

# 基于博弈论优化的高效联邦学习方案

周全兴<sup>1</sup>, 李秋贤<sup>1</sup>, 丁红发<sup>2</sup>, 樊玫玫<sup>3</sup>

(1.凯里学院 大数据工程学院, 贵州 凯里 556011; 2.贵州财经大学 信息学院, 贵阳 550025;

3.贵州大学 数学与统计学院, 贵阳 550025)

**摘要:** 随着网络信息技术与互联网的发展,数据的隐私与安全问题亟待解决,联邦学习作为一种新型的分布式隐私保护机器学习技术应运而生。针对在联邦学习过程中存在个人数据信息泄露的隐私安全问题,结合 Micali-Rabin 随机向量表示技术,基于博弈论提出一种具有隐私保护的高效联邦学习方案。根据博弈论激励机制,构建联邦学习博弈模型,通过设置合适的效用函数和激励机制保证参与者的合理行为偏好,同时结合 Micali-Rabin 随机向量表示技术设计高效联邦学习方案。基于 Pedersen 承诺机制实现高效联邦学习的隐私保护,以保证联邦学习各参与者的利益和数据隐私,并且全局达到帕累托最优状态。在数字分类数据集上的实验结果表明,该方案不仅提高联邦学习的通信效率,而且在通信开销和数据精确度之间实现平衡。

**关键词:** 联邦学习; 博弈论; 帕累托最优; 隐私保护; Micali-Rabin 随机向量表示技术

开放科学(资源服务)标志码(OSID):



中文引用格式:周全兴,李秋贤,丁红发,等.基于博弈论优化的高效联邦学习方案[J].计算机工程,2022,48(8):144-151,159.

英文引用格式:ZHOU Q X, LI Q X, DING H F, et al. Efficient federated learning scheme based on game theory optimization[J]. Computer Engineering, 2022, 48(8): 144-151, 159.

## Efficient Federated Learning Scheme Based on Game Theory Optimization

ZHOU Quanxing<sup>1</sup>, LI Qiuxian<sup>1</sup>, DING Hongfa<sup>2</sup>, FAN Meimei<sup>3</sup>

(1.School of Big Data Engineering, Kaili University, Kaili, Guizhou 556011, China;

2.School of Information, Guizhou University of Finance and Economics, Guiyang 550025, China;

3.School of Mathematics and Statistics, Guizhou University, Guiyang 550025, China)

**[Abstract]** With the continuous development of network information technology and Internet technology, data privacy and security issues need to be addressed urgently. Federated learning has emerged as a new distributed privacy protection machine learning framework. This study proposes an efficient federated learning scheme with privacy protection based on game theory and Micali-Rabin random vector representation technology to address privacy and security issues, such as personal data information leakage in the federated learning process. It uses game theory to design a federated learning game theory model, sets appropriate utility functions and incentive mechanisms to ensure participants' reasonable behavioral preferences, and combines Micali-Rabin random vector representation technology to construct an efficient federated learning scheme. Furthermore, it integrates the Pedersen commitment mechanism to realize the privacy protection of efficient federated learning to ensure the security and privacy of each participant in the federated learning and the interests of each participant, and global achieve Pareto optimal state. The experimental result on the digital classification data set shows that the scheme not only improves the communication efficiency of federated learning but also achieves a balance between communication overhead and data accuracy.

**[Key words]** federated learning; game theory; Pareto optimality; privacy protection; Micali-Rabin random vector representation technology

DOI: 10.19678/j.issn.1000-3428.0062413

**基金项目:** 国家自然科学基金(61772008, 62002080); 贵州省教育厅自然科学研究项目(黔教合KY字[2020179], [2020180], [2021140]); 凯里学院做特市(州)高校专项计划项目“基于区块链的黔东南从江香猪溯源体系博弈演化技术研究”; 贵州省科技重大专项计划(20183001); 贵州财经大学校级科研课题(2020XYB02)。

**作者简介:** 周全兴(1987—),男,副教授,主研方向为安全协议分析; 李秋贤,工程师; 丁红发(通信作者),副教授、博士; 樊玫玫,副教授、硕士。

**收稿日期:** 2021-08-19 **修回日期:** 2021-10-04 **E-mail:** aqxgzs@163.com

## 0 概述

随着大数据技术的快速发展,各类移动设备的计算及通信能力得到显著提高。因此,基于机器学习的新型学习框架应运而生<sup>[1]</sup>。机器学习技术能够有效提高各类移动设备的应用性能,但是需要将敏感的私有信息和数据上传至中央服务器并对模型进行训练,存在严重的隐私泄露风险、额外的计算与通信开销问题<sup>[2-3]</sup>。为加强用户数据信息的隐私与安全,联邦学习<sup>[4-5]</sup>作为一种新型的分布式机器学习技术应运而生。联邦学习使大规模的移动设备在不泄露本地数据的前提下,通过协作使用各自的数据集来训练机器学习共享模型。联邦学习作为一种去中心化分布式的训练模型方法,利用各移动设备的数据采集与计算能力解决数据的隐私安全问题<sup>[6]</sup>。

由于联邦学习不需要各类移动设备直接进行数据交换,因此在一定程度上保护了用户的数据安全与隐私<sup>[7]</sup>。文献[8]提出一种基于贪婪算法的联邦学习方案,利用分布式移动设备数据和计算资源来训练高性能机器学习模型,同时保护客户端的隐私和安全。文献[9]通过增强本地移动设备的计算能力减少联邦学习通信频率,设计典型的联邦平均算法,通过云处理中心对局部的移动设备进行整合,大幅减少了传输局部模型的数量,节省通信开销。文献[10]通过无线网络构造联邦学习框架,并对其学习时间和数据的准确度进行优化,以控制用户的数据训练能量成本。文献[11]提出一种三元联邦平均协议,减少联邦学习系统中的上下游通信,该方案从保护物联网设备的隐私和安全出发,在降低通信成本和提高学习性能方面取得一定成效。文献[12]为满足联邦学习的环境需求,提出稀疏三元压缩新的压缩联邦学习框架,解决了在联邦学习训练期间存在通信开销量大的问题。

