计算机科学
COMPUTER SCIENCE

隐私保护的非线性联邦支持向量机研究

杨鸿健, 胡学先, 李可佳, 徐阳, 魏江宏

引用本文

杨鸿健, 胡学先, 李可佳, 徐阳, 魏江宏隐私保护的非线性联邦支持向量机研究[J]. 计算机科学, 2022, 49(12): 22-32.

YANG Hong-jian, HU Xue-xian, LI Ke-jia, XU Yang, WEI Jiang-hong. Study on Privacy-preserving Nonlinear Federated Support Vector Machines [J]. Computer Science, 2022, 49(12): 22-32.

相似文章推荐（请使用火狐或 IE 浏览器查看文章）

Similar articles recommended (Please use Firefox or IE to view the article)

基于联邦学习的暖通空调系统故障检测与诊断

Fault Detection and Diagnosis of HVAC System Based on Federated Learning

计算机科学, 2022, 49(12): 74-80. https://doi.org/10.11896/jsjkx.220700280

基于联邦学习的Gamma回归算法

FL-GRM:Gamma Regression Algorithm Based on Federated Learning

计算机科学, 2022, 49(12): 66-73. https://doi.org/10.11896/jsjkx.220600034

基于联邦学习的车联网多维资源动态分配算法

Multi-dimensional Resource Dynamic Allocation Algorithm for Internet of Vehicles Based on Federated Learning

计算机科学, 2022, 49(12): 59-65. https://doi.org/10.11896/jsjkx.211000123

边缘场景下动态权重的联邦学习优化方法

Federated Learning Optimization Method for Dynamic Weights in Edge Scenarios

计算机科学, 2022, 49(12): 53-58. https://doi.org/10.11896/jsjkx.220700136

联邦学习激励机制研究综述

Survey of Incentive Mechanism for Federated Learning

计算机科学, 2022, 49(12): 46-52. https://doi.org/10.11896/jsjkx.220500272

计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.220500240

隐私保护的非线性联邦支持向量机研究

杨鸿健　胡学先　李可佳　徐　阳　魏江宏
中国人民解放军战略支援部队信息工程大学数据与目标工程学院　郑州 450001
(henuyanghongjian@163.com)

摘　要　联邦学习为解决“数据孤岛”下的多方联合建模问题提出了新的思路。联邦支持向量机能够在数据不出本地的前提下实现跨设备的支持向量机建模,然而现有研究存在训练过程中隐私保护不足、缺乏针对非线性联邦支持向量机的研究等缺陷。针对以上问题,利用随机傅里叶特征方法和CKKS同态加密机制,提出了一种隐私保护的非线性联邦支持向量机训练(PPNLFedSVM)算法。首先,基于随机傅里叶特征方法在各参与方本地生成相同的高斯核近似映射函数,将各参与方的训练数据由低维空间显式映射至高维空间中;其次,基于CKKS密码体制的模型参数安全聚合算法,保障模型聚合过程中各参与方模型参数及其贡献的隐私性,并结合CKKS密码体制的特性对参数聚合过程进行针对性优化调整,以提高安全聚合算法的效率。针对安全性的理论分析和实验结果表明,PPNLFedSVM算法可以在不损失模型精度的前提下,保证参与方模型参数及其贡献在训练过程中的隐私性。

关键词:联邦学习;隐私保护;同态加密;支持向量机;多方安全随机种子协商;随机傅里叶特征
中图法分类号　TP309.2

Study on Privacy-preserving Nonlinear Federated Support Vector Machines

YANG Hong-jian,HU Xue-xian,LI Ke-jia,XU Yang and WEI Jiang-hong
School of Data and Target Engineering,PLA Strategic Support Force Information Engineering University,Zhengzhou 450001,China

Abstract　Federated learning offers new ideas for solving the problem of multiparty joint modeling in “data silos”. Federated support vector machines can realize cross-device support vector machine modeling without local data,but the existing research has some defects such as insufficient privacy protection in a training process and a lack of research on nonlinear federated support vector machines. To solve the above problems,this paper utilizes the stochastic Fourier feature method and CKKS homomorphic encryption system to propose a nonlinear federated support vector machine training(PPNLFedSVM) algorithm for privacy protection. Firstly,the same Gaussian kernel approximate mapping function is generated locally for each participant based on the random Fourier feature method,and the training data of each participant is explicitly mapped from the low-dimensional space to the high-dimensional space. Secondly,the model parameter security aggregation algorithm based on CKKS cryptography ensures the privacy of model parameters and their contributions during the model aggregation process. Moreover,the parameter aggregation process is optimized and adjusted according to the characteristics of CKKS cryptography to improve the efficiency of the security aggregation algorithm. Security analysis and experimental results show that the PPNLFedSVM algorithm can ensure the privacy of participant model parameters and their contributions to the training process without losing the model accuracy.

Keywords　Federated learning,Privacy preserving,Homomorphic encryption,Support vector machines,Multi-party secure random seed negotiation,Random Fourier features

人工智能的高速发展离不开海量数据的支撑。数据作为战略性、基础性资源,不但是连接虚拟空间与实体空间的纽带,也是数字经济体系中技术创新[1]、需求挖掘、效率提升的重要动能。近年来,频繁曝出的用户隐私泄露问题,不仅加剧了隐私保护技术的转化与落地[2-4],同时也促使世界各国政府针对隐私泄露问题立法,如欧盟的《通用数据保护条例》(General Data Protection Regulation,GDPR)以及我国的《网络安全法》《个人信息保护法》《数据安全法》等。然而,严苛的法律使得数据在不同的企业、组织、部门中流动愈加困难,加剧了“数据孤岛”现象。

联邦学习为解决“数据孤岛”下的多方联合建模问题提出了新的思路。联邦学习能够在数据不出本地的条件下进行多方联合建模,实现合规的数据共享[5]。然而,在联邦学习应用快速落地的过程中,却逐渐暴露出中间参数(梯度、模型参数)

到稿日期:2022-05-26　返修日期:2022-07-07
基金项目:国家自然科学基金(62172433,62172434,61862011,61872449)
This work was supported by the National Natural Science Foundation of China(62172433,62172434,61862011,61872449).
通信作者:胡学先(xuexian_hu@hotmail.com)

存在的隐私泄露问题。仅通过中间参数，内部攻击者就能提取到大量的隐私信息[6-7]。Zhu 等[8]提出了一种从泄露梯度中推理参与方本地数据的算法 DLG，该算法能够在数轮迭代中以较高的准确度恢复出训练深度神经网络模型的本地数据与标签值。Zhao 等[9]在 Zhu 等[8]研究的基础上提出了适用范围更广泛的 iDLG 算法，该算法可利用标签与相应梯度符号之间的关系，从共享梯度中直接提取标签。Wang 等[10]提出了一种从模型参数中提取训练数据的算法，该算法利用中心服务器接收到的局部模型参数训练生成式对抗网络（Generative Adversarial Networks，GAN），并通过所得模型生成训练数据的模拟数据。因此，如何有效保护联邦学习的中间参数的隐私性成为了联邦学习研究中必须解决的问题。

支持向量机（Support Vector Machines，SVM）作为机器学习中常用的分类算法，可用于线性与非线性数据的分类问题，在恶意流量识别、智能诊断、药物发现、自然语言处理、图像识别等领域均有着广泛应用。然而，在训练样本明显不足的情况下，难以训练出泛化能力强的 SVM。为解决此问题，研究者们开始尝试通过联邦学习进行联合建模。然而，目前现有的联邦 SVM 算法存在隐私泄露的隐患，且缺少对非线性数据分类的联邦 SVM 训练的相关研究。

目前关于联邦 SVM 的研究多以应用为主，Bakopoulou 等[11]与 Ge 等[12]开展了联邦 SVM 在移动端数据包分类及生产线故障监测方面的应用研究。然而，上述两种方案均未考虑联邦 SVM 算法的隐私保护，存在隐私泄露的隐患。针对联邦 SVM 中的隐私保护问题，Hartmann 等[13]提出了一种隐私保护的联邦 SVM 训练算法 SecVM，该算法利用高碰撞 hash 函数将不同维度的数据混合，实现对原始数据的加噪与降维，通过向原始数据中增加扰动来保护中间参数的隐私性。但该方案无法量化向原始数据中添加的噪声，难以控制向原始数据中注入的噪声量，并且约束了训练数据必须是整数，限制了算法的适用范围。

本文提出了一种适用于非线性数据分类任务的隐私保护的非线性联邦 SVM 算法（Privacy-preserving Nonlinear Federated Support Vector Machines，PPNLFedSVM），该算法通过引入同态加密的方式来保护中间参数的隐私性，解决了联邦学习中间参数的隐私泄露问题，并借助随机傅里叶特征（Random Fourier Features，RFF）方法实现了高斯核的近似映射，给出了一种基于高斯核的非线性联邦 SVM 的训练方案。

本文的主要贡献如下：

（1）基于 Burmester-Desmedt 组密钥协商协议[14]，设计并实现了一种安全随机种子协商算法。参与方通过该算法安全协商出一个相同的密钥，并将此密钥作为伪随机数生成器（Pseudo Random Number Generator，PRNG）的种子，实现在各参与方本地安全生成相同随机种子的目的。

（2）提出了一种基于高斯核的非线性联邦 SVM 训练算法，利用随机傅立叶特征方法，求解出高斯核的近似映射函数，进一步通过映射函数，显式地将低维的非线性数据映射到高维空间中使其线性可分，从而将低维空间中的非线性分类问题转化为高维空间中的线性分类问题。

（3）设计了一种基于 CKKS 密码体制的联邦模型安全聚合算法，在保护参与方模型参数的同时隐藏其贡献（各参与方本地模型在全局模型中的占比）。为达到上述目的，本文选用实现了单指令多数据流（Single Instruction Multiple Data，SIMD）的 CKKS 密码体制[15]进行全局模型聚合，并对其进行针对性优化，避免模型聚合阶段同态乘法的使用，进一步降低了计算开销，使得本方案在实现相同隐私保护程度的同时，还可保持较低的计算与通信开销。

