面向联邦算力网络的隐私计算自适激励机制

周 赞[1),2)] 张笑燕[1)] 杨树杰[1),2)] 李鸿婧[1),2)] 况晓辉[1),3)]
叶何亮[4)] 许长桥[1),2)]

[1)](北京邮电大学计算机学院(国家示范性软件学院) 北京 100876)
[2)](网络与交换技术全国重点实验室 北京 100876)
[3)](信息系统安全技术国家重点实验室 北京 100101)
[4)](中国电信股份有限公司研究院 广州 510630)

摘 要 面对“人-机-物”超融合与万物智能互联远景的现实需求,联邦算力网络充分发挥联邦学习等分布式智能技术的数据聚合优势以及“信息高铁(低熵算力网)”的计算协同优势,高效利用网络中泛在离散部署的海量数据与算力资源,从而最大化满足多种高性能、智能化计算任务需求瓶颈.同时,为建立用户泛在协作计算过程中的全生命周期安全保障和对联邦算力网络的互信任基础,差分隐私等隐私计算技术的引入成为基础性需求之一.因此,在用户自身安全和隐私不受模型逆转、梯度泄露等新兴攻击威胁的前提下,如何对大量的个性化参与用户进行有效激励,促使其积极参与并真实共享本地数据和算力,是实现联邦算力任务实际部署的关键步骤之一.然而,当前联邦算力网络的激励机制大多主要侧重于用户数据评估与公平性等计算性能相关指标研究,缺少对用户隐私需求的关注,无法有效规约隐私噪声注入过程.边缘算力节点出于自身利益考量,往往夸大隐私预算需求,造成严重的冗余精度损失.针对这一问题,本文基于改进的斯塔克伯格主从博弈模型,提出一种面向联邦算力网络的隐私计算自适应激励方法,通过两阶段的动态博弈根据分布式计算过程中隐私注入尺度进行差异化定价激励.基于反向归纳法,参与用户之间首先进行博弈均衡获取最优的本地隐私噪声预算设置策略,随后联邦参数服务器求取最优的隐私支付策略.通过理论分析,本文所提方案能够取得纳什均衡下的最优解.此外,本文还进一步对参与用户的限制条件进行了讨论,得出了用户隐私成本需求的约束上界.在EMNIST、CIFAR等公有标准数据集上的实验结果也表明,该方法相比于基于合约理论、三方博弈等理论的现有隐私激励机制,能够显著提升分布式智能协同计算任务参与各方的平均效用,在满足用户隐私需求的同时提升计算性能,大幅减少冗余损耗.

关键词 联邦算力网络;隐私计算;隐私定价;个性化隐私;动态博弈;算力网络
中图法分类号 TP391 **DOI号** 10.11897/SP.J.1016.2023.02705

Adaptive Incentive Mechanism for Privacy Computing in Federated Compute First Networks

ZHOU Zan[1),2)] ZHANG Xiao-Yan[1)] YANG Shu-Jie[1),2)] LI Hong-Jing[1),2)]
KUANG Xiao-Hui[1),3)] YE He-Liang[4)] XU Chang-Qiao[1),2)]

[1)](*School of Computer Science, Beijing University of Posts and Telecommunications, Beijing* 100876)
[2)](*State Key Laboratory of Networking and Switching Technology, Beijing* 100876)
[3)](*National Key Laboratory of Science and Technology on Information System Security, Beijing* 100101)
[4)](*Research Institute of China Telecom Co., Ltd., Guangzhou* 510630)

Abstract In consideration of the practical demands derived from “human-machine-thing” super-

收稿日期:2023-02-19;在线发布日期:2023-08-22.本课题得到国家自然科学基金(62225105, 62001057)资助.**周 赞**,博士,主要研究领域为隐私计算、网络主动防御、数据隐私保护.E-mail: zanezanzhou@gmail.com. **张笑燕**,博士,教授,主要研究领域为网络安全、移动网络与未来网络技术. **杨树杰**,博士,副教授,中国计算机学会(CCF)会员,主要研究领域为网络安全、漏洞挖掘与网络资源优化等. **李 鸿婧**,硕士研究生,主要研究领域为算力网络隐私保护与污染防治. **况晓辉**,博士,教授,主要研究领域为无线网络与信息安全. **叶 何亮**,硕士,高级工程师,主要研究领域为网络管理与信息安全. **许长桥**(通信作者),博士,教授,中国计算机学会(CCF)杰出会员,国家杰出青年科学基金入选者,主要研究领域为网络主动防御、人工智能隐私安全、新型网络技术等.E-mail: cqxu@bupt.edu.cn.

fusion and the vision of ubiquitous intelligence interconnection during the era of the internet of everything, federated compute first network are regarded as a promising solution, which jointly leverages the data aggregation advantages of distributed intelligent technologies, such as federated learning, and the collaborative computing advantages of the "information high-speed rail (i.e., low-entropy compute first network)" in the same time. The federated compute first networks efficiently utilize the abundant data and computing resources deployed ubiquitously and fragmentally in the network to maximize the satisfaction of various high-performance and intelligent computing tasks. Simultaneously, to establish comprehensive security guarantees for users engaged in ubiquitous collaborative computing processes throughout the entire life cycle, as well as foster mutual trust between distributed clients and aggregation servers within the federated compute first network, introducing privacy-preserving computing technologies like differential privacy has become one of the most essential requirements. Therefore, under the premise that users' security and privacy are not subject to newly emerging threat patterns such as model reverse attacks and gradient leakage attacks, how to effectively motivate a large number of personalized participants to participate in actively and honestly sharing local data and computing power is one of the key steps to realize the real-world deployment of multiple different federated computing tasks. However, current incentive mechanisms in federated compute first networks primarily focus on training performance-oriented factors such as data quality evaluation and fairness research, with more attention to be paid to user privacy requirements. These methods cannot effectively regulate the privacy noise injection process during collaborative training and information sharing. At the same time, edge computing nodes usually exaggerate their local privacy budget demands due to their goals of maximizing personal privacy protection levels. The irreconcilable conflict between the unsuspecting aggregator and self-interested participants may result in severe redundant accuracy loss. To address this problem, we propose an adaptive incentive approach of privacy computing in this work for federated compute first networks based on an improved Stackelberg leader-follower game model. The proposed method employs a two-stage dynamic game to offer differential pricing incentives based on the scale of privacy injection during distributed computing. Using a backward induction approach, participating users first engage in game equilibrium to obtain the optimal local privacy budget of the noise injection strategy, followed by the optimal privacy payment strategy determined by the federated parameter server. Theoretical analysis shows that the proposed solution achieves the optimal Nash equilibrium. Furthermore, the paper discusses the constraints on participating users and derives an upper bound for their privacy cost requirements. Experimental results on two public image classification datasets such as EMNIST and CIFAR, which serve as standard benchmarks for distributed learning tasks over a long period, demonstrate that compared to existing privacy incentive mechanisms based on contract theory or three-party games, the proposed method significantly improves the average utility of all parties involved in distributed intelligent collaborative computing tasks while enhancing computational performance and considerably reducing redundancy loss while ensuring user privacy requirements are guaranteed.

Keywords federated; compute first network; private-preserving computation; privacy pricing; personalized privacy; dynamic game; compute first network

1　引　言

长期以来，数据与算力在网络中泛在离散化部署、缺乏有效统筹利用，一直是制约“人机物”融合的智能万物互联远景实现的关键瓶颈[1-4]. 为突破这一桎梏，联邦算力网络相关技术在近年来迅速发展[5-7]. 例如，中国移动与多家国内外运营商、标准组织和产业联盟提出的《2022年算力网络技术白皮书》就将联邦学习(federated learning，FL)，隐私计算为代表的多方协作、可信共享的算网服务列为行业发展新业态与主要技术方向[8]，中国工程院院士李国杰也指出，未来算力网络研究应避免单一“帝国制”机制，探索新型的“联邦制”管理模式，满足低熵算力网络作为“信息高铁”对高通量、高良率计算的需求[9]. 在此基础上，紫金山实验室、北京邮电大学、香港科技大学、亚信科技等不断提出融智算力网络、算力内生网络、算力内生联邦学习等技术实现方案[10-11]，充分发挥联邦学习与算力网络在数据聚合与算力协同方面的理论优势[12-14]，实现算网深度融合，逐步构建联邦算力网络基础架构与协作计算处理模式.

尽管联邦算力网络可以通过统筹数据本地化的边缘算力节点规避传输过程中隐私泄露的风险，但如Deep leakage[15]和Model-inversion[16]等更为复杂的新型高级持续性攻击，仍有可能通过可见的梯度权重或模型参数逆向推断或获取用户个人信息. 如图1所示，在联邦计算任务完成的初始模型下发、本地模型训练上传、梯度收集与全局模型聚合生成的全过程中通过模型窃取技术、截取梯度等交互信息或分析模型更新恢复本地原始数据，来获取敏感信息并侵犯参与者的隐私[17-21]. 因此，必须采取适当的隐私保护措施，保障联邦算力网络的隐私安全. 为了进一步保护用户隐私，同态加密[22-23]、安全多方计算[24-26]等技术也被逐步引入联邦算力网络，对其进行隐私计算增强. 其中，差分隐私(differential privacy，DP)[27-28]技术通过添加零和噪声提供理论可证的隐私性能保障，具有通信效率高、性能损耗小和隐私可量化等诸多优点，受到了学术界与工业界的重点关注.

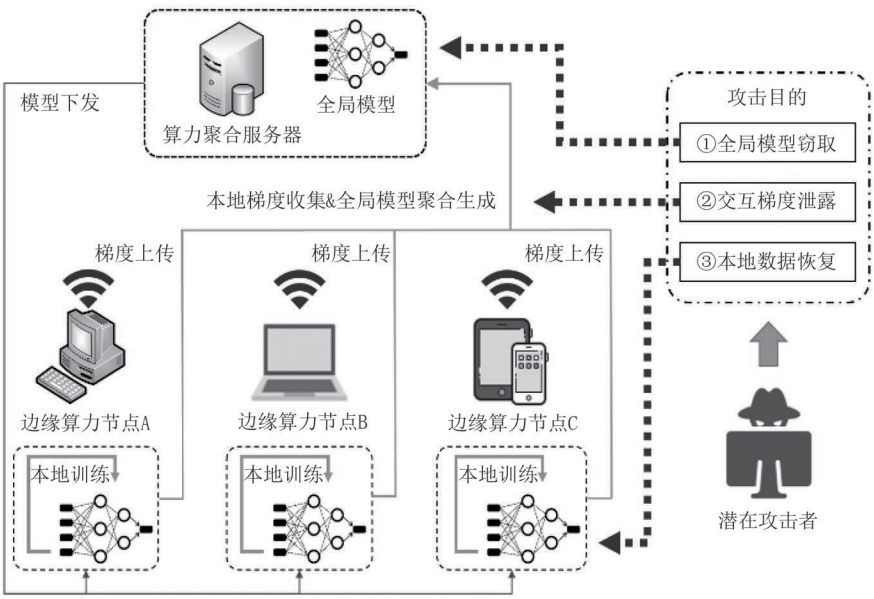


图1　联邦算力网络架构与主要隐私攻击威胁

联邦计算任务的数据和算力通常被部署在边缘算力节点，导致服务方对参与用户个人数据的真实情况缺乏充分了解，从而无法有效监管[29]. 因此，出于追求个人隐私收益的最大化，参与者往往倾向于上报相比真实值更大的隐私损失，即夸大个体隐私需求. 由于联邦计算任务往往需要涵盖大量用户的时空离散数据，这种夸大个体隐私需求造成的误差在多轮迭代训练的长期集聚效应和长效时间累积作用下，可能会导致严重的冗余性能损耗，甚至无效化整个隐私计算模型. 同时，即便用户真实上报隐私损失，由于用户规模较大，动态网络环境下的极个别离群值用户也可能导致极大的隐私预算开销，其“掉队者(straggler)”拖尾效应[18]反而降低了全局计算效率.

