软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2019,30(11):3503−3517 [doi: 10.13328/j.cnki.jos.005573]
©中国科学院软件研究所版权所有.
E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel: +86-10-62562563

支持隐私保护的 *k* 近邻分类器*

徐 剑[1,2], 王安迪[1], 毕 猛[1,3], 周福才[1]

[1](东北大学 软件学院,辽宁 沈阳 110169)

[2](信息安全国家重点实验室(中国科学院 信息工程研究所),北京 100093)

[3](沈阳工业大学,辽宁 沈阳 110023)

通讯作者: 王安迪, E-mail: 13940201525@163.com

摘 要: *k* 近邻(*k*-nearest neighbor,简称 kNN)分类器在生物信息学、股票预测、网页分类以及鸢尾花分类预测等方面都有着广泛的应用.随着用户隐私保护意识的日益提高,kNN 分类器也需要对密文数据提供分类支持,进而保证用户数据的隐私性,即设计一种支持隐私保护的 *k* 近邻分类器(privacy-preserving *k*-nearest neighbor classifier,简称 PP-kNN).首先,对 kNN 分类器的操作进行分析,从中提取出一些基本操作,包括加法、乘法、比较、内积等.然后,选择两种同态加密方案和一种全同态加密方案对数据进行加密.在此基础上设计了针对基本操作的安全协议,其输出结果与在明文数据上执行同一方法的输出结果一致,且证明该协议在半诚实模型下是安全的.最后,通过将基本操作的安全协议进行模块化顺序组合的方式实现 kNN 分类器对密文数据处理的支持.通过实验,对所设计的 PP-kNN 分类器进行测试.结果表明,该分类器能够以较高效率实现对密文数据的分类,同时为用户数据提供隐私性保护.

关键词: kNN 分类器;加密数据;隐私保护;同态加密;监督学习

中图法分类号: TP309

中文引用格式: 徐剑,王安迪,毕猛,周福才.支持隐私保护的 *k* 近邻分类器.软件学报,2019,30(11):3503−3517. http://www.jos.org.cn/1000-9825/5573.htm

英文引用格式: Xu J, Wang AD, Bi M, Zhou FC. Privacy-preserving *k*-nearest neighbor classifier. Ruan Jian Xue Bao/Journal of Software, 2019,30(11):3503−3517 (in Chinese). http://www.jos.org.cn/1000-9825/5573.htm

Privacy-preserving *k*-Nearest Neighbor Classifier

XU Jian[1,2], WANG An-Di[1], BI Meng[1,3], ZHOU Fu-Cai[1]

[1](Software College, Northeastern University, Shenyang 110169, China)

[2](State Key Laboratory of Information Security (Institute of Information Engineering, Chinese Academy of Sciences), Beijing 100093, China)

[3](Shenyang University of Technology, Shenyang 110023, China)

Abstract: *k*-nearest neighbor (kNN) classifier has wide applications in many areas such as bioinformatics, stock forecasting, Web-page classification, and Iris classification prediction. With the increasing awareness of user privacy protection, kNN classifier classification also needs to provide supports for encrypted data, so privacy-preserving kNN classifier (PP-kNN) is designed to keep the privacy of user data. Firstly, the operation of kNN classifier is analyzed, and a set of basic operations is extracted, including addition, multiplication, comparison, inner product, etc. Then, two homomorphic encryption schemes and one fully homomorphic encryption scheme are selected to encrypt the data. Security protocols are designed for each of these, which outputs are consistent with the same operation over plaintext data and proved that protocol is secure in the semi-honest model. Finally, these security protocols are designed in a modules composable

* 基金项目: 国家自然科学基金(61872069); 中央高校基本科研业务费专项资金(N171704005, N181704004); 沈阳市科技计划(18-013-0-01)

Foundation item: National Natural Science Foundation of China (61872069); Fundamental Research Funds for the Central Universities (N171704005, N181704004); Science and Technology Plan of Shenyang Municipality (18-013-0-01)

收稿时间: 2017-11-27; 修改时间: 2018-01-04; 采用时间: 2018-02-09

© 中国科学院软件研究所 http://www.jos.org.cn

way to achieve the encryption of the kNN classifier. The PP-kNN classifier is implemented and evaluated based on real data, the result show that the classifier could classify the ciphertext data with higher efficiency, and also provide privacy protection for user data.

Key words: kNN classifier; encrypted data; privacy-preserving; homomorphic encryption; supervised learning

分类器是数据挖掘中对样本进行分类的方法的统称.其设计目标是在通过学习后,能够将数据分到已知类别.分类器不仅应用在搜索引擎以及各种检索程序中,而且也大量应用在数据分析与预测领域.kNN 分类器是一种重要的分类器,广泛应用于生物信息学、股票预测、网页分类、鸢尾花类别预测等领域.

分类器在广泛应用的同时,也产生了严重的用户隐私泄露问题[1,2],一旦泄露,会给数据拥有者带来危害.比如,不法分子盗取患者癌症信息,利用患者迫切希望治愈的心理,向患者销售高价药品,骗取钱财;在利用 kNN 进行股票预测时,如果股民的个股信息在分类过程中被泄露,就会给股票市场带来混乱.分类器处理的数据量大、种类多,与之相关的用户数据隐私保护形势也非常严峻.目前,针对数据分类过程中的隐私保护研究主要集中在密文数据运算方面,但是该类技术也存在如下问题:(1) 一些分类器对密文数据的运算复杂,运算效率较低;(2) 加密技术针对的是特定的分类器,缺乏普适性.

kNN 分类器是监督学习中“懒惰学习”(lazy learning)的典型代表,监督学习过程由两个阶段构成.

(1) 样本训练阶段:在此阶段,首先获取在准备工作阶段处理好的训练数据;然后根据分类器类型选择分类算法,对训练数据进行训练得到模型 W,以此作为分类阶段的一项输入.

(2) 应用阶段(分类阶段):分类器 C 通过模型 W 对测试向量 X 进行分类预测,得到最终的分类结果 $C(W,X)$.

在样本训练和分类阶段,都可能发生用户隐私信息的泄露:在样本训练阶段,数据拥有者不希望自己拥有的数据信息被泄露出去,甚至对训练者也要进行保密,这就需要对训练数据进行加密处理;在分类阶段,训练者会将得到的模型 W 作为分类器的构成部分,并将分类器发布出去提供服务,但不希望成果被第三方获取,这就需要对分类模型和测试向量进行加密.总而言之,分类器要保证数据的隐私性必须从两方面入手:(1) 训练数据集和模型 W 的隐私保护;(2) 测试向量 X 和分类结果 $C(W,X)$的隐私保护.

目前已有一些关于分类器隐私保护的研究成果,但大多数方案都是针对训练阶段数据的隐私保护,很少有针对分类模型和分类过程的保护.因此,设计基于加密数据的基本操作加密协议并以模块化顺序组合的方法构造安全的分类器,使其从训练阶段到分类过程都能保证安全性,同时保证待测数据能够获得一个准确的类别,是当前机器学习隐私保护的重要研究方向之一.

1 相关工作

分类器的构造和实施过程就决定其在隐私保护方面存在隐患,例如,在训练样本上执行分类器算法,生成分类模型,很容易造成样本数据的泄露;在测试样本上执行分类模型,生成预测结果时,客户端会很容易得到分类模型,而服务器端也可以轻易获取到输入的测试数据.因此,分类器在样本训练和分类阶段的数据隐私问题已成为分类器隐私保护中最为重要的研究内容之一.

