基于零集中差分隐私的联邦学习激励方案

李梦倩[1,2]，田有亮[1,3]，张军鹏[4]，赵冬梅[4]

（1.贵州大学公共大数据国家重点实验室，贵州 贵阳 550025；2.贵州大学计算机科学与技术学院，贵州 贵阳 550025；
3.贵州大学大数据与信息工程学院，贵州 贵阳 550025；4.河北师范大学河北省网络与信息安全重点实验室，河北 石家庄 050024）

摘　要：针对联邦学习场景下客户端选择不公平及模型训练低效问题，提出了一种基于激励机制的隐私保护联邦学习框架（zCDP-FL）。该框架将第二价反向拍卖应用到客户端的选择策略，设计了激励机制算法（SRAI），最大化系统效益。此外，采用零集中差分隐私，提出了隐私预算动态分配算法，实现训练过程中噪声规模的动态调整，在严格隐私计算边界的情况下提供更强的隐私保护。理论分析与仿真实验证明，zCDP-FL 能够有效防止隐私泄露，并提升了 2.13%~3.62% 模型训练效率。

关键词：联邦学习；零集中差分隐私；激励机制；隐私预算；动态分配

中图分类号：TN92

文献标志码：A

DOI：10.11959/j.issn.1000−436x.2025008

Incentive scheme for federated learning based on zero-concentrated differential privacy

LI Mengqian[1,2], TIAN Youliang[1,3], ZHANG Junpeng[4], ZHAO Dongmei[4]

1. State Key Laboratory of Public Big Data, Guizhou University, Guiyang 550025, China
2. College of Computer Science and Technology, Guizhou University, Guiyang 550025, China
3. College of Big Data and Information Engineering, Guizhou University, Guiyang 550025, China
4. Hebei Provincial Key Laboratory of Network & Information Security, Hebei Normal University, Shijiazhuang 050024, China

Abstract: To solve problems of unfair client selection and inefficient model training in federated learning, a privacy-preserving federated learning framework was proposed based on the incentive mechanism named zCDP-FL. An incentive mechanism algorithm, SRAI, was designed to maximize system benefits by applying the second price and the reverse auction to the client's selection strategy. In addition, a dynamic allocation algorithm for the privacy budget was proposed based on the zero-concentrated differential privacy to realize the dynamic adjustment of noise scale during the training, which provided a stronger privacy guarantee under the strict privacy constraint. Theoretical analyses and simulation experiments demonstrate that zCDP-FL can effectively prevent privacy leakage and enhance 2.13%~3.62% model training efficiency.

Keywords: federated learning, zero-concentrated differential privacy, incentive mechanism, privacy budget, dynamic allocation

---

收稿日期：2024–09–14；**修回日期：**2024–12–11

通信作者：田有亮，youliangtian@163.com

基金项目：国家自然科学基金资助项目（No.62272123, No.61672206, No.62062020）；中央引导地方科技发展基金资助项目（No.236Z0104G）；河北省科技计划基金资助项目（No.22567606H）；贵州省高层次创新型人才基金资助项目（No.[2020]6008）；贵州省科技计划基金资助项目（No.[2020]5017, No.[2022]065）

Foundation Items: The National Natural Science Foundation of China (No.62272123, No.61672206, No.62062020), Central Government Guides Local Science and Technology Development Found Projects (No.236Z0104G), The Science and Technology Program of Hebei Province (No.22567606H), The Project of High-Level Innovative Talents of Guizhou Province (No.[2020]6008), The Science and Technology Program of Guizhou Province (No.[2020]5017, No.[2022]065)

0 引言

目前，以语言模型为核心的ChatGPT等产品的推广应用，将人工智能由感知模拟引领为学习创造，这些智能平台的研发离不开机器学习（ML, machine learning）的支撑[1]。ML旨在挖掘现实世界中海量数据的潜在联系，提炼出有价值的知识，训练高质量模型用于分析、预测、推荐等。数据收集是ML的首要步骤，人们出于对数据安全考虑而不愿意分享私有信息，导致无法训练出有效的模型，因此数据的安全防护是ML系统所面临的固有挑战。作为一种分布式ML范式，联邦学习（FL, federated learning）为数据安全提供了新的解决思路，在保持客户端数据私有的情况下进行模型更新的交换，实现了新型的数据共享[2]。

FL通常基于客户端无条件地共享本地数据的假设，然而这在实际应用中是不现实的。客户端由不同通信能力、计算资源和数据分布的实体组成，本地训练消耗不同成本却获得相同的全局模型，如果没有合理的激励策略，将导致拥有高质量数据集的理性客户端不愿意贡献私有数据[3]。例如，智能家居设备通过FL实现个性化推荐、语音识别优化等功能。然而，许多资源设备的计算能力有限，或者设备厂商为了节约成本，不愿意投入大量计算资源进行本地训练。这就造成设备可能仅参与少量的训练步骤，或者选择伪造数据参与联合建模。此外，为降低通信开销，服务器将按照一定比例挑选客户端进行模型聚合，选择不同的客户端进行协同训练会产生不同的训练结果[4]。因此，激励更多优质的客户端积极参与协同训练是高效构建FL训练模型的关键思路。

在FL中，客户端数据由于不出本地降低了信息泄露的风险，但是现有研究表明，FL所面临的数据安全问题依然存在。模型更新是由本地数据训练得到的，依旧蕴含着客户端的私有数据。敌手可以通过攻击更新参数恢复私有数据，如深度梯度泄露[5]（DLG, deep leak from gradients）攻击和生成式对抗网络攻击[6]。面对多种潜在的隐私威胁，构造安全有效的防御方案，确保模型训练过程的机密性成为近年来研究的主要目标。

从隐私保护的方法看，现有的FL安全方案基于安全多方计算（SMC, secure multi-party computation）[7]、同态加密（HE, homomorphic encryption）[8]和差分隐私（DP, differential privacy）[9]等技术实现。SMC在互不信任的FL系统中，通过不经意传输[10]、混淆电路[11]、秘密共享[12]等手段，使客户端在不泄露各自私有输入信息且不影响数据运算结果的前提下开展联合隐私计算，但是频繁的信息交互带来了巨大的通信开销。HE直接在密文上进行运算，解密后的结果与明文运算结果相同，实现了敏感数据的无损保护，然而加解密操作和密文数据膨胀势必会给FL系统造成运行压力。具有严格数学定义的DP[13]采用混淆机制对数据进行扰动，使敌手无法通过随机化的结果还原隐私数据。相对于前2种方法，DP的轻量级计算使其拥有低时延和易部署的优点，更适用于大规模数据计算、多端点通信的FL场景[13]。噪声规模控制是DP应用的关键，大规模噪声在提高数据机密性的同时也会降低模型训练准确性。因此，如何在DP保护下提高模型训练效率是构建一个高质量FL系统的关键挑战。针对此问题，本文提出了一种基于激励机制的隐私保护联邦学习框架（zCDP-FL）。本文主要贡献如下。

1) 基于密封式第二价反向拍卖理论提出了一种真实的、个人理性的自适应激励方案SRAI，实现了客户端的资源配置优化。构造了灵活公平的奖励分配算法，激励客户端诚实地贡献高质量数据，防止恶意参与者合谋定价，使系统效益近似最大化。

2) 采用零集中差分隐私（zCDP, zero-concentrated differential privacy）技术设计了隐私预算动态分配算法，避免多余噪声注入，增强隐私保护效能，最大化利用数据实现模型训练精度的提升。该算法相比于传统的差分隐私方法拥有更强的隐私保护，并且提高了模型训练效率和性能。

3) 提出了隐私保护的FL激励框架zCDP-FL，解决了随机选择客户端的FL系统存在的训练效率低及隐私泄露问题。从理论分析与系统测试对本文方案进行了验证，zCDP-FL具有良好的隐私保护性与收敛性。

1 相关工作

1.1 联邦学习中的激励机制

在FL中引入激励机制，能够提高客户端参与训练的积极性，促使其贡献出高质量的本地模型更

新[14-16]。具体来说，Jin 等[17]提出了一个具有多维采购拍卖的激励机制，分析客户端的最优策略，运用期望效用指导服务器选择优质客户端进行模型训练。田有亮等[18]采用时间和训练损失进行客户端信誉值的量化，委托高性能雾节点进行本地数据训练。Zhang 等[19]基于博弈论提出了一种联合 DP 的 FL 方案，旨在刺激客户端参与协同训练，保护数据隐私。Chen 等[20]将动态博弈模型与激励机制相结合，对用户在数据共享中的博弈过程进行建模，鼓励用户参与数据共享的协同任务，保证模型训练的有效性。Deng 等[15]考虑将评估的节点学习质量与激励机制相结合鼓励客户端积极参与协同训练，提升模型性能。此外，通过剔除一些与训练无关的客户端，也可以提升模型训练效率[21-22]。然而，上述研究没有考虑到成本消耗与系统效益问题，致使客户端选择不公平，且 FL 系统不稳定，无法高效地协同训练全局模型。