现有的联邦学习框架假设各移动设备都无条件参与联邦学习<sup>[13-14]</sup>。在训练数据模型中,各移动设备都会产生相应的训练成本,如果没有激励策略,自私的数据拥有者将不愿意参加联邦学习<sup>[15-16]</sup>。此外,由于联邦学习中任务发布者不知道参加模型训练的数据拥有者的数据质量,以及可计算资源量,因此任务发布者和数据拥有者之间存在信息不对称的情况。

为进一步考虑理性参与者的存在,文献[17]提出一种参与者是理性参与方的理性证明系统,将博弈论中的理性用户<sup>[18-21]</sup>引入到各安全协议中。文献[22]研究了计算能力受限的理性参与者问题。

为解决联邦学习的安全隐私与通信开销问题,本文结合 Micali-Rabin 随机向量表示技术和博弈论框架,提出一种高效的联邦学习方案。根据博弈论激励机制,构建联邦学习的博弈模型,其包括联邦学习的各参与者、效用函数等扩展式博弈各要素。利

用 Micali-Rabin 随机向量表示技术和 Pedersen 承诺机制保障联邦学习中各参与者训练数据的安全与隐私,以达到全局帕累托最优状态。

## 1 相关理论

### 1.1 博弈论

本文对博弈论中扩展式博弈和帕累托最优的基本概念进行简单说明。

**定义 1(扩展式博弈)** 博弈论是一门用于数学模型研究理性决策者之间如何互动的学科,参与者之间的互动可能涉及到冲突,也可能涉及到合作。扩展式博弈是个六元组  $(P, S, \phi, \rho, U, E)$ , 包括以下 6 个要素: 1) 参与者集合  $P$ , 表示参与联邦学习的所有参与者集合, 包括任务发布者和数据拥有者; 2) 参与者的行动策略集合  $S$ , 指某个参与者在某个时间采取的某种行动策略的集合; 3) 外生随机变量  $\phi$ , 不受任何参与方控制的随机影响方案的变量参数; 4) 参与者的风险规避  $\rho$ , 当每次方案执行时, 各个理性参与者在联邦学习方案中能够承担的各类风险规避程度; 5) 参与者的效用函数  $U$ , 在采取某种行动策略结束后, 每个参与者会获得相应收益; 6) 参与者的期望效用  $E$ , 表示达到帕累托最优状态后, 所有参与者达到最大化的期望效用。

**定义 2(帕累托最优)** 帕累托最优是将所有资源进行合理分配的一种理想状态, 当全局参与者模型达到帕累托最优状态后, 不会存在一方的效用利益变好, 而另一方的效用收益就会因此而受到损失的情况。在这个状态下, 所有的理性参与方都会选择合理的行动策略, 使得自己的效用利益最大化, 并且全局的效用也是最大化。

如果全局参与者模型达到帕累托最优状态, 那么就会满足交换最优、生产最优和产品最优等条件。各个理性参与者在生产交易过程中, 即使交换或更改生产条件或者环境, 都不会从中再获得利益, 从而不影响他人利益。各资源已达到理想状态, 不存在帕累托改进的状态, 即帕累托最优。

### 1.2 Pedersen 承诺机制

Pedersen 承诺机制是满足无条件秘密性的同态承诺机制, 构造承诺机制需要 3 个阶段: 1) 初始化阶段, 选择任意乘法群  $G_q$ , 其中  $q$  为大素数, 群  $G_q$  的生成元为  $g, h$ , 并公布  $(g, h, q)$ ; 2) 承诺阶段, 发送承诺方随机选择值  $r \in Z_q$ , 并计算承诺值  $COM = g^m h^r \bmod q$ , 其中  $m$  是需要加密的信息, 然后将承诺值  $COM$  发送给接收方; 3) 打开阶段, 发送方将  $(m, r)$  一同发送给接收方, 接收方验证承诺值  $COM$  是否等于  $g^m h^r \bmod q$ , 若是  $g^m h^r \bmod q$ , 则接收, 否则拒绝接收任何信息。

### 1.3 Micali-Rabin 随机向量表示技术

Micali-Rabin 随机向量表示技术是基于 Pedersen 承诺, 通过零知识证明技术证明方案中等式的正确

性。假设 Micali-Rabin 随机向量表示技术存在有限域  $F_p$ ,  $p$  为 256 bit 的素数,  $g, h$  是群  $G_q$  的生成元,  $q$  为大素数, 且  $q > p$ , 具有以下 3 个性质: 1) 设  $X$  的随机向量表示是  $X = (u, v)$ , 其中  $u, v \in F_p$ ,  $X$  的值是  $\text{val}(X) = (u + v) \bmod p$ ; 2) 对随机向量  $X = (u, v)$  的分量进行承诺,  $\text{COM}(X) = (\text{COM}(u), \text{COM}(v))$ , 其中  $\text{COM}(u) = e(P, Q)^u$ ,  $\text{COM}(v) = e(P, Q)^v$ ,  $P, Q \in G$  是群  $G$  的两个生成元; 3) 假设存在一行承诺值  $\text{COM}(X^1)$ ,  $\text{COM}(X^2), \dots, \text{COM}(X^j)$ , 对于任意  $i (1 \leq i < j)$  都有  $\text{val}(X^i) = \text{val}(X^{i+1})$ , 那么这两行的承诺值是一致的。

## 2 联邦学习博弈模型

高效联邦学习博弈模型是结合博弈论与联邦学习, 从联邦学习参与方自利的角度出发, 通过效用函数来保证联邦学习数据的安全与隐私。为激励具有高质量的数据所有者积极参加联邦学习, 本文基于博弈论框架设计合理有效的激励合约, 将各理性参与者贡献的资源映射到适当的货币奖励中。参与者在追求自身利益最大化的同时满足联邦学习全局的利益最大化, 从而达到帕累托最优状态。本节设计的高效联邦学习博弈模型包括七元组  $(P, \phi, S, P(\cdot), \rho, U, E)$ 。