(1) 样本训练阶段

为了保证在样本训练阶段原始数据的隐私性,应将原始数据隐藏起来,在此阶段,不同的分类器会选择不同的算法来训练原始数据,比如贝叶斯算法、支持向量算法、决策树算法等.这些算法包含了点积运算、加法运算、比较运算.为了保证隐藏后的数据仍然能够进行上述运算,本阶段使用的隐私保护技术应满足 3 个方面的要求:(1) 不改变原始数据的整体分布趋势;(2) 不能从隐藏后的数据中直接推算出原始数据值;(3) 确保经过变换后的数据不会降低分类器的分类效果.目前,研究人员采用的技术主要分两类:数据干扰和数据加密.文献[3]提出一种基于非线性维数降低(即非度量多维缩放)来干扰原始数据的隐私保护框架,使用 k-Nearest Neighbor 分类算法对分类任务中的新型隐私保护数据挖掘(privacy-preserving data mining,简称 PPDM)方法进行了测试,在隐藏隐私数据的同时,保证了数据的有效性;文献[4]提出了数据扰动技术并利用该技术构建了决策树分类器,之后,相继提出了不同的扰动方法[5,6].但是,扰动技术不能保证密文数据的语义安全,且数据添加了统计噪声易

© 中国科学院软件研究所 http://www.jos.org.cn

造成分类器的分类精度下降.文献[7]提出了两方参与的决策树分类器,其假定数据分布在两方;文献[8–10]利用安全多方计算(secure multi-party computation,简称 SMC)技术构造了安全的分类器;文献[11]设计了一种基于主成分分析(primary component analysis,简称 PCA)的协同学习隐私保护方法,其利用 PCA 实现了在协同学习过程中对压缩数据的隐私保护;文献[12]设计了一种加法同态代理聚合方案实现了云端患者的历史数据的隐私保护,引入了隐私保护的 top-k 疾病名称检索协议保证了朴素贝叶斯分类器的安全性;文献[13]提出了一种分布式系统的隐私保护数据分类和相似性评估方案,该方案在分类和相似度评估过程中不泄露任何关于新到达数据和训练模型的信息,其最终的分类结果除外;文献[14]提出了将线性分类器和 IPE(inner product encryption)相结合的方法来对加密数据进行分类,其隐私保护分类方案允许用户的数据被加密,但服务器能够获知最终的加密结果;文献[15]设计了实用的安全模型,通过研究在安全的两方计算框架中的一些多元统计分析方法,生成了一些构造块,解决了安全的两方多元线性回归问题和安全的两方多变量问题;文献[16]基于安全多方协议与同态加密方案训练几种简单的分类器,例如线性分类器,该分类器是支持加密数据分类的,但是其构造的模型安全性较低,导致客户端不仅能够得知最终的分类结果,而且可能会获取分类模型的信息,造成分类模型信息的泄露.综上所述,在样本训练阶段不仅要隐藏原始数据,还要将分类规则进行隐藏,即保护服务器参与分类数据的隐私性,防止通过模型或分类过程推导出个人信息.

(2) 分类阶段

在分类阶段,支持用户数据隐私性保护的研究成果较少.在文献[17]中,第三方运行医疗预测函数对全同态加密(fully homomorphic encryption,简称 FHE)的患者数据进行运算,得到预测结果.该算法仅隐藏了来自云端的输入数据,在分类阶段,任何一方都可以获取到分类模型,容易泄露患者隐私给第三方或各参与方.文献[18,19]构造了线性分支程序的安全评估,用此实现了心电图(electrocardiogram,简称 ECG)信号的安全分类.这项技术是基于 finely-tuned garbled 电路的,虽然保证了分类过程的安全性,但分支程序的运行速度较慢.文献[20]利用神经网络[21]构造了安全的分类器,这是感知器分类器的泛化,使神经网络分类器能够支持对密文数据的分类.

综上所述,在分类样本训练阶段的隐私保护研究成果较多,在分类过程中的隐私保护研究成果则不多见,容易造成用户隐私信息的泄露.为此,本文首先对 kNN 分类器的操作进行分析,提取出从样本训练阶段到分类过程中所包含的基本操作,包括加法、乘法、点积、比较;针对上述基本操作,设计了相应的安全协议,然后以模块化顺序组合的方式将其组合生成 PP-kNN 分类器,从而保证了样本训练阶段和分类过程的数据隐私性.本文所设计的 PP-kNN 分类器的基本操作的隐私保护协议是基于差分隐私的,给加密数据加入噪声,防止在交互式环境中信息的泄露.在设计基本操作的安全协议时,选择了两种同态加密方案对数据进行加密,以增加隐私保护的强度.同时,所设计的基本协议在半诚实模型下是安全的,模块化顺序组合方法在该模型下也是安全的,因此通过顺序组合构造的 PP-kNN 分类器也是安全的.

本文第 1 节对 kNN 分类器和本文使用的加密方法进行描述.第 2 节给出基本操作安全协议的设计.第 3 节详细说明支持隐私保护的 kNN 分类器的构造过程.第 4 节从计算代价、存储代价等方面对基本操作安全协议及 PP-kNN 分类器进行性能评估.最后,对全文进行总结.

2 预备知识

2.1 kNN分类器

在 kNN 分类过程中,待分类对象的类别可以通过在它附近的训练数据的类别来确定,所以采取的策略就是找到离待分类对象最近的 k 个邻居进行分析.kNN 分类器的工作流程如下.

Step 1. 确定 k 值(最近邻居的个数).一般为奇数,通常是采用交叉检验来确定(经验规则:k 一般低于训练样本数的平方根).

Step 2. 确定距离度量公式.以文本分类为例,采用夹角余弦,得出待分类数据点和所有已知分类数据点的夹角余弦值.按夹角余弦值从大到小排列,获取距离最近的 k 个样本(夹角余弦值越大,角度就越小,距离也就越近).

© 中国科学院软件研究所 http://www.jos.org.cn

- 夹角余弦: $\cos\theta=\frac{AB}{|A||B|}=\frac{\langle A,B\rangle}{\sqrt{\langle A,A\rangle}\sqrt{\langle B,B\rangle}}$,其中,$A=(x_1,x_2,\ldots,x_n)$,$B=(y_1,y_2,\ldots,y_n)$.
- 距离度量公式还可使用欧式距离:

$$d_{AB}=\sqrt{(x_1-y_1)^2+(x_2-y_2)^2+\ldots+(x_n-y_n)^2}=\sqrt{\sum_{k=1}^{n}(x_k-y_k)^2}=\sqrt{(A-B)(A-B)^T}.$$

Step 3. 统计这 k 个样本点中各个类别的数量 $classCount[i]$.通过比较,得到类别数量最多的样本对应的分类 c_i,该类便是待分类样本所属分类.

2.2 加密方法

2.2.1 加密方案

本文使用了两种同态加密方案(goldwasser-micali 的二次剩余加密系统(QR)[22]和 Paillier 加密系统[23])及一种全同态加密方案(FHE)[24]对数据进行加密,前两种加密方案满足加法同态,后一种方案同时满足加法同态与乘法同态.同态加密体制[25]的加法同态与乘法同态的概要描述如下.

设 R 和 S 为整数环,R 表示明文空间,S 表示密文空间.$a,b\in R$,E 是 $R\to S$ 上的加密函数.如果存在算法 PLUS 和 MULT,使其满足:

$$E(a+b)=PLUS(E(a),E(b));E(a\times b)=MULT(E(a),E(b)).$$

这样可以利用 $E(a)$和 $E(b)$的值计算出 $E(a+b)$和 $E(a\times b)$,而不需要知道 a,b 的值.它分别满足加法同态和乘法同态.

2.2.2 加密假设

下面对本文用到的二次剩余假设、判定性合数剩余假设和判定性 RLWE 困难性假设进行介绍.

1) 二次剩余假设.假设 $N=p\times q$(p,q 为奇素数),$\mathbb{QR}_N$ 为模 N 的二次剩余集,$\mathbb{QNR}_N$ 为模 N 二次非剩余集(如果 x 是模 N 的非平方剩余,则 $x\in\mathbb{QNR}_N$,且 *Jacobi* 符号等于 1).$\{(N,\mathbb{QR}_N):|N|=\lambda\}$和$\{(N,\mathbb{QNR}_N):|N|=\lambda\}$是概率多项式时间计算不可区分的.
2) 判定性合数剩余假设.令 $N=p\times q$,$|N|=\lambda$,N 为两个值不等但长度相等的奇素数 p 和 q 乘积.z 称为模 N^2 的第 N 个剩余,如果存在 $y\in\mathbb{Z}_{N^2}$,使得 $z=y^N \bmod N^2$,其中,第 N 个剩余和第 N 个非剩余是概率多项式时间计算不可区分的.
3) 判定性 RLWE 困难性假设.对于安全参数λ,令 $f(x)=x^d+1$,其中,d 是 2 的方幂,令 $q\geqslant 2$ 为一个整数.令整数多项式环 $R=\mathbb{Z}[x]/f(x)$,$R_q=R/qR$,χ是 R 上的分布.$DRLWE_{d,q,\chi}$问题是指对下面 2 种分布进行区分:(1) $(a_i,\ b_i)$随机均匀取自 R_q^2;(2) 首先随机均匀选取 $s\leftarrow R_q$,然后随机均匀选取 $a_i\leftarrow R_q$ 和 $e_i\leftarrow\chi$并计算 $b_i=a_i\cdot s+e_i$,最终得到 $(a_i,b_i)\in R_q^2$.$DRLWE_{d,q,\chi}$假设是指 $DRLWE_{d,q,\chi}$问题中的两种分布是不可区分的.