1.2　联邦学习中的差分隐私

在模型更新上传服务器之前，客户端应用 DP 保护机制对更新参数进行噪声扰动，保证本地数据的机密性[23]。从噪声类型来看，现有方案常用的是拉普拉斯噪声和高斯噪声。例如，Abadi 等[24]提出了随机梯度下降算法的 DP 保护方案，通过在梯度更新上添加高斯噪声来实现隐私保护，设计了 Moments Accountant 机制跟踪 DP 在迭代训练过程中的隐私损失。此外，考虑到神经网络模型的分层结构，通过量化模型权重的重要性构建自定义扰动方案，提高模型的训练精度[25-26]。现有研究表明，DP 能够有效防御 DLG 攻击，但是均匀分配的隐私预算会降低模型的训练精度。值得注意的是，不限于传统的数值型噪声，Truex 等[27]提出了一种基于指数机制的 FL 框架，该框架使用本地 DP 将每个参数更新转换为整数来执行压缩扰动。上述解决方案将隐私预算设置为固定值，未考虑到随着 FL 训练轮数的增加，参数更新的数值范围将逐渐缩小，此时噪声会显得过大，进而加剧对模型聚合的影响。

2　理论知识

2.1　差分隐私

基于混淆机制的 DP 通过随机扰动方法实现隐私保护，即使对数据集中的单条数据进行了修改，算法的输出结果对其变化也不会敏感，因此，可以有效抵御差分攻击。

定义 1　(ε,δ)-DP。对于任意相邻数据集 D 和 D'，在机制 M 的扰动下，所有可能输出的结果集 O，如果满足

$$\Pr\left[M(D')\in O\right]\leqslant \mathrm{e}^{\varepsilon}\Pr\left[M(D)\in O\right]+\delta \tag{1}$$

则机制 M 满足 (ε,δ)-DP。其中，ε 为隐私预算，其值越小隐私保护性越强，δ 为松弛项，当 $\delta=0$ 时，有 $\mathrm{e}^{-\varepsilon}\leqslant\dfrac{\Pr\left[M(D')\in O\right]}{\Pr\left[M(D)\in O\right]}\leqslant \mathrm{e}^{\varepsilon}$，此时 M 为提供更强隐私保护的纯 DP 机制。

高斯机制被广泛应用于 DP，加噪过程表示为 $M(D)=f(D)+Y$，其中噪声 $Y\sim\mathcal{N}(0,\sigma^2)$ 服从高斯分布，σ 为噪声规模的标准差。在 DP 中，敏感度是衡量噪声作用在相邻数据集上查询结果最大差异的重要指标，高斯机制的敏感度采用二阶范式 L_2，定义为

$$\Delta s=\max_{D,D'}\left\|f(D)-f(D')\right\|_2 \tag{2}$$

敏感度与标准差的关系表示为 $\sigma\geqslant\dfrac{\kappa\Delta s}{\varepsilon}$，其中，$\kappa=\sqrt{2\ln\left(\dfrac{1.25}{\delta}\right)}$。

2.2　零集中差分隐私

零集中差分隐私[28-29]是根据 Rényi 散度定义的 DP 新变体，具有更严格的隐私成本限制。

定义 2　ρ-zCDP。zCDP 仅包含一个隐私参数 ρ，对于任意相邻数据集 D 和 D'，如果满足

$$\mathbb{D}_{\alpha}\left(M(D)\|M(D')\right)\leqslant\alpha\rho \tag{3}$$

则机制 M 满足 ρ-zCDP，其中，$\mathbb{D}_{\alpha}(M(D)\|M(D'))$ 为 α 阶的 Rényi 散度，$\alpha\in(1,\infty)$。

引理 1　对于任意 n 个满足 ρ-zCDP 的机制 M_1，$M_2,\cdots,M_n$，作用于同一个数据集，其序列组合满足 $\left(\sum_{i=1}^{n}\rho_i\right)$-zCDP。

引理 2　对于具有 L_2 敏感度的函数 $f\colon D\to\mathbb{R}^k$，机制 M 满足 ρ-zCDP，即 $M(D)=f(D)+Y'$，其中，$Y'\sim\mathcal{N}(0,\sigma'^2)$ 服从高斯分布，噪声标准差为 $\sigma'=\dfrac{\Delta s}{\sqrt{2\rho}}$。

引理 3　如果机制 M 提供 ρ-zCDP 保护，则对

于任意的$\delta > 0$，机制M满足$\left(\rho + 2\sqrt{\rho \log\left(\frac{1}{\delta}\right)}, \delta\right)$-DP。

3 问题定义

3.1 系统模型

zCDP-FL的系统模型由两类实体组成，包括中心聚合服务器（CAS, central aggregation server）和本地训练客户端（LTC, local training client），如图1所示，假设系统中包含一个CAS和N个LTC。表1为本文涉及的系统参数说明。

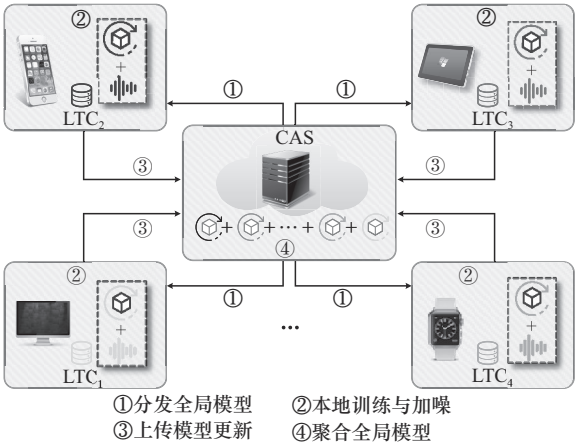


图1 zCDP-FL 系统模型

表1 系统参数

参数	含义
N	LTC总数量
k	参与训练的LTC数量
T	训练总轮数
D_i	第i个LTC的私有数据集
ω_G	全局模型
ω_i	第i个LTC的本地模型
g_G	全局模型梯度
g_i	第i个LTC的模型梯度
u_i	第i个LTC的效用收益
u_0	CAS的效用收益
ρ^t	第t轮训练的隐私参数
α	全局模型损失差阈值
θ	隐私参数增加速度
C	梯度裁剪阈值

1) 中心聚合服务器。CAS接收LTC上传的本地模型更新并执行安全聚合操作，将聚合结果发送给LTC。此外，CAS还负责激励协议的制定，其中包含设计成本函数、确定竞拍成功LTC与发放收益的规则。

2) 本地训练客户端。LTC利用私有数据进行模型训练，将本地模型更新提交至CAS。此外，LTC参与联邦训练的竞拍，根据激励协议计算相应的训练成本，并返回结果给CAS。

每个LTC都拥有本地数据集$D_i, i=1, \cdots, N$，用于接收来自CAS的全局模型ω_G，根据经验风险最小化目标计算本地模型。首先，利用全局模型ω_G计算模型梯度$g_i = \nabla L\left(\omega_i, D_i\right)$。随后，对$g_i$进行隐私保护处理，添加人工噪声为$\widehat{g_i} = g_i + \mathcal{N}(0, \sigma'^2)$。接下来，LTC更新本轮次局部模型为$\omega_i^{j+1} = \omega_i^j - \eta \widehat{g_i}$，$j=1, \cdots, E$。经过$E$轮本地迭代训练后，最终将模型更新$\Delta\omega_i = \omega_i^E - \omega_G$上传至CAS。按照zCDP-FL的激励协议，CAS遴选k个LTC参与协同训练，并进行安全聚合，更新FL系统全局模型为

$$\omega_G \leftarrow \omega_G + \frac{1}{k}\sum_{i=1}^{k}\Delta\omega_i \tag{4}$$

3.2 威胁模型

FL系统的隐私威胁来自CAS与LTC两类实体。假设CAS是诚实且好奇的，在忠实地履行协同训练协议的前提下，尝试利用特定LTC提交的模型更新获取私有数据。同时，FL系统中可能存在恶意LTC，其通过观察通信迭代过程中传递的全局模型和辅助信息推断其他LTC的敏感数据。

3.3 设计目标

zCDP-FL旨在完成一个具有激励性能的隐私保护FL框架，设计目标具体如下。

1) 效益最优。zCDP-FL应激励理性LTC贡献高质量数据集，并诚实报告成本价格，实现FL系统效益最优。

2) 数据安全。zCDP-FL应保证模型参数交互过程的安全，实现对敏感数据的保护。

3) 模型准确。zCDP-FL应确保模型可靠性并提升模型训练效率，实现高效建模。

4 方案设计

本节主要描述基于激励机制的隐私保护FL算法。为了鼓励潜在的拥有高质量数据集的LTC参与协同训练，本文提出了基于密封式第二价反向拍卖理论的激励机制SRAI，综合考虑数据质量和成本