目前，联邦算力网络激励机制主要关注用户参

与度与公平性，针对联邦算力网络隐私计算的激励机制研究较少，缺乏对用户个人隐私噪声注入过程的理性规约．例如，文献[30]设计了一种基于深度强化学习的激励机制，以确定参数服务器的最优定价策略和边缘节点的最优训练策略．文献[31]则提出层次激励机制框架，利用契约论自我揭示机制和联盟博弈论方法，根据模型所有者的边际贡献来奖励模型所有者．文献[32]针对数字孪生驱动的工业移动群智感知，设计了基于斯塔克伯格博弈的客户端间激励机制和基于合同的声誉机制，激励并筛选参与者参与联邦学习．然而，现有研究强调用户在计算过程中产生的训练成本和通信成本，个人隐私泄露风险并没有得到补偿．部分研究如Erato[33]等涉及对隐私定价问题的初步探索，也取得了较好的无套利支付策略．文献[34]提出了一种改进的随机梯度下降定价算法，该算法可以根据数据所有者与数据收集者的交互来推断数据所有者的成本模型，量化并补偿偏差，尽可能地减少本地差分噪声的影响．然而，这些方案并未考虑用户个性化隐私需求与差异化的模糊处理过程对双方动态博弈的影响，从而不能有效限制用户根据实际隐私损失理性选取，仍旧无法针对性解决上述冗余性能损耗的问题．因此，本文针对联邦算力网络中客户个性化的隐私需求，以及服务方对于尽可能减少精度损失的可用性需求，提出了基于改进的两阶段斯塔克伯格动态博弈的隐私定价与个性化隐私预算选取机制．服务器和客户分别通过求取纳什均衡下的最优解获取各自的策略，即服务方给予用户的总支付报酬和参与者个人的隐私预算，最大化自身效用，实现客户隐私和模型性能的平衡．

本文的主要贡献包括以下3个方面：

(1) 考虑到现有联邦算力网络的激励机制对隐私定价与个性化隐私噪声选取缺乏考量的缺陷，从而导致的冗余性能损失，本文将参与用户与服务方基于各自成本收益的动态策略选取过程构建为一对多的斯塔克伯格模型，提出了一种基于两阶段动态博弈的联邦算力网络隐私计算自适激励机制，有效引导参与者根据差异化隐私需求理性选取噪声注入尺度．

(2) 基于反向归纳法，用户以跟随者身份在第二阶段进行非合作博弈确定各自对隐私噪声注入尺度的个人最佳响应，随后服务方在第一阶段反向求取纳什均衡下的最优定价策略．理论分析证明该解的唯一性，同时也对用户参与条件进行了限制，有效降低差分隐私中个别离群用户带来的敏感度膨胀问题．

(3) 通过对EMNIST和CIFAR-10等公开数据集上的系列实验结果分析，本文方法具有优异的性能表现与鲁棒性．此外，在实验中，与静态策略、随机策略、三方博弈策略以及合约论策略等最新的隐私计算激励方案相比，本文的方法显著提升了多方平均效用，取得了更好的激励效果．

2 相关工作

由于在联邦算力网络中，进行本地训练的客户不可避免地承担了计算和通信开销以及本地数据隐私泄露的风险．在协同计算的过程中，为了激励客户积极地参与联邦计算任务，许多研究人员设计相应的激励机制来提高客户参与模型训练的积极性．针对客户和模型拥有者以及模型拥有者之间的激励不匹配问题，文献[2]提出的层次激励机制框架利用了契约论中的自我揭示机制和联盟博弈论方法，根据模型所有者的边际贡献来奖励模型所有者．文献[35]以拍卖博弈的形式进行客户选择．通过客户出价和服务器选择支付策略间的博弈，解决激励客户参与联邦模型训练的实际问题．文献[36]利用区块链记录联邦学习模型训练过程的中间参数，通过模型参数验证，惩罚上传虚假参数或低质量模型的参与节点，提高其积极性．文献[37]为联邦算力网络平台提出了一种基于博弈的激励机制，该平台将分布式深度学习和群智感知结合，用于移动客户端上的大数据分析．平台发布任务和奖励，通过移动客户端最大化自身效用提高客户训练数据的积极性．文献[38]在分散联邦学习的基础上加入了基于契约理论的激励机制，提出了一种优化全局模型效应的联邦学习激励模型．联邦学习的参与者基于本地数据质量对合同发布者制定和分发的合同进行选择，并根据本地训练的评估结果获取合同中规定的奖励．在参与者获得合理的奖励基础上，基于奖励结果来聚合，提高联邦学习训练的模型效果．

联邦计算系统中服务器和多个客户的结构特征与斯塔克伯格博弈模型中一个领导者和多个跟随者的结构相符，一些研究人员根据联邦计算任务的特点，利用斯塔克伯格博弈模型进行激励机制的设计．例如，文献[39]设计针对联邦学习系统斯塔克伯格博弈的激励机制，可以确保服务器实现最佳效用，同时激励员工尽最大努力训练全局聚合模型．

文献[40]设计了一种基于斯塔克伯格博弈的激励的方法来激励员工为本地训练分配更多的计算资源. 文献[41]针对边缘网络的联邦计算任务，通过斯塔克伯格博弈对全球服务器和参与设备之间基于激励的交互进行建模，以促进设备参与协同计算过程. 文献[42]设计了基于斯塔克伯格的服务定价机制. 对于模型所有者的训练任务，移动设备非合作地决定对单位训练数据的价格，以实现个体效用的最大化，并协作传输模型更新量. 然而，文献[39-42]只考虑到用户在隐私计算中产生的训练成本和通信成本，参与者个人隐私泄露风险并未得到补偿.

对客户参与计算任务造成的隐私损失进行定价并进行补偿也是激励客户参与联邦智能业务的一种方式. 一些研究人员也针对数据隐私的定价机制展开研究. 文献[33]设计了针对私有相关数据的综合统计定价框架Erato，包括服务定价机制和隐私补偿机制. Erato很好地平衡了效用和隐私，实现了套利自由，更公平地补偿了数据所有者. 文献[43]提出一个实用的无套利的个人数据交易框架，能够在利润和隐私之间取得平衡. 文献[44]通过数据收集器在数据提供者和数据用户之间博弈，实现隐私保护级别和数据价格的均衡. 数据收集器使用k-匿名算法对数据进行隐私处理，在保证数据质量的基础上最大化其收益. 文献[45]结合声誉和契约理论，提出了一种动态的长期激励机制，激励移动用户参与到移动众包网络中. 针在纵向联邦学习的场景中，为了公平地联邦学习参与者的收益，文献[46]提出了一种基于参与者对联合模型贡献的科学、公平的动态博弈数据定价方法. 文献[47]提出了一个基于斯塔克伯格博弈的数据卖家的公平补偿模型，将定价问题建模为数据卖家，买家和市场代理机构三方的斯塔克伯格博弈过程，以计算在合理补偿数据销售者隐私损失的情况下最大化数据销售者和购买者的共同利益的最优价格. 文献[48]针对移动群体感知场景设计了基于任务捆绑的两阶段拍卖机制来激励请求者和用户. 通过将任务聚类为束，并收集各个束中的预算. 再在此基础上进行双重拍卖，排序预算和出价，以最大限度地匹配任务代理和用户. 文献[49]提出的基于合约理论的个性化隐私感知数据交易方法和IC-MLE算法，考虑到自私的数据所有者的个性化隐私偏好，为数据所有者提供了一组具有不同隐私保护级别和数据交易价格的最优合约. 数据所有者根据协商的隐私保护上传扰动的数据水平，并使用组加权最大似然估计方法聚合数据，通过最大化聚合结果的准确性来最大化众包数据的数据效用. 尽管上述文献针对数据隐私实现了公平的定价机制，给予数据提供者有效的补偿. 然而，针对含有差分隐私模糊化处理的联邦算力网络隐私计算任务，上述激励机制均不能满足客户的个性化隐私补偿需求. 在联邦算力网络场景中，针对客户的差异化隐私需求，如何通过合理的隐私定价机制补偿客户的隐私损失，激励客户选择合适的隐私级别，是亟待解决的问题.

因此，本文针对联邦算力网络分布式协同隐私计算任务中客户个性化的隐私需求，提出了基于两阶段斯塔克伯格动态博弈的隐私定价激励机制. 服务器和客户分别通过选择总隐私支付和个人隐私预算，最大化自身效用，实现客户隐私和模型性能的平衡.

3　系统设计

3.1　系统概述

图2描述了面向联邦算力网络的隐私计算自适激励机制的基本框架. 右下角的有向(带箭头)实线表示基于联邦算力网络的分布式计算中梯度聚合的过程，左上角的有向(带箭头)虚线描述了隐私定价激励的博弈过程. 隐私定价的两阶段动态博弈过程包括了服务器和边缘节点间的主从动态博弈和边缘节点间的非合作博弈. 该机制的主要工作流程如图3所示，概括如下：

初始化阶段

首先，在联邦学习开始之前：(1)节点和服务器基于各自的收益和成本分别定义效用函数；(2)服务器初始化全局模型.

联邦隐私计算阶段

然后，在联邦算力网络的每一轮通信中，依次进行以下工作流程：(3) 边缘算力节点更新本地模型；(4) 边缘算力节点基于本地数据执行本地训练；(5) 边缘算力节点隐私需求选择个性化的隐私预算；(6) 边缘算力节点在梯度中注入满足隐私预算的高斯噪声；(7) 边缘算力节点将加噪梯度和隐私预算上报服务器；(8) 服务器聚合梯度.

隐私定价与回报阶段

(9) 服务器根据节点上报的隐私预算选择该轮次的总体支付并计算服务器效用；(10) 服务器下发聚合梯度并支付报酬，一个轮次的分布式协作智能

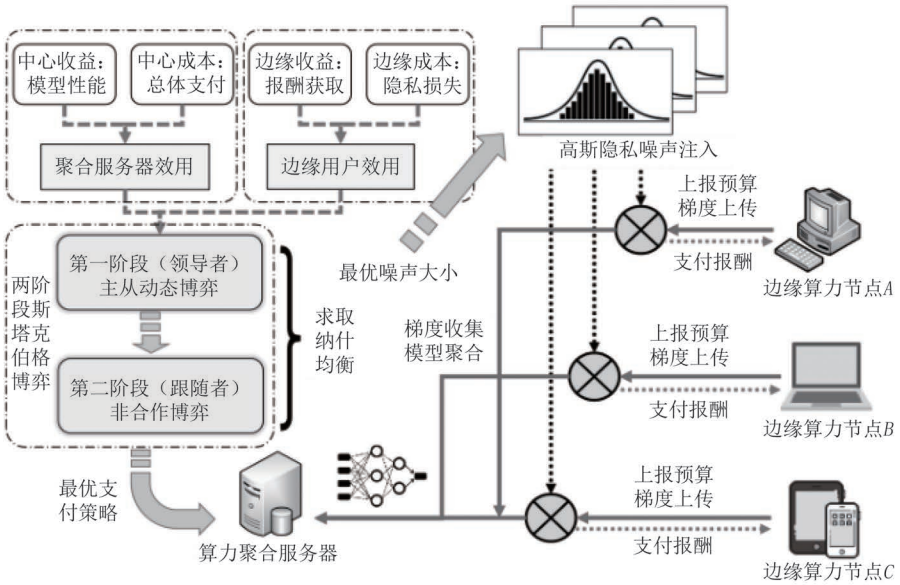


图2 面向联邦算力网络的隐私计算自适激励机制基本框架

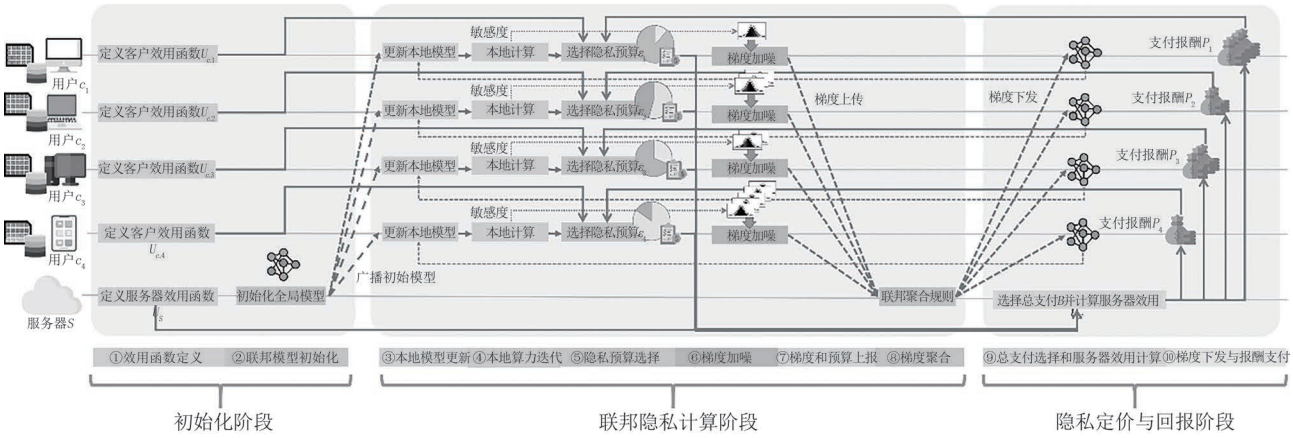


图3 面向联邦算力网络的隐私计算自适激励机制的主要工作流程

隐私计算完成.

服务器和边缘算力节点经过多轮交互,了解互相的偏好和参数信息.在交互的过程中,服务器和节点均根据对方的策略动态调整己方的策略选择来寻求各自效用的最大化.同时,为了尽可能多地争取有限的总体支付,节点间也进行着动态的非合作博弈.最终,服务器和节点均找到能同时满足各自效用最大化的最优决策,服务器-节点的主从博弈和节点间的非合作博弈均达到纳什均衡.

可以看出,如果用户上报更大的隐私预算并添加更少噪声,就可以获得更多的报酬.通过支付报酬,系统为用户承担隐私损失,激励客户上传更真实的梯度.

同时,在用户具有不同数据分布的异构情况下,用户本地数据的差异和数据敏感度越大,越倾向于选择更小的隐私预算,获得的报酬也就越少.

3.2 差分隐私

差分隐私为分布式系统的隐私安全提供了强有力的保障.通过在查询结果上添加随机噪声,在保证数据查询的准确性的同时最大限度减少数据隐私泄露的风险.