一般来讲,噪声分布χ通常为高斯分布.

2.2.3 安全两方计算框架与模块化顺序组合

本文的基本操作安全协议都是两方协议,其安全性依赖于两方的安全计算框架.而本文将基本操作安全协议通过模块顺序组合技术构成安全的分类器,因此分类器的安全性应遵循模块化顺序组合的安全性和安全两方计算框架的安全性.定义 1 和定理 1 分别对半诚实模型下的安全两方计算定义和模块化顺序组合定理进行了描述.

定义 1(半诚实模型下的安全性). 设 $f=(f_A,f_B)$为概率多项式函数,A,B 为参与方,f_A(相应地,f_B)记为 $f(a,b)$的第一元素(相应地,第 2 个元素),Π为计算 f 的两方协议.A 输入 a,B 输入 b,A,B 在通过Π和安全参数λ执行 $f(a,b)$过程中的视图标记为 $V_A(\lambda,a,b)$,即 $V_A(\lambda,a,b)=(1^\lambda;a;r^A;m_1^A,\ldots,m_t^A)$,其中,$r^A$为 A 内部掷币过程的输出,m_i^A 为参与方 A 接收到的第 i 个消息,B 的视图标记与 A 类同.

在协议Π执行完毕后,A,B 基于输入(a,b)的输出分别记为 $Output_A^\Pi(\lambda,a,b)$ 和 $Output_B^\Pi(\lambda,a,b)$,显然,输出包含在参与者的视图中,且有: $Output^\Pi(\lambda,a,b)=(Output_A^\Pi(\lambda,a,b),Output_B^\Pi(\lambda,a,b))$.

© 中国科学院软件研究所 http://www.jos.org.cn

(一般情况)称Π秘密地计算了 f,若存在概率多项式算法分别标记为 S_A 和 S_B,且使得等式(1)和等式(2)成立.

$$\{S_A(1^\lambda,a,f_A(a,b),f(a,b))\}\equiv_c\{V_A(\lambda,a,b),Output^\Pi(\lambda,a,b)\} \quad (1)$$

$$\{S_B(1^\lambda,b,f_B(a,b),f(a,b))\}\equiv_c\{V_B(\lambda,a,b),Output^\Pi(\lambda,a,b)\} \quad (2)$$

其中,$\equiv_c$ 表示概率多项式时间计算不可区分,忽略不计安全参数λ.这里需要强调的是,$V_A(\lambda,a,b),V_B(\lambda,a,b)$, $Output_A^\Pi(\lambda,a,b),Output_B^\Pi(\lambda,a,b)$ 为相关的随机变量,由相同的随机执行函数定义.特别地, $Output_i^\Pi(\lambda,a,b)$ 完全由 $V_i(\lambda,a,b)$确定.

(确定情况)对一个确定的函数 f,称Π秘密地计算了 f,如果存在概率多项式算法分别标记为 S_A 和 S_B,且使得等式(3)和等式(4)成立.

$$\{S_A(a,f_A(a,b))\}\equiv_c\{V_A(\lambda,a,b)\} \quad (3)$$

$$\{S_B(b,f_B(a,b))\}\equiv_c\{V_B(\lambda,a,b)\} \quad (4)$$

为了简化符号和证明,本文在确定情况下的符号表示省略了安全参数.由于主要考虑确定性函数 f,因此在进行安全性证明时,统一使用等式(3)和等式(4)的符号表示.

模块化顺序组合方法借鉴了文献[26]中安全协议模块化组合技术,通过顺序组合的方式,一个接一个简单地运行多个安全协议,构成了完整的、安全的分类器协议.其思想是:首先,为给定任务设计一个“高级”协议,假设可以安全的执行其他简单的子任务;然后,为简单的子任务设计安全协议;最后,通过在“高级”协议中插入简单的安全协议作为子例程,为给定任务构建一个完整的协议.

定理 1(模块化顺序组合). 设 $f_1,\ldots,f_m$ 和 g 为两方概率多项式函数,假设协议$\rho_1,\ldots,\rho_m$基于半诚实模型分别安全地评估函数 $f_1,\ldots,f_m$,协议Π基于半诚实模型安全地评估函数 g,同时使用子程序调用理想函数 $f_1,\ldots,f_m$.然后从协议Π导出的协议 $\prod^{\rho_1,\ldots,\rho_m}$ 通过替换协议Π的每个子程序调用安全地评估 g,则称 $\prod^{\rho_1,\ldots,\rho_m}$ 在半诚实模型上安全评估了函数 g.

3 面向基本操作的安全协议

3.1 符号描述

在进行面向基本操作的安全协议构造之前,先给出相关符号的描述.安全协议由两方构成,协议双方分别记作 A 和 B.分类器的双方分别记作 C 和 S,C 表示客户端,S 表示服务器.

本文的加密方案有 3 种:QR 表示二次剩余加密方案,Paillier 表示 Paillier 加密方案,FHE 表示全同态加密方案.在实现第 3.2.1 节的比较协议时,使用了 Damgard,Geisler and Krøigaard(DGK)加密方案[27],符号描述见表 1.

Table 1 Notation description

表 1 符号描述

类型	明文空间	密文表示	公钥	私钥
QR	F_2	$[b]$	PK_{QR}	SK_{QR}
Paillier	$\mathbb{Z}_N$	$[\![m]\!]$	PK_P	SK_P
FHE	F_P	$[\![[b]]\!]$	PK_{FHE}	SK_{FHE}
DGK	$\mathbb{Z}_u$	[m]	PK_{DGK}	SK_{DGK}

注:b 表示一个比特位,m 表示整型数据

对于常量 b,$a\leftarrow b$ 表示将 b 赋值给 a.

对于分布 D,$a\leftarrow D$ 表示在分布 D 中随机抽样一个元素 a.

3.2 比较协议

比较协议是构造分类器的安全协议之一,用于比较两个用 Paillier 加密的密文数据,获取 QR 加密的比较结果,比较协议的相关符号描述见表 2.

© 中国科学院软件研究所 http://www.jos.org.cn

Table 2 Comparison protocol

表 2 比较协议

类型	输入 A	输入 B	输出 A	输出 B
1	SK_{DGK},SK_{QR},a	PK_{DGK},PK_{QR},b	–	$[a\leqslant b]$
2	$PK_P,SK_{QR},[\![a]\!],[\![b]\!]$	SK_P,PK_{QR}	–	$[a\leqslant b]$
3	$PK_P,SK_{QR},[\![a]\!],[\![b]\!]$	SK_P,PK_{QR}	$a\leqslant b$	$[a\leqslant b]$

3.2.1 改进的 DGK 比较协议

DGK 比较协议[28]是两方协议,参与方分别记为 A,B,输入分别为整数 a,b,其比特位数相同,输出分别为 δ_A,δ_B.其计算思路是,从最高有效位开始依次比较 a_i,b_i 的值,$c_i=s+a_i-b_i+3\sum_{j=i+1}^{l-1}(a_i\oplus b_i)$ 记录比较结果,其中,$0\leqslant i\leqslant l$,l 表示比特位数,$s=a-2\cdot\delta_B,\delta_B=\{0,1\}$由 B 方随机选取.若 $c_i=0$,则 $\delta_A=1$;否则,$\delta_A=0,\delta_A\oplus\delta_B=(a\leqslant b)$.值得注意的是,在此过程中,$a_i,b_i$ 都是以 DGK 加密的密文形式参与运算.

表 2 的第 1 行是基于 DGK 比较协议的,并对其进行修改以适应 PP-kNN 分类器的应用需求.其目的是比较两个未加密的数据 a 和 b,得出通过 QR 加密的比较结果.本文增加以下操作满足应用需求:(1) A 通过 QR 对 δ_A 进行加密,将加密的 $[\delta_A]$ 发送给 B;(2) B 通过 QR 对 δ_B 进行加密,计算 $[\delta_A]\cdot[\delta_B]$.因为 $[\delta_A]\cdot[\delta_B]\equiv[\delta_A\oplus\delta_B] \bmod N\equiv [a\leqslant b]$,因此通过计算 $[\delta_A]\cdot[\delta_B]$,可得出比较结果 $[a\leqslant b]$.在此过程中,B 没有 QR 私钥,因此无法对 δ_A 进行解密,保证了计算过程中数据的安全性.