价格，设计LTC的竞拍与定价算法。此外，为解决FL训练过程中的隐私泄露问题，本文引入zCDP，通过动态调整隐私参数和噪声规模，达到提升模型训练效率的效果。

4.1　基于反向拍卖的激励机制

在FL环境中，LTC具有异构性，不同LTC拥有的数据质量、设备计算能力和通信能力等均有差别。对训练能力参差不齐的LTC支付相同的报酬，降低了高质量LTC参与训练的积极性。本文结合LTC数据质量评估与成本价格计算设计了基于密封式第二价反向拍卖理论的激励机制（SRAI），实现FL系统效益最大化。

假设zCDP-FL系统中LTC的抽样比例为q，$k=qN$，k表示最终选择参与训练的LTC数量。在训练初始阶段，LTC根据CAS发放的训练任务与激励协议利用反向拍卖方式进行竞标b_i，竞标优胜者记为集合S。LTC的效用函数可表示为CAS支付的报酬p_i与LTC训练消耗的成本c_i之间的差值，即

$$u_i=\begin{cases}p_i-c_i, i\in S\\ A, \text{其他}\end{cases} \tag{5}$$

其中，$A\geqslant\frac{b_{i\in N}}{T}$，$\frac{b_{i\in N}}{T}$是根据竞标失败者提交的竞价计算出其训练一轮消耗的成本。

CAS的效用函数为LTC竞标优胜者完成FL训练任务为CAS带来的总价值与CAS支付给LTC集合N的总报酬之间的差值，即

$$u_0=W(S)-\sum_{i\in S}p_i-(N-k)A \tag{6}$$

其中，$W(S)$为竞标优胜者集合S参与训练任务为CAS带来的价值总和。

根据式(5)和式(6)，整个FL训练所产生的系统效益可表示为

$$u_{\text{system}}=u_0+\sum_{i\in N}u_i=W(S)-\sum_{i\in S}c_i-(N-k)A \tag{7}$$

由于系统效益受竞标优胜者参与训练时提供的数据质量的直接影响。因此，本文采用模型相似度指标对LTC的数据质量进行度量。利用余弦相似度函数比较LTC本地训练结束后的模型更新与CAS的全局模型更新之间的距离，即

$$\text{Con}_i=\cos\left(\Delta\omega_i,\Delta\omega_G\right)=\frac{\left\langle\Delta\omega_i,\Delta\omega_G\right\rangle}{\left\|\Delta\omega_i\right\|\left\|\Delta\omega_G\right\|} \tag{8}$$

如果LTC在本地训练时所产生的本地模型更新与全局模型更新方向越相近，则数据质量贡献度越高，且参与协同训练任务为CAS带来的总价值越大。CAS的价值收益函数定义为所有LTC带来价值收益的总和，表示为

$$W(S)=\sum_{i\in S}w_i=\sum_{i\in S}\gamma\text{Con}_i \tag{9}$$

其中，w_i为LTC$_i$参与训练产生的价值，γ为常系数。

为了便于衡量LTC参与协同训练带来的系统效益，本文定义了边际系统效益函数$v_i=\gamma\text{Con}_i-b_i$，其中$v_i\in V$。为此，最大化系统效益的目标函数被定义为

$$\max\sum_{i\in S}v_i=\max\sum_{i\in S}\left(\gamma\text{Con}_i-b_i\right) \tag{10}$$

其中，b_i是LTC竞标的价格，依据训练消耗的成本c_i产生。

SRAI的具体过程如算法1所示。优先挑选边际系统效益为非负的LTC为优胜者，若此时优胜者数目少于k，则从边际系统效益为负的集合中挑选边际系统效益影响小的LTC，直至有k个LTC竞拍成功。在计算CAS的支付价格集合P时，采用优胜者排除策略。在计算优胜者i的支付价格时，寻找其他LTC$_j$，使其边际系统效益影响与LTC$_i$的边际系统效益影响最接近，即

$$\frac{\left|\gamma\text{Con}_i-b_i'\right|}{\text{Con}_i}\approx\frac{\left|v_j\right|}{\text{Con}_j} \tag{11}$$

因此，有$p_i=b_i'\approx\gamma\text{Con}_i\pm\frac{\left|v_i\right|\text{Con}_i}{\text{Con}_j}$。

算法1　基于密封式第二价反向拍卖理论的激励机制（SRAI）

输入　总LTC数量N，抽样LTC数量k，边际系统效益v_i, $v_i\in V$，数据质量贡献度集合Con，LTC竞价集合b，支付价格A

输出　竞标优胜者集合S，CAS的支付价格集合P

1)$S\leftarrow\varnothing,S'\leftarrow\varnothing,N^-\leftarrow\varnothing,P\leftarrow\varnothing$
2) for $i\leftarrow 1$ to N do
3)　if $v_i\geqslant 0$
4)　　$S'\leftarrow S'\cup\{i\}$
5)　　if $|S'|\geqslant k$
6)　　选择b_i小的前k个LTC作为优胜者并将其放入集合S
7)　　else

8) $S \leftarrow S'$

9) end if

10) else

11) $N^- \leftarrow N \backslash S$

12) end if

13) end for

14) while $|S| < k$ do

15) 计算边际系统效益影响，挑选LTC，即

$$m = \arg\min_{i \in N^-} \frac{|v_i|}{\mathrm{Con}_i}$$

16) $S \leftarrow S \cup \{m\}$

17) end while

18) for $i \in S$ do

19) for $j \in N \backslash \{i\}$ do

20) 寻找LTC_j，其Con_j最接近于Con_i

21) $$p_i = b_i' \approx \gamma \mathrm{Con}_i \pm \frac{|v_i| \mathrm{Con}_i}{\mathrm{Con}_j}$$

22) $P \leftarrow P \cup \{p_i\}$

23) end for

24) end for

25) for $i \in N^-$ do

26) $p_i \leftarrow A$

27) $P \leftarrow P \cup \{p_i\}$

28) end for

29) return S and P

定理1 SRAI满足真实性。

证明 假设竞标优胜者i竞价为b_i，现考虑该优胜者另一竞价为b_i'，且$b_i' < b_i$。若$v_i = \gamma \mathrm{Con}_i - b_i \geqslant 0$，则有$v_i' = \gamma \mathrm{Con}_i - b_i' > v_i > 0$。若$v_i = \gamma \mathrm{Con}_i - b_i < 0$，则有$v_i' \geqslant 0$或者边际系统效益影响减小。此时，该竞标者$i$依旧是优胜者，由此可见，改变竞价并不会为竞标者$i$带来其他好处。因此，根据第二竞价规则，竞标优胜者获得的报酬与竞价无关，理性竞标者不会选择瞒报其真实竞价。此外，理性竞标者不会提高自己的竞价，即$b_i' > b_i$，在收益报酬保持不变的情况下，降低被选择的概率。综上所述，该激励机制满足真实性。证毕。

定理2 SRAI满足个人理性。

证明 定理1表明，该激励机制满足真实性，则有LTC会利用真实消耗的成本c_i进行竞标，对于任何竞标获胜者，都能够保证CAS对其支付价格$p_i \geqslant c_i$。竞标失败者效用收益为A，且$A \geqslant \frac{c_{i \in N}}{T}$，使所有竞标者有非负效用收益。因此，该激励机制满足个人理性。证毕。

定理3 SRAI满足计算效率。

证明 算法1中初始LTC选择阶段，最坏情况下会在N次迭代后终止，时间复杂度为$O(N)$，对b_i的排序算法的时间复杂度为$O(N\log N)$，所以总算法复杂度为$O(N^2\log N)$。在计算竞标者报酬阶段，对所有LTC进行遍历，算法时间复杂度为$O(N)$。综上可知，算法可在多项式时间内求解，该激励机制满足计算效率。证毕。

4.2 隐私预算动态分配

为了构建具有隐私保护功能的高效FL框架，将轻量级隐私保护技术DP引入训练过程。然而，DP在提供隐私安全的同时会造成一定程度的模型性能损失。随着训练轮数的迭代，使用与初始训练阶段相同的噪声规模会致使模型偏离正常结果。因此，本文考虑伴随迭代轮数动态地调整噪声规模。

定义FL中最大迭代轮数T、损失差阈值α、隐私参数ρ的最小值$\rho_{\min}$和最大值$\rho_{\max}$。考虑通过观察迭代训练中模型损失值的变化而动态地调整隐私参数ρ的设置。若当前轮的全局模型损失与前一轮的全局模型损失差值的绝对值小于损失差阈值时，即$\left|L_G^t - L_G^{t-1}\right| \leqslant \alpha$，则开始调整隐私参数$\rho$，并重新进行本轮训练，表示为

$$\rho^t = \begin{cases} \rho_{\min} + (t-1)\theta, t < T \text{和} \left|L_G^t - L_G^{t-1}\right| \leqslant \alpha \\ \rho^{t-1}, \text{其他} \end{cases} \tag{12}$$