（4）从启发式分析、形式化分析两个角度，对所提方案进行了安全性证明，证明了其安全性。

（5）通过仿真实验，验证了本文算法的可用性。进一步地，对所提方案的时间、空间开销进行了测量及分析。实验结果表明，所提方案能够在模型精度几乎无损的情况下实现隐私保护训练，且在模型参数规模未超过单个密文能承载的最大值时，训练所需要的时间与空间开销趋于定值。

1 相关工作

除联邦学习外，还有一些基于安全多方计算、数据扰动、安全外包计算技术的隐私保护 SVM 的相关工作。

在安全多方计算方面，Yu 等[16]针对纵向数据分割场景，提出了一种隐私保护的多方安全建模方案，该方案通过安全矩阵加法构建出全局 Gram 矩阵，使得多方能够在保证本地数据隐私的前提下，求得对偶优化问题的最优解。但该方案在参与方数量小于 3 时是不安全的[16]。在此之后，Yu 等[17]针对横向数据分割的场景，在面向纵向数据分割 SVM 隐私保护方案[16]的基础上，引入了可交换 hash 函数与安全交集基数等安全组件来提高算法的安全性，但该方案仅适用于二进制数据集。Vaidya 等[18]在 Yu 等[16-17]的基础上，提出了面向任意数据划分的隐私保护 SVM 训练方案，该方案通过引入同态加密来保证参与方 Gram 矩阵的隐私性，并将模型参数的优化任务委托给了第三方，从而防止隐私泄露。

除了安全多方计算外，一些研究者基于数据扰动技术实现对 SVM 多方训练过程的隐私保护。Mangasarian 等[19]借鉴了约简支持向量机（Reduced Support Vector Machine，RSVM）的思想[20]，提出了随机核方法，该方法将约简核函数中训练数据的子集替换为随机矩阵，从而实现对 Gram 矩阵的扰动，但存在模型性能不稳定的问题[21]。Sun 等[21]在随机核方案[19]上进行改进，将随机核方法中的矩阵置换为注入高斯噪声后的约简核矩阵，相比随机核方法，此方案能够显著降低向 Gram 矩阵中注入的扰动，使得其在训练效率及模型性能上均优于随机核方案。

在面向 SVM 的多方安全外包计算研究中，Liu 等[22]基于 DT-PKC 密码体制[23]，设计并实现了一套基础运算（如安全加法、安全乘法、安全比较）的安全计算协议，并以此构建出安全序列最小优化算法（Sequential Minimal Optimization，SMO），给药物发现场景下的隐私保护 SVM 训练提供了一种解决方案。Wang 等[24]从计算及通信效率上，对 Liu 等[22]提出的安全计算协议进行优化，并基于优化后的安全计算协议提出一种安全随机梯度下降算法，为医疗物联网背景下 SVM 的安全建模问题提供了新的解决思路。

2 预备知识

本节主要介绍联邦学习、支持向量机、核方法、SIMD 编码与同态加密的基本概念。其中核方法是非线性支持向量机的支撑技术，同态加密用于保障联邦 SVM 训练过程中的隐私性，SIMD 编码是同态加密体制 CKKS 用于压缩密文大小、提高同态运算效率的方法。

2.1 联邦学习

联邦学习的概念最早由 Google 于 2016 年提出[25]。联邦学习能够在各方数据不出本地的条件下实现多方联合建模。具体而言，假设有 N 个参与方$\{F_i\}_{i=1}^N$需要使用其本地数据集$\{\boldsymbol{D}_i\}_{i=1}^N$进行联合建模。根据联邦学习参与方持有数据特征的不同，又可将联邦学习分为：横向联邦学习、纵向联邦学习、联邦迁移学习 3 类，其数据特征的对比如表 1 所列。

表 1 3 种联邦学习数据特征的对比

Table 1 Comparison of three federated learning data characteristics

类型	数据特征
横向联邦学习	特征相同、样本不同
纵向联邦学习	样本相同、特征不同
联邦迁移学习	特征及样本的重合度均小

其中，横向联邦学习具有跨设备进行协同建模的能力，能够在满足数据合规分享的前提下，有效利用散落在 IoT 设备、智能终端中具有相同特征的海量数据进行协同建模，具有重要的实际应用价值。因此，本文以横向联邦学习为背景，结合 SVM，提出一种面向非线性数据分类任务的隐私保护非线性联邦 SVM 的训练算法。

2.2 支持向量机

支持向量机是机器学习中常用的线性分类模型。一般的，将样本空间定义为 $\boldsymbol{D}=\{(\boldsymbol{x}_1,y_1),(\boldsymbol{x}_2,y_2),\cdots,(\boldsymbol{x}_m,y_m)\}$，其中 $y_i\in\{-1,1\}$。支持向量机通过在样本空间中求解一个超平面 $\boldsymbol{\omega}^{\mathrm{T}}\boldsymbol{x}+b=0$，使得该超平面能够最大程度地将两类数据分割开。其中 $\boldsymbol{\omega}=(\omega_1,\omega_2,\cdots,\omega_d)$为法向量，决定着超平面的方向，$b$ 为位移项，决定着超平面与原点的距离。当样本能够被正确分类时，对于任意的样本$(\boldsymbol{x}_i,y_i)\in\boldsymbol{D}$，满足如下关系：

$$\begin{cases}\boldsymbol{\omega}^{\mathrm{T}}\boldsymbol{x}_i+b\geqslant 1, & y_i=+1\\ \boldsymbol{\omega}^{\mathrm{T}}\boldsymbol{x}_i+b\leqslant -1, & y_i=-1\end{cases}$$

将正好位于 $\boldsymbol{\omega}^{\mathrm{T}}\boldsymbol{x}_i+b=1$，$\boldsymbol{\omega}^{\mathrm{T}}\boldsymbol{x}_i+b=-1$ 上的样本数据称为支持向量，如图 1 所示。

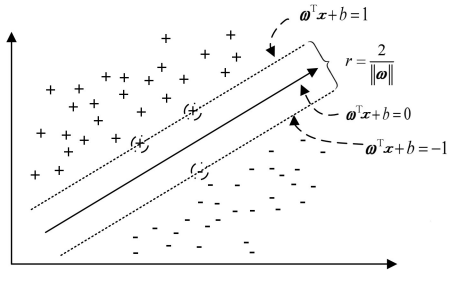


图 1 支持向量机示意图

Fig. 1 Schematic diagram of support vector machine

支持向量机的目标是寻找一个使得异类支持向量到超平面距离最大的超平面，对应的优化目标如下：

$$\min_{\boldsymbol{\omega},b}\frac{1}{2}\|\boldsymbol{\omega}\|^2$$

$$\text{s.t. } y_i(\boldsymbol{\omega}^{\mathrm{T}}\boldsymbol{x}_i+b)\geqslant 1,i=1,2,\cdots,m$$

2.3 核方法

核方法是一类把低维空间的非线性可分问题转化为高维空间中线性可分问题的方法。通过在高维空间中求解线性超平面等价地解决数据在原始空间中线性不可分问题。主要做法是利用核函数直接求得两数据在高维空间中的内积，避免对映射函数的显式求解。核函数的定义如下。

定义 1(核函数) 设 $\mathcal{X}$ 为输入空间，$\mathcal{H}$ 为特征空间，其中 $\boldsymbol{x}_i\in\mathcal{X}$，若存在一个从 $\mathcal{X}$ 到 $\mathcal{H}$ 的映射 $\phi(\boldsymbol{x}):\mathcal{X}\to\mathcal{H}$ 对任意的 $\boldsymbol{x},\boldsymbol{z}\in\mathcal{X}$，函数 $k(\boldsymbol{x},\boldsymbol{z})$ 均满足 $k(\boldsymbol{x},\boldsymbol{z})=\langle\phi(\boldsymbol{x}),\phi(\boldsymbol{z})\rangle$，则称 k 为核函数。

常用的核函数如表 2 所列。

表 2 常用的核函数

Table 2 Common kernel functions

名称	表达式
线性核	$k(\boldsymbol{x}_i,\boldsymbol{x}_j)=\boldsymbol{x}_i^{\mathrm{T}}\boldsymbol{x}_j$
多项式核	$k(\boldsymbol{x}_i,\boldsymbol{x}_j)=(\boldsymbol{x}_i^{\mathrm{T}}\boldsymbol{x}_j)^d$
高斯核	$k(\boldsymbol{x}_i,\boldsymbol{x}_j)=\exp\left(\frac{\|\boldsymbol{x}_i-\boldsymbol{x}_j\|^2}{2\sigma^2}\right)$

2.4 SIMD 编码

SIMD 是一种基于硬件的并行计算技术。SIMD 编码技术的核心思想是通过多项式中国剩余定理，将一些“小的”明文编码到一个明文中。其本质上是在明文多项式 a 与一组小的明文多项式向量 $\boldsymbol{a}$ 之间建立了一种映射关系，记为 $a\leftrightarrow\boldsymbol{a}$，其中 $a\in A_p$。经这种方式编码生成的明文被称为 SIMD 明文。

根据中国剩余定理，A_p 中两个明文的加法与乘法运算，相当于其 SIMD 映射的两个“小的”明文向量对应元素的加法与乘法运算。令 $a\leftrightarrow\boldsymbol{a}=\{a_1,\cdots,a_l\}$，$b\leftrightarrow\boldsymbol{b}=\{b_1,\cdots,b_l\}$，有性质：

$$a+b\leftrightarrow\boldsymbol{a}+\boldsymbol{b}=(a_1+b_1,\cdots,a_l+b_l)$$

$$a\cdot b\leftrightarrow\boldsymbol{a}\cdot\boldsymbol{b}=(a_1\cdot b_1,\cdots,a_l\cdot b_l)$$