3.2.2 加密数据的比较协议

本文的比较协议是两方协议,其中,一方 A 拥有待比较数据 $[\![a]\!],[\![b]\!]$,另一方 B 拥有解密密钥.本文的比较协议是基于 Veugen 比较协议[29]的,并对其进行了修改以适应 PP-kNN 分类器的应用需求.具体修改如下:首先,在 Veugen 的比较协议中调用一个子程序实现两个未加密数据的比较,本文使用表 2 第 1 行的比较协议替换该子程序;然后,将该子程序的两方角色进行置换,即输出方由 A 方置换为 B 方;然后,B 进行计算并将计算结果发送给 A,A 进行解密得到未加密的比较结果.协议 1 是对加密数据比较协议的描述.

比较协议的主要思想是,计算 $x=2^l+b-a$,得到 x 的第 $l+1$ 位(这一位正好对应 2^l)的值:若是 1,则 $a\leqslant b$;否则,$a>b$.本文的假设加密方案是加法同态的,其中,N 表示 Paillier 加密的模量.

协议 1. 加密数据的比较协议.

输入方 A:$[\![a]\!],[\![b]\!],a$ 和 b 的比特长度 l,私钥 SK_{QR},公钥 PK_P.

输入方 B:私钥 SK_P,公钥 PK_{QR},比特长度 l;

输出方 A:$(a\leqslant b)$.

1: A 计算加密数据 $[\![a]\!],[\![b]\!]$,即 $[\![x]\!]\leftarrow[\![b]\!]\cdot[\![2^l]\!]\cdot[\![a]\!]^{-1} \bmod N^2\triangleright x\leftarrow b+2^l-a$

2: A 从数据域 $(0,2^{\lambda+l})\cap\mathbb{Z}$ 中随机选择数 r,即 $r\leftarrow(0,2^{\lambda+l})\cap\mathbb{Z}$

3: A 为 $[\![x]\!]$ 增加噪音 $[\![r]\!]$,即 $[\![z]\!]\leftarrow[\![x]\!]\cdot[\![r]\!] \bmod N^2\triangleright z\leftarrow x+r$

4: A 将 $[\![z]\!]$ 发送给 B

5: B 解密 $[\![z]\!]$

6: A:$c\leftarrow r \bmod 2^l$

7: B: $d\leftarrow z \bmod 2^l$

8: 调用第 3.2.1 节修改的 DGK 比较协议,A,B 作为输入方,输入数据分别为 c,d,B,得到比较结果 $[t']$,其中,$t'=(d<c)$,$[t']$ 是 t' 的密文

9: A 对 r 的第 $l+1$ 位 r_{l+1} 进行加密,将加密的 $[r_{l+1}]$ 值传送给 B

10: B 对 z 的第 $l+1$ 位 z_{l+1} 进行加密,得到 $[z_{l+1}]$

11: B 计算第 $l+1$ 位的值并赋给 $[t]$,即 $[t]\leftarrow[t']\cdot[z_{l+1}]\cdot[r_{l+1}]\triangleright t\leftarrow t'\oplus z_{l+1}\oplus r_{l+1}$

12: B 将 $[t]$ 发送给 A

© 中国科学院软件研究所 http://www.jos.org.cn

13: A 解密$[t]$得到 t

3.2.3 比较协议的正确性分析

协议 1 中,a,b 是 l 位整数,$x=2^l+b-a$ 是 $l+1$ 位整数,$x\div 2^l$ 表示 x 的最高有效位,其运算为 $t=t'\oplus z_{l+1}\oplus r_{l+1}$,当该值等于 1 时,$a\leqslant b$.下面将给出其正确性证明.

证明:x 是 $l+1$ 位整数,$x\div 2^l$ 表示 x 的最高有效位,即第 $l+1$ 位的值,此时有:

$$x=2^l(x\div 2^l)+(x \bmod 2^l).$$

其中,$0\leqslant x \bmod 2^l\leqslant 2^l$.

因为 $z=x+r$,所以有:

$$z=2^l(z\div 2^l)+(z \bmod 2^l)=2^l((x\div 2^l)+(r\div 2^l))+((x \bmod 2^l)+(r \bmod 2^l)).$$

当$(x \bmod 2^l)+(r \bmod 2^l)<2^l$时,有:

$$z\div 2^l=(x\div 2^l)+(r\div 2^l) \tag{5}$$

当$(x \bmod 2^l)+(r \bmod 2^l)\geqslant 2^l$时,有:

$$z\div 2^l=(x\div 2^l)+(r\div 2^l)+1 \tag{6}$$

将公式(5)、公式(6)整合可得:

$$z\div 2^l=(x\div 2^l)+(r\div 2^l)+t'.$$

则 $t'=0\Leftrightarrow(x \bmod 2^l)+(r \bmod 2^l)<2^l$,即

- 当 $t'=0$ 时,$z \bmod 2^l=(x \bmod 2^l)+(r \bmod 2^l)$;
- 当 $t'\neq 0$ 时,$z \bmod 2^l=(x \bmod 2^l)+(r \bmod 2^l)-2^l$.

因此,$t'=0\Leftrightarrow z \bmod 2^l=(x \bmod 2^l)+(r \bmod 2^l)\Leftrightarrow z \bmod 2^l\geqslant r \bmod 2^l\Leftrightarrow d\geqslant c$.

因为 $x\div 2^l$ 的值非 0 即 1,所以有 $x\div 2^l=(z\div 2^l)-(r\div 2^l)-t' \bmod 2=z_{l+1}\oplus r_{l+1}\oplus t'$. □

综上所述,x 的最高有效位可以通过 $z_{l+1}\oplus r_{l+1}\oplus t'$正确计算,因此本文的比较协议是正确的.

3.2.4 比较协议在半诚实模型下的安全性分析

假设加密位$[t']$是通过理想计算得到的.本节分析比较协议在半诚实模型下的安全性,并使用模块化顺序组合定理(定理 1)得出结论.

A 方的元组表示为 $V_A=([\![a]\!],[\![b]\!],l,SK_{QR},PK_P;r,coins,[t])$,其中,$coins$ 为加密 $2^l,r,r_{l+1}$ 的随机数,给定$([\![a]\!],[\![b]\!],l,SK_{QR},PK_P,a\leqslant b)$,模拟器 S_A 的构建过程如下.

Step 1. 计算$[\tilde{t}]$,其为$(a\leqslant b)$在 QR 下的加密比特位.

Step 2. 选择 $\tilde{r}\leftarrow(0,2^{\lambda+l})\cap\mathbb{Z}$.

Step 3. 令 $\widetilde{coins}$ 为两个 Paillier 加密和一个 QR 加密的随机硬币值.

Step 4. 输出 $V_A=([\![a]\!],[\![b]\!],l,SK_{QR},PK_P;\tilde{r},coins,[\tilde{t}])$.

元组 $V_A([\![a]\!],[\![b]\!],l,SK_{QR},PK_{QR},SK_P,PK_P)$和 $S_A([\![a]\!],[\![b]\!],SK_{QR},PK_P,a\leqslant b)$的分布是相同的,因为这两种情景下的随机值取值相同且 QR 加密的是同一比特位.

B 方元组表示为 $V_B(PK_{QR},SK_P,l,[\![z]\!];coins;[\tilde{t}],[r_i])$, 其中,$coins$ 为加密 z_{l+1} 的随机数,则模拟器 $S_B(PK_{QR},SK_P,l)$的构造过程如下.

Step 1. 选择 $\tilde{z}\leftarrow(0,2^{\lambda+l})\cap\mathbb{Z}$.

Step 2. 在用 Paillier 加密 $\tilde{z}:[\![\tilde{z}]\!]$.

Step 3. 生成 QR 加密的两个随机比特值 $[\tilde{t}']$ 和 $[\tilde{r}_{l+1}]$.

Step 4. 令 $\widetilde{coins}$ 为一个 QR 加密的随机硬币值.

Step 5. 输出 $(PK_{QR},SK_P,l,[\![\tilde{z}]\!];\widetilde{coins};[\tilde{t}'],[\tilde{r}_{l+1}])$.

