同态加密在加密机器学习中的应用研究综述

崔建京 龙 军 闵尔学 于 洋 殷建平
(国防科学技术大学计算机学院 长沙 410073)

摘 要 现有的机器学习算法不能对加密后的数据进行分析计算,而很多领域如医疗、金融等又要求数据保持机密性和安全性,这促进了加密机器学习的产生和发展。同态加密技术是解决这一问题的主要思路,它可以保证在不解密的情况下对密文进行计算,使得解密后的结果与对明文执行相同计算得到的结果相同。文中对同态加密在加密机器学习中的相关应用研究进行了综述,主要介绍了目前用同态加密实现加密机器学习的3种算法(加密神经网络、加密k-NN、加密决策树和完全随机森林),并从正确性、安全性、执行效率方面分析了方案设计,总结并对比了不同加密机器学习算法的构造思路,指出了同态加密用于加密机器学习的关键问题和进一步研究需要关注的内容,为同态加密和加密机器学习提供参考。

关键词 同态加密,加密机器学习,隐私保护数据挖掘

中图法分类号 TP181 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2018.04.006

Survey on Application of Homomorphic Encryption in Encrypted Machine Learning

CUI Jian-jing LONG Jun MIN Er-xue YU Yang YIN Jian-ping
(College of Computer, National University of Defense Technology, Changsha 410073, China)

Abstract Nowadays, the existing machine learning algorithms can not analyze and calculate the encrypted data, at the same time, many areas (such as medical industry, financial industry) strongly require data to keep private and secure while analyzed and calculated by untrusted person or company. All these lead to the generation and development of encrypted machine learning. Homomorphic encryption is the primary idea of solving this problem by ensuring that calculations on the cipher text without decrypting, which can result in the same result of the same calculations on the plain text. This paper conducted a survey on application of homomorphic encryption in encrypted machine learning. This work mainly introduced three kinds of algorithms (encrypted neural network, encrypted K-nearest Neighbor, encrypted decision tree and completely random forest) which are used to realize encrypted machine learning with homomorphic encryption, and also analyzed the scheme design from the aspects of correctness, security and efficiency. This paper summarized the construction of different encrypted machine learning algorithms, pointed out the key problems of homomorphic encryption for encrypted machine learning and the content that needs to be focused on in further studies, and provided some referen-ces for homomorphic encryption and encrypted machine learning.

Keywords Homomorphic encryption, Encrypted machine learning, Privacy preserving data mining

当今机器学习持续火热,各大研究领域都试图用机器学习算法来实现人工智能。例如,用于图像识别的深度学习框架,用于多实例学习(MIL)分类的分层极限学习机[1],用于集成多源信息预测的多核学习算法[2],用于图像补全的生成对抗网络(GAN)等。但是,现有的机器学习算法没有考虑到应用过程中数据的隐私性和安全性。传统的加密方法可以保证数据在长期存储中的安全性,但一旦要进行分析计算,就必须先解密。数据的隐私处理将会出现在现代数据分析的诸多领域,例如即将到来的"智能穿戴时代"、智能手表及智能眼镜等会产生大量的个人生物医学数据;云计算的出现使得许多数据的所有者开始寻求外包存储计算,由于医疗、金融等领域对数据有较高的安全性要求,因此云端需要对隐私数据进行存储和分析计算等。数据分析中的安全问题不容忽视,加密机器学习的概念由此诞生。

加密机器学习是指在加密数据上实现机器学习任务,如分类和聚类等。由于涉及到密文的操作,理想的情况是对密文的处理结果与明文一致,这与同态加密的思想不谋而合,因此同态加密是实现加密机器学习的主要思路。