在进行同态运算时，使用 SIMD 技术能够很大程度地节约计算开销，因为其能够使用一次加(乘)法操作代替 l 次加(乘)法开销。但以上方案仅适用于加密数据为整数的情况，而 CKKS 的加密数据是实(复)数向量，需要通过自然映射(Canonical Embedding)与快速傅里叶逆变换(Inverse Fast Fourier Transform，IFFT)实现 SIMD 编码，过程如图 2 所示。

$$\sigma:\mathbb{Q}[X]/(X^n+1)\to\mathbb{C}^n,\sigma(a)=(a(\zeta),a(\zeta^3),\cdots,a(\zeta^{2n-1}))$$

$$\tau:\mathbb{Q}[X]/(X^n+1)\to\mathbb{C}^{n/2},\tau(a)=(a(\zeta),a(\zeta^5),\cdots,a(\zeta^{2n-3}))$$

其中，$\zeta=\exp\left(\frac{\pi i}{n}\right)$。

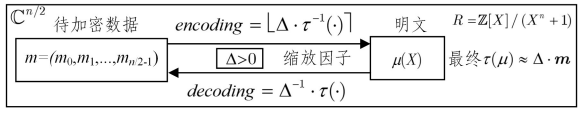


图 2 CKKS 编解码过程图

Fig. 2 Diagram of CKKS encoding and decoding process

2.5 同态加密

同态加密的概念最早由 Rivest 等[26]于 1978 年提出，是一种能够直接在密文数据上进行同态加法、乘法运算的特殊的公钥密码体制。在密文上的同态运算结果与在明文上进行相应运算后再加密的结果相同。按密码体制对同态运算的支持程度，又可以将其分为部分同态加密、近似同态加密与全同态加密 3 种，它们的区别如表 3 所列。

表 3 3 种类型同态加密的对比

Table 3 Comparison of three types of homomorphic encryption

类型	支持运算	特点
部分同态加密	仅支持同态加法或同态乘法一种运算	支持无限次同态加法或无限次同态乘法
近似同态加密	同时支持同态加法与同态乘法运算	支持无限次同态加法及数次同态乘法
全同态加密		支持无限次同态加法及无限次同态乘法

本文选用 CKKS 近似同态加密(Somewhat Homomorphic Encryption，SHE)体制设计参数的安全聚合算法。与其他同态加密算法不同，CKKS 设计的目的是做近似计算，不保证加密与解密结果完全一致，故其相较于相同困难假设的同态加密算法而言具有更高的效率。同时，CKKS 还支持 SIMD 编码，能够直接将实(复)数向量打包为一个密文进行加密与计算，比较契合运算单位为实数向量的机器学习场景。下面将对 CKKS 密码系统进行详细介绍。

初始化阶段，选取一个固定值 p 作为近似计算中缩放的一个基，其中 $p>0$；并选取模数 q_0，其中，第 l 层的模数为 $q_l=p^l\cdot q_0$，第 l 层的密文为环 $R_{q_l}^k$ 上的向量，k 为固定整数；之后，给定安全参数 λ 和密文的最大层次 L，用于计算分圆多项式环参数 M，$M=M(\lambda,q_L)$。为方便理解，下文将基于 $R=\mathbb{Z}[X]/(\Phi_M(X))$环描述整体密码构造。

CKKS 同态加密算法由 {keyGen，Enc_{pk}，Dec_{sk}，Add，Mult，ReScale} 6 个算法组成，具体描述如下。

keyGen(1^λ)：给定安全参数 λ，生成一个私钥 sk、公钥 pk，以及一个辅助计算密钥 evk。

$\mathrm{Enc}_{pk}(m)$：对于任意的一个明文多项式 $m\in R$，输出密文 $c\in R_{q_L}^k$，m 的密文 c 满足$\langle c,sk\rangle=m+e(\mathrm{mod}\ q_L)$，其中 e 为一个很小的噪声。

$\mathrm{Dec}_{sk}(c)$：对一个密文层次为 l 的密文 c，输出其明文多项式 $m'\leftarrow\langle c,sk\rangle(\mathrm{mod}\ q_l)$。

Add(c_1，c_2)：给定 m_1，m_2 的密文 c_1，c_2，输出 m_1+m_2 的密文，输出密文的误差将以两个输入密文的误差之和为界。

$\mathrm{Mult}_{\mathrm{evk}}(c_1,c_2)$：对一对给定密文$(c_1,c_2)$，输出密文 $c_{\mathrm{mult}}\in R_{q_l}^k$，满足$\langle c_{\mathrm{mult}},sk\rangle=\langle c_1,sk\rangle\cdot\langle c_2,sk\rangle+e_{\mathrm{mult}}(\mathrm{mod}\ q_l)$，其中 $e_{\mathrm{mult}}\in R$。

$\mathrm{ReScale}_{l\to l'}(c)$：给定 l 层密文 $c\in R_{q_l}^k$ 与一个层次更低的层 l'，输出 $R_{q_l}^k$ 上的密文$(q_l'/q_l)c$ 向最近整数的舍入结果 c'。

3 隐私保护的非线性联邦 SVM 算法

本节首先分析联邦 SVM 现有研究中的不足，并针对现存不足提出解决方案，然后对本文算法进行详细解释说明。

3.1 问题描述

设有 k 个参与方与 1 个中心服务器。设 $\boldsymbol{D}$ 为所有设备数据的集合，各设备上的本地数据可看作是对 $\boldsymbol{D}\in\mathbb{R}^{n\times d}$ 进行横向划分，其中第 i 个设备上的数据集为 $\boldsymbol{D}_i=(\boldsymbol{x}_{i1},\boldsymbol{x}_{i2},\cdots,\boldsymbol{x}_{in_i})\in\mathbb{R}^{n_i\times d}$，其中 d 为数据维数，各设备数据结构相同，n_i 为第 i 个设备上拥有的数据量，$n=\sum n_i$ 为本次训练的数据总量。

横向联邦学习训练过程如下：1)服务器将模型的初始化参数 $\boldsymbol{\omega}$ 发送至各参与方；2)每个参与方 i 使用本地数据 $\boldsymbol{D}_i$ 在本地进行模型训练，得到本地模型参数 $\boldsymbol{\omega}_i^t$，并将其发送给负责模型聚合的中心服务器；3)中心服务器使用 FedAvg 算法[25]对各参与方上传的模型参数进行聚合，得到全局模型参数 $\boldsymbol{\omega}^t$；4)中心服务器将本轮聚合得到的全局模型参数 $\boldsymbol{\omega}^t$ 发送给各参与方；5)各参与方在全局模型参数的基础上更新参数，重复迭代直到收敛或达到最大迭代次数。训练过程示意图如图 3 所示。

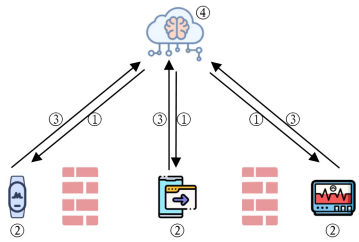


图 3 横向联邦学习训练过程示意图

Fig. 3 Schematic diagram of horizontal federated learning training process

在横向联邦 SVM 的研究中，主要存在以下两个问题：

(1)横向联邦 SVM 训练过程中存在中间参数隐私泄露的隐患。在联邦 SVM 的训练过程中，为保证参与方训练数据的隐私性，不会将参与方本地数据上传至中心服务器，而是将使用本地数据训练的模型参数上传至中心服务器，由中心服务器进行模型的聚合。

通常，中心服务器是诚实且好奇的(Honest But Curious)，这意味着，中心服务器会按照协议对参数进行聚合，但会尝试从接收到的数据及计算的中间结果中推断用户的隐私数据。这将会使用户数据面临隐私泄露的威胁。最近的研究表明，诚实且好奇的服务器能够从用户上传的梯度或模型参数中推理出参与方的原始数据[27]，达成窃取用户隐私数据的目的。

(2)横向联邦学习中非线性 SVM 的求解问题。主流的横向联邦学习通过梯度下降进行模型参数求解，暂无通过 SMO 算法求解的相关研究，原因是对偶问题计算的全局最优系数与局部数据计算的局部最优系数不同。由于每一方都有一个数据子集的数据，求解数据子集上的对偶问题难以生成全局最优系数[16]，这意味着在横向联邦学习场景下，将难以利用核技巧直接求解非线性联邦 SVM。

为解决上述问题，本文提出了 PPNLFedSVM 算法，利用随机傅里叶特征方法[28]显式求解出高斯核的近似映射函数，将原始数据显式映射到高维空间中，使得非线性数据在此空间中线性可分。之后，设计并实现基于 CKKS 同态加密的模型聚合的算法，并结合 CKKS 密码体制的特性进行针对性优

化，在保证模型聚合过程中模型参数及贡献（各参与方本地模型在全局模型中的占比）隐私性的同时，缓解了因引入密码系统带来的性能降低问题。

3.2 高斯核的近似映射

基于核函数 $k(\boldsymbol{x},\boldsymbol{y})$ 的核方法可以直接求得两个样本在高维空间的内积，但是对偶问题计算的全局最优系数与局部数据计算的局部最优系数不同，求解数据子集上的对偶问题难以生成全局最优系数。因此，本文采用随机傅里叶特征方法，将原始数据 $\boldsymbol{x}$ 通过显式的映射函数 $\boldsymbol{z}(\boldsymbol{x})$ 映射至一个相对低维的欧几里得空间中 $\boldsymbol{z}:\mathbb{R}^D\rightarrow\mathbb{R}^R$，其中 R 是相对于核函数的映射空间而言较小的维数值，用于解决海量数据背景下利用核技巧优化机器学习模型参数导致的时间、空间开销大的问题。