其中，$0 < \theta < 1$代表增长速度。如果在调整隐私参数后出现$\rho^t > \rho^{\max}$的情况，则取$\rho^t = \rho^{\max}$，此后隐私参数ρ不再增加，均使用$\rho_{\max}$直到训练结束。因此，在FL训练过程中对梯度加噪后的结果为

$$\widehat{g_i^t} = \begin{cases} g_i^t + N\left(0, \frac{(\Delta s)^2}{2\rho^t}\right), \rho_{\min} \leqslant \rho^t < \rho_{\max} \\ g_i^t + N\left(0, \frac{(\Delta s)^2}{2\rho_{\max}}\right), \rho^t \geqslant \rho_{\max} \end{cases} \tag{13}$$

该方案在动态调整隐私参数并重新进行本轮训练时，通常有$\rho^{t\prime} \geqslant \rho^t$，即本轮训练的隐私参数$\rho^t$小于或等于采用动态调整隐私参数后重复训练本轮的隐私参数$\rho^{t\prime}$。根据zCDP算法的序列组合特性，得到隐私参数增量$\rho^{t\prime} - \rho^t$。利用隐私参数

ρ^t加噪之后的梯度表示为$g^{t\prime}=g^t+\mathcal{N}\left(0,\frac{(\Delta s)^2}{2\rho^t}\right)$，隐私参数增量$\rho^{t\prime}-\rho^t$对梯度$g^t$的加噪结果为$g^{t\prime\prime}=g^t+\mathcal{N}\left(0,\frac{(\Delta s)^2}{2\left(\rho^{t\prime}-\rho^t\right)}\right)$，结合$g^{t\prime}$和$g^{t\prime\prime}$有

$$\widehat{g}^t=\frac{\rho^t g^{t\prime}+\left(\rho^{t\prime}-\rho^t\right)g^{t\prime\prime}}{\rho^{t\prime}} \tag{14}$$

式(14)满足无偏估计，即

$$\mathrm{E}\left[\widehat{g}^t\right]=g^t,\mathrm{Var}\left(\widehat{g}^t\right)=\frac{(\Delta s)^2}{2\rho^{t\prime}} \tag{15}$$

最终，通过计算发现对加噪梯度$\widehat{g}^t$的估计满足使用动态调整噪声规模后的情况，即在隐私参数为$\rho^{t\prime}$时，噪声规模为$\frac{(\Delta s)^2}{2\rho^{t\prime}}$，证明本文方案可行。基于隐私预算动态分配的联邦学习算法如算法2所示。

算法 2　基于隐私预算动态分配的联邦学习算法

输入　LTC数量k，初始化全局模型ω_G，训练最大轮数T，本地迭代次数E，隐私损失增长速度θ，隐私参数最小值$\rho_{\min}$与最大值$\rho_{\max}$，损失差阈值α

输出　全局模型ω_G^T

LTC

1)for $i\leftarrow 1$ to k do

2)　$\omega_i^0\leftarrow\omega_G,\rho_i\leftarrow\rho^t$

3)　for $j\leftarrow 1$ to E

4)　本地梯度更新$g_i^j=\nabla L(\omega_i^j,D_i)$

5)　梯度裁剪$\bar{g}_i^j\leftarrow\frac{g_i^j}{\max\left(1,\frac{\left\|g_i^j\right\|}{C}\right)}$

6)　梯度加噪$\bar{g}_i^j=\bar{g}_i^j+\mathcal{N}\left(0,\frac{(\Delta s)^2}{2\rho_i}\right)$

7)　模型更新$\omega_i^{j+1}=\omega_i^j-\eta g_i^j$

8)　end for

9)　计算本地参数更新$\Delta\omega_i=\omega_i^E-\omega_G$

10)　上传本地参数更新$\Delta\omega_i$至CAS

11)end for

CAS

12)for $t\leftarrow 1$ to T do

13)　全局模型聚合$\omega_G^t=\omega_G^{t-1}+\frac{1}{k}\sum_{i=1}^{k}\Delta\omega_i^t$

14)　计算本次迭代全局模型损失L_G^t

15)　if $t<T$ and $\left|L_G^t-L_G^{t-1}\right|\leqslant\alpha$ then

16)　$\rho^t=\rho_{\min}+(t-1)\theta$

17)　if $\rho^t<\rho_{\max}$

18)　$\rho^t\leftarrow\rho^t$

19)　else

20)　$\rho^t\leftarrow\rho_{\max}$

21)　end if

22)　LTC重新执行第t轮训练

23)　else

24)　$\rho^t\leftarrow\rho^{t-1}$

25)　end if

26) end for

27) return ω_G^T

算法2中CAS选中的k个LTC参与基于隐私预算动态分配的联邦学习训练，每个LTC在本地进行E轮Epoch迭代，因此本地训练的算法复杂度为$O(E)$。由于全局联邦训练需要进行T轮，在理想情况下，LTC不再重新对某轮进行训练，算法复杂度为$O(TE)$。最坏情况下，需要进行T轮重新训练，算法复杂度为$O(T^2E)$。

4.3　zCDP-FL系统框架

本节将详细介绍zCDP-FL系统框架设计流程，该过程包括以下3个阶段。

1) 系统初始化。CAS初始化全局模型ω_G和隐私参数ρ，制定激励协议，并将上述内容下发至每个LTC。

2) LTC选择。首先，LTC根据激励协议计算并提交竞标价格b_i。随后，CAS根据接收到的竞标价格利用算法1选择出k个LTC参与FL训练。

3) 模型训练。选中的k个LTC利用全局模型ω_G和本地数据集根据算法2进行本地训练。在本地训练过程中，利用接收到的隐私参数ρ对本轮梯度进行加噪处理。在迭代E轮后，上传本地参数更新到CAS。CAS根据参数更新聚合全局模型，并计算新一轮训练中的隐私参数ρ，该过程至多迭代T轮。

综上所述，LTC和CAS完成本次任务的FL训练。

5　性能分析

5.1　敏感度与隐私分析

假设第i个LTC拥有相邻数据集D_i和D_i'，定义梯度裁剪$\|g\|\leqslant C$，损失函数$L_i(\omega,D)$，敏感度Δs表

示为

$$\Delta s = \max\left\| \arg\min_{\omega} L_i(\omega,D) - \arg\min_{\omega} L_i(\omega,D') \right\|_2 = \eta \max\left\| g_i - g_i' \right\|_2 = \frac{\eta}{|D_i|} 2C \tag{16}$$

接下来证明本文方案满足(ε,δ)-DP。

定理4 算法2满足(ε,δ)-DP。

证明 在FL中，考虑前t轮使用相同的隐私参数$\rho_{\min}$。若经过T轮训练与隐私参数动态调整后，隐私参数ρ未达到最大值$\rho_{\max}$，证明算法2保证ρ-zCDP如式(17)所示。

$$\begin{aligned}\rho_{\text{sum}} &= \rho^1 + \rho^2 + \cdots + \rho^t + \rho^{t+1} + \cdots + \rho^T = \\ &(t-1)\rho_{\min} + (T-t+1)\rho_{\min} + \\ &(T-t+1)(T-t)\frac{\theta}{2} = \\ &T\rho_{\min} + (T-t+1)(T-t)\frac{\theta}{2}\end{aligned} \tag{17}$$

若在第$t+\tau$轮训练后，经过隐私参数动态调整，隐私参数达到最大值$\rho_{\max}$，证明算法2保证ρ-zCDP如式(18)所示。

$$\begin{aligned}\rho_{\text{sum}} &= \rho^1 + \rho^2 + \cdots + \rho^t + \rho^{t+1} + \cdots + \rho^T = \\ &\rho^1 + \rho^2 + \cdots + \rho^t + \rho^{t+1} + \cdots + \\ &\rho^{t+\tau} + \rho_{\max}^{t+\tau+1} + \cdots + \rho_{\max}^{T} = \\ &(t-1)\rho_{\min} + (\tau+1)\rho_{\min} + \\ &\tau(\tau+1)\frac{\theta}{2} + (T-t-\tau)\rho_{\max} = \\ &(t+\tau)\rho_{\min} + \tau(\tau+1)\frac{\theta}{2} + (T-t-\tau)\rho_{\max}\end{aligned} \tag{18}$$

由此可证明，在$\varepsilon = \rho + 2\sqrt{\rho\log\left(\frac{1}{\delta}\right)}$的情况下，算法2满足$(\varepsilon,\delta)$-DP。证毕。

