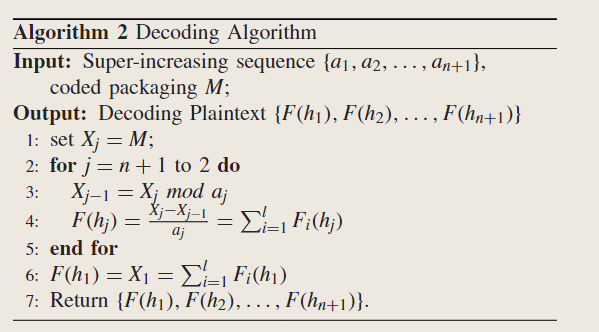
其中 C 是聚合密文，服务器将聚合密文返回给所有客户端，请注意它们的梯度信息是密文，服务器无法获得明文。中央服务器通常不受信任。为了节省自己的计算资源，服务器可能会伪造结果。对于云服务器返回的聚合结果，客户端应该能够验证结果是否正确。由于客户端可能在系统中离线，加密机制和验证机制必须支持客户端灵活参与。

### E.上传本地模型阶段

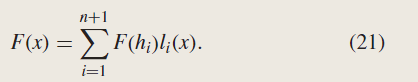
在接收到聚合结果后，每个客户端首先使用Paillier解密算法对聚合密文C进行解密

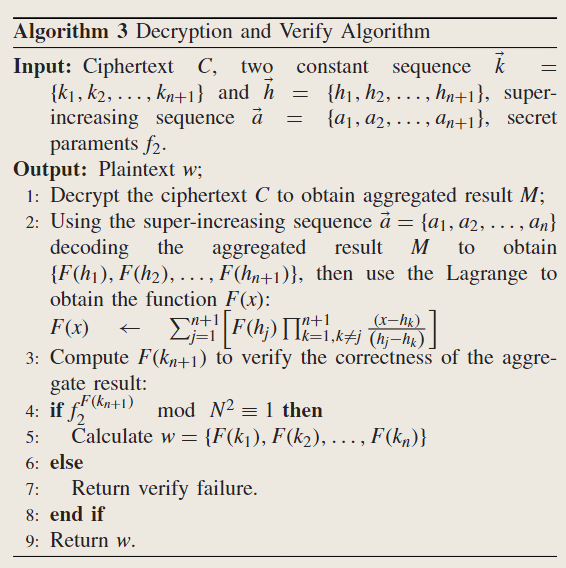


其次，我们将解码过程总结为算法 2，每个客户端使用超递增序列 a = {a1, a2,., a+1} 解码聚合结果，每个客户端获得结果 {F(h1)、F(h2)。, F(hn+1)}。



正如算法 3 所示，客户端需要对数据集 {(h1, F(h1)), (h2, F(h2)) 进行拉格朗日插值。, (hn+1, F(hn+1))}





在得到函数F(X)后，客户端将x=kn+1输入到函数F(X)中，计算F(Kn+1)，然后通过秘密参数f2验证聚合结果的正确性。如果 f F(k n+1)2 mod N2 ≡ 1，则客户端确信聚合结果是正确的。然后，客户端输入常数序列 k 进入函数 F(x)，计算 w = {F(k1)、F(k2)。, F(kn)}。函数 F(x) 结果对应于每个模型的梯度聚合结果。