联邦学习各个参与者集合  $P$  是联邦学习中任务发布者和拥有若干能够训练模型的各个数据所有者。外生随机变量  $\phi$  是指各个参与方无法预料与控制的外生随机变量。策略集合  $S$  是联邦学习中各个参与方有可能会采取的行动策略集合。支付函数  $P(\cdot)$  是任务发布者激励数据所有者提供更高质量数据, 以获得支付报酬与奖励。风险规避函数  $\rho$  是联邦学习中所有参与者在模型训练时所能承受的风险规避程度。期望效用函数  $U, U_n: S \rightarrow R$  (其中  $R$  为实数空间), 表示第  $n$  位局中人在不同的行动策略组合下所获得的期望收益效用函数。总期望效用函数  $E$  是在联邦学习总的模型中, 所有参与者达到的最大期望收益效用函数。

### 2.1 参与者集合

高效联邦学习首先需要建模其方案中各个参与者, 在博弈模型中主要存在两类参与方, 即联邦学习任务发布者  $P_i$  和数据所有者  $P_j$ , 并且两类参与方都是理性自利的。任务的发布者在保证联邦学习模型中全局利益最优的前提下, 需要实现个体利益最优。数据所有者在完成的任务前提下, 实现个体利益的最大化。因此, 在本文博弈模型中参与者集合为  $P = (P_i, P_j)$ 。

### 2.2 外生随机变量

在联邦学习博弈模型中存在一些不受任何参与方控制的影响因素, 本文将其称为外生随机变量  $\phi$ ,

且  $\phi$  是服从均值为 0、方差为  $\sigma^2$  的正态分布。联邦学习中存在不确定外生因素的任务发布者与数据所有者之间的博弈树, 如图 1 所示, 其中变量  $s$  和  $d$  分别表示任务发布者和数据所有者的收益。

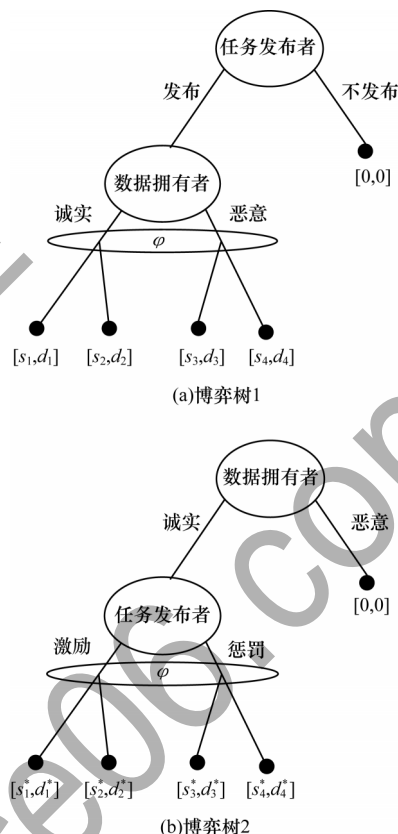


图 1 任务发布者与数据所有者之间博弈树

Fig.1 Game tree between task publisher and data owner

### 2.3 策略集合

在高效的联邦学习博弈模型中, 由于所有参与者都是自利的, 因此任务发布者在发布任务后可以选择“激励”或者“惩罚”数据所有者。令  $s_{i1}$  表示选择“激励”策略, 此时  $s_{i1} = 1$ 。而  $s_{i2}$  表示选择“惩罚”对方的策略, 此时  $s_{i2} = 0$ 。因此, 任务发布者的行动策略集合为 (激励, 惩罚), 即  $s_i = (s_{i1}, s_{i2})$ 。

自私的数据所有者在接收到任务后可以选择“诚实”或者“恶意”策略进行训练数据与反馈。令  $s_{j1}$  表示选择“诚实”执行任务策略, 此时  $s_{j1} = 1$ , 而  $s_{j2}$  表示选择“恶意”的策略, 此时  $s_{j2} = 0$ 。因此, 数据所有者的行动策略集合为 (诚实, 恶意), 即  $s_j = (s_{j1}, s_{j2})$ 。

当双方都选择利于自己的行为策略时, 且双方都能达到最大效用, 令  $\pi = ks + \phi$  表示双方达到最大效用时的货币表示形式,  $k (k \geq 0)$  表示参与方选择不同行动策略时对双方整体效用的影响系数。在执行任务过程中存在不受控制的环境变量  $\phi$ , 且  $\phi$  服从正态分布, 因此联邦学习的双方总期望效用函数为  $E(\pi) = E(ks + \phi) = ks$ ,  $\text{var}(\pi) = \sigma^2$ 。参与方采取的行为策略会影响全局中整体的效用均值。

## 2.4 支付函数

在联邦学习博弈模型中,任务发布者通过激励数据所有者训练数据模型,从而获得高质量数据。因此,本文将任务发布者给予数据所有者的奖励金额设置为线性函数,如式(1)所示:

$$P_i(\pi) = \alpha + \beta\pi \quad (1)$$

其中: $\alpha$ 为模型中数据所有者进行训练数据的固定收入金额; $\beta$ 为任务发布者给予数据所有者的激励奖金系数。针对式(1)中的固定收入金额和激励奖金系数是根据博弈论中委托代理理论计算得到的,其中数据所有者的奖励金额是随着激励金额的增加而增加。在本文方案中,任务发布者和数据所有者的风险规避函数 $\rho_1$ 和 $\rho_2$ 不会影响各自的收入水平,因此任务发布者给予数据所有者的奖励金额可以设置为线性函数。

在参与者学习的过程中,参与者将付出一定的努力使得自身的利益最大化,此时会产生相应的努力成本。本文用货币成本来衡量参与者的努力成本,当任务发布者采用不同的策略时,其努力成本如式(2)所示:

$$C(s_i) = \frac{1}{2} x_i (\pi - \eta\pi)^2 \quad (2)$$

同理,数据所有者采取不同策略时的努力成本如式(3)所示:

$$C(s_j) = \frac{1}{2} x_2 s_j^2 \quad (3)$$

其中: $x_1$ 和 $x_2$ 分别表示任务发布者和数据所有者选择不同行动策略时的努力成本系数,且 $x_1 > 0, x_2 > 0$ ;  $\eta$ 表示数据所有者选择不同的行动策略后取得相应的成效系数,并且 $0 < \eta < 1$ 。数据所有者越努力获取高质量的数据,任务的发布者所获得实际收益与预期收益之间的差距越小。