5.2 收敛性分析

本节对zCDP-FL进行收敛性理论证明。为了方便分析，首先做如下假设。

假设1：$L_i(\omega)$是凸函数。

假设2：损失函数$L_i(\omega)$满足正参数β的Polyak-Lojasiewicz条件，则对于最优参数$\hat{\omega}^*$有$L(\hat{\omega}^t) - L(\hat{\omega}^*) \leqslant \frac{1}{2\beta}\left\|\nabla L(\hat{\omega}^t)\right\|^2$。

假设3：对于任意$\omega,\omega'\in\mathbb{R}^d$，损失函数$L_i(\omega)$是Lipschitz连续，则存在常数$\mu$，有$\left\|\nabla L_i(\hat{\omega}) - \nabla L_i(\widehat{\omega'})\right\| \leqslant \mu\left\|\hat{\omega} - \widehat{\omega'}\right\|$。

假设4：$\eta \leqslant \frac{1}{\mu}$，$\eta$为学习率。

定理5 如果满足以上假设，则zCDP-FL的收敛性上界为

$$\begin{aligned}&L(\hat{\omega}^T) - L(\hat{\omega}^*) \leqslant \\ &\left(\frac{\mu\beta\eta^2}{k^2} - 2\beta\eta + 1\right)^T \left(L(\hat{\omega}^0) - L(\hat{\omega}^*)\right) + \\ &\sum_{j=0}^{T-1}\left(\frac{\mu\beta\eta^2}{k^2} - 2\beta\eta + 1\right)^j \left(\frac{\mu}{2}\sqrt{\frac{2\Delta s^2 T}{k}\sum_{i=1}^{k}\frac{\ln\left(\frac{1}{\delta_i}\right)}{\varepsilon_i^2}}\right)\end{aligned} \tag{19}$$

证明 首先，基于假设4利用二阶泰勒展开式进行计算，如式(20)所示。

$$\begin{aligned}&L(\hat{\omega}^{t+1}) - L(\hat{\omega}^t) \leqslant \\ &\nabla L(\hat{\omega}^t)^T(\hat{\omega}^{t+1} - \hat{\omega}^t) + \frac{\mu}{2}\left\|\hat{\omega}^{t+1} - \hat{\omega}^t\right\|^2\end{aligned} \tag{20}$$

LTC的本地模型可以表示为

$$\hat{\omega}_i^{t+1} = \hat{\omega}^t - \eta\nabla L_i(\hat{\omega}^t) \tag{21}$$

CAS聚合的全局模型为

$$\hat{\omega}^{t+1} = \sum_{i=1}^{k} p_i\hat{\omega}_i^{t+1} = \sum_{i=1}^{k} p_i(\hat{\omega}_i^{t+1} + n_i^{t+1}) \tag{22}$$

定义CAS聚合时LTC的噪声总和为

$$n^{t+1} = \sum_{i=1}^{k} p_i n_i^{t+1} \tag{23}$$

第（t+1）轮与第t轮的全局模型差可以表示为

$$\hat{\omega}^{t+1} - \hat{\omega}^t = -\eta\sum_{i=1}^{k} p_i\nabla L_i(\hat{\omega}^t) + n^{t+1} \tag{24}$$

将式(21)、式(22)和式(24)代入式(20)，则有

$$\begin{aligned}&L(\hat{\omega}^{t+1}) - L(\hat{\omega}^t) \leqslant \\ &\nabla L(\hat{\omega}^t)^T\left(-\eta\sum_{i=1}^{k} p_i\nabla L_i(\hat{\omega}^t) + n^{t+1}\right) + \\ &\frac{\mu}{2}\left\|-\eta\sum_{i=1}^{k} p_i\nabla L_i(\hat{\omega}^t) + n^{t+1}\right\|^2 = \\ &-\eta\nabla L(\hat{\omega}^t)^T\sum_{i=1}^{k} p_i\nabla L_i(\hat{\omega}^t) + \\ &\frac{\mu\eta^2}{2}\left\|\sum_{i=1}^{k} p_i\nabla L_i(\hat{\omega}^t)\right\|^2 + \frac{\mu}{2}\left\|n^{t+1}\right\|^2\end{aligned} \tag{25}$$

根据式(25)可以得到

$$\mathbb{E}\left[L\left(\hat{\omega}^{t+1}\right)\right]-L\left(\hat{\omega}^{*}\right)\leqslant$$
$$\mathbb{E}\left[L\left(\hat{\omega}^{t}\right)\right]-L\left(\hat{\omega}^{*}\right)-\eta\left\|\nabla L\left(\hat{\omega}^{t}\right)\right\|^{2}+$$
$$\frac{\mu\eta^{2}}{2}\mathbb{E}\left[\left\|\sum_{i=1}^{k}p_{i}\nabla L_{i}\left(\hat{\omega}^{t}\right)\right\|^{2}\right]+\frac{\mu}{2}\mathbb{E}\left[\left\|n^{t+1}\right\|^{2}\right] \quad (26)$$

CAS第t轮全局聚合的噪声为

$$\mathbb{E}\left[\left\|n^{t+1}\right\|\right]=\sqrt{\frac{2\Delta s^{2}(t+1)}{k}\sum_{i=1}^{k}\frac{\ln\left(\frac{1}{\delta_{i}}\right)}{\varepsilon_{i}^{2}}} \quad (27)$$

此外，还有

$$\mathbb{E}\left[\left\|\sum_{i=1}^{k}p_{i}\nabla L_{i}\left(\hat{\omega}^{t}\right)\right\|^{2}\right]=\frac{1}{k^{2}}\mathbb{E}\left[\sum_{i=1}^{k}\left\|\nabla L_{i}\left(\hat{\omega}^{t}\right)\right\|^{2}\right]+$$
$$\frac{1}{k^{2}}\mathbb{E}\left[\sum_{i=1,i\neq j}^{k}\left[\nabla L_{i}\left(\hat{\omega}^{t}\right)\right]^{\mathrm{T}}\nabla L_{j}\left(\hat{\omega}^{t}\right)\right]=\frac{1}{k^{2}}\left\|\nabla L\left(\hat{\omega}^{t}\right)\right\|^{2} \quad (28)$$

将式(27)和式(28)代入式(26)，可以得到

$$\mathbb{E}\left[L\left(\hat{\omega}^{t+1}\right)\right]-L\left(\hat{\omega}^{*}\right)\leqslant$$
$$\mathbb{E}\left[L\left(\hat{\omega}^{t}\right)\right]-L\left(\hat{\omega}^{*}\right)-\eta\left\|\nabla L\left(\hat{\omega}^{t}\right)\right\|^{2}+$$
$$\frac{\mu\eta^{2}}{2}\left(\frac{1}{k^{2}}\left\|\nabla L\left(\hat{\omega}^{t}\right)\right\|^{2}\right)+\frac{\mu}{2}\sqrt{\frac{2\Delta s^{2}(t+1)}{k}\sum_{i=1}^{k}\frac{\ln\left(\frac{1}{\delta_{i}}\right)}{\varepsilon_{i}^{2}}}\leqslant$$
$$\mathbb{E}\left[L\left(\hat{\omega}^{t}\right)\right]-L\left(\hat{\omega}^{*}\right)+$$
$$\left(\frac{\mu\eta^{2}}{2k^{2}}-\eta\right)\left\|\nabla L\left(\hat{\omega}^{t}\right)\right\|^{2}+\frac{\mu}{2}\sqrt{\frac{2\Delta s^{2}(t+1)}{k}\sum_{i=1}^{k}\frac{\ln\left(\frac{1}{\delta_{i}}\right)}{\varepsilon_{i}^{2}}} \quad (29)$$

由于损失函数$L_i(\omega)$满足Polyak-Lojasiewicz条件，即

$$L\left(\hat{\omega}^{t}\right)-L\left(\hat{\omega}^{*}\right)\leqslant\frac{1}{2\beta}\left\|\nabla L\left(\hat{\omega}^{t}\right)\right\|^{2} \quad (30)$$

因此，可以得出

$$L\left(\hat{\omega}^{T}\right)-L\left(\hat{\omega}^{*}\right)\leqslant$$
$$\left(\frac{\mu\beta\eta^{2}}{k^{2}}-2\beta\eta+1\right)^{T}\left(L\left(\hat{\omega}^{0}\right)-L\left(\hat{\omega}^{*}\right)\right)+$$
$$\sum_{j=0}^{T-1}\left(\frac{\mu\beta\eta^{2}}{k^{2}}-2\beta\eta+1\right)^{j}\left(\frac{\mu}{2}\sqrt{\frac{2\Delta s^{2}T}{k}\sum_{i=1}^{k}\frac{\ln\left(\frac{1}{\delta_{i}}\right)}{\varepsilon_{i}^{2}}}\right) \quad (31)$$

证毕。

根据定理5可知，当隐私保护程度降低时，即隐私预算值变大，损失函数之差会减小，这符合实际情况。在FL中所加噪声越少，训练的全局模型越趋近于最优全局模型。根据假设4，得到$\mu\eta\leqslant 1$，所以$\frac{\mu\beta\eta^{2}}{k^{2}}-2\beta\eta+1<1$，因此$T$轮迭代后的全局损失函数与最优损失函数之差趋向于一个较小的稳定差值。