对于差分隐私作用的数据,邻接数据集的定义如下:若对于两个数据集D和D',有$\|D-D'\|_1\leqslant 1$,则数据集D和D'称为邻接数据集.邻接数据集之间最多有一个记录差异.可得(ϵ,δ)-DP的定义如下:

一个随机机制$M:X\to R$,若对任意可测量集合$S\subseteq R$且对任意两个邻接数据集$D,D'\in X$,满足如下公式则其满足(ϵ,δ)-DP:

$$\Pr[M(D)\in S]\leqslant \Pr[M(D')\in S]+\delta \quad (1)$$

高斯差分隐私提供松弛的$(\epsilon,\delta)-$DP,其中ϵ

表示隐私预算，δ表示松弛项. 当隐私预算$\epsilon\in(0,1)$，对于任意函数$f:N^{|X|}\to R^k$的高斯机制定义为

$$M_G(x,f(\cdot),\epsilon)=f(x)+n \tag{2}$$

其中，n符合高斯分布$n\sim N(0,\sigma^2)$. 当噪声标准差$\sigma\geqslant\frac{d\triangle_2 f}{\epsilon}$，常数$d$满足$d\geqslant\sqrt{2\ln\left(\frac{1.25}{\delta}\right)}$时，$M_G(x,f(\cdot),\epsilon)$满足$(\epsilon,\delta)$-DP. 其中，$\triangle_2 f=\max\limits_{D,D'\in N^{|X|}\atop \|D-D'\|_2\leqslant 1}\left\|f(D)-f(D')\right\|_2$是查询数据的L2范数的敏感度.

4　隐私自适应激励模型

在本节中，针对含有隐私噪声注入的联邦算力网络中客户的隐私计算定价激励问题，提出了一种基于两阶段的斯塔克伯格博弈的隐私定价机制. 首先，本文给出了客户隐私支付策略，然后分别定义客户和服务器的效用. 最后，本文将效用优化问题建模为以服务器为领导者，所有客户为跟随者的两阶段斯塔克伯格博弈模型. 主要的参数定义如表1所示.

表1　参数定义

参数	函数
c_i	第i个客户
S	服务器
C	客户集合
N	客户数量
B	支付上限
ϵ,δ	差分隐私的参数
ϵ_i	客户c_i的隐私预算
ϵ_{-i}	除客户c_i外全部客户的隐私预算之和
ϵ_g	全局模型的隐私预算
ρ_i	客户c_i的隐私成本相关参数
α,β	模型收益相关参数
f	模型收益函数
P_i	服务器对客户c_i的隐私支付
$C_{C,i}$	客户c_i的成本
C_S	服务器S的成本
$E_{C,i}$	客户c_i的收益
E_S	服务器S的收益
$U_{C,i}$	客户c_i的效用函数
U_S	服务器S的效用函数
M	随机机制
M_G	高斯机制

4.1　服务器隐私支付策略

首先，本文定义了服务器的支付上限B，并在此基础上定义客户的隐私支付策略.

服务器通过改变其支付上限B，影响所有客户的总支付. 对于任意客户，服务器向客户支付的报酬表示为

$$P_i=B\frac{\epsilon_i}{\sum_{j=1}^{N}\epsilon_j} \tag{3}$$

其中，ϵ_i是客户c_i向服务器提交的预期隐私预算，代表了客户c_i期望达到的隐私保护级别. 根据公式(3)，客户获得的报酬与其上报的隐私预算成正比. 客户和服务器均可以影响最终支付的报酬，但服务器决定了支付的上界.

4.2　客户的效用

客户c_i的收益为服务器对其上报隐私预算支付的报酬P_i：

$$E_{C,i}=P_i=B\frac{\epsilon_i}{\sum_{j=1}^{N}\epsilon_j} \tag{4}$$

客户c_i的成本为客户参与联邦计算任务的隐私损失，表示为

$$C_{C,i}=\rho_i\epsilon_i \tag{5}$$

其中，$\rho_i>0$是客户成本参数，用于描述客户单位隐私预算的隐私损失.

在差分隐私的定义中，要求邻接数据集整体分布的最大差距小于ϵ. 也就是说，隐私预算ϵ越小，数据相对于正确的中心值越分散，通过差分攻击识别出真实中心值的概率越低. 因此，客户c_i的隐私预算ϵ_i越小，添加的噪声越大，对客户的隐私保护程度越高，客户的隐私损失也就越小. 所以，客户c_i的隐私损失成本$C_{C,i}$和隐私预算ϵ_i是正相关的. 并且根据文献[33]，客户的隐私损失成本$C_{C,i}$符合隐私数据的无套利定价标准[43]，合理地规定了客户参与联邦学习损失数据隐私的价格，这表示数据买家不能通过多次访问隐私数据进行价格规避，保证了隐私数据定价的公平性. 因此，本文中假设客户的隐私损失成本和隐私预算成正比，相关系数为ρ_i.

综上，客户c_i的效用$U_{C,i}$定义为

$$U_{C,i}=E_{C,i}-C_{C,i}=B\frac{\epsilon_i}{\sum_{j=1}^{N}\epsilon_j}-\rho_i\epsilon_i \tag{6}$$

4.3　服务器的效用

根据上述分析可知，对于相同的数据敏感度，差分隐私中模型的隐私预算ϵ与噪声大小成反比，并且已知模型性能(即模型准确度)随添加噪声的增大

而降低. 因此,模型性能与隐私预算ϵ正相关. 而且,由于模型性能存在上限且性能越高,模型性能提升越困难. 连续增加单位隐私预算,模型性能的提升依次递减,模型增加的收益也将逐渐减少,模型收益函数符合边际效用递减定律[40]. 因此,对于常数$\alpha,\beta>0$,本文定义模型性能为$\ln(1+\alpha\epsilon)$. 对于隐私预算的定义域$\epsilon\in(0,+\infty)$,模型性能恒大于0,满足理论和实际应用上的合理性.

针对添加(ϵ,δ)-差分隐私的联邦算力网络模型,基于边际效用递减定理,定义它的模型收益为

$$f(\epsilon)=\beta ln(1+\alpha\epsilon) \tag{7}$$

在边际效用递减定理中,收益函数是导数递减的增函数. 也就是说,函数$f(\epsilon)$的导数$f'(\epsilon)=\frac{\alpha\beta}{1+\alpha\epsilon}$和二阶导数$f''(\epsilon)=-\frac{\alpha^2\beta}{(1+\alpha\epsilon)^2}$需要满足$f'(\epsilon)>0$和$f''(\epsilon)<0$的条件. 由此可得模型收益函数的系数$\alpha,\beta$的取值范围均为$(0,+\infty)$.

服务器的收益可以由全局模型的收益表示:

$$E_S=f(\epsilon_g)=\beta ln\left(1+\alpha\frac{1}{N}\sum_{i=0}^{N}\epsilon_i\right) \tag{8}$$

其中,$\epsilon_g=\frac{1}{N}\sum_{i=0}^{N}\epsilon_i$为全局模型的平均隐私预算.

服务器的成本则可以表示为对客户隐私的总支付:

$$C_S=\sum_{i=1}^{N}P_i=B \tag{9}$$

服务器的效用函数U_S表示为

$$U_S=E_S-C_S=\beta ln\left(1+\alpha\frac{1}{N}\sum_{i=0}^{N}\epsilon_i\right)-B \tag{10}$$

4.4 斯塔克伯格博弈

本节将客户的差分隐私请求以及服务器的定价建模为一个两阶段的斯塔克伯格博弈模型. 基于效用函数,分析了服务器和客户间博弈的最优策略. 隐私定价机制的定价过程如下:

(1)首先,为保护本地数据隐私,基于隐私损失成本和个性化的隐私需求,客户向服务器提交差分隐私请求.

(2)根据客户提交的隐私预算,服务器计算需要支付客户的相应报酬,进而计算服务器的效用.

(3)服务器和客户经过过去几轮的交易了解彼此的策略和各自的参数信息. 然后,服务器根据已知的信息计算最优策略以最大化效用,并将最优支付上限发送给客户.

(4)客户根据服务器的最优支付上限考虑各自成本确定申请隐私预算的最优策略.

由于隐私定价机制中的个体都是理性且自私的,各方都希望最大化自己的效用,因此,上述隐私定价过程可以表述为效用优化问题.

对于服务器,可以表述为

$$Maximize\ U_S(B,\epsilon_i,\epsilon_{-i}) \tag{11}$$

对于客户,可以表述为

$$Maximize\ U_{C,i}(B,\epsilon_i,\epsilon_{-i}) \tag{12}$$

上述隐私定价的过程,参与各方互相了解各自的回报和决策,符合斯塔克伯格博弈的特点. 本文将效用优化问题建模为两阶段斯塔克伯格博弈. 在隐私定价机制的斯塔克伯格博弈模型中,服务器作为领导者,在博弈的第一阶段确定所有客户的隐私支付上限. 所有客户作为跟随者,根据服务器确定的支付上限和本地隐私损失成本,选择能最大化各自效用的隐私预算. 同时,第二阶段的博弈中,客户间存在着非合作博弈. 在支付上限一定的条件下,客户可能通过提高自己隐私预算占比以获取更高的支付. 在客户间对隐私支付的竞争中,各自的隐私预算策略相互影响.

让$\langle B^*,\epsilon_i^*\rangle$作为最优均衡解,可得:

$$B^*=arg\max_{B}\ U_S(B,\epsilon_i,\epsilon_{-i}) \tag{13}$$

$$\epsilon_i{}^*=arg\max_{\epsilon_i}\ U_{C,i}(B,\epsilon_i,\epsilon_{-i}) \tag{14}$$

其中,$\epsilon_{-i}=\sum_{j=1}^{N}\epsilon_j-\epsilon_i=\sum_{j\neq i}^{N}\epsilon_j$,斯塔克伯格博弈的过程可以转化为求解上述最优均衡解的过程.

5 隐私计算自适定价博弈的均衡分析

本节将详细阐述使用反向归纳法求解斯塔克伯格博弈模型的过程. 在第二阶段的博弈中,通过最大化客户效用,得到客户的隐私级别选择的最优策略. 基于第二阶段博弈的最优策略,服务器通过求解第一阶段博弈的效用最优化问题确定最优的支付上限.

5.1 第二阶段客户的策略分析

当服务器确定了隐私支付上限时,客户需要确定上报的隐私预算以便于最大化其效用. 为了求客户的最优隐私预算,计算客户效用函数对隐私预算的一阶导数如下:

$$\frac{\partial U_{C,i}}{\partial\epsilon_i}=\frac{Bz}{(\epsilon_i+\epsilon_{-i})^2}-\rho_i \tag{15}$$

基于上式，取第i个客户效用$U_{C,i}$相对于其隐私预算ϵ_i的二阶导数：

$$\frac{\partial^2 U_{C,i}}{\partial {\epsilon_i}^2}=-\frac{2B\epsilon_{-i}}{(\epsilon_i+\epsilon_{-i})^3}=-\frac{2B\epsilon_{-i}}{\left(\sum_{i=1}^{N}\epsilon_i\right)^3}<0 \quad (16)$$

公式(16)说明客户效用$U_{C,i}$的一阶导数随隐私预算ϵ_i严格减小. 由于客户隐私预算$0<\epsilon_i<\infty$，本文分别考虑客户隐私预算ϵ_i趋近于0和∞两种情况.

(1)客户隐私预算ϵ_i趋近于0时：

$$\lim_{\epsilon_i\to 0}\frac{\partial U_{C,i}}{\partial \epsilon_i}=\lim_{\epsilon_i\to 0}\frac{B\epsilon_{-i}}{(\epsilon_i+\epsilon_{-i})^2}-\rho_i=\frac{B}{\epsilon_{-i}}-\rho_i \quad (17)$$

由于在本文的环境中客户效用大于0，表示如下：

$$U_{C,i}=B\frac{\epsilon_i}{\sum_{j=1}^{N}\epsilon_j}-\rho_i\epsilon_i>0 \quad (18)$$

可得：

$$B>\rho_i(\epsilon_i+\epsilon_{-i}) \quad (19)$$

根据公式(19)的条件，可进一步限制公式(17)的结果：

$$\lim_{\epsilon_i\to 0}\frac{\partial U_{C,i}}{\partial \epsilon_i}=\frac{B}{\epsilon_{-i}}-\rho_i>\frac{\rho_i(\epsilon_i+\epsilon_{-i})}{\epsilon_{-i}}-\rho_i=\frac{\rho_i\epsilon_i}{\epsilon_{-i}}>0 \quad (20)$$

由公式(20)可知，当客户隐私预算ϵ_i趋近于0时，客户效用的一阶导数$\frac{\partial U_{C,i}}{\partial \epsilon_i}$大于0.

(2)客户隐私预算ϵ_i趋近于∞时：

$$\lim_{\epsilon_i\to \infty}\frac{\partial U_{C,i}}{\partial \epsilon_i}=\lim_{\epsilon_i\to \infty}\frac{B\epsilon_{-i}}{(\epsilon_i+\epsilon_{-i})^2}-\rho_i=-\rho_i<0 \quad (21)$$

由公式(21)可知，当客户隐私预算ϵ_i趋近于∞时，客户效用的一阶导数$\frac{\partial U_{C,i}}{\partial \epsilon_i}$小于0.