## 2.5 风险规避

由于所有的参与者都是理性的,个体间会存在一定的差异性和特殊性,因此各个参与者之间对联邦学习过程中的风险规避程度也会存在一定的差异。在博弈模型中,本文设计的风险规避效用函数为 $u = -e^{\rho\omega}$ ,其中 $\rho$ 为参与者的绝对风险规避度量, $\omega$ 为实际获取的收益。由于参与者都具有风险规避的特性,因此会存在相应的风险成本。任务发布者承担风险的成本如式(4)所示:

$$P_{ir} = \frac{1}{2} \rho_1 \text{var}(\pi - P_i(\pi)) = \frac{1}{2} \rho_1 (1 - \beta)^2 \sigma^2 \quad (4)$$

数据所有者承担风险的成本如式(5)所示:

$$P_{jr} = \frac{1}{2} \rho_2 \text{var}(P_j(\pi)) = \frac{1}{2} \rho_2 \beta^2 \sigma^2 \quad (5)$$

其中: $\rho_1$ 和 $\rho_2$ 分别表示任务发布者和数据所有者的风险规避程度,且 $\rho_1 > 0, \rho_2 > 0$ 。

## 2.6 期望效用函数

在博弈模型下分析联邦学习方案最关键的是定义参与者的效用函数。在本文方案中,由于参与者都是理性自利且具有风险规避特性,因此其效用函数需要通过参与者的实际收益进行建模。任务发布

者的实际收益如式(6)所示:

$$v_i = \pi - P_i(\pi) - C(s_i) \quad (6)$$

数据所有者的实际收益如式(7)所示:

$$w_j = P_j(\pi) - C(s_j) \quad (7)$$

根据参与者的实际收益与他们分别存在的风险成本,可以得到任务发布者的期望效用函数,如式(8)所示:

$$U_i = E(\pi - P_i(\pi) - C(s_i) - P_{ir}) = (1 - \beta)ks_j - \alpha - \frac{1}{2} x_i (1 - \eta)^2 k^2 s_j^2 - \frac{1}{2} \rho_1 (1 - \beta)^2 \sigma^2 \quad (8)$$

同理,数据所有者的期望效用函数,如式(9)所示:

$$U_j = E(P_j(\pi) - C(s_j) - P_{jr}) = \alpha + \beta ks_j - \frac{1}{2} x_2 s_j^2 - \frac{1}{2} \rho_2 \beta^2 \sigma^2 \quad (9)$$

## 2.7 总期望效用

由于联邦学习框架中的参与者都是理性自利的,因此数据所有者选择与任务发布者签订激励合约后,得到的最大效益必须大于不签署该合约。数据所有者通过与任务发布者签署激励合约后的期望效用不得小于不接受该任务得到的最小保留效用 $\bar{u}$ ,此时数据所有者需要考虑与自己相关的参与约束IR,如式(10)所示:

$$\alpha + \beta ks_j - \frac{1}{2} x_2 s_j^2 - \frac{1}{2} \rho_2 \beta^2 \sigma^2 \geq \bar{u} \quad (10)$$

任务发布者不知道数据所有者提供的数据质量,在双方存在信息不对称的情况下,并且理性的数据所有者总会选择使自己期望效用最大化的行为策略。因此,任务发布者希望得到的最大效用通过数据所有者的最大效用来实现,且全局达到帕累托最优状态。

根据任务发布者和数据所有者签署的激励合约及帕累托最优状态情况,只有当数据所有者选择行动策略 $s_j$ 时,其效用比其他行动策略 $s_j'$ 更大。因此,数据所有者根据其理性行为将会选择行动策略 $s_j$ ,使得自己的利益最大化,以及全局的利益最大化,此时有 $\max_{s_j}(w)$ 。令 $\frac{\partial w}{\partial s_j} = 0$ ,可以得到 $s_j = \frac{\beta k}{x_2}$ ,在联邦学习博弈模型中存在一个激励相容约束IC,如式(11)所示:

$$s_j = \frac{\beta k}{x_2} \quad (11)$$

将参与约束IR和激励相容约束IC带入任务发布者期望最大效用的目标函数中,构建拉格朗日函数,可得:

$$L(\alpha, \beta) = (1 - \beta) \frac{\beta k^2}{x_2} - \alpha - \frac{1}{2} x_i (1 - \eta)^2 k^2 \left( \frac{\beta k}{x_2} \right)^2 - \frac{1}{2} \rho_1 (1 - \beta)^2 \sigma^2 + \phi \left( \alpha + \beta ks_j - \frac{1}{2} x_2 s_j^2 - \frac{1}{2} \rho_2 \beta^2 \sigma^2 - \bar{u} \right) \quad (12)$$

将模型中构建的拉格朗日函数  $L(\alpha, \beta)$  求关于  $\alpha$  和  $\beta$  的一阶导数, 令  $\frac{\partial L}{\partial \alpha} = 0$ , 且  $\frac{\partial L}{\partial \beta} = 0$ , 此时  $\lambda = 1$ , 可得到:

$$\beta^* = \frac{k^2 x_2 + x_2^2 \rho_2 \sigma^2}{k^2 x_2 + x_1(1-\eta)^2 k^4 + x_1(\rho_1 + \rho_2) \sigma^2} > 0 \quad (13)$$

$$\frac{\partial \beta}{\partial \rho_1} = \frac{x_2^2 \sigma^2 (x_2^2 \sigma^2 \rho_2 + x_2(1-\eta)^2 k^4)}{(k^2 x_2 + x_1(1-\eta)^2 k^4 + x_2^2 \rho_2 \sigma^2)^2} > 0 \quad (14)$$

根据以上函数的变化趋势可以看出, 任务发布者的风险规避程度  $\rho_1$  与其给予数据拥有者的激励系数  $\rho$  呈正相关。因此, 当双方利益最大化时, 数据拥有者所选择的行动策略如式(15)所示:

$$s_j = \frac{k\beta}{x_2} = \frac{k^3 + x_2 \rho_2 \sigma^2 k}{k^2 x_2 + x_2(1-\eta)^2 k^4 + x_2(\rho_1 + \rho_2) \sigma^2} \quad (15)$$