6　实验性能评估

6.1　实验设置

本文的所有实验均在配置CentOS 7.9，Intel (R) Xeon(R) Silver 4210R 2.40 GHz CPU和32 GB RAM的服务器上完成，采用PyTorch库构建FL环境。基于MNIST和CIFAR-10数据集对zCDP-FL进行性能评估。

6.2　实验性能

6.2.1　激励机制性能分析

为了验证zCDP-FL方案中SRAI激励机制的有效性，仿真实验测试在LTC数量$N=400$、采样率$q=0.5$的情况下，MNIST和CIFAR-10数据集训练达到指定精度所需的迭代轮数。为清晰地验证激励机制的有效性，将SRAI方案应用于FL训练，并与其他基于拍卖的FL激励机制方案进行对比[21,30-31]，如表2和表3所示。结果表明，SRAI比FedSGD[32]、GCA（gradient-cluster-auction）[32]和RRAFL[21]方案需要更少的迭代轮数就可达到指定精度。此外，验证了训练迭代指定轮数后不同方案在2种数据集下所达到的模型精度，如表4所示，SRAI方案能够使训练模型达到更高的精度。因此，SRAI方案拥有良好的激励性能，能够选择拥有高质量数据集的LTC参与训练，提升模型训练效率。

表2　FL达到指定模型精度所需训练轮数（MNIST）

方案	模型精度为92%	模型精度为93%
FedSGD	2	3
LDP-FL	4	23
RRAFL	3	6
GCA	3	5
SRAI	2	2
zCDP-FL	3	7

表3　FL达到指定模型精度所需训练轮数（CIFAR-10）

方案	模型精度为50%	模型精度为55%
FedSGD	24	49
LDP-FL	35	70
RRAFL	24	47
GCA	22	45
SRAI	19	43
zCDP-FL	26	54

表4　25轮训练后所达到的模型精度

方案	MNIST数据集	CIFAR-10数据集
FedSGD	96.30%	50.40%
LDP-FL	93.20%	47.90%
RRAFL	97.20%	51.30%
GCA	97.00%	51.50%
SRAI	98.60%	53.10%
zCDP-FL	94.50%	49.80%

综上所述，本文设计的SRAI方案能够鼓励客户端积极参与FL训练，且模型可用性好。

6.2.2　模型精度对比

本节将zCDP-FL方案与FedSGD[2]和LDP-FL方案[31]进行模型精度实验对比，分别测试经过多轮训练不同方案所能达到的模型精度。实验设置LTC数量$N=400$，采样率$q=0.5$，隐私参数最小值$\rho_{\min}=50$，隐私参数最大值$\rho_{\max}=70$，松弛项$\delta=1\times10^{-5}$，zCDP-FL方案与其他FL方案在2种数据集上的模型精度如图2和表5所示。

观察图2可以发现，在LTC数量保持相同的情况下，加入DP保护的FL会在一定程度上降低模型精度，由此说明添加的人工噪声会影响模型训练结果，可通过调整噪声规模提升模型性能。此外，随着模型训练的多轮迭代，传统DP的序列组合特性会产生隐私损失较大且模型精度不高的问题。图2(a)和图2(b)均显示，在整个训练周期，zCDP-FL方案的模型精度始终高于LDP-FL方案，且训练结果接近于基线方案FedSGD，证明了本文方案的性能优于LDP-FL方案。这是因为zCDP-FL方案相比于LDP-FL方案能够降低隐私损失且提供更严格的隐私保护，更适用于FL多轮迭代训练的加噪保护。并且通过观测模型训练损失值，对噪声规模进行实时动态调整，能够实现隐私保护并提高模型精度。

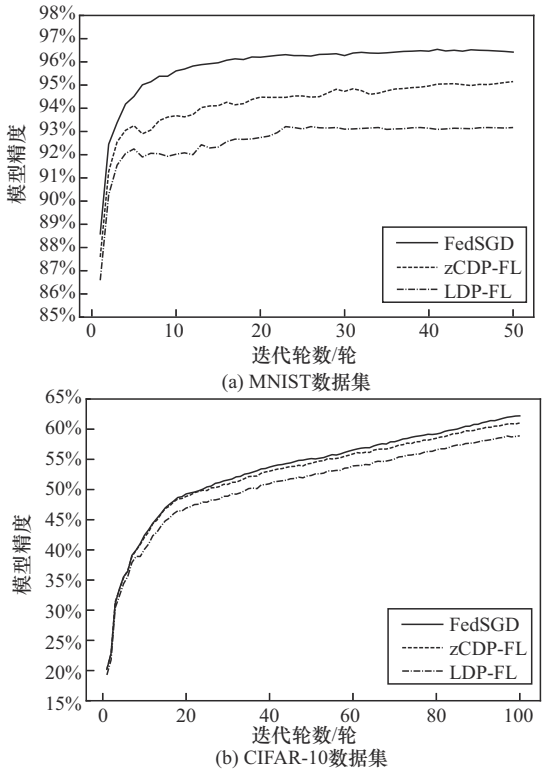


图2　zCDP-FL与其他FL方案在2种数据集上的模型精度

表5　本文方案与现有方案的模型精度对比

方案	MNIST数据集	CIFAR-10数据集
FedSGD	96.42%	62.21%
LDP-FL	93.17%	58.90%
zCDP-FL	95.15%	61.03%

综上所述，利用zCDP-FL方案能够降低传统DP保护技术所产生的隐私损失，防止模型训练偏离正常结果，提升模型性能。

6.2.3　LTC数量影响对比

本节测试不同LTC数量对模型精度的影响。实验在批处理Batch=128、LTC本地训练轮数Epoch=5和采样率$q=1$的参数设置下，将LTC数量分别设置为50、100、150和200，对比模型精度的变化情况，如图3所示。

观察图3可以发现，在保持LTC本地私有数据集大小不变的情况下，zCDP-FL方案中的模型精度随着LTC数量的增加而提高。在$N=50$时，MNIST数据集的模型精度最高达到94.06%，CIFAR-10数据集的模型精度最高达到51.81%。在$N=200$时，MNIST数据集的模型精度最高达到96.17%，CIFAR-10数据集的模型精度最高达到61.03%。这是因为随着参与训

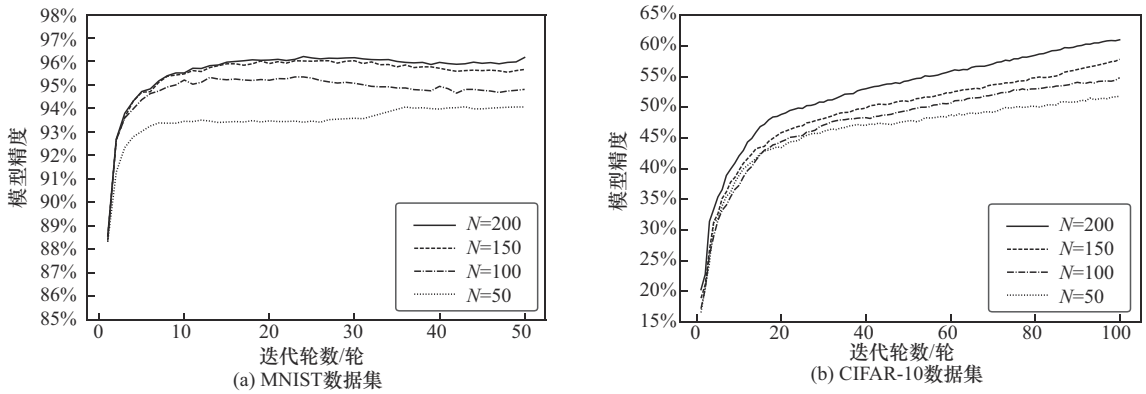


图3　LTC数量对模型精度的影响

练的LTC数量增加，训练的模型性能会随之提升。图4分别设置LTC数量为100、150和200，对3种FL方案模型精度进行了对比，其中zCDP-FL方案相比于LDP-FL方案更接近基线方案FedSGD的实验结果。

综上所述，在相同的超参数设置下，随着LTC数量的增加模型精度在不断提升，表明增加LTC数量可以有效提高模型训练的准确率。在测试数据集上的实验结果证实，zCDP-FL方案始终优于LDP-FL方案，证明了zCDP-FL方案的有效性。

6.2.4　隐私参数影响对比

本节测试隐私参数对FL训练的影响，在保证其他参数相同的情况下，分别验证了在LTC数量$N = 100$和$N = 200$时，调整$\rho_{\min}$对模型精度的影响，如图5所示。