首先，我们注意到高斯核具有正定的移位不变性，即满足 $k(\boldsymbol{x},\boldsymbol{y})=k(\boldsymbol{x}-\boldsymbol{y})$。令 $\boldsymbol{x}-\boldsymbol{y}=\boldsymbol{\delta}$，设 $k(\boldsymbol{\delta})$ 的傅里叶变换为 $p(\boldsymbol{\omega})$，$p(\boldsymbol{\omega})=\frac{1}{2\pi}\int e^{-j\boldsymbol{\omega}^{\mathrm{T}}\boldsymbol{\delta}}k(\boldsymbol{\delta})\mathrm{d}\boldsymbol{\delta}$，则有傅里叶逆变换 $k(\boldsymbol{x}-\boldsymbol{y})=\int_{R^d}p(\boldsymbol{\omega})e^{j\boldsymbol{\omega}^{\mathrm{T}}(x-y)}\mathrm{d}\boldsymbol{\omega}$。

定理 1（Bochner 定理[29]） $\mathbb{R}^d$ 上连续的核函数 $k(\boldsymbol{x},\boldsymbol{y})=k(\boldsymbol{x}-\boldsymbol{y})$ 是正定的，当且仅当 $k(\boldsymbol{\delta})$ 是一个非负测度的傅里叶变换。

依据定理 1 的结论可知，在对核函数 $k(\boldsymbol{\delta})$ 进行合适的缩放后，可以保证其傅里叶变换 $p(\boldsymbol{\omega})$ 刚好是一个概率分布[29]。此时有：

$$k(\boldsymbol{x}-\boldsymbol{y})=\int_{R^d}p(\boldsymbol{\omega})e^{j\boldsymbol{\omega}^{\mathrm{T}}(x-y)}\mathrm{d}\boldsymbol{\omega}=E_{\boldsymbol{\omega}}[e^{j\boldsymbol{\omega}^{\mathrm{T}}(x-y)}] \tag{1}$$

这意味着，可以将 $\exp(j\boldsymbol{\omega}^{\mathrm{T}}(\boldsymbol{x}-\boldsymbol{y}))$ 作为 $k(\boldsymbol{x}-\boldsymbol{y})$ 的一个无偏估计。进一步，我们注意到核函数 $k(\boldsymbol{x}-\boldsymbol{y})$ 与 $p(\boldsymbol{\omega})$ 都是实函数，因而在式(1)中无须考虑虚部，故在积分 $\int_{R^d}p(\boldsymbol{\omega})e^{j\boldsymbol{\omega}^{\mathrm{T}}(x-y)}\mathrm{d}\boldsymbol{\omega}$ 中，只需考虑 $\exp(j\boldsymbol{\omega}^{\mathrm{T}}(\boldsymbol{x}-\boldsymbol{y}))$ 的实部 $\cos(\boldsymbol{\omega}^{\mathrm{T}}(\boldsymbol{x}-\boldsymbol{y}))$ 即可，即 $k(\boldsymbol{x},\boldsymbol{y})=k(\boldsymbol{x}-\boldsymbol{y})=E_{\boldsymbol{\omega}}[\cos(\boldsymbol{\omega}^{\mathrm{T}}(\boldsymbol{x}-\boldsymbol{y}))]$。

若我们定义 $z_{\boldsymbol{\omega},b}(\boldsymbol{x})=\sqrt{2}\cos(\boldsymbol{\omega}^{\mathrm{T}}\boldsymbol{x}+b)$，其中 $\boldsymbol{\omega}\sim p(\boldsymbol{\omega})$ 是依据概率密度函数 $p(\boldsymbol{\omega})$ 得到的随机变量，$b\sim Uniform(0,2\pi)$ 是服从均匀分布的随机变量，则可以按照下述方法计算核函数 $k(\boldsymbol{x},\boldsymbol{y})$。

定理 2 对于任意的 $\boldsymbol{x}\in\mathbb{R}^D$，向量 $\boldsymbol{z}(\boldsymbol{x})$ 的定义如下：

$$\boldsymbol{z}(\boldsymbol{x})=\left[\frac{1}{\sqrt{R}}z_{\boldsymbol{\omega}_1,b_1}(\boldsymbol{x}),\frac{1}{\sqrt{R}}z_{\boldsymbol{\omega}_2,b_2}(\boldsymbol{x}),\cdots,\frac{1}{\sqrt{R}}z_{\boldsymbol{\omega}_R,b_R}(\boldsymbol{x})\right]^{\mathrm{T}}$$

其中，$\boldsymbol{\omega}_1,\boldsymbol{\omega}_2,\cdots,\boldsymbol{\omega}_n\sim p(\boldsymbol{\omega})$，$b_1,b_2,\cdots,b_n\sim Uniform(0,2\pi)$，则成立 $k(\boldsymbol{x},\boldsymbol{y})=k(\boldsymbol{x}-\boldsymbol{y})\approx\boldsymbol{z}(\boldsymbol{x})^{\mathrm{T}}\cdot\boldsymbol{z}(\boldsymbol{y})$。

证明：由 $z_{\boldsymbol{\omega},b}(\boldsymbol{x})=\sqrt{2}\cos(\boldsymbol{\omega}^{\mathrm{T}}\boldsymbol{x}+b)$，有[30]：

$$E_{\boldsymbol{\omega},b}[z_{\boldsymbol{\omega},b}(\boldsymbol{x})z_{\boldsymbol{\omega},b}(\boldsymbol{y})]=E_{\boldsymbol{\omega},b}[\sqrt{2}\cos(\boldsymbol{\omega}^{\mathrm{T}}\boldsymbol{x}+b)\cdot\sqrt{2}\cos(\boldsymbol{\omega}^{\mathrm{T}}\boldsymbol{y}+b)]$$

经三角函数变换，可得：

$$E_{\boldsymbol{\omega},b}[z_{\boldsymbol{\omega},b}(\boldsymbol{x})z_{\boldsymbol{\omega},b}(\boldsymbol{y})]=E_{\boldsymbol{\omega},b}[\cos\boldsymbol{\omega}^{\mathrm{T}}(\boldsymbol{x}+\boldsymbol{y})+2b)]+E_{\boldsymbol{\omega}}[\cos(\boldsymbol{\omega}^{\mathrm{T}}(\boldsymbol{x}-\boldsymbol{y}))]$$

其中，第一项 $E_{\boldsymbol{\omega},b}[\cos(\boldsymbol{\omega}^{\mathrm{T}}(\boldsymbol{x}+\boldsymbol{y})+2b)]$ 满足 $E_{\boldsymbol{\omega},b}[\cos(\boldsymbol{\omega}^{\mathrm{T}}(\boldsymbol{x}+\boldsymbol{y})+2b)]=E_{\boldsymbol{\omega}}\{E_b[\cos(\boldsymbol{\omega}^{T}(\boldsymbol{x}+\boldsymbol{y})+2b)|\boldsymbol{\omega}]\}$。令 $t=\boldsymbol{\omega}^{\mathrm{T}}(\boldsymbol{x}-\boldsymbol{y})$，则上式右边期望中的项可以变换为：

$$\begin{aligned}E_b[\cos(t+2b)|\boldsymbol{\omega}]&=\int_0^{2\pi}\frac{\cos(t+2b)}{2\pi}\mathrm{d}b\\&=\frac{1}{2\pi}\int_0^{2\pi}\cos(t+2b)\mathrm{d}b\\&=\frac{1}{2\pi}[\sin(t+2b)|_0^{2\pi}]\\&=\frac{1}{2\pi}[\sin(t)-\sin(t+4\pi)]\\&=0\end{aligned}$$

这意味着：

$$\begin{aligned}E_{\boldsymbol{\omega},b}[z_{\boldsymbol{\omega},b}(\boldsymbol{x})z_{\boldsymbol{\omega},b}(\boldsymbol{y})]&=E_{\boldsymbol{\omega}}\{0\}+E_{\boldsymbol{\omega}}[\cos(\boldsymbol{\omega}^{\mathrm{T}}(\boldsymbol{x}-\boldsymbol{y}))]\\&=E_{\boldsymbol{\omega}}[\cos(\boldsymbol{\omega}^{\mathrm{T}}(\boldsymbol{x}-\boldsymbol{y}))]\end{aligned}$$

进一步成立：

$$\begin{aligned}\boldsymbol{z}(\boldsymbol{x})^{\mathrm{T}}\boldsymbol{z}(\boldsymbol{y})&=\frac{1}{R}\sum_{r=1}^{R}z_{\boldsymbol{\omega}_r}(\boldsymbol{x})z_{\boldsymbol{\omega}_r}(\boldsymbol{y})\\&=\frac{1}{R}\sum_{r=1}^{R}2\cos(\boldsymbol{\omega}_r^{\mathrm{T}}\boldsymbol{x}+b_r)\cos(\boldsymbol{\omega}_r^{\mathrm{T}}\boldsymbol{y}+b_r)\\&=\frac{1}{R}\sum_{r=1}^{R}\cos(\boldsymbol{\omega}_r^{\mathrm{T}}(\boldsymbol{x}-\boldsymbol{y}))\\&\approx E_{\boldsymbol{\omega}}[\cos(\boldsymbol{\omega}^{\mathrm{T}}(\boldsymbol{x}-\boldsymbol{y}))]\\&=k(\boldsymbol{x},\boldsymbol{y})\end{aligned}$$

依据上述定理，可以给出高斯核函数的随机傅里叶特征计算方法，如算法 1 所示。

算法 1 随机傅里叶特征算法

输入：正定的移位不变核 $k(\boldsymbol{x},\boldsymbol{y})$，其满足 $k(\boldsymbol{x},\boldsymbol{y})=k(\boldsymbol{x}-\boldsymbol{y})$

输出：映射函数 $\boldsymbol{z}(\boldsymbol{x})$

1. 计算正定核的傅里叶变换

$$p(\boldsymbol{\omega})=\frac{1}{2\pi}\int e^{-j\boldsymbol{\omega}^{\mathrm{T}}}k(\boldsymbol{\delta})\mathrm{d}\boldsymbol{\delta}$$