Rivest等于1978年最早提出了同态加密[3]的概念:同态加密是一种加密形式,允许用户直接对密文进行特定的代数

到稿日期:2017-05-11 返修日期:2017-08-23 本文受国家自然科学基金项目(61105050)资助。

崔建京(1994-),男,硕士,主要研究方向为网络安全、机器学习;龙 军(1978-),男,副教授,主要研究方向为机器学习、信息安全,E-mail:junlong@nudt.edu.cn(通信作者);闵尔学(1994-),男,硕士,主要研究方向为机器学习、大数据、流量分析等;于 洋(1992-),女,硕士,主要研究方向为机器学习与网络安全;殷建平(1963-),男,教授,主要研究方向为人工智能、网络算法和信息安全。

运算，得到的数据仍是加密的结果，且与对明文进行同样的操作再将结果加密一样。同态加密若只支持加法运算，就是加法同态加密；若只支持乘法运算，就是乘法同态加密；若同时支持加法和乘法运算，就为全同态加密。然而，直到 2009 年，Gentry 才从数学上提出了基于理想格的全同态加密方案[4]，这是同态密码学上的一个里程碑。

虽然理论上的全同态加密可以进行任意计算，但现在提出的实际方案仍然有许多约束，例如只支持整数类型的数据[5-6]；需要固定乘法深度，不能无限进行加法和乘法运算[7]；以及全同态加密不支持比较和取最大值等运算。因此，加密机器学习不能简单地套用现有的同态加密方案，目前有两种常见的策略：1）借助安全多方计算构造适合基于同态加密的加密机器学习算法的协议，通过执行协议来完成算法（以下简称多方计算）；2）寻求原有机器学习算法的近似算法，使其在不依赖交互方案的条件下，仍可以满足同态加密方案的数据及运算要求（以下简称算法近似）。

安全多方计算（Secure Multi-party Computation，SMC）起源于姚期智的百万富翁比较问题，主要研究如何解决一组互不信任的参与方之间保护隐私的协同计算问题。SMC 要确保输入的独立性和计算的正确性，同时不泄露各输入值给参与计算的其他成员[8]。因此，SMC 可以作为实现基于同态加密的加密机器学习的一种手段。

本文对同态加密在加密机器学习中的应用研究进行了调研，指出了当前应用的优缺点，并提出了下一步的发展设想。本文第 1 节介绍加密神经网络的研究现状，并分别选取了多方计算和算法近似两种策略的代表性方法进行简要介绍；第 2 节介绍加密 k-NN 算法的研究现状，并对多方计算策略的代表性方法进行简要介绍；第 3 节介绍加密决策树和完全随机森林的研究现状，并简要介绍一种多方计算的加密决策树和一种算法近似的完全随机森林；第 4 节列举了其他机器学习算法使用同态加密的研究现状；最后总结并分析了多方计算和算法近似两种策略的优缺点，提出了当前研究的主要问题，并展望了未来的研究方向。

1　加密神经网络

1.1　研究进展

人工神经网络（Artificial Neural Networks，ANN）系统是 20 世纪 40 年代后出现的。它由众多的神经元可调的连接权值连接而成，具有大规模并行处理、分布式信息存储、良好的自组织与自学习能力等特点。近年来，神经网络模型在优化、信号处理与模式识别等许多领域都有着出色的表现。考虑到数据的隐私性和安全性，研究人员提出了加密神经网络的概念。

加密神经网络，就是在密文上进行训练或测试的神经网络模型。将同态加密用于加密神经网络的工作有：Barni 等[9]提出了利用多方计算技术来实现神经网络处理安全数据的问题；Orlandi 等[10]提出了利用同态加密技术和多方计算方案来解决神经网络进行安全数据处理的问题，而且考虑到了神经网络本身也需要保护的情况；Barni 等[11]提出了使用同态加密神经网络做 ECG（心电图）分类的多方计算协议方案；Dowlin 等[12]提出了一种可应用于加密数据的近似神经网络 CryptoNets，并在 MNIST 手写识别数据集上做了测试，取得了 99% 的准确率和单台 PC 机每小时超过 51000 次预测的成果。

1.2　方案构造

1.2.1　多方计算典型方案构造

Orlandi 等[10]使用典型的双方计算结构来实现他们的加密神经网络，下面做简单介绍。

（1）加密方案

采用 Paillier 提出的同态和概率加密方案[13]，后来由 Damgård 和 Jurik[14]进行了修改。Paillier 密码系统基于判定合数剩余问题，支持任意多次的加法同态操作。