由于客户效用的一阶的导数在取值区间$(0,\infty)$严格递减，上述两个不等式表明客户效用$U_{C,i}$首先随着隐私预算ϵ_i逐渐增加，然后不断减少. 因此，客户的效用函数$U_{C,i}$在区间$(0,\infty)$上是严格凹函数，存在唯一极大值. 通过使$\frac{\partial U_{C,i}}{\partial \epsilon_i}=0$，求得第i个客户隐私预算的最优解如下所示：

$$D(\epsilon^*_{-i})=\epsilon_i^*=\sqrt{\frac{B\epsilon_{-i}}{\rho_i}}-\epsilon_{-i} \quad (22)$$

当所有客户的隐私预算都取其最优解，即$\langle\epsilon_1^*,\epsilon_2^*,\cdots,\epsilon_N^*\rangle$时，在斯塔克伯格博弈的第二阶段，客户间形成非合作博弈的纳什均衡，求解过程如下：

假设隐私预算$\langle\epsilon_1^*,\epsilon_2^*,\cdots,\epsilon_N^*\rangle$是斯塔克伯格博弈第二阶段的纳什均衡. 当客户效用的一阶导数$\frac{\partial U_{C,i}}{\partial \epsilon_i}=0$时，公式(15)转化为

$$\rho_i\left(\sum_{i=1}^{N}\epsilon_i^*\right)^2=B\sum_{j\neq i}^{N}\epsilon_j^* \quad (23)$$

将每个客户$c_i, i\in N$的方程(23)相加，可以得到：

$$\sum_{j=1}^{N}\rho_j\left(\sum_{i=1}^{N}\epsilon_i^*\right)^2=B(N-1)\sum_{i=1}^{N}\epsilon_i^* \quad (24)$$

进而转化为

$$\left(\sum_{i=1}^{N}\epsilon_i^*\right)^2\sum_{i=1}^{N}\rho_i=B(N-1)\sum_{i=1}^{N}\epsilon_i^* \quad (25)$$

因此，可以得到第二阶段纳什均衡下的所有客户隐私预算的和$\sum_{i=1}^{N}\epsilon_i^*$：

$$\sum_{i=1}^{N}\epsilon_i^*=\frac{B(N-1)}{\sum_{i=1}^{N}\rho_i} \quad (26)$$

同样地，根据公式(15)，ϵ^*_{-i}可以表示为

$$\epsilon^*_{-i}=\frac{\rho_i\left(\sum_{i=1}^{N}\epsilon_i^*\right)^2}{B} \quad (27)$$

把公式(26)代入公式(27)，可得：

$$\epsilon^*_{-i}=\frac{\rho_i\left(\sum_{i=1}^{N}\epsilon_i^*\right)^2}{B}=\frac{\rho_i B(N-1)^2}{\left(\sum_{i=1}^{N}\rho_i\right)^2} \quad (28)$$

因此，通过使$\epsilon_i^*=\sum_{i=1}^{N}\epsilon_i^*-\epsilon^*_{-i}$，客户$c_i$的隐私预算$\epsilon_i^*$可以表示为

$$\epsilon_i^*=\sum_{i=1}^{N}\epsilon_i^*-\epsilon^*_{-i}=\frac{B(N-1)}{\sum_{i=1}^{N}\rho_i}\left(1-\frac{\rho_i(N-1)}{\sum_{i=1}^{N}\rho_i}\right) \quad (29)$$

由于对任意客户$c_i, i\in N$满足$\frac{\partial U_{C,i}}{\partial \epsilon_i}=0$，公式(29)为斯塔克伯格博弈第二阶段的纳什均衡解. 同样，通过将公式(26)和公式(28)代入公式(22)，可得：

$$\epsilon_i^*=\sqrt{\frac{B\epsilon_{-i}}{\rho_i}}-\epsilon_{-i}=\frac{B(N-1)}{\sum_{i=1}^{N}\rho_i}\left(1-\frac{\rho_i(N-1)}{\sum_{i=1}^{N}\rho_i}\right) \quad (30)$$

公式(30)和公式(29)相同，说明公式(29)为公式(22)的特殊形式. 因此，公式(29)也是斯塔克伯格博弈第二阶段的最优客户隐私预算.

将公式(26)和公式(29)代入公式(6)，可得当任意客户$c_i, i\in N$取其最优隐私预算ϵ_i^*时，最优客户效用$U_{C,i}^*$.

$$U_{C,i}^{*}=B\frac{\epsilon_i}{\sum_{j=1}^{N}\epsilon_j}-\rho_i\epsilon_i=B\left(1-\frac{\rho_i(N-1)}{\sum_{i=1}^{N}\rho_i}\right)^2 \quad (31)$$

5.2 第一阶段服务器的策略分析

服务器根据第二阶段客户的最优隐私预算,在第一阶段最大化服务器效用的最佳隐私支付上限.将第二阶段纳什均衡下客户的最优隐私预算$\langle\epsilon_1^*,\epsilon_2^*,\cdots,\epsilon_N^*\rangle$带入服务器的效用函数,第一阶段的服务器的效用可以表示为

$$U_S=\beta ln\left(1+\frac{\alpha B(N-1)}{N\sum_{i=1}^{N}\rho_i}\right)-B \quad (32)$$

通过计算服务器效用对隐私支付上限的导数,得到斯塔伯格博弈第一阶段的最优隐私上限.

$$\frac{\partial U_S}{\partial B}=\frac{\alpha\beta(N-1)}{N\sum_{i=1}^{N}\rho_i+\alpha(N-1)B}-1 \quad (33)$$

服务器效用U_S对隐私支付上限B的二阶导数表示为

$$\frac{\partial^2 U_S}{\partial B^2}=-\frac{\alpha^2\beta(N-1)^2}{\left(N\sum_{i=1}^{N}\rho_i+\alpha(N-1)B\right)^2}<0 \quad (34)$$

公式(34)说明服务器效用U_S的一阶导数随隐私支付上限B严格减少.

在本文的假设中,隐私支付上限B严格大于0,并由于服务器效用严格大于0,可以得到隐私支付上限B的取值范围:

$$0<B<\beta ln\left(1+\frac{\alpha}{N}\left(\sum_{i=1}^{N}\epsilon_i\right)\right) \quad (35)$$

在第二阶段客户间隐私预算达到纳什均衡的条件下,将公式(26)中带入公式(35)中,隐私支付上限B的取值范围为

$$0<B<\beta ln\left(1+\frac{\alpha(N-1)}{N\sum_{i=1}^{N}\rho_i}B\right) \quad (36)$$

设$f_1(x)=x,f_2(x)=\beta ln\left(1+\frac{\alpha(N-1)}{N\sum_{i=1}^{N}\rho_i}x\right)$,由于$f_1(0)=0,f_2(0)=0$根据式(36)的右式,可得,$f_1'(x)\leqslant f_2'(x)$,即$B\leqslant\beta-\frac{\rho N^2}{\alpha(N-1)}$,所以,隐私支付上限$B$的取值区间为

$$0<B\leqslant\beta-\frac{N\sum_{i=1}^{N}\rho_i}{\alpha(N-1)} \quad (37)$$

其中,$\beta-\frac{N\sum_{i=1}^{N}\rho_i}{\alpha(N-1)}>0$.分别考虑服务器的隐私支付上限$B$趋近于0和等于$\beta-\frac{N\sum_{i=1}^{N}\rho_i}{\alpha(N-1)}$两种情况.

(1)服务器的隐私支付上限B趋近于0时:

$$\lim_{B\to 0}\frac{\partial U_S}{\partial B}=\lim_{B\to 0}\frac{\alpha\beta(N-1)}{N\sum_{i=1}^{N}\rho_i+\alpha(N-1)B}-1=\frac{\alpha\beta(N-1)}{N\sum_{i=1}^{N}\rho_i}-1 \quad (38)$$

由于$\beta-\frac{N\sum_{i=1}^{N}\rho_i}{\alpha(N-1)}>0$,可得:

$$\lim_{B\to 0}\frac{\partial U_S}{\partial B}=\frac{\alpha\beta(N-1)}{N\sum_{i=1}^{N}\rho_i}-1>1-1=0 \quad (39)$$

根据公式(39),当服务器的隐私支付上限B趋近于0时,服务器效用的一阶导数$\frac{\partial U_S}{\partial B}$大于0.

(2)服务器的隐私支付上限B等于$\beta-\frac{N\sum_{i=1}^{N}\rho_i}{\alpha(N-1)}$时:

将$B=\beta-\frac{N\sum_{i=1}^{N}\rho_i}{\alpha(N-1)}$带入$\frac{\partial U_S}{\partial B}$,可得:

$$\left.\frac{\partial U_S}{\partial B}\right|_{B=-\frac{N\sum_{i=1}^{N}\rho_i}{\alpha(N-1)}}=0 \quad (40)$$

由公式(39)和公式(40)可知,服务器效用的一阶导数$\frac{\partial U_S}{\partial B}\geqslant 0$在$B$的取值区间$\left(0,\beta-\frac{N\sum_{i=1}^{N}\rho_i}{\alpha(N-1)}\right)$上恒成立.因此,服务器效用函数在区间$\left(0,\beta-\frac{N\sum_{i=1}^{N}\rho_i}{\alpha(N-1)}\right)$上递增.服务器效用在区间右边界取得唯一最大值的同时满足$\frac{\partial U_S}{\partial B}=0$.可得服务器的最优隐私支付上限$B^*$为

$$B^*=\beta-\frac{N\sum_{i=1}^{N}\rho_i}{\alpha(N-1)} \quad (41)$$

此时,服务器的最优效用U_S^*为

$$U_S^*=\beta ln\left(\frac{\alpha\beta(N-1)}{N\sum_{i=1}^{N}\rho_i}\right)-\beta+\frac{N\sum_{i=1}^{N}\rho_i}{\alpha(N-1)} \quad (42)$$

6　参与用户限制条件分析

在得到均衡解的基础上，通过进一步分析，同样可以得到上述隐私定价机制设计下，对用户参与的限制条件：

将公式(26)代入公式(19)，可得：

$$\frac{\rho_i B(N-1)}{\sum_{i=1}^{N}\rho_i}<B \tag{43}$$

又由于$B>0$恒成立，可知：

$$\frac{\rho_i(N-1)}{\sum_{i=1}^{N}\rho_i}<1 \tag{44}$$

根据公式(37)，$\beta-\frac{N\sum_{i=1}^{N}\rho_i}{\alpha(N-1)}>0$可得：

$$\frac{N\sum_{i=1}^{N}\rho_i}{\alpha(N-1)}<\beta \tag{45}$$

本文中，参数满足公式(45)的限制条件. 由公式(44)和公式(45)可得：

$$(N-1)\rho_i<\sum_{i=1}^{N}\rho_i<\frac{\alpha\beta(N-1)}{N} \tag{46}$$

$$\rho_i<\frac{\sum_{i=1}^{N}\rho_i}{N-1}<\frac{\alpha\beta}{N} \tag{47}$$

设$\sum_{i=1}^{N}\rho_i=\tau$，成本参数$\rho_i$的限制条件可表示：

$$\rho_i<\frac{\tau}{N-1} \tag{48}$$

由以上分析可知，本文所设计的隐私定价机制下，单位隐私成本ρ_i过高的用户将会因为效用为负而出局. 在用户隐私需求差异度较小的情况下，基于理性人假设，用户为了获取更大效用，并不会尝试盲目扩大隐私预算尺度，从而有效减少了不必要的隐私冗余精度损耗.

此外，在用户隐私需求差异度较高的情况下，该方法同样通过报酬支付的激励作用定向筛选出相似度较高的用户，避免现有差分隐私方法中由于个别离群值用户而导致性能急剧下降的现象发生.

根据差分隐私的定义(1)，对于拥有较大本地数据差异和数据敏感度的离群用户，为保护自己的隐私信息，倾向于选择较小的隐私预算. 根据公式(4)，用户上报的隐私预算越小，其参与协同训练获得的报酬也就越少. 离群用户将由于无法同时满足隐私安全和隐私服务成本，而被排除联邦学习.

7　实验设计

在本节中，通过部署在Intel i7-1065G7 CPU @ 1.30 GHz的计算机上进行单机模拟和实际仿真来评估本文提出的机制的性能，其中启动1000个客户进程和1个服务器进程. 为了验证所提出隐私定价机制的有效性，本节分别从效用，参数设置和对比试验三个方面对隐私定价机制的性能进行分析.

7.1　实验设置

本文基于Pytorch深度学习框架进行实验，且使用EMNIST和CIFAR-10作为基准数据集. EMNIST包含10个数字类别和52个大小写英文字母类别共62种类别，所有图像均按照28×28像素进行缩放. 本文对EMNIST按照8:2的比例划分训练集和验证集. CIFAR-10包含10个类的60 000个32×32彩色图像，每个类有6000个图像. 同样地，按照8:2的比例划分训练集和验证集.

本文使用有两个5×5卷积层、一个全连接层和一个softmax输出层的四层CNN神经网络在EMNSIT数据集上完成学习任务. 对于CIFAR-10数据集，采用有两个5×5卷积层、两个全连接层和一个softmax输出层的五层CNN神经网络. 本文在实验中设置N=10～1000个客户端，共进行200个轮次的通信. 对于每个客户端，本地训练周期E=5，批处理大小b=128，学习率$\eta=0.1$，动量$m=0.9$. 具体实验参数设置如表2所示.