2. for(i=0;i < R;i++)
3. 从分布 $p(\boldsymbol{\omega})$，Uniform(0,2π)中抽样 $\boldsymbol{\omega}_i,b_i$
4. end for
5. 求得映射函数

$$\boldsymbol{z}(\boldsymbol{x})=\left[\frac{1}{\sqrt{R}}z_{\boldsymbol{\omega}_1,b_1}(\boldsymbol{x}),\frac{1}{\sqrt{R}}\boldsymbol{z}_{\boldsymbol{\omega}_2,b_2}(\boldsymbol{x}),\cdots,\frac{1}{\sqrt{R}}\boldsymbol{z}_{\boldsymbol{\omega}_R,b_R}(\boldsymbol{x})\right]^{\mathrm{T}}$$

3.3 PPNLFedSVM 算法

PPNLFedSVM 算法具体可分为训练数据的非线性映射和联邦 SVM 的安全训练两个阶段。

(1)训练数据的非线性映射。首先，通过随机种子安全协商算法（见算法 2），利用 Burmester-Desmedt 协议及 PRNG 在 N 个参与方之间协商得到随机种子。然后，联合随机傅里叶特征算法（见算法 1）及高斯核函数，得到高斯核的近似映射算法（见算法 3）；进一步，通过算法 3，得到高斯核的近似映射函数。最后，通过高斯核的近似映射函数将原始数据映射至高维空间中。

(2)联邦 SVM 的安全训练。经阶段(1)后，各参与方的本地数据已映射至同一高维空间中，客户端运行 PPNLFedSVM-Client 算法（见算法 4），中心服务器运行 PPNLFedSVM-Server 算法（见算法 5），两者通过模型参数密文交互完成联邦 SVM 的安全建模。

整体算法流程及结构如图 4 所示，下文将对整个算法流程进行详细介绍。

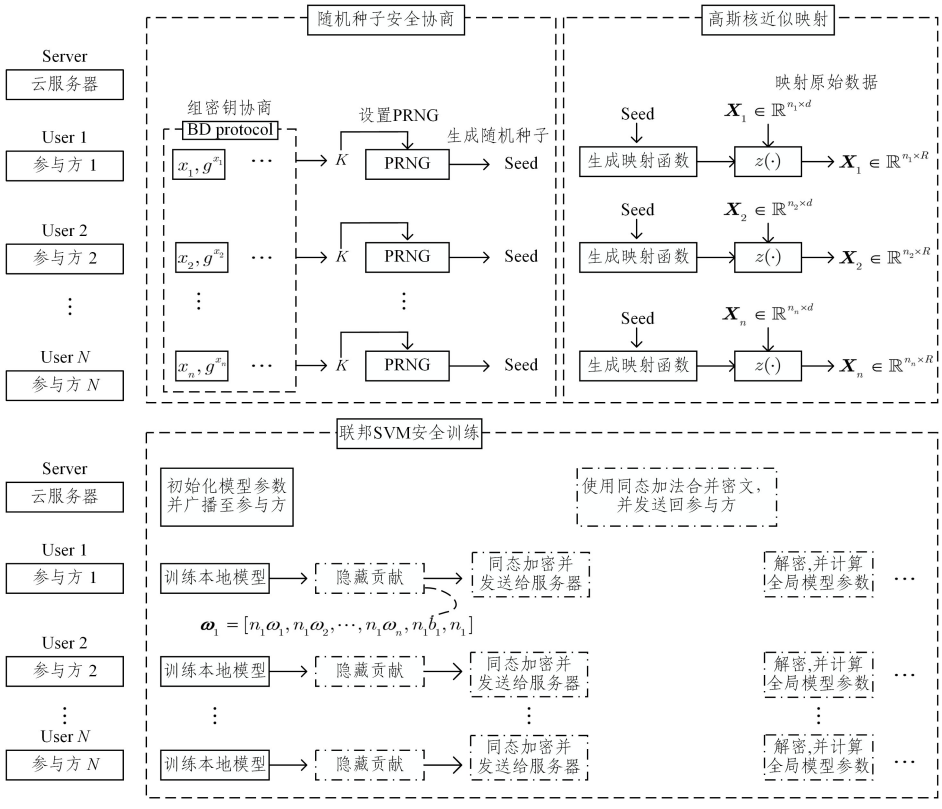


图 4 PPNLFedSVM 算法整体结构

Fig. 4 Overall structure of PPNLFedSVM algorithm

首先，通过 Burmester-Desmedt 协议进行组密钥的安全协商。共分为两个阶段。在第一阶段，各参与方先从乘法循环群 $\mathbb{Z}_p^*$ 中随机选取私钥 x_i，并计算公钥 g^{x_i}，记为 $z_i=g^{x_i}$，之后将其广播至所有参与方。第二阶段，各参与方 U_i 在其本地计算 X_i，并将其广播至所有参与方，其中 $X_i=Z_{i+1}/Z_i$，$Z_k=g^{x_K-1-x_K}$。最后，各参与方 U_i 在本地计算此次协商的组密钥 K_i，其中 $K_i=Z_i^nX_i^{n-1}X_{i+1}^{n-2}\cdots X_{i+n-2}$。显然，对于任意的参与方 U_i，有 $K_i=\prod_{j=1}^{j=n}Z_j=g^{x_1x_2+x_2x_3+\cdots+x_nx_1}$。至此，组密钥协商阶段完成，之后进行随机种子生成。经组密钥协商后，各参与方已拥有相同的组密钥 K，各方将密钥 K 作为 PRNG 的种子，运行 PRNG，得到相同的随机种子。上述过程的算法描述如算法 2 所示。

算法 2 随机种子安全协商算法

输出：随机种子 seed

1. 初始化生成元 g，阶数 p，素数 q；
2. 从乘法循环群中随机选取私钥 x_i，并计算公钥 g^{x_i}，$i\in[1,n]$，其中 n 为参与方的数量
3. (for j=1;j <= n;j++)
4. if(j !=i)
5. 将 g^{x_i} 发送给 U_j
6. end if
7. end for
8. 根据接收到的 $g^{x_{i+1}}$，$g^{x_{i-1}}$，计算出
   $Z_{i+1}=(g^{x_{i+1}})^{x_i} \bmod q$，$Z_i=(g^{x_{i-1}})_i^x \bmod q$，
   $X_i=Z_{i+1}/Z_i \bmod q$
9. (for j=1;j <= n;j++)
10. if(j ! =i)
11. 将 X_i 发送给 U_j
12. end if
13. end for
14. 计算组密钥：
    $K_i=Z_i^nX_i^{n-1}X_{i+1}^{n-2}\cdots X_{i+n-2} \bmod q$
15. 运行伪随机数生成器 seed=PRNG(K_i)，得到随机种子 seed

之后，各参与方使用安全协商得到的随机种子 *seed*，结合随机傅里叶特征算法将原始数据映射至同一高维空间中，如算法 3 所示。

算法 3 高斯核的近似映射算法

输入：初始化目标空间的维度 R，高斯核的 Gamma 值 γ，随机种子 seed

输出：映射后的数据集 $\mathbf{X}_i$

1. 利用随机种子安全协商阶段得到的随机种子 seed，设置并得到随机数生成器 random
2. 通过 random 生成分布 p($\boldsymbol{\omega}$)，Uniform(0，2π)
3. for(i=0;i < R;i++)
4. 从分布 p($\boldsymbol{\omega}$)，Uniform(0，2π)中抽样 $\boldsymbol{\omega}_i$，b_i.
5. $\boldsymbol{\omega}_i=\sqrt{2\gamma}\boldsymbol{\omega}_i$
6. end for
7. 得到映射函数 $\mathbf{z}(\mathbf{x})$
8. 使用 $\mathbf{z}(\mathbf{x})$将数据集 $\mathbf{D}_i$ 映射至高维空间，得到映射后的数据集 $\mathbf{X}_i$

进一步地，各参与方以映射后的数据 $\boldsymbol{X}_i$ 为训练数据来训练本地模型，得到本地模型参数 $\boldsymbol{\omega}^t=(\omega_1,\omega_2,\cdots,\omega_n,b)$。因 CKKS 密码体制存在同态乘法的开销大的问题，为了尽可能地避免同态乘法的使用，并隐藏各参与方在本轮迭代中的贡献(本地训练数据集的大小 n_i)，故将本轮训练得到的模型参数 $\boldsymbol{\omega}^t$ 乘以 n_i，并将 n_i 置于模型参数明文向量的最后一维，

得到明文向量 $\boldsymbol{\omega}^t=(n_i\omega_1, n_i\omega_2, \cdots, n_i\omega_n, n_ib, n_i)$，对其加密，得到密文 c_i 并发送给中心服务器，如算法 4 所示。

算法 4 PPNLFedSVM-Client 算法

输入：CKKS 密码系统参数，学习率，密文向量长度，通信轮数

1. 如果当前为客户端与服务器的首次交互，则从服务端接收初始化模型参数 $\boldsymbol{\omega}^0$
2. 否则，从服务端接收第 t 轮迭代的密文模型参数$[\![\boldsymbol{\omega}^t]\!]$
3. 解密接收到的密文模型参数 $\boldsymbol{\omega}^t=\mathrm{Dec}_{sk}([\![\boldsymbol{\omega}^t]\!])$
4. 计算得到全局模型参数 $\boldsymbol{\omega}^t=\boldsymbol{\omega}^t/\boldsymbol{\omega}^t[n+2]$
5. 使用本地数据集 $\mathbf{D}_i$ 训练得到本轮更新的参数 $\mathbf{g}_b$
6. 更新模型参数 $\boldsymbol{\omega}^{t+1}=\boldsymbol{\omega}^t-\eta\mathbf{g}_b$
7. 隐藏贡献 $\boldsymbol{\omega}^{t+1}=n\boldsymbol{\omega}^{t+1}$，$\boldsymbol{\omega}^{t+1}[n+2]=n$
8. 对向量 $\boldsymbol{\omega}^{t+1}$ 进行加密 $c_i=\mathrm{Enc}_{pk}(\boldsymbol{\omega}^{t+1})$
9. 将密文 c_i 发送给服务器
10. 直至达到通信轮数