（2）神经网络的构造

1）阈值函数

由于同态加密方案不能进行比较运算，因此使用了如下方法：

$$E_{pk}(\langle x,w\rangle-\delta)\sim E_{pk}(a(\langle x,w\rangle-\delta))$$

其中，x 是输入，w 是权值，δ 是阈值，$\sim$ 代表左右两项具有相同的明文，$a>0$。

这样，数据拥有方就可以对结果进行解密。若 $a(\langle x,w\rangle-\delta)>0$，则表明超过了阈值；反之则在阈值内。

2）sigmoid 函数

sigmoid 函数的形式为：$\sigma(y,\alpha)=\frac{1}{1+e^{-\alpha y}}$。注意到，sigmoid 函数实际上只与 y 和 α 有关，将其简记为 $\sigma(y,\alpha)$。因此，计算方计算 $E_{pk}(y)^a\sim E_{pk}(\alpha y)$，然后数据拥有方再计算 $\sigma(y,\alpha)$，从而得到正确的结果。

同时，为了隐藏网络拓扑，要求计算方随机地向神经网络的隐藏层添加一些假神经元来模糊数据拥有者的认知。这些假神经元的权重应设为 0，以免对计算结果造成影响。

1.2.2　算法近似典型方案构造

Dowlin 等[12]于 2016 年提出的 CryptoNets 神经网络模型，使用了 Bos 等于 2013 年提出的同态加密方案[15]。该方案是一种全同态加密方案，允许加法和乘法加密消息，但是需要指定目标数据的运算电路复杂度。换句话说，该密码系统允许计算加密数据上固定的最大次数的多项式函数。

（1）加密方案

Bos 等[15]加密的原理是将明文从环 R_t^n 映射到环 R_q^n，其中，$R_t^n:=Z_t[x]/(x^n+1)$，$R_q^n:=Z_q[x]/(x^n+1)$；解密则是从环 R_q^n 映射到环 R_t^n 上，其中在加密过程中添加了随机扰动来增强安全性。

（2）编码方案

由于神经网络中的参数多为实数，与同态加密方案中的 R_t^n 上的多项式不匹配，因此需要先对原始数据进行编码才能进行加密。编码方案应该以保持加法和乘法运算的方式将数据从实数域映射到环 R_t^n 上。Brakerski 等[5]使用的方法是将固定精度的数字编码为常数多项式。

（3）神经网络构建

Dowlin 等[12]搭建的神经网络有两种：训练用神经网络和简化版神经网络。后者仅用于预测。训练用神经网络有 9

层，简化版有 5 层，如表 1 所列。

表 1 两种神经网络结构的比较

Table 1 Comparison of two neural network sturctures

	训练用神经网络	简化神经网络
1	卷积层	卷积层
2	平方激活层	平方激活层
3	池化层	线性池化层
4	卷积层	
5	池化层	
6	全连接层	
7	平方激活层	平方激活层
8	全连接层	输出层
9	sigmoid 激活函数层	

其中，3－6 层进行的都是线性操作，因此可以视为矩阵乘法，并组合成一层，而因为神经网络的预测由其输出向量的最大值的指标给出，最后一层的 sigmoid 函数是单调递增的，因此在训练完成、权值固定后可以将其丢弃。这样，简化后的神经网络就只剩下 5 层。

1.3 方案分析

1.3.1 多方计算典型方案分析

(1)正确性

首先，Goldreich[16]已经证明，对于任何多项式函数，都有一个安全的多方计算解决方案。这里的加密方案的正确性由 Paillier 密码系统[13]保证。在神经网络的构建中，将同态加密无法计算的非线性函数和 sigmoid 函数都进行了协议交互，使得计算结果与未加密时一致，因此方案是正确的。