在联邦学习博弈模型中任务发布者和数据拥有者总的期望效用达到最大, 如式(16)所示:

$$E(\pi) = \frac{k^4 + x_2 \rho_2 \sigma^2 k^2}{k^2 x_2 + x_2(1-\eta)^2 k^4 + x_2(\rho_1 + \rho_2) \sigma^2} \quad (16)$$

由此可以看出, 在联邦学习模型中, 即使任务发布者不知道数据拥有者所选择的行动策略和其努力程度, 但是根据双方签署的激励合约, 数据拥有者会选择最优的行动策略  $s_j$ , 使得双方都达到最大的期望效用。此时联邦学习模型的总期望效用  $E(\pi)$  也达到最大, 即模型的全局达到帕累托最优状态。

### 3 高效联邦学习方案

本文基于上述设计的联邦学习博弈模型, 结合 Micali-Rabin 随机向量表示技术构造高效安全的联邦学习方案。在本文方案中, 各参与者为了使自身利益最大化必须遵循双方签署的激励合约, 通过各自的效用函数约束个人理性行为, 任何偏离合约的一方都会受到远大于自身成本价值及影响自身声誉的惩罚。

#### 3.1 初始化阶段

任务发布者  $P_i$  公布需要训练学习的初始模型任务  $T$ , 并将其送至中央服务器, 同时与满足条件的各数据拥有者  $P_j$  签署激励合约, 建立安全的连接。任务发布者和数据拥有者为保证数据的安全与隐私, 根据椭圆曲线的密码体制随机选取密钥对, 用于双方在方案中交易的验证。本文方案选择一条安全的椭圆曲线  $E$ , 其中  $G$  为该椭圆曲线的一个基点, 基点  $G$  的阶数为  $n$ 。本文选择随机数  $\lambda$  计算  $d = \lambda G$ , 其中  $d$  为公钥, 随机数  $\lambda$  为私钥, 并公开  $(G, d)$ 。

#### 3.2 本地训练阶段

各数据拥有者  $P_j$  从中央服务器下载公布的初始模型参数  $\theta_i$ 。每个数据拥有者利用自己的本地数据选择行动策略  $s_j$ , 并训练初始化模型, 之后将更新后的参数  $\theta_i'$  返回至中央服务器, 使得自身利益最大化。在此过程中, 数据拥有者对已更新的参数  $\theta_i'$  进行  $3k$

行承诺  $\langle T, \text{COM}(\theta_i') \rangle$ , 以便于追溯与认定恶意数据拥有者返回的无用数据。形成的  $3k$  行承诺采用 Micali-Rabin 随机向量表示技术可以表示为:

$$\begin{aligned} \text{COM}((\theta_i')^l) &= (\text{COM}(u_i'), \text{COM}(v_i')) \\ (\theta_i')^l &= (u_i', v_i'), \text{val}((\theta_i')^l) = (u_i' + v_i') \bmod p, \\ 1 \leq l \leq 3k \end{aligned} \quad (17)$$

在这个阶段中要求任意概率多项式时间的接收方都不能获取有关承诺的任何信息, 以保护所有数据的隐私和安全。

#### 3.3 聚合验证阶段

中央服务器接收各个数据拥有者返回的更新参数  $\theta_i'$  和承诺值  $\langle T, \text{COM}(\theta_i') \rangle$ , 通过安全的通道反馈给任务发布者。任务发布者  $P_i$  与各数据拥有者  $P_j$  进行秘密通信。数据拥有者在安全通道中向任务发布者打开承诺分量  $(\theta_i')^l = (u_i', v_i')$ , 其中  $u_i', v_i' \in F_p$ 。任务发布者对各个数据拥有者发来的承诺值进行验证, 判断  $\text{val}((\theta_i')^l) = (u_i' + v_i') \bmod p$  是否成立。若成立, 任务发布者将接收更新的参数  $\theta_i'$ , 并根据激励合约对数据拥有者进行奖励; 反之, 任务发布者拒绝接收更新的参数  $\theta_i'$ , 并根据合约对相应的数据拥有者进行惩罚。

任务发布者  $P_i$  与各数据拥有者  $P_j$  进行交互式证明后, 若通过承诺值的验证, 任务发布者将接收更新的参数  $\theta_i'$ , 此时  $P_i$  通过各参与者得到期望效用函数  $U_i = E(\pi - P_j(\pi) - C(s_i) - P_{ir})$  和  $U_j = E(P_j(\pi) - C(s_j) - P_{jr})$ , 并对各自在联邦学习中的收益成效进行判断, 双方是否选择最优的行动策略来执行方案。若任意一方参与者的效用值未达到最大偏离方案, 根据激励合约的规定, 需要支付对方远大于自己期望效用  $U_i$  或者  $U_j$  的赔偿金作为未遵守方案的补偿。

#### 3.4 模型更新阶段

当任务发布者  $P_i$  确定接收更新的参数  $\theta_i'$  后, 中央服务器根据各参与方更新参数的聚合结果, 并对全局模型的参数进行更新。更新后的参数被重新发送至各数据拥有者  $P_j$ , 各数据拥有者  $P_j$  重新利用自己的本地数据进行训练模型, 重复本地训练阶段, 直到全局模型的各项性能指标满足任务发布者的要求后, 联邦学习阶段结束。

由于构造的方案中各方参与者都是理性自利的, 他们会为了使自身利益得到最大化选择最优的行动策略。在该方案中, 根据双方签署的激励合约, 一旦有参与者选择偏离方案的恶意行为, 将会受到严重的资金惩罚。各参与方通过激励合约约束并激励自己遵守方案, 降低各参与方通信的风险, 并提高联邦学习的通信效率。高效联邦学习系统架构如图2所示。