表2　实验参数设置

参数	符号	实验取值
客户数量	N	[1,1000]
通信轮次	T	200
本地训练周期	E	5
批处理大小	b	128
学习率	η	0.1
动量	m	0.9

此外，由于参数α代表了隐私预算对模型性能的影响，α不宜设置过大或过小. 本文将根据实验的具体设置和效果对参数α进行具体和合理的设置. 同样，对于参数β，根据公式(45)，需要满足$\beta>\frac{N\sum_{i=1}^{N}\rho_i}{(N-1)\alpha}$，因此，在下文中，参数$\beta$要综合具体实验中的客户数量N，客户成本系数和$\sum_{i=1}^{N}\rho_i$与参数$\alpha$进行设置.

7.2 效用分析

为了验证隐私定价机制中效用的合理性，分别对客户和服务器的效用进行分析.

(1)客户效用分析

为了验证客户最优效用的存在性和唯一性，在客户隐私成本ρ_i一定的情况下，考虑客户选择不同隐私预算ϵ_i对客户效用的影响. 为了便于实验，统一设置客户的成本参数$\rho_i=0.001$. 在客户间的非合作博弈中，其他客户的隐私选择也会对当前客户的效用产生影响. 为了在当前实验中消除其他客户的影响，将其他客户$c_j\in C, c_j\neq c_i$的隐私预算固定为$\epsilon_j=\epsilon^*$.

当前客户效用随隐私预算的变化如图4所示. 可以看出，随着客户选择隐私预算的增加，当前客户的效用随之增加，当客户选择最优隐私预算$\epsilon_i=\epsilon^*$时，客户效用达到峰值. 当$\epsilon_i>\epsilon^*$时，客户效用随隐私预算的增加而减少. 这是由于随着客户选择更宽松的隐私预算，服务器支付客户更多的隐私补偿，客户承担的隐私损失成本也随之缓慢增加，隐私支付和成本的增长速度在ϵ^*达到平衡. 此后，过大的隐私预算增加了客户隐私泄露的风险，隐私补偿增加的速度无法负担隐私成本的快速增长，客户效用开始下降. 容易看出，客户的效用函数是在其取值区间是严格的凹函数，并在最佳隐私预算ϵ^*处取得其唯一最优解.

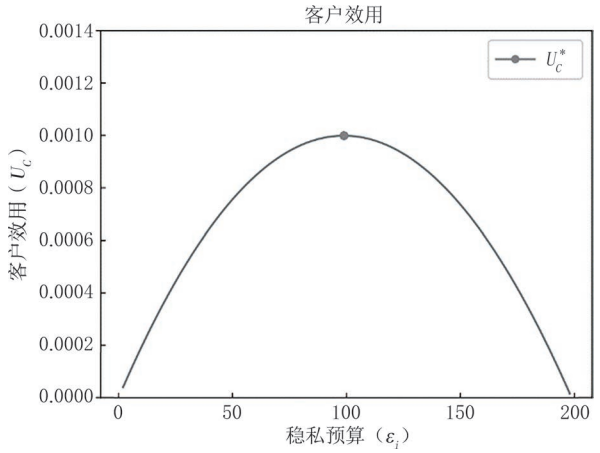


图4 客户效用函数

由于在联邦算力网络梯度上传，聚合等过程中普遍存在着窃取客户信息以侵害客户隐私安全的差分攻击. 本文的隐私定价机制为了保证客户数据的隐私安全，通过考虑隐私成本对客户高风险的隐私预算选择行为进行限制. 为有效保障客户的隐私安全，防止客户盲目追求高收益而忽略个人隐私泄露的风险选择过大的隐私预算，本文的客户效用不仅受到数据收益的激励，还有隐私成本的限制. 本文的客户效用如公式(6)所示，根据博弈论中的个体理性(IR)假设，作为博弈参与者的客户的效用必须非负，如公式(49)所示：

$$U_{C,i}=B\frac{\epsilon_i}{\sum_{j=1}^{N}\epsilon_j}-\rho_i\epsilon_i>0 \tag{49}$$

上述公式可以进一步转换如下：

$$\sum_{j=1}^{N}\epsilon_j<\frac{B}{\rho_i} \tag{50}$$

因为$\sum_{j=1}^{N}\epsilon_j=\epsilon_i+\sum_{i\neq j}^{N}\epsilon_j$，公式(50)可写作：

$$\epsilon_i+\sum_{i\neq j}^{N}\epsilon_j<\frac{B}{\rho_i} \tag{51}$$

在每轮定价交互中客户的隐私成本系数ρ_i和服务器的总预算B一定的情况下，客户的隐私预算选择存在约束上界$\frac{B}{\rho_i}$.

$$\epsilon_i<\frac{B}{\rho_i} \tag{52}$$

即$\epsilon_i<\frac{B}{\rho_i}$恒成立，且当所有其余客户$c_j\in C, c_j\neq c_i$的隐私预算$\epsilon_j\to 0$时，当前客户$c_i$的隐私预算$\epsilon_i$最大，$\epsilon_i\to\frac{B}{\rho_i}$.

如图4所示，在客户效用的实验中，当固定成本系数ρ_i，总预算$B=B^*=\beta-\frac{N\sum_{i=1}^{N}\rho_i}{\alpha(N-1)}=\frac{980}{99}$和其余客户隐私预算$\epsilon_j=\epsilon_i^*=\frac{B(N-1)}{\sum_{i=1}^{N}\rho_i}\left(1-\frac{\rho_i(N-1)}{\sum_{i=1}^{N}\rho_i}\right)=98$时，可以看出当前客户的隐私预算$\epsilon_i$存在取值范围$0<\epsilon_i<\frac{19\,502}{99}$. 因此，在图4中，当$\epsilon_i=\frac{19\,502}{99}$时，客户效用$U_{C,i}=0$，$\epsilon_i$的取值范围$(0,\frac{19\,502}{99})$能够保证客户隐私的安全性. 并且客户的效用函数$U_{C,i}$在其取值范围内是严格凹函数，在隐私预算的最优解$\epsilon^*$取得最大值$U_{C,i}^*$.

(2)服务器效用分析

为了验证服务器最优效用的存在性和唯一性，当客户选择隐私预算ϵ_i一定的情况下，考虑服务器

选择不同隐私支付上限B对服务器效用的影响. 在服务器效用分析的实验中,本文设置服务器效用参数$\alpha=\beta=10$. 由于客户隐私预算的选择也会对服务器的效用产生影响. 在当前实验中,假设所有客户隐私成本参数均为$\rho_i=0.01$,并且给定隐私支付上限B,客户均能通过最优化自身效用选择其最优的隐私预算$\epsilon_i=\epsilon^*$.

当前服务器效用随隐私支付上限B的变化如图5所示. 可以看出,随着服务器选择隐私支付上限的增加,服务器的效用随之增加,当服务器选择最优隐私支付上限$B=B^*$时,服务器效用达到峰值. 之后,服务器效用随隐私支付上限的增加而减少. 由于服务器隐私支付上限的增加,不断增加的隐私补偿激励客户选择更宽松的隐私预算,噪声干扰更小,模型性能更好,服务器的收益也逐渐提升. 然而,过大的隐私支付增加了服务器的成本,随着隐私预算越来越宽松,模型所加差分隐私噪声趋近于零,模型性能提升也不再明显. 模型收益增长减缓,而成本仍在增加,服务器的效用随着隐私支付的增加逐渐降低. 容易看出,服务器的效用函数是在其取值区间是严格的凹函数,并在最佳隐私预算B^*处取得其唯一最优解.

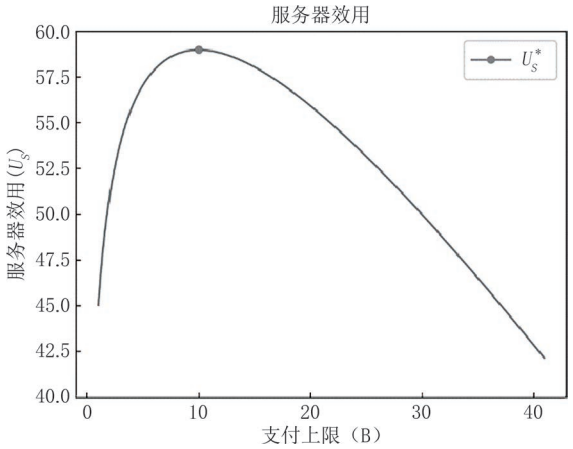


图5　服务器效用函数

从图4和图5可知,客户和服务器的效用函数都是严格凹函数,且在取值区间存在唯一的最优解,满足隐私定价机制中效用函数的合理性.

7.3　参数分析

本节将对隐私定价机制中的参数进行分析,评估各参数在斯塔克伯格博弈第一阶段和第二阶段最优化问题中的影响,分别考虑参数对客户最优隐私预算ϵ^*,最优客户效用U_C^*,最优隐私支付上限B^*和最优服务器效用U_S^*的影响.

(1)客户最优隐私预算ϵ^*随参数的变化

① 隐私成本参数ρ_i对客户最优隐私预算ϵ^*的影响

为了评估隐私成本参数对计算客户最优隐私预算的影响,设置客户数量N=100,模型收益系数$\alpha=\beta=10$,且假设所有客户的ρ_i相等. 分别在服务器的隐私支付上限B=1,5,10,20的条件下观察客户的最优隐私预算ϵ^*随着隐私成本参数$\rho_i\in[0.001,1]$的变化情况.

图6中,随着成本参数ρ_i的增加,最优隐私预算的值快速减少至接近0,再缓慢递减. 且隐私支付上限B越大,客户的最优隐私预算ϵ^*越大. 因为当客户的隐私成本增加时,为了使自身效用最大化,客户倾向于选择更小的隐私预算ϵ_i,减少隐私损失的成本. 并且隐私支付上限B越大,越能在一定程度上抵消成本增长的影响,达到最优客户效用的隐私预算值越大.

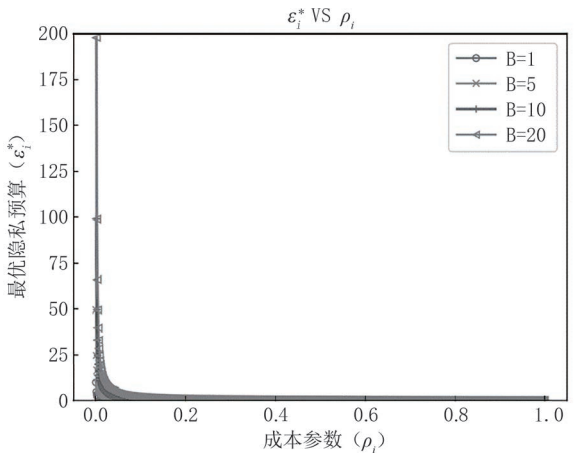


图6　隐私成本参数对最优隐私预算的影响

② 客户数量N对客户最优隐私预算ϵ^*的影响

为了评估客户数量对计算客户最优隐私预算的影响,设置模型收益系数$\alpha=\beta=10$,且统一设置所有客户的$\rho_i=0.01$. 分别在服务器的隐私支付上限B=1,5,10,20的条件下观察客户的最优隐私预算ϵ^*随着客户数量$N=1,\cdots,1000$的变化情况.

如图7所示,随着客户数量N的增加,最优隐私预算的值从0快速增加,再缓慢递减. 且隐私支付上限B越大,客户的最优隐私预算ϵ^*越大. 当客户数量大于1时,大量的客户使得客户得到隐私支付的份额急剧减少,最优隐私预算也相应降低. 隐私支付上限B越大,越有能力抵消客户数量增长的冲击,客户能够保持更大的最优隐私预算.

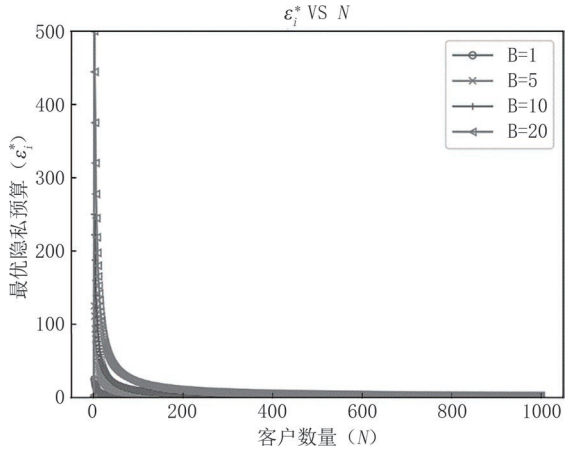


图7 客户数量对最优隐私预算的影响

(2)最优客户效用U_C^*随参数的变化

① 客户数量N对最优客户效用U_C^*的影响

为了评估客户数量对计算客户最优隐私预算的影响，设置模型收益系数$\alpha=\beta=10$，且统一设置所有客户的$\rho_i=0.001$. 分别在服务器隐私支付上限B=1,5,10,20的条件下观察客户最优隐私预算ϵ^*随着客户数量$N=1,\cdots,100$的变化情况.

从图8可以看出，随着客户数量N的增加，最优客户效用不断减少. 且隐私支付上限B越大，客户的最优客户效用U_C^*越大. 客户数量越多，每个客户分得的隐私补偿越少，最优客户效用越小. 隐私支付上限B越大，越有能力抵消客户数量增长的冲击，客户能够保持更大的最优效用.