(2)安全性

Paillier 密码系统[13]基于判定合数剩余问题。数论上定义 $z\in\mathbb{Z}_{n^2}^*$ 是模 n^2 的第 n 个剩余是指，存在 $y\in\mathbb{Z}_{n^2}^*$ 满足 $z=y^n \bmod n^2$。这个问题在密码学界被认为是计算困难的，与大整数质因子分解的难度相当。

同时，方案使用的假神经元对网络拓扑起到了模糊的效果，这使得数据拥有者无法窥探计算方的神经网络结构，对计算方的知识模型起到了保护的作用。

(3)执行效率

Orlandi 等[10]提出的加密神经网络由 5 层共 15 个神经元组成，它们被部署在两台中档笔记本电脑上，整个预测过程仅耗时 11.7 s，其中服务器端耗时 9.3 s，通信的内存开销仅为 76kb，效率很高。

1.3.2 算法近似的典型方案分析

(1)正确性

1)加密方案的正确性：Bos 等[15]提出的加密方案基于环带误差学习(R-LWE)假设，已被证明满足加法和乘法同态性，是理论正确的全同态加密方案。

2)在构建神经网络时，Dowlin 等[12]使用平方激活函数 $sqr(z):=z^2$ 来代替原有的 sigmoid 和 ReLu 函数，这是因为理论上可以用低次多项式来近似这些非线性函数(Livni 等[17])。

(2)安全性

Dowlin 等[12]使用了 Bos 等的加密方案[15]。方案的构造依赖于同态加密经典的环带误差学习(R-LWE)的假设，其安全性可以归约到一般格上的标准困难问题，属于第二代全同态加密方案。该方案还提出了 The Decisional Small Polynomial Ratio(DSPR)问题，Bos 等[15]证明了 DSPR 问题在特定条件下也是计算困难的。

(3)执行效率

在大数编码过程中，可以使用中国剩余定理(CRT)将一个系数为大数的多项式转化为 k 个多项式，也可以将 n 个值编码成单个多项式，对该多项式进行操作，并解码出 n 个不同的结果。这样，就可以使用单指令多数据操作技术(SIMD)来提高速度。Dowlin 等[12]的实验表明，对一张 28×28 像素图片的编码及加密平均可以在 0.060 s 内完成，解码及解密平均可以在 0.046 s 内完成。因此，算法的执行效率较高。

1.3.3 两种典型方案的对比分析

对于实际效果，两种方案都有不错的表现：Orlandi 等[10]使用了 UCI 机器学习数据库中的数据集，用标准反向传播算法训练了具有 12 个隐藏神经元和 sigmoid 激活函数的 NN，在训练集上获得了 99.8% 的准确度，在测试集上获得了 84.7% 的准确度；Dowlin 等[12]在 MNIST 手写识别数据集上做了测试，并取得了 99% 的准确率。

从安全性上考虑，同态加密安全计算的协议有一个明显的弱点，即延展性攻击。延展性攻击是指，若存在恶意的竞争者获取到了处理数据方的公钥，则他可以用相同的方式对数据进行随机噪声扰动，从而使得计算无意义或使得数据发送方无法分辨接收到的是正确的结果还是攻击者的干扰。除了使用安全通道传输外，是否可以从同态加密方案的构造上预防这种威胁呢？算法近似可以一定程度上避免这个问题。

从执行效率上讲，两种方案都很高效，但算法近似的方案还有许多问题没有解决：有无更高效的编码方案？如果对大数据进行编码和训练，操作时间将会显著增加，除了使用高性能的 GPU 和 FPGA 外，能否从算法上进行改进？这些都有待进一步研究。

2 加密 k-NN 算法

2.1 研究进展

k-NN 算法(k-最近邻)适用的问题类型为：给定查询对象 q 和查询参数 k，k-NN 查询从数据集 S 中检索 k 个对象，该对象在某些距离函数 d 下与 q 最相似。令所得的 k-NN 集合为 $N_k(q)$，所有对象的集合为 o。Qi 等[18]给出了如下 k-NN 算法的形式化定义。