在这个阶段结束时，每个客户端使用聚合结果在第 k 轮本地更新相应的模型参数 M：Mk+1 = Mk - η(wk/m)。

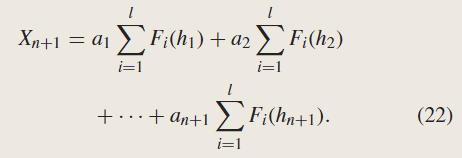
## 5.FVFL的正确性分析

在这一部分中，我们将从理论上分析我们提出的模型FVFL的正确性、数据隐私和验证能力。

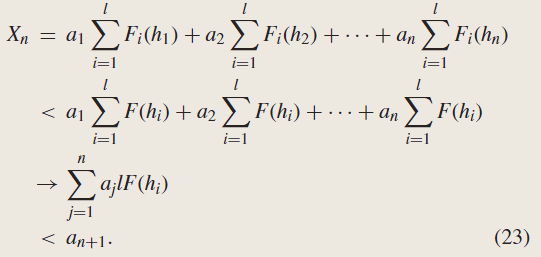
### A.正确性

在本文中，我们使用超递增序列来编码梯度数据。超递增序列的编码和解码的正确性如下。

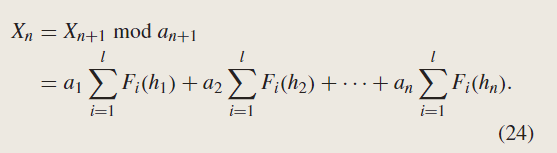
客户端i解密服务器聚合的结果，明文结果Xn+1



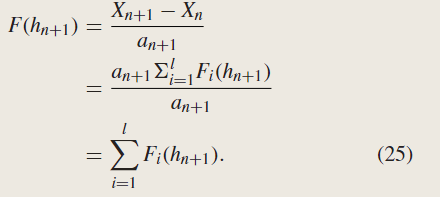
将F(hi)作为梯度数据中的最大值，聚合结果的不等式满足以下不等式:



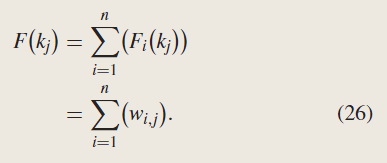
因此我们可以得到Xn如下:



然后，可以得到每个维度对应的聚合结果如下：



在本文中，我们还使用拉格朗日插值多项式对梯度数据和验证密钥进行编码。如果中央服务器诚实地执行聚合，客户端可以获得正确的模型聚合结果和满足验证条件的聚合结果的验证值。正确性可以通过以下等式获得：

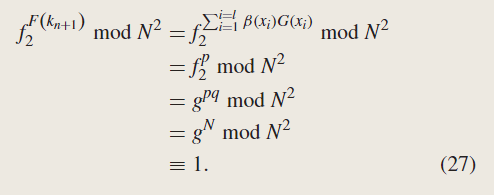


基于上述正确性分析，我们可以发现，如果中央服务器和客户端诚实地实现了上述协议，客户端可以获得正确的聚合结果。

### B.可验证性

在我们的系统中，我们使用拉格朗日插值和 Shamir 的秘密共享来确保正确的聚合。我们首先用Shamir的秘密共享拆分私钥p，并将拆分结果和f2 = gq发送给每个客户端。客户端使用拉格朗日插值对私钥和数据进行编码。云聚合数据和私钥以恢复 p。

当正确聚合时，很明显以下等式成立：



(m, t) Shamir 的秘密共享允许在没有所有客户端参与的情况下进行验证，确保系统的鲁棒性。

### C.灵活性

我们在验证机制和Paillier加密算法中使用相同的秘密共享算法，保证了整个联邦学习系统很好地支持客户端灵活地参与整个联邦学习过程。

我们将Paillier同态加密算法与秘密共享算法相结合，使同态算法使用多个不同的私钥对数据进行加密。当联邦系统中的客户端数量大于秘密共享阈值时，加密算法可以正确操作，同态加密的聚合结果可以使用相同的公钥解密。该算法的改进不仅可以保证客户端的数据安全，还可以支持客户端灵活地参与加密过程。

我们将验证机制与 Shamir 的秘密共享算法相结合。在验证云聚合结果时，秘密共享算法使客户端更加灵活，客户端不会误判云聚合结果的正确性，因为联邦学习过程中有几个客户端退出。只要联邦学习聚合过程中的客户端数量大于秘密共享阈值t，客户端就不会误判服务器的真实行为。我们的改进使验证机制更加健壮和灵活。