中心服务器接收到各参与方发送来的密文 c_i 后，使用同态加法，聚合所有参与方的密文，得到聚合密文 C。之后将聚合后的密文发送给各参与方，如算法 5 所示。

算法 5 PPNLFedSVM-Server 算法

输入：CKKS 密码系统参数，学习率，密文向量长度，通信轮数

1. 接收所有参与方的加密模型参数 c_i
2. (for i=1;i <= n;i++)
3. 使用同态加法聚合全局模型参数 C=Add(C,c_i)
4. end for
5. (for i=1;i <= n;i++)
6. 将聚合密文 C 发送给各参与方 i
7. end for
8. 直至达到通信轮数

参与方在接收到聚合密文 C 后，对其解密，将其还原为对应的明文形式 $\boldsymbol{\omega}^t$，详细过程如下：首先取出 $\boldsymbol{\omega}^t$ 的最后一维，记为 $CountN$，其中 $CountN=\sum_{i=1}^{N}n_i$，使用 $\boldsymbol{\omega}^t$ 除以 $CountN$，得到本轮训练的全局模型参数 $\boldsymbol{\omega}^t$，其中 $\boldsymbol{\omega}^t=\sum_{i=1}^{N}\frac{n_i}{CountN}\boldsymbol{\omega}_i^t$；然后，参与方使用本地数据训练得到本轮的梯度 g_b，更新本地模型参数 $\boldsymbol{\omega}^{t+1}=\boldsymbol{\omega}^t-\eta\boldsymbol{g}_i$；进一步，将 n_i 置于模型参数 $\boldsymbol{\omega}^{t+1}$ 的最后一维；最后，将其加密后发送给服务器。重复上述过程直至达到通信轮数。

4 安全性分析

本节将从启发式分析和形式化分析两方面证明所提方案的安全性。

4.1 启发式分析

定理 3 本文提出的 PPNLFedSVM 方案可抵御内部重建攻击与内部属性推断攻击，如果 CKKS 是 IND-CPA 安全的，且 PRNG 是密码学安全的伪随机数生成器。

证明：

(1)内部重建攻击：若半诚实的中心服务器欲实施重建攻击，需要从参与方上传的局部模型参数密文中获取局部模型参数的明文。在所提方案中，半诚实中心服务器在接收参数阶段，会得到来自于随机选取的 k 个参与方的加密模型参数 $Enc_{pk}(\boldsymbol{\omega}_i)$，构成集合 $S=\{Enc_{pk}(\boldsymbol{\omega}_1), Enc_{pk}(\boldsymbol{\omega}_2), \cdots, Enc_{pk}(\boldsymbol{\omega}_k)\}$。在实际场景中，各参与方发送时间会受网络、计算性能的影响，使得密文的参数接收顺序与发送顺序无严格对应关系；又观察到，CKKS 密码体制是 IND-CPA 安全的[31]，故半诚实中心服务器无法在多项式时间中从密文模型参数中获取局部模型参数的任何有效信息。在模型聚合阶段，中心服务器会通过同态加法对集合 $\boldsymbol{S}$ 中的所有密文进行求和，得到聚合后的全局模型参数密文 $Enc_{pk}(\boldsymbol{\omega}^t)$。由于 CKKS 密码体制是 IND-CPA 安全的，故半诚实中心服务器在多项式时间内无法从聚合模型参数密文 $Enc_{pk}(\boldsymbol{\omega}^t)$ 中获取全局模型参数的任何有效信息。

(2)内部属性推断攻击：若半诚实的中心服务器欲实施内部属性推断攻击，需要同时拥有辅助数据集与全局模型参数。在所提方案的模型聚合阶段，中心服务器通过同态加法进行模型参数合并，又因 CKKS 密码体制是 IND-CPA 安全的，故半诚实中心服务器无法在多项式时间中获取全局模型参数的任何有效信息。此外，所提方案通过随机傅里叶特征方法对原始数据进行了显式映射，在未持有随机种子的情况下，难以将辅助数据集映射至与训练数据相同的空间中，加之所使用的 PRNG 也是密码学安全的，因此无法在多项式时间内得到安全协商的随机种子，故半诚实服务器无法在多项式时间内实施内部属性推断攻击。

4.2 形式化分析

满足安全两方计算的协议在面对诚实且好奇的对手时是安全的[32]，在本节中的形式化分析部分将通过证明本方案满足安全两方计算的定义，来证明本文所提模型的安全。

在证明中，将沿用 Bost 等[33]研究中的符号定义，设 $F=(F_A, F_B)$ 为一个多项式函数，其中 π 为计算 F 的协议，a 是 A 方的输入，b 是 B 方的输入，A，B 两方想要通过协议 π 计算 $F=(a,b)$，A 的视图被表示为元组 $view_A^{\pi}(\lambda,a,b)=(\lambda;a;m_1, m_2, \cdots, m_n)$ 其中 $m_1, m_2, \cdots, m_n$ 为 A 在执行时接收到的消息，使用相同的方式定义 B 的视图，并将 A 与 B 的输出记为 $output_A^{\pi}(a,b)$ 与 $output_B^{\pi}(a,b)$，将协议 π 的全局输出记为：

$$output^{\pi}(a,b)=(output_A^{\pi}(a,b), output_B^{\pi}(a,b))$$

定义 2(安全两方计算) 对于所有可能的输入 (a,b)，若模拟器 S_A 和 S_B 满足如下条件：

$$\{S_A, f_2(a,b)\}\approx\{view_A^{\pi}(a,b), output^{\pi}(a,b)\}$$

$$\{f_1(a,b), S_B)\}\approx\{output^{\pi}(a,b), view_B^{\pi}(a,b)\}$$

则证明模拟输出与协议的实际执行结果的输出在计算上是不可区分的。

欲证明所提算法在模型聚合过程中是安全的，只需证明 PPNLFedSVM-Server 在接收密文参数和聚合模型参数两阶段是安全的。首先，需要为挑战者 $\mathcal{A}$ 构造两个多项式时间的模拟器 S_1，S_2，模拟执行流程如下：

(1)在 $\mathcal{A}$ 接收到消息 (x, pk) 后，S_1 模拟 $\mathcal{A}$ 的执行如下：首先使用公钥 pk 执行加密算法得到 $\langle x\rangle_{pk}$，将 $\langle x\rangle_{pk}$ 返回给 $\mathcal{A}$。此时，$\mathcal{A}$ 在此次模拟中的视图表示为 $view_A^{\pi}(\langle x\rangle_{pk}, pk)=S_1(x, r, e_0, e_1, pk; r\cdot pk+(m+e_0, e_1))$。由于 CKKS 是 IND-CPA 安全的，这使得实际执行的视图与 $\mathcal{A}$ 的视图无法区分，故接收密文参数阶段是安全的。

(2)$\mathcal{A}$ 在接收到消息 $(\langle x\rangle_{pk}, \langle y\rangle_{pk})$ 后，S_2 模拟 $\mathcal{A}$ 的执行流程如下：首先使用 Add 算法，按照 $\langle z\rangle_{pk}=\langle x\rangle_{pk}+\langle y\rangle_{pk}$ 将

两个密文$\langle x\rangle_{pk}$，$\langle y\rangle_{pk}$相加，得到同态运算的结果$\langle z\rangle_{pk}$。S_2将结果$\langle z\rangle_{pk}$返回给$\mathcal{A}$，此时，$\mathcal{A}$在此次模拟中的视图为$view_{\mathcal{A}}^{\prime}(\langle z\rangle_{pk}, pk)=S_2(\langle x\rangle_{pk}, \langle y\rangle_{pk}, pk; \langle x\rangle_{pk}+\langle y\rangle_{pk})$，在半诚实的中心服务器假设下，中心服务器仅会尝试从接收到的数据中获取有效信息，加之 CKKS 是 IND-CPA 安全的，故$\mathcal{A}$在此次模拟中的视图与实际协议执行的视图无法区分。

上述证明表明，PPNLFedSVM-Server 协议在接收密文参数和聚合模型参数两阶段均满足两方安全计算的定义，故 PPNLFedSVM-Server 协议是安全的。

5 仿真及分析

本节首先对仿真环境及数据进行介绍，然后分别针对模型性能、随机种子安全协商、模型训练 3 部分进行仿真实验，并结合仿真实验结果进行分析。

5.1 仿真环境及数据

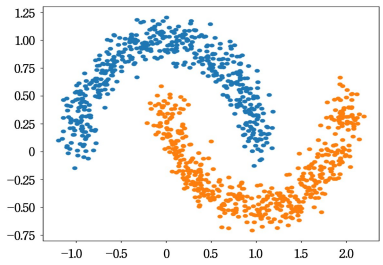
本文的仿真环境为 Intel（R）Core（TM）i7 6700HQ CPU，2.60 GHz，16 GB 内存，Windows 10 64 位操作系统。仿真实验代码使用 Python 编写，并基于 Pytorch，TenSEAL，randomgen 等库设计完成。

仿真实验整体使用 4 个数据集，如表 4 所列。其中 Moon 和 Circle 是用于检测模型非线性数据分类能力的生成数据集，两个数据集的正例与负例样本分别呈交叠的双月牙状及同心圆状，且包含 10% 的噪声数据，如图 5、图 6 所示。Ring 和 BCD 是两个真实的数据集。