定义 1(k-NN 算法) 给定数据集 S、查询对象 $q\in o$ 和查询参数 k，k-NN 算法返回集合 $N_k(q)\subseteq S$，集合的势为 k，且：

$$\forall o\in N_k(q),\forall \hat{o}\in S:\hat{o}\notin N_k(q)\Rightarrow d(o,q)\leqslant d(\hat{o},q)$$

处理加密 k-NN 问题的相关研究有：Zhan 等[19]提出了一种用于多方通信的加密 k-NN 分类的协议；Qi 等[18]给出了一种在仅有通信双方的条件下实现加密 k-NN 搜索的协议，这个协议可以保证通信的双方协同计算 k-NN 算法，而不会泄露彼此的私有数据；同年，Kumar 等[20]提出了加密最近邻算法，利用同态加密技术在数据用户终端对私有数据进行加密，其中训练样本中的数据是加密后的数据，但在计算过程中需要可信第三方参与；Zhu[21]提出了基于同态加密和 EIGamal

加密系统的加密 k-NN 分类挖掘方法，在计算 k-NN 时利用同态加密技术来保证数据的隐私性；Utsunomiya 等[22]提出了用于划分 POI 表（用户附近兴趣点）的轻量级私有循环查询协议和相应的加密 k-NN 搜索的部分同态加密方案，其在减少计算和通信成本的同时，保持了高安全性和高精度。

2.2　典型方案构造

加密 k-NN 算法的研究主要集中于使用多方计算框架。这里介绍 Zhan 等使用的协议[19]，该协议可以满足如下要求：每个计算方拥有所有实例的数据集，但每个计算方的特征集互不相同，且不被任何其他计算方了解，所有计算方都参与加密并计算出需要的 k-NN 分类器。他们也使用 Paillier 的同态加密方案[13]对各方的私有数据进行加密。协议中使用的同态加密函数具有以下特殊性质：

$$e(a_1)\times e(a_2)=e(a_1+a_2)$$

其中，e 是加密函数，a_1 和 a_2 是需要加密的数据。

不失一般性，假设计算方 P_l 有第 i 个训练实例的隐私距离数据 s_{il}（$i\in[1,N]$，$l\in[1,n]$）。Barni 等[11]给出了如下安全计算协议。

第一步　对每个 $i\in[1,N]$，计算 $e(\sum_{l=1}^{n}s_{il})$。

（1）P_n 生成密钥并发布，P_l 生成 N 个随机数 r_{il}，$l\in[1,n]$；

（2）前向传播：每个 P_l 生成 $e(s_{il}+r_{il})$，并向后传递；

（3）反向传播：每个 P_l 生成 $e(-r_{il})$，并向前传递。

第二步　计算 $e(\sum_{l=1}^{n}-s_{jl})$，$j\in[1,N]$。

具体步骤与第一步类似，这里不再赘述。

第三步　计算 k 个最近的“邻居”。

P_{n-1} 计算 $e(\sum_{l=1}^{n}s_{il})\times e(\sum_{l=1}^{n}-s_{jl})=e(\sum_{l=1}^{n}s_{il}-\sum_{l=1}^{n}s_{jl})$，其中 $i\in[1,N]$，$j\in[1,N]$，并将结果存储到队列 ϕ 中；ϕ 经过随机换位后传递给 P_n，P_n 按符号函数（大于或等于 0 时为+1，否则为−1）对其进行编码后返回 P_{n-1}，最后由 P_{n-1} 计算出 k 个最小的元素。这 k 个元素就是给定查询元素 x_q 的 k 个最近邻。

2.3　典型方案分析

（1）正确性

决定协议正确性的关键在于第三步中 P_{n-1} 是否正确找到了给定查询元素 x_q 的 k 个最近邻。

在 P_n 用符号函数编码后，P_{n-1} 通过计算每个元素在 ϕ''' 中的值并求和，将求和结果作为距离度量权重，就可以得出 k 个最小值，即 k 个最近邻。求和结果越小，代表两个类间的距离越“近”；求和结果越大，代表两个类间的距离越“远”。