随机变量 $coins$ 和 $\widetilde{coins}$ 生成方式相同且与其他参数独立,因此,

$$(PK_{QR},SK_P,l,[\![\tilde{z}]\!];\widetilde{coins};[\tilde{t}'],[\tilde{r}_{l+1}])=(PK_{QR},SK_P,l,[\![\tilde{z}]\!];coins;[\tilde{t}'],[\tilde{r}_{l+1}]).$$

© 中国科学院软件研究所 http://www.jos.org.cn

从第 3.2.2 节加密数据比较协议可知,$z=x+r \bmod N$,其中,x 为 l 位整数,r 为 $\lambda+l$ 位整数.

因为本文的 $\lambda+l+1<\log_2^N$, 所以有 $z=x+r$.在统计学中,z 和 $\tilde{z}$ 的区分度不大,因此有 $(SK_P,[\![\tilde{z}]\!])\equiv_s(SK_P,[\![z]\!])$;又 z 和 $\tilde{z}$ 的分布是独立于 $\tilde{t}'$ 和 $\tilde{r}_{l+1}$ 的,所以有:

$$(PK_{QR},SK_P,l,[\![\tilde{z}]\!];coins;[\tilde{t}'],[\tilde{r}_{l+1}])\equiv_s(PK_{QR},SK_P,l,[\![z]\!];coins;[\tilde{t}'],[\tilde{r}_{l+1}]).$$

因为 QR 是语义安全的,因此有:

$$(PK_{QR},SK_P,l,[\![z]\!];coins;[\tilde{t}'],[\tilde{r}_{l+1}])\equiv_c(PK_{QR},SK_P,l,[\![z]\!];coins;[t'],[\tilde{r}_{l+1}]),$$

$$S_B(PK_{QR},SK_P,l)\equiv_c V_B([\![a]\!],[\![b]\!],l,SK_{QR},PK_{QR},SK_P,PK_P).$$

本文使用模块化顺序组合来实现协议执行过程中的安全性衔接,使用改进的 DGK 协议取代了理想计算得到的$[t']$,使用定理 1 证明了其在半诚实模型下的安全性.综上所述,本文的比较协议在半诚实模型下是安全的.

3.3 点积协议

本文通过欧式距离计算测试样本与训练样本之间的距离.为了保证 PP-kNN 分类器中距离计算的安全性,本文设计了点积协议.

协议处理的是密文数据,所有操作皆在密文空间进行.它由 A 和 B 两方参与:A 表示客户端,输入测试样本,记作 x;B 表示服务器,输入训练样本,记作 y.协议 2 是点积协议的具体描述.

协议 2. 点积协议.

输入方 A:$x=(x_1,\ldots,x_d)\in\mathbb{Z}^d$,公钥 PK_{FHE}.

输入方 B:$y=(y_1,\ldots,y_d)\in\mathbb{Z}^d$,私钥 SK_{FHE}.

输出方 A:$[\![[v]]\!]$.

1: B 对向量 $y_1,\ldots,y_d$ 进行加密,然后将加密后的数据$[\![[y]]\!]$发送给 A

2: A 对向量 $x_1,\ldots,x_d$ 进行加密,得到加密数据$[\![[x]]\!]$

3: A 计算$[\![z]\!]\leftarrow[\![y]\!]\cdot[\![x]\!]^{-1} \bmod N^2\triangleright z=y-x$

4: A 计算 $[\![[v]]\!]\leftarrow\prod_i[\![[z]]\!]^{[\![z]\!]}$,然后输出加密的 $[\![[v]]\!]\triangleright v=\sum z_i^2$

协议 2 在半诚实模型下的安全性:在本协议中,B 未接收任何信息,仅提供了数据及用于加密的随机数,则模拟器 S_B 可表示为 $S_B(y,SK_{FHE})=(y,SK_{FHE};coins)=V_B(x,y,SK_{FHE},PK_{FHE})$,其中,$coins$ 为 B 方生成的随机数.A 的元组表示为 $V_A(x,PK_{FHE};r^A;[\![z_1]\!],\ldots,[\![z_n]\!])$,模拟器 S_A 的构造过程如下.

Step 1. 生成 n 个 FHE 加密的 0:$c_n,\ldots,c_0$.

Step 2. 生成随机数 $\widetilde{coins}$.

Step 3. 输出 $(x,PK_{FHE};\widetilde{coins};(c_n,...,c_0))$.

$coins$ 和 $\widetilde{coins}$ 的分布相同,因此,

$$\{(x,PK_{FHE};\widetilde{coins};(c_n,..,c_0));[\![[\langle z,z\rangle]]\!]\}\equiv_c\{(x,PK_{FHE};coins;(c_n,..,c_0));[\![[\langle z,z\rangle]]\!]\}.$$

由于 FHE 加密方案的语义安全,所以有:

$$\{(x,PK_{FHE};coins;(c_n,\ldots,c_0));[\![[\langle z,z\rangle]]\!]\}\equiv_c\{(x,PK_{FHE};coins;[\![[z_1]]\!],\ldots,[\![[z_n]]\!]);[\![[v]]\!]\}.$$

函数 f 满足 $f(x,y,SK_{FHE},PK_{FHE})=([\![[\langle z,z\rangle]]\!],\varnothing)$时,有:

$$\{S_A(x,PK_{FHE},[\![[v]]\!]);f(x,y,SK_{FHE},PK_{FHE})\}\equiv_c\{V_A(x,y,SK_{FHE},PK_{FHE});Output(x,y,SK_{FHE},PK_{FHE})\}.$$

本协议中,B 将加密好的数据$[\![[y]]\!]$发送给 A,A 没有私钥无法对其解密,保证了数据的安全性.加密方案是加法与乘法同态的,因此密文数据计算过程是安全且同态的.上述过程通过定义 1 证明了其在半诚实模型下的安全性.综上所述,本文的点积协议在半诚实模型下是安全的.

3.4 加密方案转换协议

PP-kNN 分类器由点积协议、比较协议通过顺序组合的方式构造而成,点积协议的输入与输出数据是 FHE

© 中国科学院软件研究所 http://www.jos.org.cn

进行加密的密文数据,比较协议的输入数据是 Paillier 进行加密的密文数据.为了保证 PP-kNN 分类器的点积协议和比较协议可以进行模块化顺序组合,本文设计了加密方案转换协议,实现了从一种加密方案到另一种加密方案的转换.协议 3 是加密方案转换协议的描述.

协议 3. 加密方案转换协议.

输入方 A:$[\![c]\!]_1$,公钥 PK_1,PK_2.

输入方 B:密钥 SK_1,SK_2.

输出方 A:$[\![c]\!]_2$.

1: A 均匀随机选择一个数 $r \leftarrow M$

2: A 计算$[\![c']\!]_1 \leftarrow [\![c]\!]_1 \cdot [\![r]\!]_1$ 将$[\![c']\!]_1$ 发送给 B ▷Blind c

3: B 解密后得到 c',用 E_2 重新加密

4: B 将重新加密后的$[\![c']\!]_2$ 发送给 A

5: A 去除噪音$[\![r]\!]_2$ 得到 $[\![c]\!]_2 = [\![c']\!]_2 \cdot [\![r]\!]_2^{-1}$ ▷Blind c

6: A 输出$[\![c]\!]_2$

加密方案转换协议中,E_1,E_2 是两种不同的加密方案,A 通过 E_1 对随机数 r 进行加密,为$[\![c]\!]_1$ 添加噪音$[\![r]\!]_1$,将处理后的$[\![c']\!]_1$ 发送给 B,B 解密后无法获取 c 的真实值,保证了该值在解密-再加密过程中数据的安全性,其中,r 是 A,B 共享,M 表示 E_1 的信息空间.B 通过 E_2 对 c'重新加密,将$[\![c']\!]_2$ 发送给 A,A 去除噪音,得到 E_2 加密的真实值$[\![c]\!]_2$,实现了从加密方案 E_1 到 E_2 的转换.整个加密方案转换过程中,密文噪音并未增加,且中间解密时数据真实值亦无法获取,因此,密文数据在加密转换协议中是安全的.根据本文的应用需求,设置加密方案 E_1 是 FHE,加密方案 E_2 是 Paillier,通过协议 3 实现了从 FHE 向 Paillier 加密方案的转换.

4 PP-kNN 分类器构造及分类过程

4.1 浮点数据处理

本文的加密方案都是对整型数据进行加密,而原始数据中部分为浮点型数据,因此对数据进行处理前,需将浮点型数据转换为整型数据,处理方法是用一个足够大的常量 K 乘以浮点数.下面详细描述浮点数的处理过程:

首先,将浮点数据表示为 IEEE 754 双精度浮点数格式,即 $V=(-1)^s \cdot M \cdot 2^{E-1023}$,其中,$S$ 为符号位占 1 比特,M 为尾数,二进制表示为$(M)_2=1.d$,占 52 比特位,$1 \leqslant M \leqslant 2$,$M$ 可重新表示为

$$M = \frac{M_i'}{2^{52}},$$

其中, $M_i' \in \mathbb{N} \cap [2^{52}, 2^{53})$.