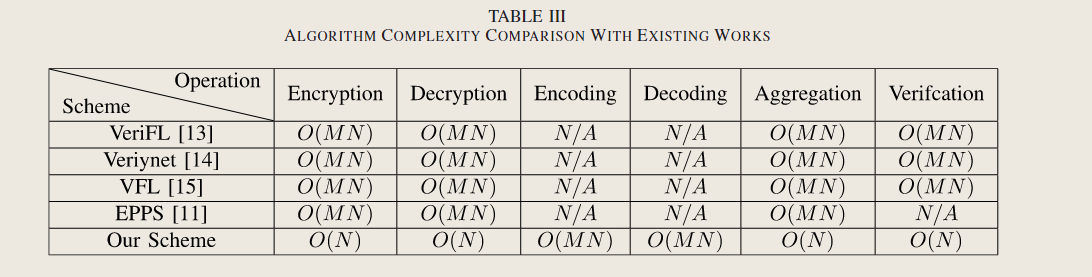
### D.功能性

为了反映我们的方案的优点，我们与现有的方案进行了功能比较。我们将我们的FVFL与四种最先进的隐私保护联邦学习方案进行比较，即EPPS[11]、VeriFL[13]、Verifynet[14]和VFL[15]。如表II所示，EPPS[11]利用阈值Paillier加密来保证客户端灵活参与，但聚合结果泄露给云服务器。VeriFL[13]利用掩蔽和秘密共享方法来保证用户的隐私，这也支持用户离线。Verifynet[14]采用昂贵的双线性映射来验证聚合结果的正确性，这将增加大量的计算和通信开销。VFL [15] 只关注如何验证聚合结果，而没有考虑用户在工作流程中退出。

与现有的方案相比，我们利用拉格朗日插值和Shamir的秘密共享来构建验证机制，利用Paillier加密和Shamir的秘密共享构造加密机制。即使多个客户端同时退出，FVFL也可以平稳地检测到。

### E.算法复杂性分析

如表 III 所示，对于联邦学习的每次迭代更新，云中只需要一个聚合。对于联邦学习的每次迭代更新，云中只需要一个聚合。假设整个系统迭代 N 次，则云中算法的复杂度将是 O(N)。



对于FVFL，客户端需要对梯度数据进行编码和加密，并对聚合结果进行解密和解码。假设每组有 M 个梯度，客户端需要首先对数据进行编码和解码。对于一组多维数据，它需要执行 M 个编码操作和 M 个解码操作。整个系统迭代N次，则编码和解码算法的复杂度分别为O(MN)，客户端加密操作和解密操作算法的复杂度为O(N)。

客户端需要使用拉格朗日插值多项式对梯度数据和子密钥进行打包，对于 M 个梯度和一个子密钥，客户端需要进行一次验证，假设整个系统迭代 N 次，验证的复杂度将是 O(N)。

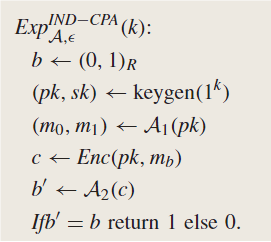
## 6.安全分析

我们相信客户端是诚实和好奇的，这意味着客户端将诚实地实现协议，不会参与恶意攻击或与服务器勾结。我们相信服务器是恶意的，这意味着服务器可能会对客户端产生虚假聚合结果。

基于上述恶意和非串通安全模型假设，我们证明了我们的客户端和服务器满足给定的安全定义，我们的整个联邦学习系统满足数据安全和隐私保护。

### A.安全定义

定义1(IND-CPA安全):如果公钥加密模型ε在语义上是安全的，那么对于任何以概率多项式时间运行的攻击者A=(A1，A2)，攻击AdvIND−CPA的优势，ε(K)=|Pr[ExpIND−CPAA，푡(K)=1]−1/2|可以忽略不计，ExpIND−CPAA，푡(K)特定实验可定义如下：