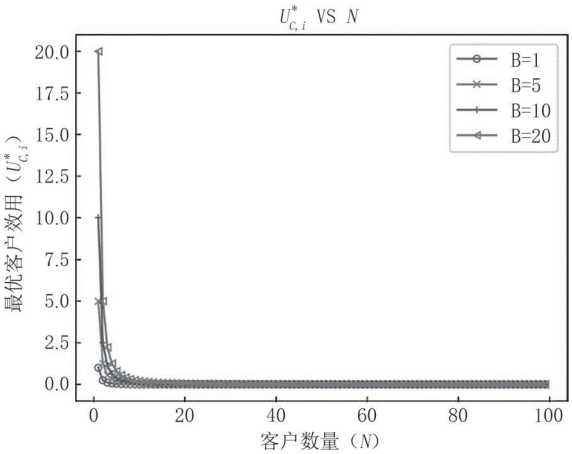


图8 客户数量对最优客户效用的影响

(3)最优隐私支付上限B^*随参数的变化

① 参数α对最优隐私支付上限B^*的影响

为了评估模型收益函数中参数α对最优隐私支付上限B^*的影响，设置客户数量N=100，模型收益系数$\beta=10$，且假设客户的成本参数和固定$\sum_{i=1}^{N}\rho_i=1$. 考虑服务器的最优隐私支付上限B^*随着参数$\alpha\in[0.2,100]$的变化情况.

从图9可以看出，随着参数α的增加，最优隐私支付上限快速增加并最终逐渐趋近于参数β大小. 根据模型的收益函数，模型收益增长的速率随着参数α的增加而增大，参数β则决定最优隐私支付上限B的上限.

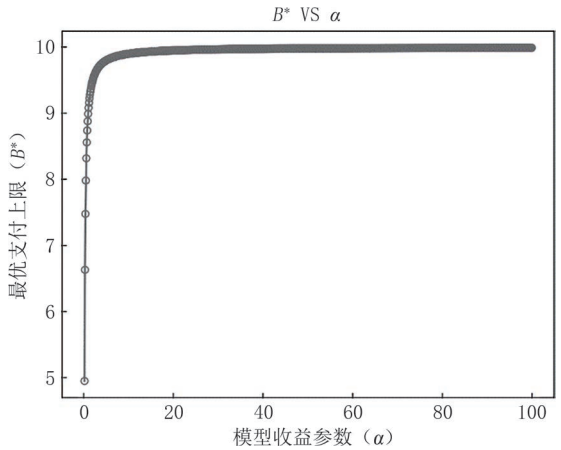


图9 参数α对最优隐私支付上限的影响

② 参数β对最优隐私支付上限B^*的影响

为了评估模型收益函数中参数β对最优隐私支付上限B^*的影响，设置客户数量N=100，模型收益系数$\alpha=10$，且假设客户的成本参数和固定$\sum_{i=1}^{N}\rho_i=1$. 考虑服务器的最优隐私支付上限B^*随着参数$\beta\in[1,100]$的变化情况.

如图10所示，随着参数β的增加，最优隐私支付上限B^*线性增加，参数β和最优隐私支付上限B^*是正相关的线性关系.

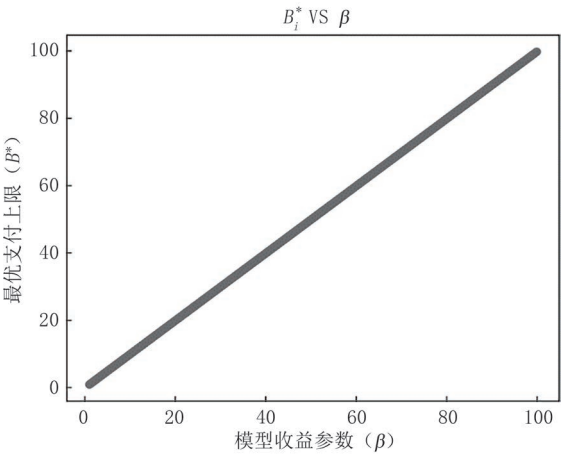


图10 参数β对最优隐私支付上限的影响

(4)最优服务器效用U_S^*随参数的变化

① 参数α对最优服务器效用U_S^*的影响

为了评估模型收益函数中参数α对最优服务器效用U_S^*的影响，设置客户数量N=100，模型收益系数$\beta=10$，且假设客户的成本参数和固定$\sum_{i=1}^{N}\rho_i=1$. 考虑服务器的最优服务器效用U_S^*随着参数$\alpha\in[0.2,100]$的变化情况.

从图11可以看出，随着参数α的增加，最优服务器效用持续增加. 这是由于模型收益随着参数α的增加而增大. 即使模型收益增长的速率不断减小，由于最优隐私支付上限B^*趋于稳定值β，最优服务器效用U_S^*仍能保持增长趋势.

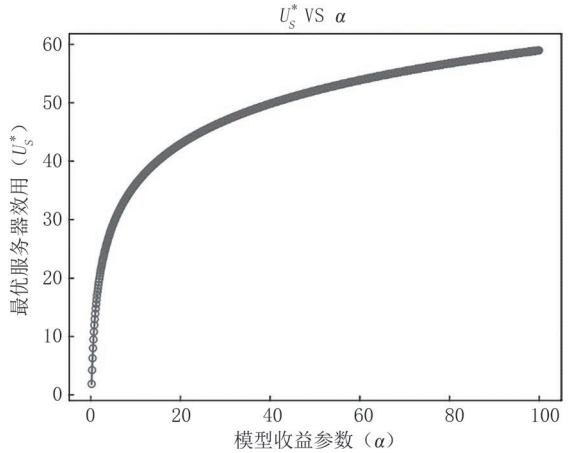


图11　参数α对最优服务器效用的影响

② 参数β对最优服务器效用U_S^*的影响

为了评估模型收益函数中参数β对最优服务器效用U_S^*的影响，设置客户数量N=100，模型收益系数$\alpha=10$，且假设客户的成本参数和固定$\sum_{i=1}^{N}\rho_i=1$. 考虑最优服务器效用U_S^*随着参数$\beta\in[1,100]$的变化情况.

如图12所示，随着参数β的增加，最优服务器效用U_S^*持续增加. 参数β和最优服务器效用U_S^*正相

上述实验证明了隐私定价机制中的参数稳定性，最优化求解过程中合理的参数设置不会影响最终结果的有效性.

7.4　对比实验

为了证明隐私定价机制的性能改进，本节将提出的隐私定价机制与随机定价[16]，静态定价[16]，IC-MLE方法[49]和Yang et al. 方法[47]进行比较.

随机定价[16]方法表示客户并不根据自身效用最大化的原则选择合适的隐私预算，而是随机选择隐

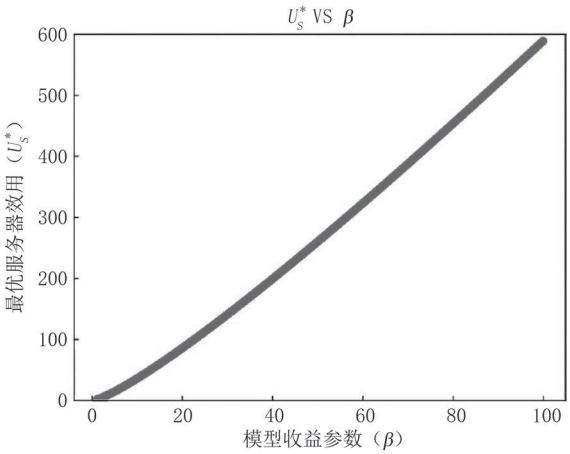


图12　参数β对最优服务器效用的影响

私预算. 静态定价[16]方法则是所有客户固定统一选择某一隐私预算.

IC-MLE方法[49]是一种基于合约理论的个性化隐私感知数据交易方法，为自私的数据所有者提供一组指定不同隐私保护级别和数据交易价格的最优合约. 该方法通过最大化数据聚合结果的准确度来最大化众包数据的数据效用，同时与自私的数据所有者的个性化隐私偏好相容. 针对不完全信息下的最优合约设计，对于类型k的数据所有者的可用数据数量m_k，最优契约问题可以表述如下：

$$\min_{\epsilon_k,p_k}\ \sum_{k=1}^{K}m_k\left(\frac{e^{\epsilon_k}+1}{e^{\epsilon_k}-1}\right)^2 \tag{53}$$

$$\text{s.t.}\ \sum_{k=1}^{K}m_k p_k\leqslant B, \tag{54}$$

$$p_k-c_k\epsilon_k\geqslant 0,\forall k, \tag{55}$$

$$p_k-c_k\epsilon_k\geqslant p_{k'}-c_k\epsilon_k,\forall k,k'\neq k \tag{56}$$

其中，p_i是数据所有者收到的报酬，ρ_i是数据的隐私成本系数，ϵ_i是数据所有者选择的隐私预算.

Yang et al. 方法[47]是一种针对买方，卖方和市场代理间隐私数据交易的三方博弈定价方法，并用逆向归纳法求解上述博弈的最优策略. 可以得到给定数据单价p_i下数据卖方i的最优数据购买策略a_i^*.

$$a_i^*=\frac{\alpha}{p_i(1+\epsilon_i)}-1 \tag{57}$$

根据数据买方的最优购买策略a_i^*，通过最优化市场效用，计算数据卖方的最优定价策略p_i^*.

$$p_i^*=\sqrt{\left(\sum_{j\neq i}\frac{1}{p_j}+\frac{1+\epsilon_i}{\alpha}\right)\left(\sum_{j\neq i}\frac{1}{p_j}+\frac{1+\epsilon_i}{c_i}\right)}-\sum_{j\neq i}\frac{1}{p_j} \tag{58}$$

基于市场机构为数据买方决定的最优定价策略，数据

买方计算其最优隐私预算ϵ_i^*，完成全部定价流程.

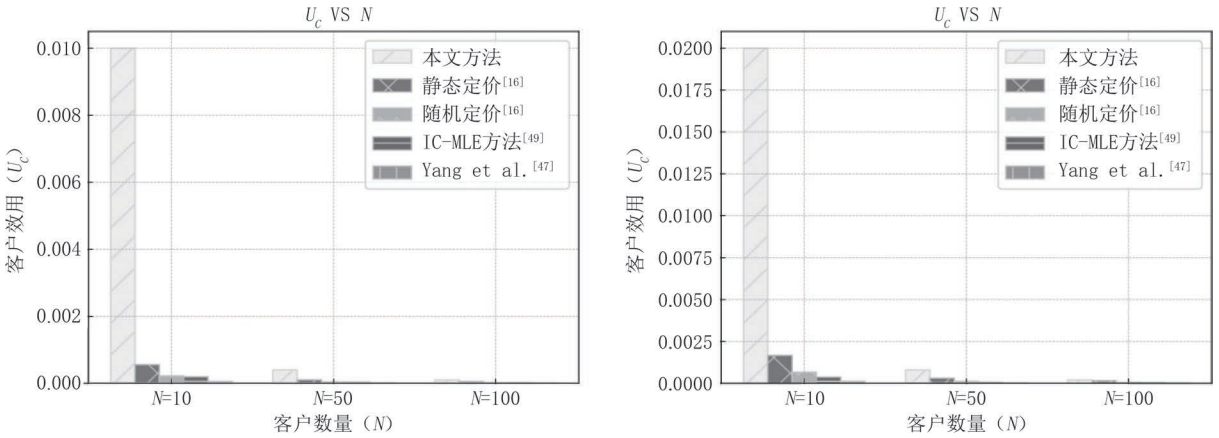
$$\epsilon_i^* = \frac{\alpha_3}{a_i^* \mathrm{p}_i^*} \tag{59}$$

根据上述方法，分别在EMNIST和CIFAR的数据集中进行不同参数设置条件下客户效用，服务器效用和激励效果的对比实验.

(1)客户效用对比实验

① 不同客户数量N下的客户效用U_C

为了评估四种方法在不同客户数量N下的客户效用U_C，EMNIST和CIFAR数据集实验中的模型收益系数分别设置为$\alpha=\beta=\{10,20\}$，服务器隐私支付上限$B=\{1,2\}$. 假设客户的成本固定$\rho_i=\{0.001,0.003\}$. 当客户数量参数$N=10,50,100$时本文方法，Yang et al. 方法，IC-MLE方法，静态方法和随机定价方法的客户效用U_C如图13所示.



(a) EMNIST 数据集　　(b) CIFAR 数据集

图13 不同客户数量N下的客户效用

其中，随机方法客户c_i的隐私预算ϵ_i在区间[1,100]随机选择. EMNIST和CIFAR中的静态定价方法中客户c_i的隐私预算则分别固定为$\epsilon_i=\{10,5\}$.