其次,寻找合适的常量 K,使得 K 满足:

$$K \cdot v_i \in \mathbb{N},$$

其中, $v_i = M_i' \cdot 2^{e_i - 52}$.

令 $e^*=\min_i e_i$,$\delta_i=e_i-e^* \geqslant 0$,则

$$v_i = M_i' \cdot 2^{\delta_i} \cdot 2^{e^* - 52}.$$

令 $K = 2^{52-e^*}$, 则

$$K \cdot v_i = M_i' \cdot 2^{\delta_i} \in \mathbb{N}.$$

因此,经过上述计算,可以得出 $K = 2^{52-e^*}$. 值得注意的是,在数据转换过程中,可能会出现空间溢出和精度损失问题,数据转换后可能会对基本操作的精准度产生影响,甚至影响分类结果.针对此类问题,本文给出如下说明.

- 首先,加密方案的明文空间大于 2^{52}, $K = 2^{52-e^*}$, 因此数据转换过程中不存在空间溢出和精度损失.

© 中国科学院软件研究所 http://www.jos.org.cn

- 其次,kNN 分类器具有的基本操作只有加法、乘法和比较,因此对转换后的数据进行操作仍能得到相同的分类结果.
- 最后,在执行加、乘、比较操作时,为确保操作不会造成密文数据的精度丢失,需要设置计算和比较所需的比特位数.以比较协议为例:令 d 表示输入数据 x 的属性个数,则比较时所需的最大比特位数为 $l_{\max}=d+1+(52+\delta^*)$,其中,$\delta^*=\max\ \delta_i$,1 表示类别标识,$52+\delta^*$表示密文数据的二进制位数.因此,比较协议中比较位数必须大于 $l_{\max}$.此外,还要确保 $\log_2^N > l_{\max}+1+\lambda$,其中,$\lambda$为安全系数,$N$ 为 Paillier 加密方案明文空间的模量.为了获得高安全性,设 $\log_2^N \geqslant 1024$, 即$\lambda=100$.

本文训练集和测试集分别用 Y 和 X 表示,其中,x_i 表示第 i 个训练样本,则转换后的数据表示为

训练集 Y:$y_i=\lceil Ky_{ij} \rceil$, 测试集 X:$x_i=\lceil Kx_{ij} \rceil$,

其中,j 表示样本 x_i 的第 j 个特征值.

4.2 PP-kNN分类器的构造过程

本节利用第 3 节的协议来构造 PP-kNN 分类器,构造过程如下.

首先,将训练数据的类型由浮点数转换为整数,使用 FHE 对其加密;其次,通过协议 2 计算测试样本与所有训练样本的欧式距离,结果是 FHE 加密的密文数据.然后,通过协议 3 将结果转换为 Paillier 加密的密文数据,再通过 *get*MIN*n* 得到距离数组中的最小值.其思想为:先将数组中的值两两比较,得到两个中较小的值,将较大的赋值为 0,较小的值的下标记为两者下标中较小方的下标值,所有较小方组成新的数组.然后继续比较新的数组,直到数组个数为 1,该值即为最小值.其比较通过协议 1 实现,每次比较得到一个最小值,然后将最小值重新赋值为最大值.循环 k 次,得出 k 近邻样本.最后,使用第 4.2.1 节中介绍的方法来统计类别个数,得出分类结果.其中,将每个协议看作一个模块,通过模块化顺序组合进行模块衔接,构造 PP-kNN 分类器,使得客户端只能获知最后的分类结果,而不能知道测试样本与训练样本间的距离;使服务器无法获取客户端的输入 x(x 是测试样本的向量表示).

4.2.1 PP-kNN 分类器的近邻样本类别个数统计

计算测试样本 $x=(x_1,\ldots,x_d)$与训练样本 $y_i=(y_{i1},\ldots,y_{id})$的距离 $d(x_i,y_i)$,通过比较进行排序,获取前 k 个训练样本对应的分类标签.

设 $N=\{y_1,\ldots,y_k\}$表示包含 k 个训练样本的数据集,则 x 对应的分类 $c_x=\max_{v\in L}\sum_{y\in N} I(v=Class(c_y))$. 其中,$L=(c_1,\ldots,c_m)$是所有标记的集合,$I(\cdot)$是用来获取 k 个样本所属分类的函数,执行情况如下.

For y in N:

$Class(c_y)$得到样本 y 所属的分类

For v in L:依次与类别标签集 L 比较,若相同,则返回 1;否则,返回 0

If $v=Class(c_y)$:v+=1

Else v+=0

按上述步骤完成对 k 个样本所属分类个数的统计,类别个数最多的分类即为待测样本的预测分类 c_x.

4.2.2 PP-kNN 分类器的分类过程

kNN 分类器由服务器端与客户端两部分组成,其处理的数据是通过 FHE 加密的密文数据,PP-kNN 分类器,其实质是将 kNN 分类器针对明文数据的基本计算用第 3 节中的安全协议替换,使 kNN 分类器在分类过程中对密文数据进行操作,保证数据在分类过程中的安全性与同态性,最后得出分类结果.协议 4 是对 PP-kNN 分类协议的描述.

协议 4. PP-kNN 分类协议.

C 输入:测试样本 $x=(x_1,x_2,\ldots,x_d)\in\mathbb{Z}^d$,公钥 PK_P,PK_{FHE},私钥 SK_{QR}.

S 端输入:私钥 SK_P,SK_{FHE},公钥 PK_{QR},训练集 $D=(y_1,\ldots,y_m)$,标记 $L=(c_1,\ldots,c_m)$,近邻数 k.

C 输出:下标 i,c_i 是 k 个近邻样本中类别个数最多的类.

1: S提供训练集 D,对训练集中的训练样本进行浮点数到整数的类型转换,然后通过 FHE 加密方案对训练

© 中国科学院软件研究所 http://www.jos.org.cn

样本进行加密

2: S 将加密的$[\![D]\!]$和近邻数 k 发送给 C

3: 设样本容量为 m,**for** $1\leqslant i\leqslant m$,C 通过点积协议计算测试样本与训练样本的距离$[\![d(x_i,y_i)]\!]$

其中,$[\![d(x,y_i)]\!]=\sqrt{\sum_{j=1}^{d}([\![x_i]\!]-[\![y_{ij}]\!])^2}$,取结果的平方存放到数组 *dis_fhe* 中

4: C,S 通过加密方案转换协议将 FHE 转换为 Paillier 加密方案,存入 *dis_paillier* 中

5: C: **for** $0\leqslant M<k$:

(1) C 和 S 通过 *get*MIN*n* 获取数组 *dis_paillier* 中的最小值 min,并将其存入队列 queue 中

(2) 将 min 对应的值重新赋值为最大值

6: C 和 S 通过第 5 步得到 k 个近邻样本$[\![d_0]\!][\![d_1]\!]\ldots[\![d_k]\!]$

7: 统计 k 个近邻样本的类别数目,然后得到类别最多的类 c_i

4.2.3 安全性分析

由于点积协议、方案转换协议、比较协议在半诚实模型下是安全的,模块化线性组合在半诚实模型下也是安全的,因此,通过模块化线性组合对点积协议、方案转换协议、比较协议进行组合构造的 PP-kNN 分类器也是安全的.

- 首先,点积协议在半诚实模型下是安全的.在通过点积协议计算测试样本与训练样本间距离时,服务器仅发送加密后的密文数据给客户端,未接收来自客户端的任何输入,保证了客户端输入数据 x 的安全性.客户端不拥有私钥,无法解密来自服务器的输入数据;又因为 FHE 加密方案的加法、乘法同态性,保证计算过程的安全性,因此,距离计算时是安全的.
- 然后,加密方案转换协议在半诚实模型下是安全的.距离数据增加噪音干扰后发送给服务器,保证其解密再加密过程无法获知距离的真实值,因此不会推测出 x 的值;重新加密后,发送回客户端,客户端不具有 Paillier 私钥,无法解密.因此,加密方案转换过程是安全的.
- 最后,比较协议在半诚实模型下是安全的,因此调用比较协议获取最小值的运算过程中数据也是安全的,又因为模块化顺序组合在半诚实模型下是安全的.