1）定义 2（模型参数安全和隐私）：对于联邦学习模型 FVFL，如果模型满足模型参数的安全性和隐私性，那么对于任何以概率多项式时间运行的攻击者 A，ExpMPPA、F VF L(k) 特定实验可以定义如下：图在论文第九页

根据上述实验，正式定义了模型副的安全性和隐私性，主要包括两个阶段:1)查询阶段和2)挑战阶段。在查询阶段，攻击者能够获得任何数据的相应加密结果。在挑战阶段，攻击者区分数据 C′0 和 C′1。联邦学习模型满足模型参数的安全性和隐私性，意味着攻击者成功攻击AdvMPP A,F VF L(k)≤negl(k)的优势，negl(k)表示输入k的可忽略的函数。

2)定义3(可验证性):对于FVFL，如果模型满足聚合结果的可验证性，对于任何概率多项式时间攻击者A, AdvV A,F VF L(k) = Pr[ExpV A,F VF L(k) = 1]的成功攻击AdvV A,F VF L(k) 特定实验的优势可定义如下：

2)定义3(可验证性):对于FVFL，如果模型满足聚合结果的可验证性，对于任何概率多项式时间攻击者A, AdvV A,F VF L(k) = Pr[ExpV A,F VF L(k) = 1]的成功攻击AdvV A,F VF L(k) 特定实验的优势可定义如下：

根据上述实验，在查询阶段，攻击者可以获取每个客户端的密文数据和数据的密文聚合结果。在挑战阶段，攻击者生成聚合结果并可以成功地验证它们。该系统模型需要攻击者伪造成功聚合结果 AdvV A,F VF L(k) =Pr[ExpV A,F VF L(k) = 1] ≤ negl(k) 的优势。

### B.客户端数据安全

1)定理1:在半诚实模型中，数据所有者的模型参数在上传阶段是安全和隐私。

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。该方案主要通过Paillier加密生成密文数据。成功区分密文数据AdvMPP A,F VF L(k) = Pr[ExpMPP A,F VF L(k) = 1−1/2]的概率可以忽略不计，因此数据所有者的模型参数在上传阶段满足安全定义2。定理 1 得到了证明。

2)定理2:在恶意模型中，数据所有者得到的联邦学习聚合结果是私有和可验证的。

证明：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，Paillier算法满足定义1。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。攻击者成功划分密文数据Adv MPPA,F VF L(k) = Pr[ExpMPPA,F VF L(k) = 1−1/2]的概率可以忽略不计。因此，聚合结果满足定义2。云在插值多项式变换后聚合多维值，客户端验证子密钥是否正确聚合。如果子键被正确聚合，则可以正确聚合梯度数据。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，这在实践中很难实现。因此，聚合结果满足定义3。我们可以得到定理2。

### C.云端数据安全

1)定理3:在半诚实模型中，数据在云聚合阶段是安全的和私有的。

证明：为了解码超递增的序列编码是一个背包问题，一般背包问题是NP困难的。在多项式时间内没有解，云无法获得特定的数据。Paillier进一步加密客户端数据，云完成同态下密文数据的聚合。Paillier加密方案满足语义安全性和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。因此，证明了定理 3。

## 7.性能分析

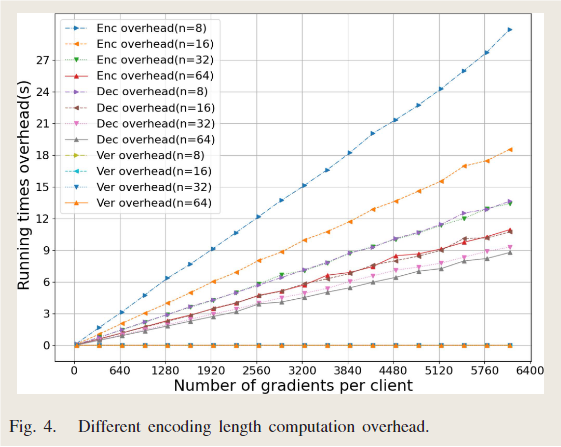
在这一部分中，我们从计算成本、通信成本和模型精度方面评估我们的FVFL模型的性能。此外，我们评估了模型聚合结果验证的额外成本。