从图13中可以看出，在EMNIST和CIFAR的数据集中，在同样的参数设置下，本文的隐私定价方法下的最优客户效用明显大于Yang et al. 方法，IC-MLE方法，静态方法和随机方法的客户效用. 并且随着客户数量的减少，本文方法与其他方法客户效用的差异越明显. 这是由于随机方法和静态方法是随机或固定选择隐私预算，选择的隐私预算与最优隐私预算的差距较大，相应的客户效用也相对较低. IC-MLE方法的数据价格与客户选择的隐私预算没有直接联系，只考虑了数据的隐私成本，无法像本文一样为客户交付隐私数据提供正向的激励，因此最优客户效用并不高. Yang et al. 方法售卖隐私数据的获利，作为数据卖方的客户并不能全部取得，还需要经过市场机构抽取部分利润并分配隐私补偿，所以相对于其他方法的客户效用最低.

(2)服务器效用对比实验

针对服务器，本文评估了本文方法，Yang et al. 方法和IC-MLE方法在EMNIST和CIFAR数据集实验环境下的服务器效用. 在EMNIST和CIFAR实验环境下客户的成本分别为$\rho_i=\{0.001,0.003\}$.

① 不同参数α下的服务器效用U_S^*

EMNIST和CIFAR实验中模型收益系数分别设置为$\beta=\{10,20\}$，当参数$\alpha=1,10,100$时，隐私定价，IC-MLE方法和 Yang et al. 方法的服务器效用U_S如图14所示.

容易看出，在不同的参数α设置下，有隐私定价机制的最优服务器效用大于IC-MLE方法和 Yang et al. 方法计算的服务器效用恒成立.

② 不同参数β下的服务器效用U_S^*

EMNIST和CIFAR实验中模型收益系数分别设置为$\alpha=\{10,20\}$，当参数$\beta=1,10,100$时，隐私定价，IC-MLE方法和 Yang et al. 方法的服务器效用U_S如图15所示. 可以看出，在不同的参数β设置下，隐私定价机制下的服务器效用优于IC-MLE方法和 Yang et al. 方法.

(3)模型性能对比实验

为了验证本文方法隐私定价激励效果的优越性和本文方法在隐私联邦学习中的安全性. 本文分别在EMNIST和CIFAR数据集的相同参数设置条件下计算本文方法，IC-MLE方法和Yang et al. 方法三种激励机制的最优隐私预算. 在EMNIST和

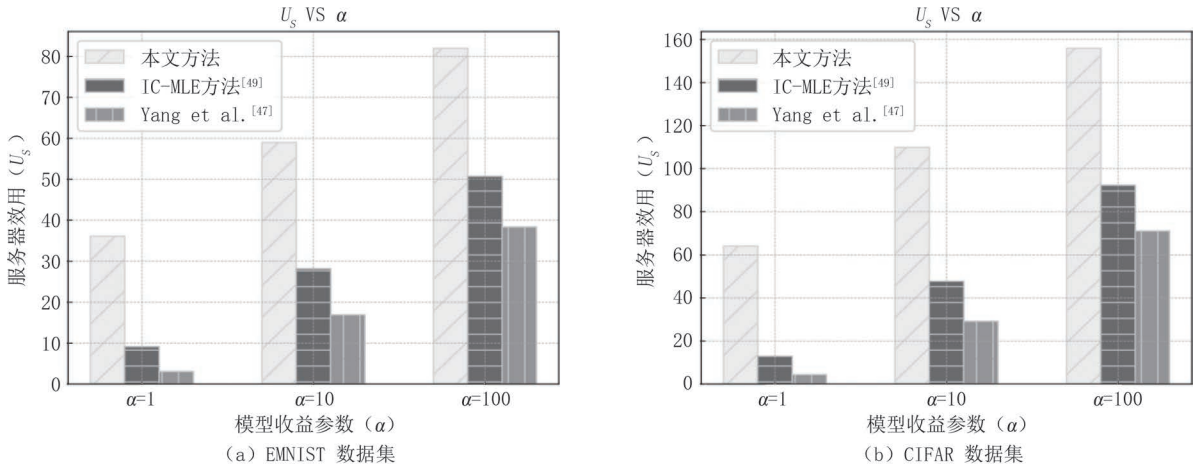


图14　不同参数α下服务器效用

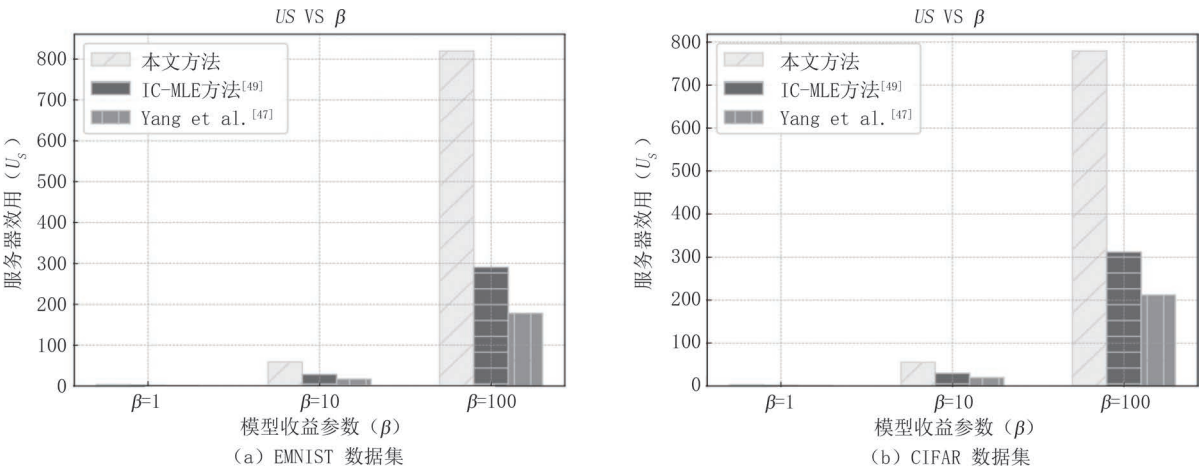


图15　不同参数β下服务器效用

CIFAR实验环境下模型收益系数分别设置为$\alpha=\beta=\{10,20\}$，服务器隐私支付上限$B=\{1,2\}$，客户的成本$\rho_i=\{0.001,0.003\}$. 三种方法在EMNIST和CIFAR实验环境下的最优隐私预算及对应的噪声大小和隐私联邦学习的准确度分别如图16和图17所示.

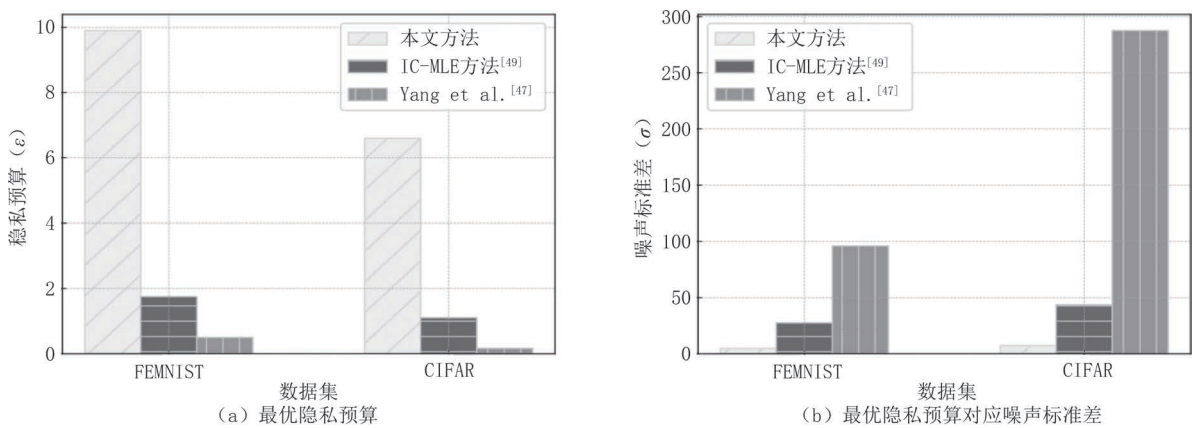


图16　最优隐私预算与噪声损失

从图16中，可以看出，在同样的实验设置下，本文提出激励机制的最优隐私预算远大于IC-MLE方法和Yang et al. 方法得出的最优隐私预算，对应的噪声标准差也更小. 证明了本文方法通过隐私补偿的方式能够有效激励客户选择更大的隐私预算，并且按照客户上报的隐私预算对其进行个性化的隐私

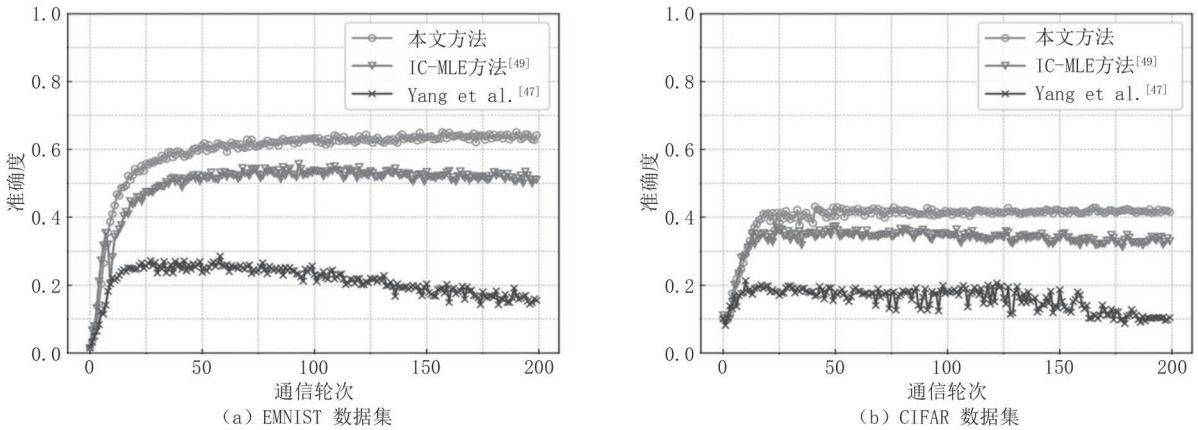


图17 隐私联邦学习的准确度

保护，根据噪声标准差的计算公式$\sigma \geqslant \frac{d\Delta_2 f}{\epsilon}$，本文方法添加的随机噪声更小. 因此，如图17所示，在联邦算力网络的应用中，由于加噪更少，应用本文方法的隐私联邦学习准确度更高，在保障客户隐私安全的同时保证了高性能的联合学习，实现隐私安全和模型安全的双保险.

上述实验证明了本文提出的隐私定价机制针对客户和服务器均能给出合理的定价的同时最大化其效用，证明了隐私定价机制的优越性和安全性.

8 结 论

本文针对联邦算力网络对用户隐私缺乏考量的缺陷，提出了一种基于两阶段动态博弈的隐私计算自适激励机制，能够有效解决现有分布式计算激励机制由于缺乏对用户隐私噪声选取的合理引导导致的冗余学习精度损耗问题. 本文将联邦隐私计算服务方与参与用户之间关于隐私噪声注入尺度选取与支付定价的动态博弈分为两个阶段进行分析. 首先，通过跟随者(用户)之间的非合作博弈，获取隐私预算个性化策略；随后，基于反向归纳，获取纳什均衡下的领导者(服务器)最优定价策略. 本文在公开数据集上进行的系列仿真实验以及与现有的IC-MLE方法和Yang et al.方法等隐私定价方案的对比结果也验证本文所提出的方法能够同时优化并提升服务方与参与者的平均效用.

未来，作者将进一步考虑实际应用场景中，海量边缘算力节点时空离散分布带来的数据异构问题. 在本文研究成果的基础上，通过设计自适应聚合激励方案，弥补梯度敏感度过大导致的隐私噪声注入超限与学习性能劣化缺陷，实现动态高度异构场景下对用户个性化隐私预算选取的有效理性规约，从而在满足用户差分隐私保障的同时提升异构计算任务性能.

致 谢 感谢对本文提出建议的所有评审专家!