综上所述,通过模块化顺序组合将点积协议、加密方案转换协议、比较协议进行组合构造的 PP-kNN 分类器也是安全的.

5 实 验

本文利用自定义加密数据对比较协议和加密方案转换协议进行性能评估,利用 4 种 UCI 数据集[30]对 PP-kNN 分类器的性能进行评估.

测试环境具体描述如下:CPU 为英特尔酷睿 i7 处理器(双核,3.4GHz);内存为 16GB.

实验在相同的网络下进行,因此,本文将一个数据包的往返时间记为 40ms 来模拟网络延迟.加密方案中的密钥长度为 1 024 位,统计安全参数λ=100.

5.1 比较协议的性能评估

首先,针对两种比特长度的加密数据,从客户端、服务器运行时间、交换数据量、交换次数这 4 个方面对比较协议进行了评估,实验结果见表 3.

Table 3 Evaluation of comparison protocol

表 3 比较协议评估

比较比特长度(bit)	客户端(ms)	服务器端(ms)	交换数据量(KB)	交换次数
64	13.15	15.47	27.91	11
128	21.16	23.04	54.91	11

然后,分别对 64 位、128 位、256 位、512 位、1 024 位比较比特长度的加密数据进行评估,如图 1 所示.

© 中国科学院软件研究所 http://www.jos.org.cn

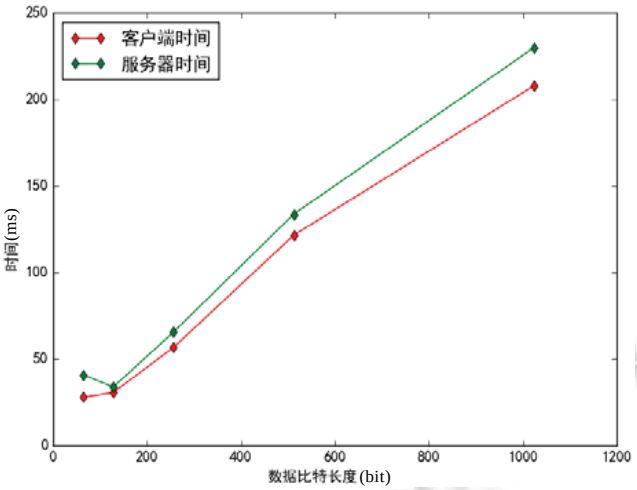

Fig.1 Performance of comparison protocol

图 1 比较协议性能

表 3 的实验结果表明,比较协议的运行时间与比较比特长度有关,比特长度越长,服务器和客户机运行时间越长,交换数据量越多.

5.2 kNN分类器性能评估

本节实验在 Iris、Wine、Zoo、Glass Identification 公共数据集上进行测试.这些数据集是 UCI 标准数据集[30],见表 4.

Table 4 Standard dataset

表 4 标准数据集

数据集	样本数	类别数	特征数	训练集样本数
Iris	150	3	4	69
Wine	178	3	13	66
Glass Identification	180	6	9	114
Zoo	101	7	16	65

测试数据与训练数据都是按一定比例随机进行抽取,各训练样本数见表 4,样本集中剩余样本作为测试集.本实验从客户端和服务端各自的计算、比较时间、交换数据总量及交换次数这几个方面进行评估,具体实验结果见表 5.

Table 5 Performance of PP-kNN classifier based on different test encrypted datasets

表 5 基于不同测试加密数据的 PP-kNN 分类器性能

数据集	k 值	比特位数	客户端(ms)			服务器(ms)			交换数据总量(MB)	交换次数
			距离计算	方案转换	k 近邻求解	距离计算	方案转换	k 近邻求解		
Iris	3	128	5 434.49	529.25	2 261.11	1 250.97	781.24	2 736.46	149.87	2 591
Wine	3	128	15 750.8	691.62	2 090.14	8 480.45	1 306.31	2 685.74	358.42	3 071
Glass	5	128	19 061.5	1 076.83	5 982.34	13 475.2	1 662.19	7 549.04	466.22	7 357
Zoo	3	64	19 394.3	679.93	2 119.72	71 080.7	1 394.69	2 751.55	423.59	3 219

表 5 的实验结果表明,PP-kNN 分类器的运行时间在几秒到几十秒不等,执行时间随着训练样本数与特征数的增加而增加.与贝叶斯分类器、线性分类器不同,kNN 分类器在训练阶段的消耗为 0,其计算全部集中在分类阶段,因此在密文数据处理的速度方面具有一定优势.

© 中国科学院软件研究所 http://www.jos.org.cn

5.3 安全两方工具比较协议评估与对比

PP-kNN 中的基本操作协议都是两方协议,并且支持当前典型两方协议(TASTY[31]、Fairplay[32,33])所支持的全部功能,为了进一步说明 PP-kNN 的性能优势,将本文中的比较协议与 TASTY 进行比对.

本文基于不同比特位数的数据设置相应的比较位数,对 TASTY 安全两方计算工具中的两方比较协议进行了性能测试,实验结果如图 2 所示.TASTY 与本文的比较操作都是基于 Garble 电路的,但 TASTY 的数据传输消耗时间长,本文的数据传送时间较短,因此安全两方比较协议总的运行时间约为 TASTY 的 1/100.综上所述,本文的两方比较协议在性能上有所提高.

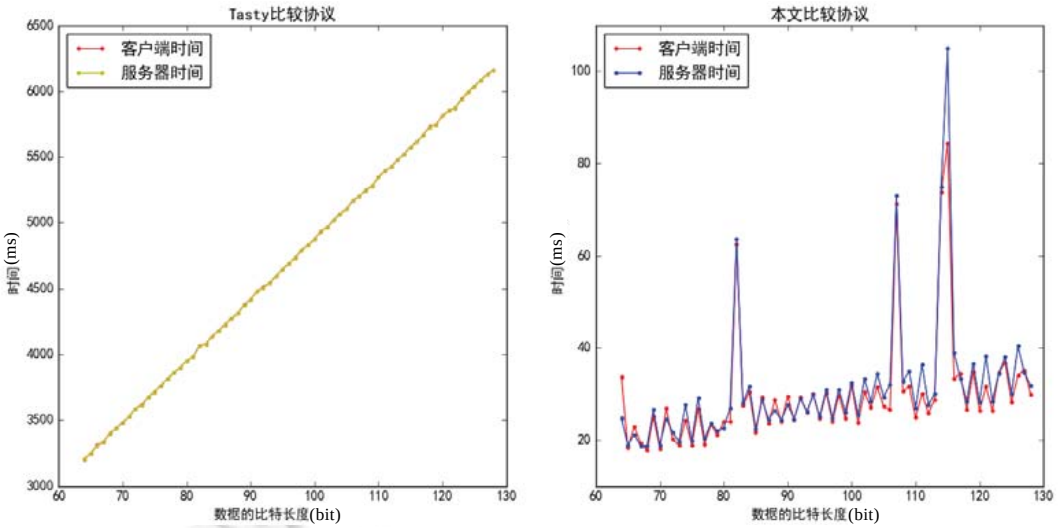

Fig.2 Secure two-party comparison protocol runtime distribution of Tasty and ours

图 2 Tasty 和本文的安全两方比较协议运行时间分布

6 结 论

本文设计了一种支持隐私保护的 kNN 分类器.首先,从 kNN 分类器中提取出了一些基本操作,包括加法、乘法、比较等;其次,选择了两种同态加密方案和一种全同态加密方案对数据进行加密,基于此,设计了针对基本操作的安全协议,并证明了协议在半诚实模型下的安全性;然后,通过将基本操作的安全协议按照模块化顺序组合的方式构造出了 PP-kNN 分类器;最后,在自定义加密数据及 4 种 UCI 标准数据集上,分别对安全协议及所构造的 PP-kNN 分类器进行了性能评估.实验结果表明,本文设计的安全协议是安全且高效的,分类器能够以较高的效率对密文数据进行分类,同时实现了对用户数据的隐私保护.

References:

[1] Fredrikson M, Jha S, Ristenpart T. Model inversion attacks that exploit confidence information and basic countermeasures. In: Proc. of the ACM SIGSAC Conf. on Computer and Communications Security. New York: ACM, 2015. 1322−1333.