### A.实验准备

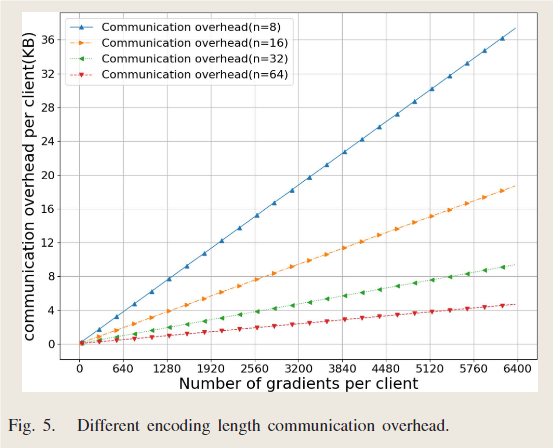
在这一部分中，我们进行了一个简单的实验来评估FVFL隐私保护联合学习模型的性能。该方案的模拟实验在 Windows 10 系统上运行，计算机配置为 Intel Core i7-11700 2.5 GHZ CPU 和 32 GB RAM。实验配置如下：所有实验都是用 Python 语言编写的，使用 PHE 库来实现 Paillier。我们将私钥 p 和 q 的长度设置为 3072 位，梯度数据的精度长度为 8 位。超递增序列 a = {1, 232,。, 2k∗32}，常数序列 k = {2,22,., 2k}，常数序列 h = {2 + 1, 22 +1，。, 2k + 1}。

### B.效率评估

1）计算开销：在这一部分中，我们分别评估我们的系统模型和客户端的计算成本。对于计算成本，我们进行了实验分析。在图 4 中，我们分别设置超序列长度 n = 8, 16, 32, 64，我们测试了 Enc、Dec 和 Ver 运行时间开销。如图 4 所示，随着每个客户端的梯度数量的增加，Enc、Dec 和 Ver 将消耗更多的时间。随着超序列长度的增加，Enc、Dec 和 Ver 的运行时间开销将更小。数据编码的维度越多，降低隐私保护联邦系统的计算成本就越有帮助。

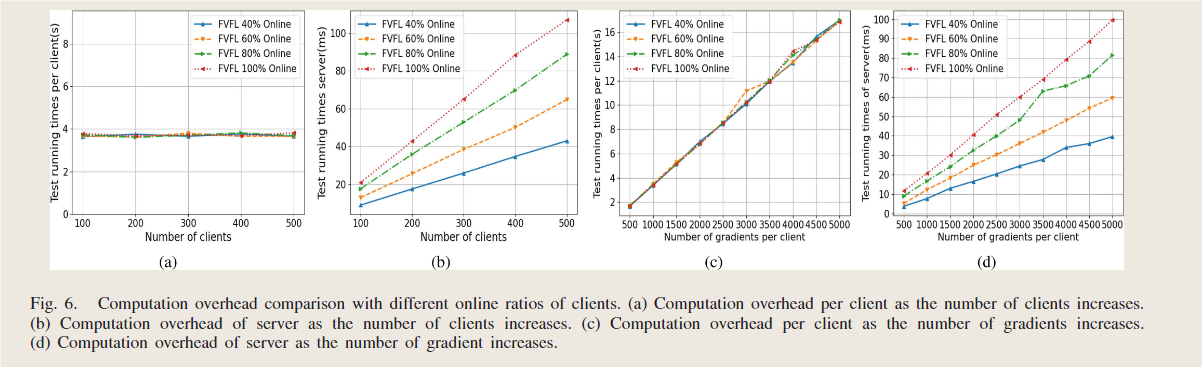


2)通信开销:在这一部分中，分析了客户端的通信开销。在图 5 中，我们分别设置超序列长度 n = 8, 16, 32, 64，我们测试了客户端的通信开销。如图 5 所示，随着梯度数量的增加，客户端通信开销逐步增加。随着超序列长度 n 的增加，客户端会消耗更少的通信开销。数据编码的维度越多，减少隐私保护联邦系统的通信开销就越有帮助。