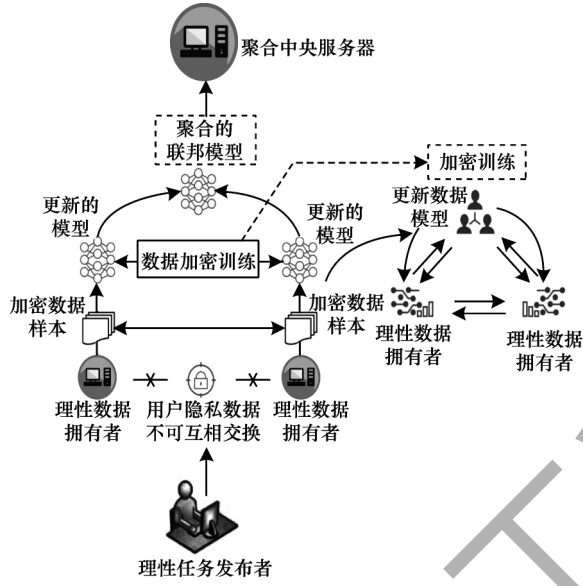


图2 高效联邦学习系统架构

Fig.2 Architecture of efficient federated learning system

## 4 方案分析

### 4.1 安全性分析

本文从安全性分析基于博弈论优化的高效联邦学习方案。

**定理1** 本文联邦学习方案具有安全性。

**证明** 在联邦学习的本地训练阶段中,各数据拥有者采用 Micali-Rabin 随机向量表示技术对承诺值  $\langle T, \text{COM}(\theta_i')^i \rangle, 1 \leq i \leq 3k$  进行  $3k$  行承诺。在聚合验证阶段中,任务发布者  $P_i$  与各数据拥有者  $P_j$  进行交互式证明,以验证承诺值的正确性。各数据拥有者在安全通道中向任务发布者打开承诺分量  $(\theta_i')^i = (u_i', v_i')$ ,以保证更新参数的安全性与隐私性。

假设本文方案是不安全的,那么会存在恶意参与者将返回至中央服务器的承诺值进行篡改  $\langle T, \text{COM}(\theta_i')^i \rangle$  为  $\langle T, \text{COM}(\theta_i')^i \rangle^*$ ,或者构造虚假承诺值上传至中央服务器。由于 Micali-Rabin 随机向量表示技术采用 Pedersen 承诺,因此承诺值  $Q_{\theta_i'} = g^{\theta_i'} h^r \bmod p$  成立,其中  $g$  和  $h$  是  $Z_p^*$  的生成元,  $r$  为随机数,根据 Pedersen 承诺存在一个  $t$ ,使得  $h = g^t \bmod p$ ,  $Q_{\theta_i'} = g^{\theta_i'} h^r \bmod p = g^{\theta_i' + tr} \bmod p$ 。如果给定一个  $y = g^x \bmod p$ ,则计算其离散对数  $x = \lg_p y$ ,并将其作为对更新参数  $\theta_i'$  的承诺。根据离散对数的假设,从承诺值获取  $\theta_i'$  的任何信息是不可能的。因此,在任何概率多项式时间内可以忽略恶意参与者篡改或伪造承诺值,说明构造的基于博弈优化的联邦学习方案是安全的。

### 4.2 正确性分析

本文从正确性分析基于博弈论优化的高效联邦学习方案。

**定理2** 本文联邦学习方案具有正确性。

**证明** 本文联邦学习方案中,如果任务发布者  $P_i$  与各数据拥有者  $P_j$  严格按照合约进行执行,那么双方都会选择最优的行动策略执行方案。在方案的初始化阶段,任务发布者和满足条件的数据拥有者签署激励合约,以建立安全的连接。在本地训练和聚合验证阶段,数据拥有者将更新的参数和承诺值返回至中央服务器。若数据拥有者选择行动策略  $s_{j2}$ ,即“恶意”的行动策略,那么得到的效用收益为  $U_j' = E(P_j(\pi) - C(s_{j2}) - P_{jr})$ 。因为策略  $s_{j2}$  的取值为0,所以由式(9)可以将其效用收益化简写为  $U_j' = \alpha + \beta k s_{j2} - \frac{1}{2} x_2 s_{j2}^2 - \frac{1}{2} \rho^2 \beta^2 \sigma^2 = \alpha$ 。对应任务发布者的效用收益为  $U_i' = E(\pi - P_j(\pi) - C(s_i) - P_{ir}) = -\frac{1}{2} \rho_1 (1-\beta)^2 \sigma^2$ 。

当参与方达到最大收益时  $\pi' = k s_{j2} + \varphi = \varphi$ ,且  $\varphi$  服从正态分布,因此,本文方案的双方总期望效用为  $E(\pi) = E(k s_{j2} + \varphi) = k s_{j2} = 0$ ,无法达到帕累托最优状态。根据激励合约的规定,选择行动策略  $s_{j2}$  的参与方将受到严重的惩罚。

由于双方都是理性的,在方案中为了自身利益最大化不会选择不利于自己的行动策略,只有双方都选择最优策略,全局才能达到最优状态  $\pi_{\max} = k s + \varphi$ ,且参与者都能获得最优收益,全局达到帕累托最优状态。因此,该高效联邦学习方案是正确的。

### 4.3 公平性分析

本文从公平性分析基于博弈论优化的高效联邦学习方案。

**定理3** 本文联邦学习方案具有公平性。

**证明** 在高效联邦学习方案中,所有参与者都是理性自私的,为了自身利益的最大化可以随意选择自己的行动策略。为保证本文方案的公平性,在方案的初始化阶段中,任务发布者需要与数据拥有者签署激励合约,严格按照合约的要求执行。

双方选择的策略在激励合约中的取值为“0”或“1”。一种情况是双方根据自己的效用函数  $U_i$  和  $U_j$  判断双方是否存在偏离方案的恶意行为,如果有恶意行为,它们总的期望效用  $E(\pi) = E(k s + \varphi)$  的结果为“0”。根据策略  $s$  可以找出恶意参与者,并对其进行惩罚。另一种情况是根据上传至中央服务器的承诺值判断是否存在恶意参与者,根据方案的安全性分析可知,任何参与者都无法更改或者虚假地更新参数,因此,本文方案对于所有参与者都是公平的。