图5表明，在zCDP-FL方案中，模型精度随着隐私参数$\rho_{\min}$的增加而提高，当$\rho_{\min} = 50$时，相比于其他2种设置$\rho_{\min} = 0.5$和$\rho_{\min} = 12.5$，在$N = 100$和$N = 200$的2种情况下，其模型精度都最接近未加噪的情况，这意味着$\rho_{\min}$的增加会使噪声规模变小，隐私保护程度降低，进而提升模型精度。在本文方案中，所设计的隐私预算动态分配算法是随损失函数差值变化而变化的，随着迭代轮数的增加，全局损失函数逐渐减小，损失函数差值也逐渐变小并趋于稳定。因此，隐私预算参数会随着训练轮数增加而变大，直到损失函数差值达到设定阈值时，隐私预算参数不再增长。以上结果表明，在zCDP-FL的隐私预算动态分配方案中，初始设置的隐私参数$\rho_{\min}$代表此次训练过程中所设置的最高隐私保护水平，所以$\rho_{\min}$的设置尤其重要。

此外，基于隐私预算测试未加激励机制时不同方案对模型精度的影响。设置LTC数量$N = 200$，观测隐私预算值ε分别分配1、5和10时模型精度的变化情况，如图6所示。在不同隐私预算值设定下，本文方案训练所得的模型精度均高于LDP-FL方案。隐私预算的动态分配会减小噪声规模，而固定隐私预算值的设定会随着训练轮次迭代使噪声对模型训练影响越来越大。

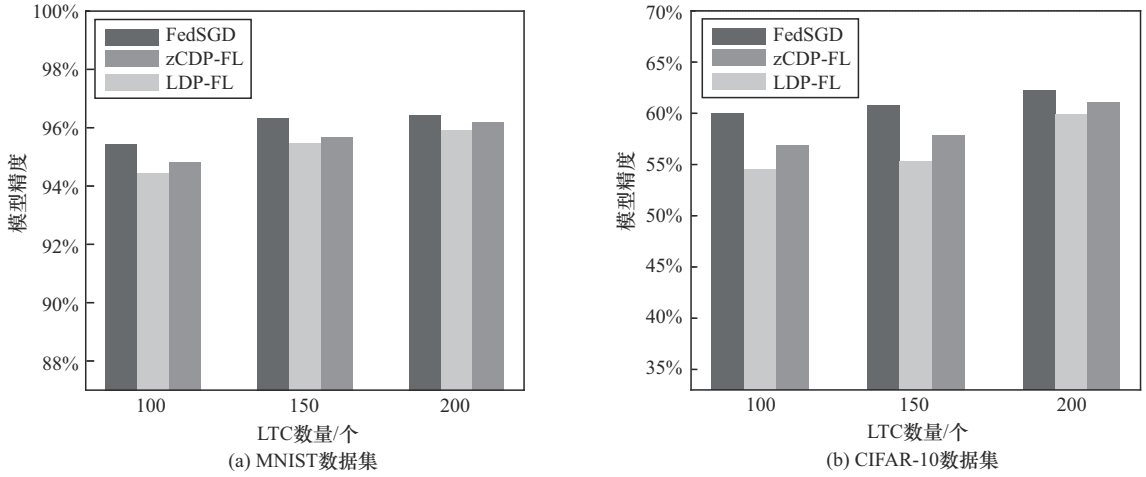
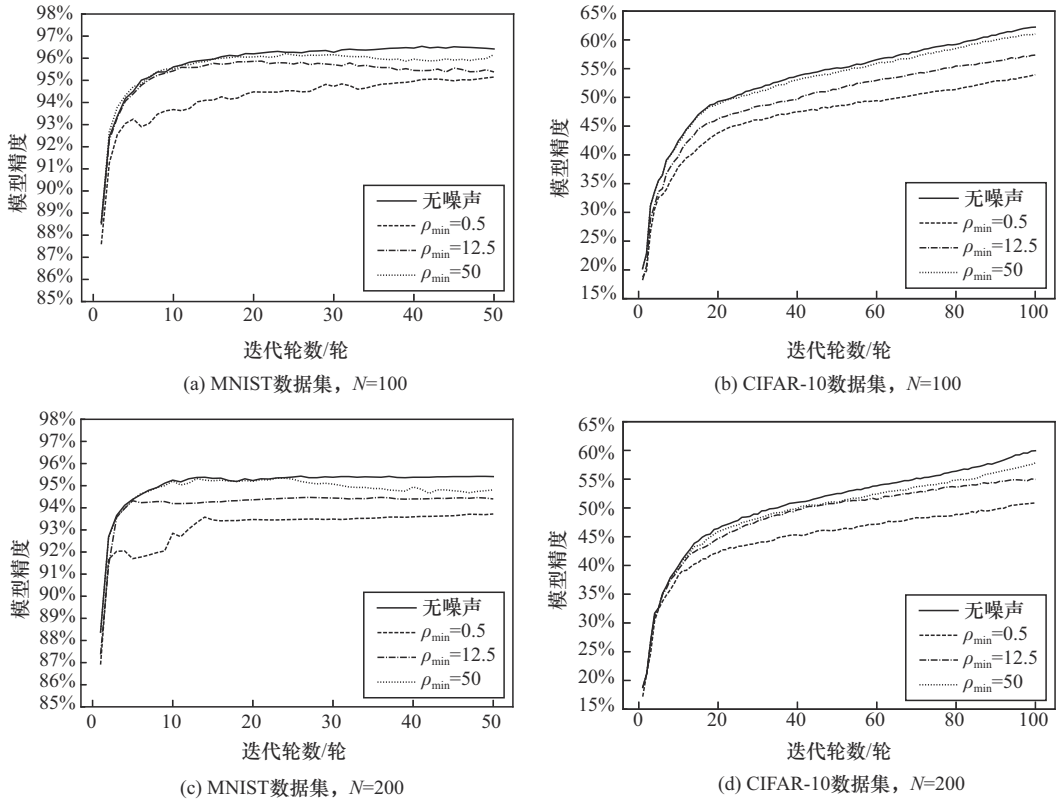


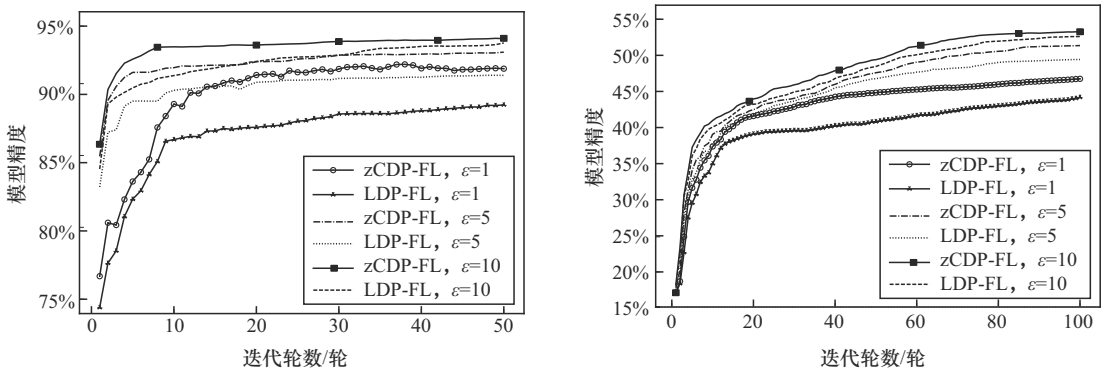
图4　3种方案中LTC数量对模型精度的影响



(a) MNIST数据集，N=100　(b) CIFAR-10数据集，N=100

(c) MNIST数据集，N=200　(d) CIFAR-10数据集，N=200

图5　ρ_{min}对模型精度的影响



(a) MNIST数据集　(b) CIFAR-10数据集

图6　隐私预算对模型精度的影响

综上所述，在其他超参数设置相同的情况下，隐私参数最小值设置越大，所训练模型精度越接近于未加噪的FL模型训练，隐私预算值的设定同理，说明不同隐私参数的设置会对FL模型训练产生不同的影响。在使用动态噪声方案时，可以通过调整隐私参数最小值的大小而改变模型精度，使得训练更高效。

6.2.5　性能对比

zCDP-FL综合考虑了抵御攻击、客户端激励、系统效益和训练效率4个方面，可以有效地解决敏感信息泄露、客户端参与不积极和模型训练效率低问题。如表6所示，通过方案对比，zCDP-FL方案明显突出诸多优势，其中，√表示方案有此项性能，×表示方案没有此项性能。首先，针对内外部攻击，zCDP-FL方案加入了具有更严格隐私保证的零集中差分隐私保护机制。其次，设计了基于密封式第二价反向拍卖理论的激励机制，激励拥有高质量数据集的LTC参与训练并保证系统效益最大化。最后，通过动态调整隐私参数，防止噪声扰动过大，提升模型训练效率。