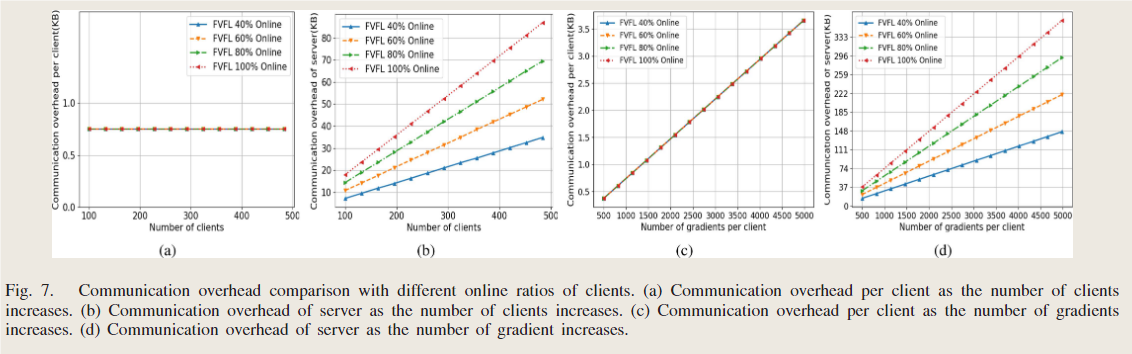


### C. 评估客户端灵活性（加入与退出）

1)计算开销:在这一部分中，我们对计算开销进行了实验分析。图 6 显示了在没有客户端退出时计算开销的比较，当在线有 40%、60% 和 80% 的客户时。我们设置超长 n = 32。



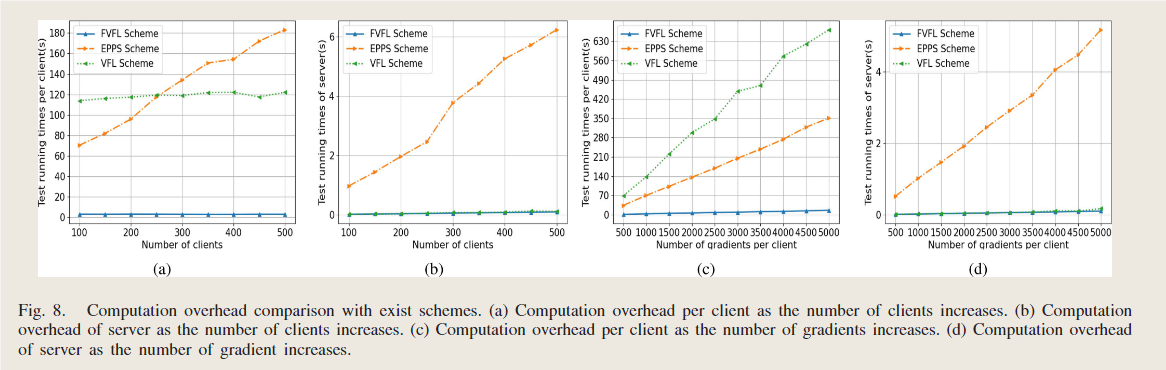
在图 6(a) 和 (b) 中，我们设置客户端的总数 m = 500，旁边我们设置每个用户的梯度数 n = 1000。图 6(a) 显示，随着客户端数量的增加，每个客户端的计算开销保持不变。图6(b)显示，服务器的计算开销随着客户端数量的增加呈线性增加。