### 4.4 方案性能分析

不同方案的安全性、正确性和公平性对比如表1

所示,其中,“√”表示方案满足上述性质,“×”表示方案不满足上述性质。

表1 不同方案的性能对比

Table 1 Performances comparison among different schemes

方案	安全性	正确性	公平性
文献[7]方案	√	√	×
文献[15]方案	√	√	×
文献[23]方案	×	√	×
本文方案	√	√	√

从表1可以看出,现有的大多数联邦学习方案考虑方案的安全性,但是通常认为参与者都是诚实的,未考虑到参与者的自利行为,即对方案的公平性方面考虑的较少,这也是影响联邦学习效率与应用的原因之一。

5 实验仿真

本文借鉴文献[24]的数字分类数据集MINIST对本文方案进行模拟评估。本文选择60 000条训练数据示例,其中包含1个任务发布者和50个数据拥有者,用于执行数据训练分类任务。数据拥有者首先与可以接受模型训练的数据拥有者签订激励合约。签订合约的数据拥有者根据任务发布者上传的任务,随机分配需要训练的数据集,并作为本地的训练数据。

为验证激励合约的有效性,本文分别对签署和未签署激励合约的参与者进行联邦学习,并对拥有不同数据字节长度的拥有者利益和任务发布者的利益关系进行分析讨论。签署与未签署激励合约的总期望效用对比如图3所示。从图3可以看出,当拥有者的数据字节长度分别为2、4和6 Byte时,无论数据类型为何种的数据拥有者,他们与任务发布者之间的效用只有当都选择签署激励合约时,双方的效用才最大,此时方案全局的利益也最大,即达到帕累托最优状态。

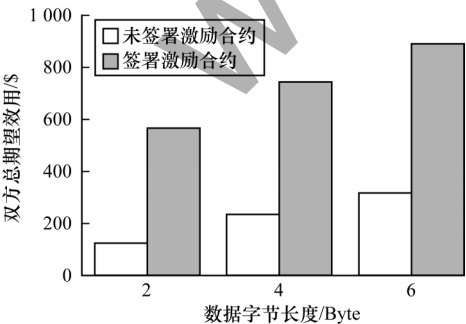


图3 签署与未签署激励合约的总期望效用对比

Fig.3 Total expected utility comparison of signed and unsigned incentive contracts

本文对任务发布者和数据拥有者的激励策略进行分析,确定任务发布者给予的激励金额大小与数据训练精确度之间的关系。数据的精确度随奖励金额的变化趋势如图4所示。随着任务发布者提供的激励奖励的增加,拥有不同数据类型数据拥有者的数据训练精确度从65%逐步提高至98%。在本文激励合约下,当任务发布者的激励奖励越高时,越能激励数据拥有者进行模型训练,最终获得的数据质量也越高,从而实现高效的联邦学习。

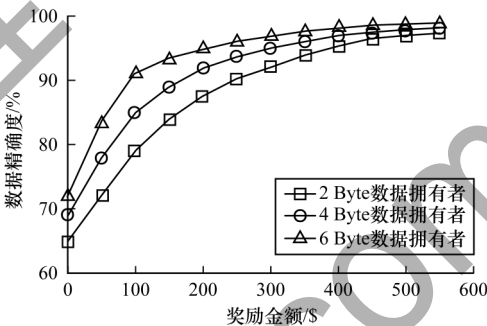


图4 不同奖励金额下数据的精确度

Fig.4 Accuracy of data under different reward amounts

签署与未签署激励合约拥有者的通信消耗能量对比如图5所示。当未签署与签署激励合约的数据拥有者从0~50逐渐增加时,其通信开销发生了很大的变化。从图5可以看出:当参与者未签署激励合约时,其数据拥有者越多,通信开销越大;有激励合约的参与者通信开销几乎无变化,验证了本文联邦学习方案的高效性。

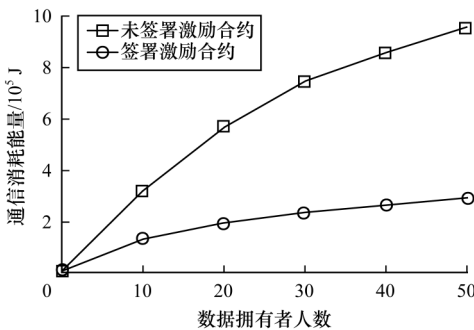


图5 签署与未签署激励合约拥有者的通信消耗能量对比

Fig.5 Energy consumption of communication comparison of owner with and without incentive contracts

本文方案性能的影响因素是参与者的自利性行为。若参与者是自私恶意的,在方案执行过程中,由双方的激励合约可知,双方将根据效用函数对自私恶意的参与者进行惩罚,并且阻止方案继续执行。不同参与者行为联邦学习效率变化如图6所示。当拥有不同数据类型的参与者若存在自私恶意的数据拥有者,方案的效率将降低。

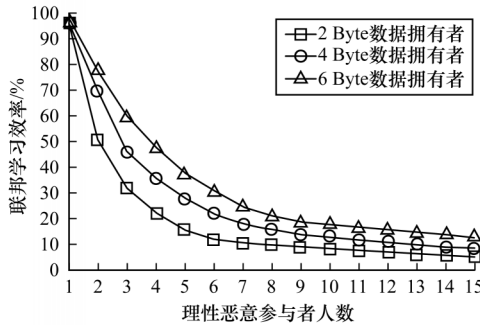


图6 不同参与者的联邦学习效率对比

Fig.6 Efficiency of federated learning comparison among different participants

本文设计的方案中用户的奖励越大,其选择积极策略的可能性越大,获得的数据准确度也越高,用户的通信消耗量远远小于用户未签署激励合约的通信量。当拥有不同数据类型的参与者存在理性恶意的数据拥有者时,极大影响联邦学习的效率,从而影响双方效用收益。因此,本文设计的方案是有效的。

## 6 结束语

本文提出基于博弈论优化的高效联邦学习方案,利用博弈论激励高质量的数据拥有者和任务发布者,同时结合 Micali-Rabin 随机向量表示技术和 Pedersen 承诺方案,实现高效联邦学习的隐私保护。仿真结果表明,该方案不仅使得全局参与者达到帕累托最优状态,而且为联邦学习的各参与者的利益和数据隐私提供了保证。后续将在多任务者同时发布模型训练任务的前提下,从不同的角度和应用场景中研究联邦学习,进一步提高学习效率。