表 4 数据集详细信息

Table 4 Dataset details

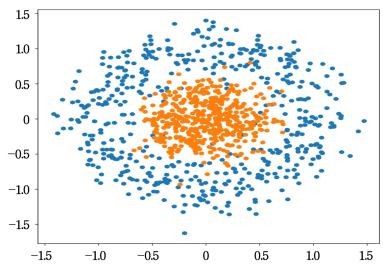
数据集	样本数	特征数
Moon	10000	2
Circle	10000	2
Ring	5920	20
BCD	455	30



注：样本量为 1000，噪声数据比例 10%

图 5 Moon 生成数据集样例图

Fig. 5 Moon generates a sample data set



注：样本量为 1000，噪声数据比例 10%，factor=0.3

图 6 Circle 生成数据集样例图

Fig. 6 Circle generates a sample data set

实验中所涉及的 Burmester-Desmedt 组密钥协商协议及 CKKS 密码系统参数、超参数设置如表 5、表 6 所列。

表 5 密码系统参数

Table 5 Cryptographic system parameters

参数名称	参数值
Burmester-Desmedt 密钥大小	2048
PRNG	Randomgen. ChaCha
CKKS. poly_modulus_degree	8192
CKKS. context. global_scale	2^{40}

表 6 各数据集的超参数设置

Table 6 Hyperparameter settings for each dataset

数据集	参数		
	batchsize	learning rate	penalty term
Moon	16	1.0×10^{-2}	1.0×10^{-2}
Circle	16	1.0×10^{-2}	1.0×10^{-2}
Ring	16	1.0×10^{-2}	1.0×10^{-5}
BCD	16	1.0×10^{-2}	1.0×10^{-2}

5.2 模型性能分析

本节将验证在所提方案下训练出的模型性能。首先验证在经过核近似映射后的数据上训练出的联邦 SVM 模型对非线性数据的分类能力，并进一步对比未添加任何隐私保护机制的 FedAvg 算法与本文提出的 PPNLFedSVM 算法所训练出的模型的性能。

在仿真实验中，最高迭代次数设置为 25，参与方数量设置为 10，并在每轮通信前，随机选取 80% 的参与方参与本轮建模，并以数据集中 80% 的数据为训练集，20% 的数据为测试集。

为使实验结果不失一般性，在仿真中，将使用 10 次仿真实验结果的均值作为最终结果，并使用测试集上的数据集准确率作为模型性能的衡量指标。

首先验证所提模型的性能，仿真实验结果如表 7 所列。

表 7 映射后数据训练出的模型的正确率

Table 7 Accuracy of model trained by mapped data

数据集	近似核映射参数	正确率/%
Circle	gamma=1，random state=16，n components=100	95.30
Moon	gamma=1，random state=16，n components=100	94.71
Ring	gamma=0.1，random state=16，n components=100	80.71
BCD	gamma=0.1，random state=16，n components=50	72.63

从结果中能够看出，通过 PPNLFedSVM 算法训练出的模型，在本文所选用的所有数据集上均取得了良好的性能，准确率分别达到了 95.30%，94.71%，80.71%，72.63%，证明了本文提出的非线性联邦 SVM 对非线性数据具有良好的分类能力。

然后分别使用 FedAvg 算法，与本文所提的 PPNLFedSVM 算法在相同的数据集下训练模型。并分别记录不同算法下正确率随迭代次数的变化，如图 7 所示。从图 7 可观察到，经 PPNLFedSVM 算法训练出的模型，与使用 FedAvg 算法训练出的模型，在实验使用的 4 个数据集上的性能几乎完全相同。

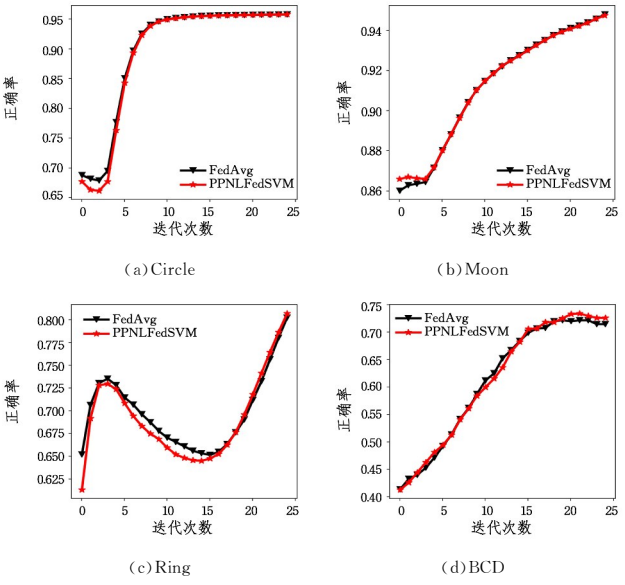


图 7 两种算法在不同数据集上的模型性能

Fig. 7 Model performance of two algorithms on different datasets

仿真实验结果表明，通过 PPNLFedSVM 算法训练出的非线性联邦 SVM 不仅对非线性数据具有良好的分类能力，并且可以在保护模型参数隐私性的同时得到近乎无损的模型。

5.3 随机种子安全协商性能分析

本节将从理论分析和实验研究两个角度，对不同参与方规模下随机种子安全协商算法的时间与通信开销进行分析说明。

首先，从算法理论角度上进行分析。由第 3 节中的算法描述可得，进行 1 次 N 方的组密钥协商，需要进行两轮通信，其对应的总时间复杂度表达式为 $O(n+n+Nn+1)$，故此算法的时间复杂度为 $O(n)$。这意味着，随机种子协商阶段的总时间开销将会随着参与方数量的增加呈线性增长。另外，我们观察到，在组密钥协商的两轮通信中，各参与方需要将自己当前的公钥或者组密钥的中间计算结果发送给其余参与方，因此，在组密钥协商中，共需进行 $2N$ 次通信。这意味着，随机种子安全协商阶段的总通信开销将会随着参与方数量的增加呈线性增长。

进一步，设计仿真实验验证随机种子协商安全算法在不同规模参与方下的时间与通信开销。实验结果如图 8 所示。

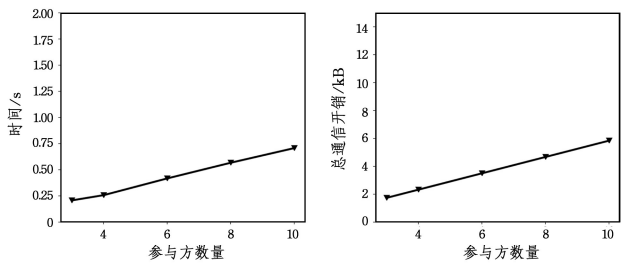


图 8 随机种子安全协商算法时间通信开销

Fig. 8 Diagram of random seed security negotiation algorithm time communication overhead

显然，所提算法在时间与通信开销上均呈线性增长，与理论分析所得结论一致。

5.4 时间开销分析

本节将对比使用 FedAvg 与 PPNLFedSVM 两种方案时单轮迭代的时间开销，分析联邦 SVM 在增加 CKKS 同态加密系统前后增加的时间开销。

首先，从理论上分析时间开销的增加，本节将使用 $O(train)$，$O(Mul)$，$O(Add)$ 表示本地训练模型、明文上的乘法、加法操作的时间开销，使用 $O(HomoAdd)$，$O(Enc_{pk})$，$O(Dec_{sk})$ 表示同态加法、加密、解密的时间开销。上述两种算法的时间复杂度如表 8 所列。

表 8 两种算法的时间复杂度

Table 8 Time complexity of two algorithms

算法	时间复杂度
FedAvg	$O(train)+(N-1)O(Add)+O(mul)$
PPNLFedSVM	$O(train)+(N-1)O(HomoAdd)+O(mul)+O(Enc_{pk})+O(Dec_{sk})$

经上述分析可得，PPNLFedSVM 相比 FedAvg 增加的时间开销，来源于 $N-1$ 次同态加法与明文加法的时间开销的差值，以及 1 次额外的加密、解密的时间消耗。

进一步设计实验来测量两种算法在 4 个数据集上的单轮迭代时间。测得数据如表 9 所列。

表 9 两种算法单轮迭代的时间差

Table 9 Time difference between two algorithms in a single iteration

数据集	FedAvg	PPNLFedSVM	时间差/s
Circle	0.1453	0.1534	0.0081
Moon	0.0897	0.1655	0.0758
Ring	0.0462	0.0549	0.0087
BCD	0.0062	0.0309	0.0247

由测量结果可知，增加隐私保护机制的 PPNLFedSVM 与未增加隐私保护机制的 FedAvg 相比，整体相差较小，其中最小差值为 0.0081s，最大差值为 0.0758s。联合两种算法的时间复杂度分析可知，PPNLFedSVM 增加的时间开销来源于同态加法运算及模型参数的加解密。

PPNLFedSVM 选择在模型训练速度上做出少量让步，以换取模型参数的隐私性。通过向系统中引入同态加密的方法，将模型聚合转移至密文域中进行，使得参数服务器无法获取有关全局模型的任何有效信息，从而防止模型聚合阶段发生隐私泄露。

为进一步探究加解密时间与模型规模的关系，本文将数据集 Circle 映射至不同规模的高维空间中进行模型训练，并分别测量不同参数规模下使用两种算法进行单轮迭代的时间，实验结果如图 9 所示。

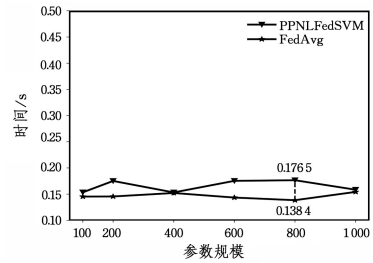


图 9 单轮迭代时间差随参数规模的变化

Fig. 9 Time difference of a single iteration varies with the scale of parameter

由图 9 中的实验结果可得，在模型参数规模由 100 增加至 1000 的过程中，两种模型下单轮迭代的时间差最大为 0.0381 s，且增大的参数规模并未对训练时间产生明显影响。