在图6(c)和(d)中，我们设置客户端的总数m = 100，每个用户n = 5000的梯度数量。图6(c)显示，随着梯度数量的增加，每个客户端的计算开销线性增加。图6(d)显示，随着梯度数量的增加，服务器的计算开销线性增加。

图6清楚地表明，客户端数量退出不会影响每个客户端的运行时间，但服务器的运行时间将受到客户端数量退出的影响，因为更多的客户端是在线的，因为服务器的消耗次数更多。

2)通信开销:在这一部分中，我们对通信开销进行了实验分析。如图7所示，我们比较了没有客户端退出时的通信开销，当在线有40%、60%和80%的客户时。我们设置超长 n = 32。



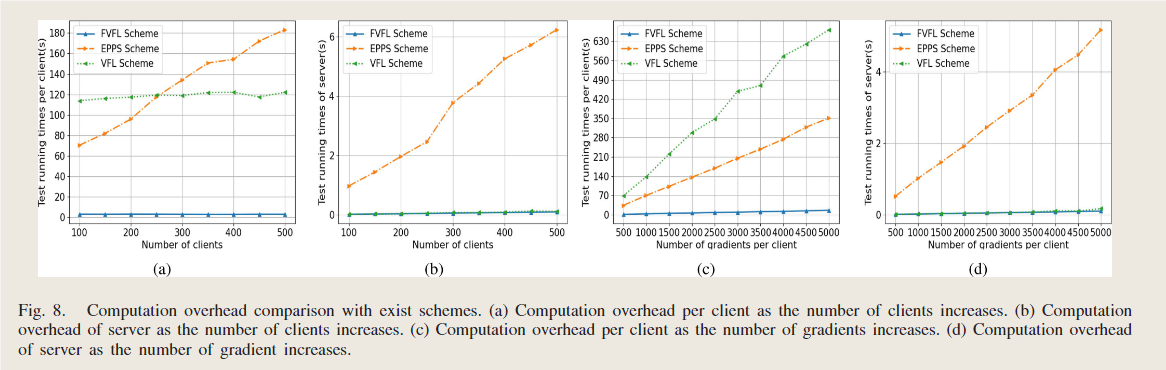
在图7(c)和(d)中，我们设置客户端的总数m = 100，除了我们设置每个用户n = 5000的梯度数量。图7(c)显示，随着梯度数量的增加，每个客户端的通信开销逐步增加。图7(d)显示，随着梯度数量的增加，服务器的通信开销逐步增加。

图 7 清楚地表明，客户端数量下降不会影响每个客户端的通信开销，但服务器的通信会受到客户端数量下降的影响，因为更多的客户端是在线的，因为服务器的通信更多。

### D. 与现有工作的比较

我们将我们的FVFL与两个最先进的隐私保护FL进行比较，即EPPS[6]和VFL[15]。

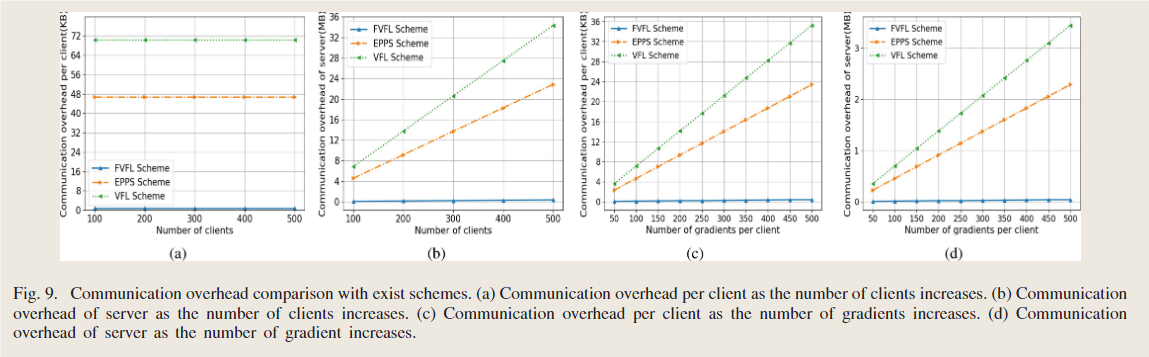
1)计算开销：在这一部分中，我们对计算开销进行了简单的实验分析。图 8 显示了计算开销 EPPS [6]、VFL [15] 和 FVFL 的比较。我们设置超长 n = 32。