（2）安全性

Zhan 等[19]证明了该协议可以经受几个恶意计算方的合伙破解而仍然保持数据是安全的。具体来说，如果恶意团队通过合作（共享数据和解密密钥）已经得到了没有乱序的 $\sum_{l=1}^{n}s_{il}-\sum_{l=1}^{n}s_{jl}$，为了准确地得到某个具体的 s_{il} 或 s_{jl}（$l\in[1,n-2]$），必须要知道其余 $n-2$ 个距离的值。因此，只要有一个计算方没有参与恶意团伙，大家的私密数据就仍然是安全的。

（3）执行效率

计算时间大部分耗费在第三步中，Zhan 等[19]证明了总体方案的计算开销和沟通成本都是 $O(N^2)$。

（4）总体分析

Zhan 等[19]的工作仍然有一些缺陷：他们使用的协议要求每个计算方保持在线，没有一个用于存储中间结果的云端，从而在完成计算前，每个计算方都不能离线，否则就会影响计算的完成；另外，这里假设数据是垂直分布的，对于更一般的情况，例如不是所有计算方都拥有全部数据时，该协议就无能为力了。因此，需要进一步对加密 k-NN 算法进行研究。

3　加密决策树和完全随机森林算法

3.1　研究进展

决策树方法起源于 20 世纪 60 年代到 70 年代末由 Quinlan 提出的 ID3 算法。C4.5 算法在 ID3 算法的基础上进行了改进，既适合于分类问题，又适合于回归问题。

随机森林算法由 Breiman[23]于 2001 年提出。随机森林是一个包含多个决策树的分类器，并且其输出的类别是由个别树输出类别的众数而定的。极度随机森林[24-25]比传统的随机森林表现更佳，且在复杂的非线性分类问题上表现良好。

加密决策树和加密随机森林算法就是在训练决策树和决策森林的过程中使用加密的密文。相关研究有：Zhan 等[26-27]提出了一种同态加密和数字信封的方法来实现合作决策树分类，参与的合作方不需要分享私有数据；Barni 等[28]提出了使用同态加密线性分支程序（特定类型的决策树）做 ECG（心电图）分类的多方计算协议方案；RaphaëlBost 等[29]开发了一个双方计算框架，并使用不同的部分和完全同态加密方案的混合，使其能够使用基于超平面决策、朴素贝叶斯和决策树的机器学习技术；Aslett 等[30]提出了对全同态加密数据进行分类的完全随机森林（CRF）算法，使用的加密方案是 Fan 等于 2012 年提出的一种全同态加密方案[31]。

3.2　方案构造

3.2.1　多方计算典型方案构造

Bost 等[29]提出了使用双方计算框架来完成对决策树的加密使用。他们针对的问题类型如下：客户端具有表示为特征向量 x 的私密数据作为输入，服务器端具有训练好的模型 w 作为输入，在客户端输入自己数据并获得分类结果的过程中，服务器端不会接触到客户端的私密数据，同时客户端也不会接收到服务器的模型参数。

（1）加密方案

方案使用 3 个加法同态密码系统：Goldwasser-Micali 开发的二次残留（QuadraticResiduosity，QR）密码系统[32]、Paillier 密码系统[13]和层次型完全同态加密（FHE）方案[33]。

（2）比较协议

假定有两个计算方 A 和 B，若 A 有 k 个值 $a_1,\cdots,a_k$，A 首先对序列进行随机置换和随机扰动，再将加密结果成对地发给 B；B 通过比较确定每对的较大值，最终得出最大值对应的序号 m；A 根据置换函数找到 m 对应的原始数据。

（3）多项式决策树

加密决策树要求客户端的输入 x 可以遍历服务器端的决策树模型，却不知道遍历时的路径，因为路径在树中的位置

和长度可能会泄露服务器模型的信息。方案用基于布尔变量的多项式来表示决策树的输出结果。每个节点对应一个布尔变量,其值决定接下来是访问左分支还是右分支。

(4)整体方案

1)S 按上述方法产生含 n 个变量的多项式 P;