5.5 通信开销分析

本节主要分析模型的明文、密文大小随模型参数规模的变化关系。

为进一步分析联邦学习系统在增加隐私保护机制前后通信开销的增长，本实验将测量模型参数交换过程中不同参数规模下需传输数据量的大小。实验结果如图 10 所示。

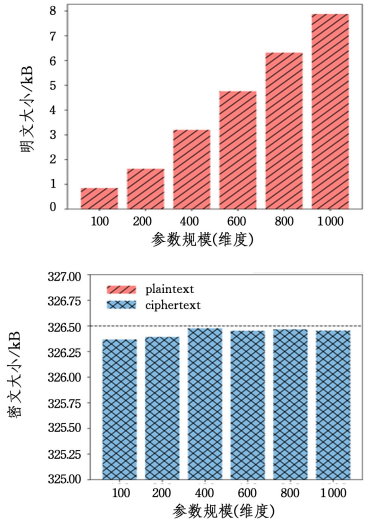


图 10 通信开销随模型参数规模的变化

Fig. 10 Communication overhead varies with the scale of model parameters

从图 10 可以看出，随着模型参数规模的增大，明文参数的大小呈线性增长，而密文参数的大小整体趋于 326.5 kB。

加密后密文大小趋于定值的原因是：CKKS 方案为实现密文计算并行化，降低内存开销，对数据进行了 SIMD 编码。首先将待加密数据表示为复数形式，并在指定位置插入其共轭复数，进一步地，通过快速傅里叶逆变换编码至多项式环中；又由于仿真实验中 CKKS 密码系统的 poly_modulus_degree 为 8192，需要保留一半的空间来存放原始数据的共轭复数，故在此参数设置下 CKKS 密码系统支持实数向量的长度为固定值 4096，使得每次加密的实数向量长度仅与密码系统的 poly_modulus_degree 有关，故加密后的密文大小不会随着参数规模的增大而增大。同样，这也是单轮迭代时间几乎不随参数规模变化的原因。

结束语 本文研究了一种隐私保护的非线性联邦支持向量机训练算法，设计了隐私保护场景下基于高斯核的非线性联邦支持向量机的训练方案，保证了联邦学习过程中各参与方模型参数及其贡献的隐私性。并根据 CKKS 密码体制特性，对参数聚合过程进行优化调整，避免开销昂贵的同态乘法运算。通过实验验证了所提模型性能与使用明文训练所得模型精度相同，实现了联邦学习场景下非线性支持向量机可用性与隐私性的平衡。在今后的研究中，将着重探究 CKKS 密码体制与其他机器学习模型结合的应用，并尝试研究去中心化联邦学习系统的隐私保护技术。

参 考 文 献

[1] ZHUANG M Q, TAN X H, FAN Y C, et al. 3D animation expression generation and emotional supervision based on convolutional neural network[J]. Journal of Chongqing University of Technology(Natural Science), 2022, 36(1): 151-158.

[2] WANG Z, GUO Y, NIE Z, et al. Privacy protection and cost management of smart meters based on dueling double deep Q-learning[J]. Journal of Chongqing University of Posts and Telecommunications(Natural Science Edition), 2021, 33(4): 554-561.

[3] WANG J, XU Y H, LI L. Data fusion privacy protection method with low energy consumption and integrity verification[J]. Journal of Jilin University(Engineering and Technology Edition), 2022, 52(7): 1657-1665.

[4] LI Q X, ZHOU Q X, WANG Z L, et al. Provable Secure Delegation Computing Protocol Based on Privacy Protection[J]. Computer Engineering, 2021, 47(5): 131-137.

[5] YANG W Q, ZHANG Y, NIE J T, et al. Energy and Information Management Strategy Based on Federated Learning for Wireless Network Nodes[J]. Computer Engineering, 2022, 48(1): 188-196, 203.

[6] LIU Y X, CHEN H, LIU Y H, et al. Privacy-Preserving Techniques in Federated Learning [J]. Ruan Jian Xue Bao/Journal of Software, 2022, 33(3): 1057-1092.

[7] WEN Y L, CHEN M J. Medical Data Sharing Scheme Combined with Federal Learning and Blockchain[J]. Computer Engineering, 2022, 48(5): 145-153, 161.

[8] ZHU L, LIU Z, HAN S. Deep Leakage from Gradients [J]. Advances in Neural Information Processing Systems, 2019, 32: 1-11.

[9] ZHAO B, MOPURI K R, BILEN H. iDLG: Improved Deep Leakage from Gradients [J]. arXiv: 2001.02610, 2020.

[10] WANG Z, SONG M, ZHANG Z, et al. Beyond Inferring Class Representatives: User-Level Privacy Leakage from Federated Learning[C]// IEEE INFOCOM 2019 — IEEE Conference on Computer Communications. IEEE, 2019: 2512-2520.

[11] BAKOPOULOU E, TILLMAN B, MARKOPOULOU A. A Federated Learning Approach for Mobile Packet Classification [J]. arXiv: 1907.13113, 2019.

[12] GE N, LI G H, ZHANG L, et al. Failure Prediction in Production Line Based on Federated Learning: An Empirical Study [J]. arXiv: 2101.11715, 2021.

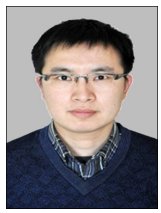
[13] HARTMANN V, MODI K, PUJOL J M, et al. Privacy-Preserving Classification with Secret Vector Machines[C]// Proceedings of the 29th ACM International Conference on Information & Knowledge Management. 2020: 475-484.

[14] BURMESTER M, DESMEDT Y. A Secure and Efficient Conference Key Distribution System[C]// Workshop on the Theory and Application of Cryptographic Techniques. Berlin: Springer, 1994: 275-286.

[15] CHEON J H, KIM A, KIM M, et al. Homomorphic Encryption for Arithmetic of Approximate Numbers[C]// International Conference on the Theory and Application of Cryptology and In-

formation Security. Cham: Springer, 2017: 409-437.
[16] YU H, VAIDYA J, JIANG X. Privacy-Preserving SVM Classification on Vertically Partitioned Data[C]// Pacific-Asia Conference on Knowledge Discovery and Data Mining. Berlin: Springer, 2006: 647-656.
[17] YU H, JIANG X, VAIDYA J. Privacy-Preserving SVM Using Nonlinear Kernels on Horizontally Partitioned Data[C]// Proceedings of the 2006 ACM Symposium on Applied Computing. 2006: 603-610.
[18] VAIDYA J, YU H, JIANG X. Privacy-Preserving SVM Classification [J]. Knowledge and Information Systems, 2008, 14(2): 161-178.
[19] MANGASARIAN O L, WILD E W. Privacy-Preserving Classification of Horizontally Partitioned Data via Random Kernels [C]// Proceedings of the 2008 International Conference on Data Mining. Las Vegas, USA, 2008: 473-479.
[20] LEE Y J, MANGASARIAN O L. RSVM: Reduced Support Vector Machines[C]// Proceedings of the 2001 SIAM International Conference on Data Mining. Society for Industrial and Applied Mathematics. 2001: 1-17.
[21] SUN L, MU W S, QI B, et al. A New Privacy-Preserving Proximal Support Vector Machine for Classification of Vertically Partitioned Data [J]. International Journal of Machine Learning and Cybernetics, 2015, 6(1): 109-118.
[22] LIU X, DENG R H, CHOO K K R, et al. Privacy-Preserving Outsourced Support Vector Machine Design for Secure Drug Discovery [J]. IEEE Transactions on Cloud Computing, 2018, 8(2): 610-622.
[23] LIU X, DENG R H, CHOO K K R, et al. An Efficient Privacy-Preserving Outsourced Calculation Toolkit with Multiple Keys [J]. IEEE Transactions on Information Forensics and Security, 2016, 11(11): 2401-2414.
[24] WANG J, WU L, WANG H, et al. An Efficient and Privacy-Preserving Outsourced Support Vector Machine Training for Internet of Medical Things [J]. IEEE Internet of Things Journal, 2020, 8(1): 458-473.
[25] MCMAHAN B, MOORE E, RAMAGE D, et al. CommunicationEfficient Learning of Deep Networks from Decentralized Data[C]// Artificial Intelligence and Statistics. PMLR, 2017: 1273-1282.
[26] RIVEST R L, ADLEMAN L, DERTOUZOS M L. On Data Banks and Privacy Homomorphisms [J]. Foundations of Secure Computation, 1978, 4(11): 169-180.
[27] LYU L, YU H, YANG Q. Threats to Federated Learning: A Survey [J]. arXiv: 2003.02133, 2020.
[28] RAHIMI A, RECHT B. Random Features for Large-Scale Kernel Machines [J]. Advances in Neural Information Processing Systems, 2007, 20: 1177-1184.
[29] RUDIN W. Fourier Analysis on Groups[M]. New York: Courier Dover Publications, 2017.
[30] GREGORY G. Predicts Random Fourier Features [EB/OL]. (2019-12-23) [2022-05-24]. http://gregorygundersen.com/blog/2019/12/23/random-fourier-features/.
[31] CHEON J H, HONG S, KIM D. Remark on the Security of CKKS Scheme in Practice [EB/OL]. (2020-12-21) [2022-05-26]. https://eprint.iacr.org/2020/1581.pdf.
[32] ODED G. Foundations of Cryptography-Basic Applications [M]. Cambridge: Cambridge University Press, 2004.
[33] BOST R, POPA R A, TU S, et al. Machine Learning Classification over Encrypted Data[C]// Network and Distributed System Security Symposium. 2014.

YANG Hong-jian, born in 1998, postgraduate. His main research interests include federated learning, homomorphic encryption and blockchain.



HU Xue-xian, born in 1982, Ph.D, associate professor, master supervisor. His main research interests include big data security, applied cryptography and network security.

(责任编辑:何杨)