## 参考文献

- [1] YANG Q, LIU Y, CHEN T J, et al. Federated machine learning: concept and applications[EB/OL]. [2021-07-15]. <https://arxiv.org/pdf/1902.04885.pdf>.
- [2] PAPERNOT N, ABADI M, ERLINGSSON U, et al. Semi-supervised knowledge transfer for deep learning from private training data[EB/OL]. [2021-07-15]. <https://arxiv.org/abs/1610.05755>.
- [3] ZHU X D, LI H, YU Y. Blockchain-based privacy preserving deep learning[C]//Proceedings of International Conference on Information Security and Cryptology. Berlin, Germany: Springer, 2018; 1-10.
- [4] BARAI A K, BHADORIA R S, BAGWARI J, et al. A blockchain-based federated learning: concepts and applications[M]//DEKA G C. Multidisciplinary functions of blockchain technology in AI and IoT applications. Hershey, USA: IGI Global Press, 2021; 158-177.
- [5] YANG W, ZHANG Y, WEI Y, et al. Privacy is not free: energy-aware federated learning for mobile and edge intelligence[C]//Proceedings of International Conference on Wireless Communications and Signal Processing. Zhengzhou, China: [s. n.], 2020; 1-10.
- [6] POSNER J, TSENG L, ALOQAILY M, et al. Federated learning in vehicular networks: opportunities and solutions[J]. IEEE Network, 2021, 35(2): 1-8.
- [7] GEYER R C, KLEIN T, NABI M. Differentially private federated learning: a client level perspective[EB/OL]. [2021-07-15]. <https://arxiv.org/abs/1712.07557>.
- [8] YOSHIDA N, NISHIO T, MORIKURA M, et al. MAB-based client selection for federated learning with uncertain resources in mobile networks[EB/OL]. [2021-07-15]. <https://arxiv.org/abs/2009.13879>.
- [9] MCMAHAN H B, MOORE E, RAMAGE D, et al. Communication-efficient learning of deep networks from decentralized data[EB/OL]. [2021-07-15]. <https://arxiv.org/pdf/1602.05629.pdf>.
- [10] TRAN N H, BAO W, ZOMAYA A, et al. Federated learning over wireless networks: optimization model design and analysis[C]//Proceedings of IEEE Conference on Computer Communications. Washington D. C., USA: IEEE Press, 2019; 1-10.
- [11] FELIX S, SIMON W, KLAUS-ROBERT M, et al. Robust and communication-efficient federated learning from non-i. i. d. data[J]. IEEE Transactions on Neural Networks and Learning Systems, 2019, 31(9): 3400-3413.
- [12] MALEKIJOO A, FADAEIESLAM M J, MALEKIJOO H, et al. FEDZIP: a compression framework for communication-efficient federated learning[EB/OL]. [2021-07-15]. <https://arxiv.org/abs/2102.01593>.
- [13] SHAYAN M, FUNG C, YOON C, et al. Biscotti: a blockchain system for private and secure federated learning[J]. IEEE Transactions on Parallel and Distributed Systems, 2020, 99: 1-10.
- [14] CHEN H, ASIF S A, PARK J, et al. Robust blockchained federated learning with model validation and proof-of-stake inspired consensus[EB/OL]. [2021-07-15]. <https://arxiv.org/abs/2101.03300>.
- [15] QU Y Y, POKHREL S R, GARG S, et al. A blockchained federated learning framework for cognitive computing in industry 4.0 networks[J]. IEEE Transactions on Industrial Informatics, 2020, 99: 1-10.
- [16] PENG Z, XU J, CHU X, et al. VFChain: enabling verifiable and auditable federated learning via blockchain systems[J]. IEEE Transactions on Network Science and Engineering, 2021, 99: 1-10.
- [17] AZAR P D, MICALI S. Rational proofs[C]//Proceedings of the 44th Annual ACM Symposium on Theory of Computing. New York, USA: ACM Press, 2012; 1017-1028.
- [18] 李朋, 陶洋, 许湘扬, 等. 基于博弈论的无线传感器网络能耗均衡分簇协议[J]. 计算机工程, 2018, 44(12): 156-162.
- [19] LI P, TAO Y, XU X Y, et al. Energy consumption balance clustering protocol in wireless sensor network based on game theory[J]. Computer Engineering, 2018, 44(12): 156-162. (in Chinese)
- [19] CHEN J, MCCAULEY S, SINGH S. Rational proofs with multiple provers[C]//Proceedings of ACM Conference on Innovations in Theoretical Computer Science. New York, USA: ACM Press, 2016; 237-248.
- [20] 田有亮, 马建峰, 彭长根, 等. 秘密共享体制的博弈论分析[J]. 电子学报, 2011, 39(12): 2790-2795.
- [20] TIAN Y L, MA J F, PENG C G, et al. Game-theoretic analysis for the secret sharing scheme[J]. Acta Electronica Sinica, 2011, 39(12): 2790-2795. (in Chinese)

(下转第159页)

(上接第 151 页)

[21] 李秋贤,田有亮,王纘. 基于全同态加密的理性委托计算协议[J]. 电子学报,2019,47(2):216-220.  
LI Q X, TIAN Y L, W Z. Rational delegation computation protocol based on fully homomorphic encryption[J]. Acta Electronica Sinica, 2019, 47(2): 216-220. (in Chinese)

[22] GUO S, HUBACEK P, ROSEN A, et al. Rational arguments; single round delegation with sublinear verification[C]//Proceedings of the 5th Conference on Innovations in Theoretical Computer Science. New York, USA; ACM Press, 2014: 523-540.

[23] KIM H, PARK J, BENNIS M, et al. On-device federated learning via blockchain and its latency analysis[EB/OL]. [2021-07-15]. <https://arxiv.org/abs/1808.03949>.

[24] KANG J W, XIONG Z H, NIYATO D, et al. Incentive design for efficient federated learning in mobile networks: a contract theory approach[C]//Proceedings of IEEE VTS Asia Pacific Wireless Communications Symposium. Washington D. C., USA; IEEE Press, 2019: 1-10.

编辑 薛晋栋