表6　本文方案与现有方案的性能对比

方案	隐私保护	客户端激励	系统效益最大化	训练效率
FedSGD	×	×	×	√
LDP-FL	√	×	×	×
RRAFL	×	√	×	√
GCA	×	√	×	√
zCDP-FL	√	√	√	√

7　结束语

在万物互联时代，FL已经广泛应用于众多领域。如何在保障私有数据安全的前提下提高模型训练效率，激励客户端参与训练是亟待解决的问题。基于此，本文提出了基于激励机制的隐私保护联邦学习框架zCDP-FL，设计了密封式第二价反向拍卖理论的激励机制SRAI，有效地激励客户端贡献高质量数据集，实现客户端的公平选择与系统效益最大化。此外，本文提出了零集中差分隐私的隐私预算动态分配算法，根据损失函数差值的变化进行自适应调整，使得FL在严格的隐私限制下拥有更好的保护性能和模型可用性。理论分析与实验结果证明了zCDP-FL方案的有效性与高效性。未来工作将致力于研究差分隐私在联邦学习方面的进一步优化，拓宽应用场景，如智慧金融和智慧医疗等方面，探究如何在保证隐私安全的同时提升模型性能。

参考文献:

[1] AHMED I, JEON G, PICCIALLI F. From artificial intelligence to explainable artificial intelligence in industry 4.0: a survey on what, how, and where[J]. IEEE Transactions on Industrial Informatics, 2022, 18(8): 5031-5042.

[2] MCMAHAN H B, MOORE E, RAMAGE D, et al. Communication-efficient learning of deep networks from decentralized data[J]. arXiv Preprint, arXiv: 1602.05629, 2016.

[3] MOTHUKURI V, PARIZI R M, POURIYEH S, et al. A survey on security and privacy of federated learning[J]. Future Generation Computer Systems, 2021, 115: 619-640.

[4] WEI K, LI J, DING M, et al. Federated learning with differential privacy: algorithms and performance analysis[J]. IEEE Transactions on Information Forensics and Security, 2020, 15: 3454-3469.

[5] ZHU L G, LIU Z J, HAN S. Deep leakage from gradients[C]//The 33rd International Conference on Neural Information Processing Systems. Massachusetts: MIT Press, 2019: 14774-14784.

[6] 汤凌韬, 陈左宁, 张鲁飞, 等. 联邦学习中的隐私问题研究进展[J]. 软件学报, 2023, 34(1): 197-229.
TANG L T, CHEN Z N, ZHANG L F, et al. Research progress of privacy issues in federated learning[J]. Journal of Software, 2023, 34(1): 197-229.

[7] ZHAO C, ZHAO S N, ZHAO M H, et al. Secure multi-party computation: theory, practice and applications[J]. Information Sciences, 2019, 476: 357-372.

[8] PAILLIER P. Public-key cryptosystems based on composite degree residuosity classes[C]//International Conference on the Theory and Applications of Cryptographic Techniques. Berlin: Springer, 2007: 223-238.

[9] 李尤慧子, 殷昱煜, 高洪皓, 等. 面向隐私保护的非聚合式数据共享综述[J]. 通信学报, 2021, 42(6): 195-212.
LI Y H Z, YIN Y Y, GAO H H, et al. Survey on privacy protection in non-aggregated data sharing[J]. Journal on Communications, 2021, 42(6): 195-212.

[10] RABIN M O. How to exchange secrets with oblivious transfer[J]. IACR Cryptology EPrint Archive, 2005, 2005: 187.

[11] BELLARE M, HOANG V T, ROGAWAY P. Foundations of garbled circuits[C]//Proceedings of the 2012 ACM Conference on Computer and Communications Security. New York: ACM Press, 2012: 784-796.

[12] KARNIN E, GREENE J, HELLMAN M. On secret sharing systems[J]. IEEE Transactions on Information Theory, 1983, 29(1): 35-41.

[13] DWORK C. Differential privacy: a survey of results[C]//International Conference on Theory and Applications of Models of Computation. Berlin: Springer, 2008: 1-19.

[14] KANG J W, XIONG Z H, NIYATO D, et al. Incentive mechanism for reliable federated learning: a joint optimization approach to combining reputation and contract theory[J]. IEEE Internet of Things Journal, 2019, 6(6): 10700-10714.

[15] DENG Y H, LYU F, REN J, et al. FAIR: quality-aware federated learning with precise user incentive and model aggregation[C]//Proceedings of the IEEE INFOCOM 2021-IEEE Conference on Computer Communications. Piscataway: IEEE Press, 2021: 1-10.

[16] ZENG R F, ZHANG S X, WANG J Q, et al. FMore: an incentive scheme of multi-dimensional auction for federated learning in MEC[C]// Proceedings of the 2020 IEEE 40th International Conference on Distributed Computing Systems (ICDCS). Piscataway: IEEE Press, 2020: 278-288.

[17] JIN H M, SU L, CHEN D Y, et al. Quality of information aware incentive mechanisms for mobile crowd sensing systems[C]//Proceedings of the 16th ACM International Symposium on Mobile Ad Hoc Networking and Computing. New York: ACM Press, 2015: 167-176.

[18] 田有亮, 吴柿红, 李沓, 等. 基于激励机制的联邦学习优化算法[J]. 通信学报, 2023, 44(5): 169-180.
TIAN Y L, WU S H, LI T, et al. Federated learning optimization algorithm based on incentive mechanism[J]. Journal on Communications, 2023, 44(5): 169-180.

[19] ZHANG L F, ZHU T Q, XIONG P, et al. A robust game-theoretical federated learning framework with joint differential privacy[J]. IEEE Transactions on Knowledge and Data Engineering, 2023, 35(4): 3333-3346.

[20] CHEN Y R, ZHANG Y Y, WANG S W, et al. DIM-DS: dynamic incentive model for data sharing in federated learning based on smart contracts and evolutionary game theory[J]. IEEE Internet of Things Journal, 2022, 9(23): 24572-24584.

[21] ZHANG J W, WU Y Z, PAN R. Incentive mechanism for horizontal federated learning based on reputation and reverse auction[C]//Proceedings of the Web Conference 2021. New York: ACM Press, 2021: 947-956.

[22] GUPTA R, GUPTA J. Federated learning using game strategies: state-of-the-art and future trends[J]. Computer Networks, 2023, 225: 109650.

[23] WEI K, LI J, MA C, et al. Personalized federated learning with differential privacy and convergence guarantee[J]. IEEE Transactions on Information Forensics and Security, 2023, 18: 4488-4503.

[24] ABADI M, CHU A, GOODFELLOW I, et al. Deep learning with differential privacy[C]//Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. New York: ACM Press, 2016: 308-318.

[25] LIU X Y, LI H W, XU G W, et al. PADL: privacy-aware and asynchronous deep learning for IoT applications[J]. IEEE Internet of Things Journal, 2020, 7(8): 6955-6969.

[26] ZHU L H, LIU X Y, LI Y M, et al. A fine-grained differentially private federated learning against leakage from gradients[J]. IEEE Internet of Things Journal, 2022, 9(13): 11500-11512.

[27] TRUEX S, LIU L, CHOW K H, et al. LDP-Fed: federated learning with local differential privacy[C]//Proceedings of the Third ACM International Workshop on Edge Systems, Analytics and Networking. New York: ACM Press, 2020: 61-66.

[28] LEE J, KIFER D. Concentrated differentially private gradient descent with adaptive per-iteration privacy budget[C]//Proceedings of the 24th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining. New York: ACM Press, 2018: 1656-1665.

[29] BUN M, STEINKE T. Concentrated differential privacy: simplifications, extensions, and lower bounds[C]//Theory of Cryptography Conference. Berlin: Springer, 2016: 635-658.

[30] 康海燕, 冀源蕊. 基于本地化差分隐私的联邦学习方法研究[J]. 通信学报, 2022, 43(10): 94-105.
KANG H Y, JI Y R. Research on federated learning approach based on local differential privacy[J]. Journal on Communications, 2022, 43(10): 94-105.

[31] LU R H, ZHANG W Z, WANG Y, et al. Auction-based cluster federated learning in mobile edge computing systems[J]. IEEE Transactions on Parallel and Distributed Systems, 2023, 34(4): 1145-1158.

[作者简介]

李梦倩（1997– ），女，河北衡水人，贵州大学博士生，主要研究方向为联邦学习、隐私保护、差分隐私技术等。

田有亮（1982– ），男，贵州盘州人，博士，贵州大学教授、博士生导师，主要研究方向为博弈论、密码学与安全协议、大数据隐私保护。

张军鹏（1982– ），男，河北石家庄人，河北师范大学副教授，主要研究方向为数据安全、隐私保护、差分隐私技术。

赵冬梅（1966– ），女，河北深州人，博士，河北师范大学教授、博士生导师，主要研究方向为网络安全主动防御、风险监测、大数据隐私保护。