[2] Fredrikson M, Lantz E, Jha S, Lin S, Page D, Ristenpart T. Privacy in pharmacogenetics: An end-to-end case study of personalized warfarin dosing. In: Proc. of the USENIX Security Symp. National Center for Biotechnology Information, U.S. National Library of Medicine, 2014. 12−32.

[3] Alotaibi K, Rayward-Smith VJ, Wang WJ, de la Lglesia B. Non-linear dimensionality reduction for privacy-preserving data classification. In: Proc. of the ASE/IEEE Int'l Conf. on Privacy, Security, Risk and Trust. IEEE, 2012. 694−701. [doi: 10.1109/SocialCom-PASSAT.2012.76]

© 中国科学院软件研究所 http://www.jos.org.cn

[4] Agrawal R, Srikant R. Privacy-preserving data mining. In: Proc. of the ACM SIGMOD Int'l Conf. on Management of Data. New York: ACM, 2000. 439−450.

[5] Bayardo RJ, Agrawal R. Data privacy through optimal *k*-anonymization. In: Proc.of the Int'l Conf. on Data Engineering (ICDE). Institute of Electrical and Electronics Engineers Computer Society, 2005. 217−228.

[6] Evfimievski A, Srikant R, Agrawal R, Gehrke J. Privacy preserving mining of association rules. Information Systems, 2004,29(4): 343−364. [doi: 10.1016/j.is.2003.09.001]

[7] Lindell Y, Pinkas B. Privacy preserving data mining. In: Proc. of the Advances in Cryptology-crypto. Springer-Verlag, 2000. 36−54.

[8] Hu HB, Xu JL, Ren CS, Choi BR. Processing private queries over untrusted data cloud through privacy homomorphism. In: Proc. of the IEEE Int'l Conf. on Data Engineering (ICDE). IEEE, 2011. 601−612.

[9] Kantarcıoğlu M, Clifton C. Privately computing a distributed *k*-NN classifier. In: Boulicaut JF, ed. Proc. of the Lecture Notes in Artificial Intelligence. Springer-Verlag, 2004. 279−290.

[10] Xiong L, Chitti S, Liu L. *k* nearest neighbor classification across multiple private databases. In: Proc. of the ACM Int'l Conf. on Information and Knowledge Management (CIKM). New York: Association for Computing Machinery, 2006. 840−841. [doi: 10.1145/1183614.1183757]

[11] Kung SY, Chanyaswad T, Chang JM, Wu PY. Collaborative PCA/DCA learning methods for compressive privacy. ACM Trans. on Embedded Computing Systems, 2017,16(3):1−18. [doi: 10.1145/2996460]

[12] Liu XM, Lu RX, Ma JF, Chen L, Qin BD. Privacy-preserving patient-centric clinical decision support system on Naïve Bayesian classification. IEEE Journal of Biomedical & Health Informatics, 2016,20(2):655−668. [doi: 10.1109/JBHI.2015.2407157]

[13] Jia Q, Guo LK, Jin ZP, Fang YG. Privacy-preserving data classification and similarity evaluation for distributed systems. In: Proc. of the IEEE Int'l Conf. on Distributed Computing Systems. Los Alamitos: IEEE Computer Society, 2016. 690−699. [doi: 10.1109/ICDCS.2016.94]

[14] Ligier D, Carpov S, Fontaine C, Sirdey R. Privacy preserving data classification using inner-product functional encryption. In: Proc. of the Int'l Conf. on Information Systems Security and Privacy. SciTePress, 2017. 423−430.

[15] Du WL, Han YS, Chen SG. Privacy-preserving multivariate statistical analysis: Linear regression and classification. In: Proc. of the SIAM Int'l Conf. on Data Mining. Society for Industrial and Applied Mathematics Publications, 2004. 222−233.

[16] Graepel T, Lauter K, Naehrig M. ML confidential: Machine learning on encrypted data. In: Proc. of the Information Security and Cryptology (ICISC). LNCS 7839, Springer-Verlag, 2013. 1−21. [doi: 10.1007/978-3-642-37682-5_1]

[17] Bos JW, Lauter K, Naehrig M. Private predictive analysis on encrypted medical data. Journal of Biomedical Informatics, 2014,50: 234−243. [doi: 10.1016/j.jbi.2014.04.003]

[18] Barni M, Failla P, Lazzeretti R, Paus A, Sadeghi AR, Schneider T, Kolesnikov V. Efficient privacy-preserving classification of ECG signals. In: Proc. of the IEEE Int'l Workshop on Information Forensics and Security (WIFS). IEEE, 2009. 91−95. [doi: 10.1109/WIFS.2009.5386475]

[19] Barni M, Failla P, Kolesnikov V, Lazzeretti R, Sadeghi AR, Schneider T. Secure evaluation of private linear branching programs with medical applications. Computer Security (ESORICS), 2009,5789:424−439.

[20] Barni M, Failla P, Lazzeretti R, Sadeghi AR, Schneider T. Privacy-preserving ECG classification with branching programs and neural networks. IEEE Trans. on Information Forensics & Security, 2011,6(2):452−468. [doi: 10.1109/TIFS.2011.2108650]

[21] GUL KSQ, Yin JZ, Pan LM, *et al*. Research on the algorithm of named entity recognition based on deep neural network. Information and Network Security, 2017,(10):29−35 (in Chinese with English abstract). [doi: 10.3969/j.issn.1671-1122.2017.10.005]

[22] Goldwasser S, Micali S. Probabilistic encryption and how to play mental poker keeping secret all partial information. In: Proc. of the ACM Symp. on Theory of Computing. Association for Computing Machinery, 1982. 365−377.

[23] Paillier P. Public-key cryptosystems based on composite degree residuosity classes. In: Proc of the Int'l Conf. on the Theory and Application of Cryptographic Techniques. Springer-Verlag, 1999. 223−238. [doi: 10.1007/3-540-48910-X_16]

[24] Halevi S, Shoup V. Algorithms in HElib. In: Proc. of the Advances in Cryptology-Crypto. LNCS 8616, Springer-Verlag, 2014. 554−571. [doi: 10.1007/978-3-662-44371-2_31]

© 中国科学院软件研究所 http://www.jos.org.cn

[25] Goldreich O. The Foundations of Cryptography—Volume 2, Basic Applications. Cambridge University Press, 2004.

[26] Canetti R. Security and composition of multi-party cryptographic protocols. Journal of Cryptology, 2000,13(1):143−202.

[27] Damgard I, Geisler M, Kroigard M. Homomorphic encryption and secure comparison. Int'l Journal of Applied Cryptography, 2008, 1(1):22−31. [doi: 10.1504/IJACT.2008.017048]

[28] Veugen T. Improving the DGK comparison protocol. In: Proc. of the IEEE Int'l Workshop on Information Forensics and Security. IEEE, 2012. 49−54.

[29] Veugen T. Comparing encrypted data. 2011. http://siplab.tudelft.nl/sites/default/files/Comparing%20encrypted%20data.pdf

[30] 2017. http://archive.ics.uci.edu/ml/datasets.html

[31] Henecka W, Kögl S, Sadeghi AR, Schneider T, Wehrenberg I. Tasty: Tool for automating secure two-party computations. In: Proc. of the ACM Conf. on Computer and Communications Security (CCS). Association for Computing Machinery, 2010. 451−462. [doi: 10.1145/1866307.1866358]

[32] Malkhi D, Nisan N, Pinkas B, Sella Y. Fairplay—A secure two-party computation system. In: Proc. of the Usenix Security Symp. Berkeley: USENIX Association, 2004. 287−302.

[33] Ben-David A, Nisan N, Pinkas B. Fairplaymp: A system for secure multi-party computation. In: Proc. of the ACM Conf. on Computer and Communications Security. ACM, 2008. 257−266.

附中文参考文献:

[21] GUL KSQ,尹继泽,潘丽敏,等.基于深度神经网络的命名实体识别方法研究.信息网络安全,2017,(10):29−35. [doi: 10.3969/j.issn.1671-1122.2017.10.005]

徐剑(1978－),男,山东胶南人,博士,副教授,CCF 专业会员,主要研究领域为网络与信息安全,云计算安全,机器学习与隐私保护.

毕猛(1982－),男,博士,工程师,主要研究领域为网络与信息安全.

王安迪(1996－),女,硕士生,CCF 学生会员,主要研究领域为机器学习,隐私保护.

周福才(1964－),男,博士,教授,博士生导师,CCF 高级会员,主要研究领域为网络与信息安全,可信计算,电子商务基础理论及关键技术.

© 中国科学院软件研究所 http://www.jos.org.cn