参 考 文 献

[1] Liang Yi, Ding Zhen-Xing, Zhao Yu, Liu Ming-Jie, Pan Yong, Jin Yi. A Collaborative Method for Resource Allocation and Batch Sizing on Distributed Deep Learning System. Chinese Journal of Computers, 2022, 45(2): 302-316 (in Chinese)
(梁毅，丁振兴，赵昱，刘明洁，潘勇，金翊. 一种面向分布式深度学习系统的资源及批尺寸协同配置方法. 计算机学报，2022，45(2)：302-316)

[2] Dalmolen S, Kollenstart M, Moonen H, et al. Trusted Data Sharing in Federated and Dynamic Mission Contexts: Improving Communication Flexibility with Emerging Data Control Architectures and Concepts. IEEE communications magazine, 2021, 59(8): 66-72

[3] Zhou Z, Chen X, Li E, et al. Edge intelligence: Paving the last mile of artificial intelligence with edge computing. Proceedings of the IEEE, 2019, 107(8): 1738-1762

[4] Wang Y, Su Z, Zhang N, et al. A survey on metaverse: Fundamentals, security, and privacy. IEEE Communications Surveys and Tutorials, 2023, 25(1): 319-352

[5] Shome D, Waqar O, Khan W U. Federated learning and next generation wireless communications: A survey on bidirectional relationship. Transactions on Emerging Telecommunications Technologies, 2022, 33(7): e4458

[6] Wang X, Xu C, Zhou Z, Yang S, and Sun L. A survey of blockchain-based cybersecurity for vehicular networks// Proceedings of the 16th International Wireless Communications and Mobile Computing Conference (IWCMC). Limassol, Cyprus, 2020: 740-745

[7] Konečný J, Brendan McMahan H, Yu F X, et al. Federated

learning：Strategies for improving communication efficiency. 2016：arXiv：1610.05492

[8] China Mobile Research Institute. Computing force network technology whitepaper，2022.（in Chinese）
（中国移动研究院，算力网络技术白皮书[R]. 2022）

[9] Xu Zhi-Wei，Li Guo-Jie，Sun Ning-Hui. Information Superbahn：Towards new type of cyberinfrastructure. Bulletin of Chinese Academy of Sciences，2022，37（1）：46-52（in Chinese）
（徐志伟，李国杰，孙凝晖. 一种新型信息基础设施：高通量低熵算力网(信息高铁). 中国科学院院刊，2022，37(1)：46-52）

[10] Jia Qing-Min，Hu Yu-Jiao，Zhang Hua-Yu，Peng Kai-Lai，Chen Ping-Ping，Xie Ren-Chao，Huang Tao. Research on deterministic computing power network. Journal on Communications，2022，43(10)：55-64（in Chinese）
（贾庆民，胡玉姣，张华宇，彭开来，陈平平，谢人超，黄韬. 确定性算力网络研究. 通信学报，2022，43(10)：55-64）

[11] Tang X，Cao C，Wang Y，et al. Computing power network：The architecture of convergence of computing and networking towards 6G requirement. China communications，2021，18(2)：175-185

[12] Xie Y A，Kang J，Niyato D，et al. Securing Federated Learning：A Covert Communication-Based Approach. IEEE Network，2023，37(1)：118-124

[13] Zhou Z，Xu C，Wang M，Ma T，and Yu S. Augmented dual-shuffle-based moving target defense to ensure cia-triad in federated learning//Proceedings of the IEEE Global Communications Conference，GLOBECOM 2021. Madrid，Spain，2021：1-6

[14] McMahan B，Moore E，Ramage D，et al. Communication-efficient learning of deep networks from decentralized data//Proceedings of the 20th International Conference on Artificial Intelligence and Statistics，AISTATS 2017. LauderdaleFort，USA，2017：1273-1282

[15] Zhu L，Liu Z，Han S. Deep leakage from gradients//Proceedings of the 33rd International Conference on Neural Information Processing Systems. BC，Canada，2019：14774-14784

[16] Fredrikson M，Jha S，Ristenpart T. Model inversion attacks that exploit confidence information and basic countermeasures//Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security. Denver，USA，2015：1322-1333

[17] Neto H N C，Hribar J，Dusparic I，et al. Securing Federated Learning：A Security Analysis on Applications，Attacks，Challenges，and Trends. IEEE Access，2023

[18] Liu Yi-Xuan，Chen Hong，Liu Yu-Han，and Li Cui-Ping. Privacy-preserving techniques in federated learning. Journal of Software，2021，33(3)：1057-1092（in Chinese）
（刘艺璇，陈红，刘宇涵，等. 联邦学习中的隐私保护技术. 软件学报，2021，33(3)：1057-1092）

[19] Zhao O，Liu X，Li X，et al. Privacy-preserving data aggregation scheme for edge computing supported vehicular ad hoc networks. Transactions on Emerging Telecommunications Technologies，2022，33(5)：e3952

[20] Zhou Z，Xu C，Wang M，Kuang X，Zhuang Y，and Yu S. A multi-shuffler framework to establish mutual confidence for secure federated learning. IEEE Transactions on Dependable and Secure Computing，2022，(01)：1-16

[21] Khan F A，Jamjoom M，Ahmad A，et al. An analytic study of architecture，security，privacy，query processing，and performance evaluation of database-as-a-service. Transactions on Emerging Telecommunications Technologies，2022，33(2)：e3814

[22] Yao P，Wang H，Zheng C，et al. Efficient Federated Learning Aggregation Protocol Using Approximate Homomorphic Encryption//Proceedings of the 2023 26th International Conference on Computer Supported Cooperative Work in Design（CSCWD）. Rio de Janeiro，Brazil，2023：1884-1889

[23] Meftah S，Tan B H M，Mun C F，et al. Doren：Toward efficient deep convolutional neural networks with fully homomorphic encryption. IEEE Transactions on Information Forensics and Security，2021，16：3740-3752

[24] Yin L，Feng J，Xun H，Sun Z，and Cheng X. A privacy-preserving federated learning for multiparty data sharing in social iots. IEEE Transactions on Network Science and Engineering2021，8(3)：2706-2718

[25] Dong Y，Hou W，Chen X J，et al. Efficient and secure federated learning based on secret sharing and gradients selection. Journal of Computer Research and Development. 2020，57(10)：2241-2250

[26] Zhou Z，Kuang X，Sun L，Zhong L，and Xu C. Endogenous security defense against deductive attack：When artificial intelligence meets active defense for online service. IEEE Communications Magazine ，2020，58(6)：58-64

[27] Feldman V，McMillan A，Talwar K. Stronger privacy amplification by shuffling for rényi and approximate differential privacy//Proceedings of the 2023 Annual ACM-SIAM Symposium on Discrete Algorithms（SODA）. Florence，Italy，2023：4966-4981

[28] Dwork C nd Roth A. The algorithmic foundations of differential privacy. Foundations and Trends in Theoretical Computer Science，2014，9(3-4)：211-407

[29] Fu Yao，Li Qing-Dan，Zhang Ze-Hui，et al. Data integrity verification scheme for privacy protection and fair payment. Journal of Computer Research and Development，2022，59(6)：1343－1355（in Chinese）
（富瑶，李庆丹，张泽辉，等. 支持隐私保护和公平支付的数据完整性验证方案. 计算机研究与发展，2022，59(6)：1343-1355）

[30] Zhan Y，Li P，Qu Z，et al. A learning-based incentive mechanism for federated learning. IEEE Internet of Things Journal，2020，7(7)：6360-6368

[31] Lim W Y B，Xiong Z，Miao C，et al. Hierarchical incentive mechanism design for federated machine learning in mobile networks. IEEE Internet of Things Journal，2020，7（10）：9575-9588

[32] Li B，Shi Y，Kong Q，et al. Incentive-Based Federated Learning for Digital Twin Driven Industrial Mobile Crowdsensing. IEEE Internet of Things Journal，2023.（Early Access）

[33] Niu C, Zheng Z, Wu F, et al. ERATO: Trading noisy aggregate statistics over private correlated data. IEEE Transactions on Knowledge and Data Engineering, 2019, 33(3): 975-990

[34] Xiao M, Li M, Zhang J J. Locally Differentially Private Personal Data Markets Using Contextual Dynamic Pricing Mechanism. IEEE Transactions on Dependable and Secure Computing, 2023. (Early Access)

[35] Zhang L, Zhu T, Xiong P, et al. A robust game-theoretical federated learning framework with joint differential privacy. IEEE Transactions on Knowledge and Data Engineering, 2022, 35(4): 3333-3346

[36] Zhu Jian-Ming, Zhang Qin-Nan, Ding Qing-Yang, Yuan Li-Ping. Privacy Preserving and Trustworthy Federated Learning Model Based on Blockchain. Chinese Journal of Computers, 2021, 44(12):2464 - 2484 (in Chinese)
(朱建明, 张沁楠, 高胜, 丁庆洋, 袁丽萍. 基于区块链的隐私保护可信联邦学习模型. 计算机学报, 2021, 44(12):2464-2484)

[37] Zhan Y, Li P, Wang K, et al. Big data analytics by crowdlearning: Architecture and mechanism design. IEEE Network, 2020, 34(3):143-147

[38] Wang Xin, Li Mei-Qing, Wang Li-Ming, Yu Yun, Yang Yang, Sun Ling-Yun. An Incentivized Federated Learning Model Based on Contract Theory. Journal of Electronics & Information Technology, 2023, 45(3): 874-883 (in Chinese)
(王鑫, 李美庆, 王黎明, 余芸, 杨漾, 孙凌云. 一种基于合同理论的可激励联邦学习模型. 电子与信息学报, 2023, 45(3): 874-883)

[39] Xiao G, Xiao M, Gao G, et al. Incentive mechanism design for federated learning: A two-stage stackelberg game approach// Proceedings of the IEEE 26th International Conference on Parallel and Distributed Systems (ICPADS). Hong Kong, China, 2020: 148-155

[40] Sarikaya Y, Ercetin O. Motivating workers in federated learning: A stackelberg game perspective. IEEE Networking Letters, 2019, 2(1): 23-27

[41] Khan L U, Pandey S R, Tran N H, et al. Federated learning for edge networks: Resource optimization and incentive mechanism. IEEE Communications Magazine, 2020, 58(10): 88-93

[42] Feng S, Niyato D, Wang P, et al. Joint service pricing and cooperative relay communication for federated learning// Proceedings of the International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData). Atlanta, USA, 2019: 815-820

[43] Nget R, Cao Y, Yoshikawa M. How to balance privacy and money through pricing mechanism in personal data market// Proceedings of the SIGIR 2017 Workshop On eCommerce co-located with the 40th International ACM SIGIR Conference on Research and Development in Information Retrieval. Tokyo, Japan, 2017, 2311: 15

[44] Su Z, Xu Q, Hui Y, et al. A game theoretic approach to parked vehicle assisted content delivery in vehicular ad hoc networks. IEEE Transactions on Vehicular Technology, 2016, 66(7): 6461-6474

[45] Zhao N, Wan Q, Chen J, et al. Dynamic incentive mechanism in mobile crowdsourcing networks by combining reputation and contract theory. International Journal of Distributed Sensor Networks, 2022, 18(6): 15501329221104352

[46] Zhang Z, Li X, Yang S. Data Pricing in Vertical Federated Learning//Proceedings of the IEEE/CIC International Conference on Communications in China (ICCC). Foshan, China, 2022: 932-937

[47] Yang M, Feng H, Wang X, et al. Data pricing with privacy loss compensation for cyber-physical systems: A Stackelberg game based approach. Internet Technology Letters, 2023,e443

[48] Zhang Y, Zhang X. Incentive Mechanism with Task Bundling for Mobile Crowd Sensing. ACM Transactions on Sensor Networks, 2023, 19(3): 1-23

[49] Feng Z, Yu S, Zhu Y. Towards personalized privacy preference aware data trading: A contract theory based approach. Computer Networks, 2023, 224: 109637

ZHOU Zan, Ph. D. His main research interests include private-preserving computing, network active defense, and data privacy protection.

ZHANG Xiao-Yan, Ph. D., professor. Her research interests include network security, mobile networking, and future Internet technology.

YANG Shu-Jie, Ph. D., associate professor. His main research interests include network security, vulnerability mining and network resource optimization.

LI Hong-Jing, M. S. candidate. Her main research interests include computing power network privacy protection and pollution prevention.

KUANG Xiao-Hui, Ph. D., professor. His main research interests include wireless network and information security.

YE He-Liang, M. S., senior engineer. His main research interests include network management and information security.

XU Chang-Qiao, Ph. D., professor, Ph. D. supervisor. Distinguished Member of CCF. His main research interests include network active defense, artificial intelligence privacy security, new network technology.

Background

By integrating an improved step-wise game theoretical framework, this paper focuses on the problem of how to properly guide and restrict participants of privacy computing in federated compute first networks (FCFN), which is a newly emerging yet important research task.

The federated compute first network is one of the research focuses currently, which can promisingly cater to multiple intelligent network services with high data and computing demands, in virtue of the advantages of federated learning workflow and compute first network jointly. Effectively motivating many personalized participants is one of the key steps to realizing the actual deployment of federated computing tasks.

The existing FCFN incentive mechanisms mainly focus on user data evaluation and fairness, which need more attention to user privacy requirements. Hence, the privacy noise injection process cannot be appropriately regulated. For their interests, edge computing nodes often exaggerate privacy budget requirements, resulting in a severe loss of accuracy.

On the contrary, in this paper, the authors consider varied personal privacy requirements and propose a feasible adaptive incentive mechanism, driven by dynamic game processes, for privacy computing in federated computing networks. Through the improved Stackelberg leader-follower model, differentiated pricing incentives are implemented according to the privacy injection scale in the distributed computing process. The incentive scheme can obtain the optimal solution under Nash equilibrium through the two-stage game. Further, theoretical analysis and experimental results indicate that the proposed solution significantly improves the participants′ average utility. The redundant computing loss can be limited without violation of differential privacy guarantees.

In a word, this paper provides a novel, feasible incentive approach to limit the redundant performance loss caused by privacy computing, which is a newly emerging yet non-negligible problem in federated compute first networks. To the authors′ knowledge, this is the first lightweight solution without any notable reforms or privacy compromises to the existing federated frameworks.

The first author and second author (corresponding author) of this work have conducted a series of research on privacy computing, poisoning resistance, and endogenous security of collaborative learning systems in recent years. Besides the outputted multiple patents and prototypes, it is worth noting that they proposed several practical, lightweight solutions to reconcile active defense and privacy protection jointly for distributed intelligent systems like federated learning, which have been published in top-tier journals such as IEEE Communications Magazine, TDSC, TC, and IOTJ.

This work was partially supported by the National Natural Science Foundation of China (No.62225105 and No.62001057)