在图 8(a) 和 (b) 中，我们设置客户端的总数 m = 500，旁边我们设置每个客户端的梯度数 = 1000。图 8(a) 显示，随着客户端数量的增加，每个客户端的计算开销。图8(B)示出了随着客户端数量的增加，服务器的计算开销。与EPPS和VFL相比，我们的FVFL方案在客户端上的计算开销很小，FVFL方案在服务器端的计算开销比EPPS少，FVFL方案在服务器端与VFL具有相同的计算开销。

在图 8(c) 和 (d) 中，我们设置客户端的总数 m = 100，旁边我们设置每个客户端的梯度数 = 5000。图 8(c) 显示，随着梯度数量的增加，每个客户端的计算开销。图 8(d) 显示服务器的计算开销随着梯度数量的增加。与EPPS和VFL相比，我们的FVFL方案在客户端上的计算开销很小，FVFL方案在服务器端的计算开销比EPPS少，FVFL方案在服务器端与VFL具有相同的计算开销。

2)通信开销:在这一部分中，我们对通信开销进行了简单的实验分析。如图9所示，我们比较了通信开销EPPS[6]、VFL[15]和FVFL。我们设置超长 n = 32。



在图 9(a) 和 (b) 中，我们设置客户端的总数 m = 500，旁边我们设置每个客户端的梯度数 = 1000。图 9(a) 显示，当每个客户端有相同数量的梯度时，当系统中的客户端数量不同时，比较每个客户端的通信开销。图9(b)显示，当每个客户端有相同数量的梯度时，当系统中的客户端数量不同时，比较服务器的通信开销。图 9(a) 和 (b) 显示，EPPS 和 VFL 确实比 FVFL 具有更高的服务器通信开销。

### E. 应用

FVFFL模型可以应用于许多现实世界的场景，即车辆网络系统和医疗系统。

1)车辆网络系统:随着车辆网络的广泛采用，多辆车通过数据共享联合预测道路交通现在很方便。然而，考虑到车辆网络系统的快速动态变化，车辆可能随时加入或退出，FVFL作为一个鲁棒的联邦学习系统。它确保整个联邦学习系统运行正确，而不管车辆的动态参与如何。此外，由于车辆网络系统中的路边单元容易受到恶意攻击，FVFL保证了私有车辆数据的安全性。每辆车都可以从路边单元验证聚合数据，从而防止恶意攻击者伪造聚合结果。

2)医疗系统:由于个别医疗机构持有的患者数据量有限，在有限的数据源进行训练时，疾病预测模型可能会被误诊。联邦学习方案可以克服数据孤岛并与多个数据源协作，以提高模型预测精度。鉴于患者数据的敏感性及其对患者安全影响的临界性，FVFL 确保了患者的私人信息的安全性，同时允许联邦参与者验证聚合结果的准确性。

## 8.结论

在本文中，我们提出了一种灵活且可验证的隐私保护联邦学习方案。FVFL的主要思想是设计灵活的可验证机制和灵活的加密机制。在此过程中，客户端的私有梯度可以保护不被泄露给其他客户端或服务器，客户端可以验证服务器的聚合结果，防止云恶意虚假聚合结果。此外，受益于我们的方案 FVFL，FVFL 对用户退出具有鲁棒性。