2)S 和 C 在比较协议中相互作用,从而通过比较 w_i 与 x 的相应属性来获得 $[b_i]$,$i\in[1,n]$;

3)S 将加密方案从 QR 转为层次型 FHE 方案,并获得 $[[b_1]],\cdots,[[b_n]]$;

4)S 使用 FHE 和 SIMD 来评估多项式 P;

5)C 对结果进行解密,从而得到二进制表示的预测结果。

3.2.2 算法近似典型方案构造

Aslett 等[30]提出的完全随机森林算法是随机森林方法的一种近似。由于方案中使用的全同态加密方案(FHE)只对整数进行操作,因此需要对原始数据进行编码,使其适用于加密方案。

(1)编码方法

Aslett 等[30]使用了基于矩阵的量化分区编码方法,将连续、分类或序数值编码成可以直接应用于同态加密方案的整数。

(2)完全随机森林算法

Aslett 等[30]提出的随机森林的近似算法如算法 1 所示。

算法 1 完全随机森林算法[30]

第 1 步 从整个预测变量集合的子集中随机且均匀地选择树中每一级的预测变量。为变量所在的分支提供指标变量,用这些指标的乘积为完整的决策树提供指标。

第 2 步 使用每棵树的预测变量的随机子集对森林中的每棵树重复步骤 1,从而构造出许多这样的树。每个观察者根据每棵树的叶子和它所属的类对每棵树进行投票。由于树彼此独立地生长,因此步骤 2 可以并行执行。

第 3 步 在预测中,可以使用与步骤 2 相同的方法来创建一个指标,该指标对每个类的预测来自从每棵树中选择适当的投票。

这个算法被称为完全随机森林,因为树的生长是随机的,构造树的过程也没有考虑数据的影响。模型返回一个加密的预测结果,作为对每个明文空间中样例是否属于某一类别的投票结果。用户使用专用的加密密钥进行解密,就可以得到一个预测性经验概率。

3.3 方案分析

3.3.1 多方计算典型方案分析

(1)正确性

Bost 等[29]所提方案的比较协议显然是正确的;层次型 FHE 方案是固定乘法深度的 FHE 方案,满足同态性,因此在层次型 FHE 上的操作也是正确的;多项式决策树是对决策树的一种同义转换,保证了对多项式 P 的评估等价于对决策树模型的遍历,因此算法的执行过程是正确的。

(2)安全性

加密方案的安全性基于密码体制的语义安全,其使用了同态加密的经典原理:二次剩余假设、决策性复合残余假设和环容错学习(R-LWE)假设等。

比较协议的安全性在于 A 不能从 B 处获得计算的中间结果,而 B 虽然知道比较的结果,但 A 使用了随机置换和随机扰动,因此 B 也不能得到 A 的数据。

执行过程的安全性在于:比较协议期间,服务器端只能了解到加密数据,接触不到原始数据,使用 FHE 期间也是安全的;客户端无法得知服务器端的模型,因为服务器端执行的是基于多项式 P 的评估,且由于比较协议的特性,客户端无法在树内部的节点处学习到模型的参数。

(3)执行效率

由于使用的是层次型 FHE 方法,因此算法的计算复杂度是关于乘法深度以及电路集合大小的多项式。

基于树的评估也可以降低乘法的深度。假定决策树的最大高度为 $h_{\max}$,如果直接用 FHE 进行评估,则乘法深度为 $h_{\max}$;而通过二叉树进行评估,可以将乘法深度降为 $\log_2 h_{\max}$,有效地提高了算法效率。

3.3.2 算法近似典型方案分析

(1)正确性

完全随机森林(CRF)在本质上是离散的,而且算法不能保证不会两次生成完全相同的树,因此相同的树将以概率 1 无限再生长。但是如果在每个新树中重新计算加密的随机分数,则能渐近地进行正确的调整,因此算法仍是正确的。

(2)安全性

算法的安全性基于 Fan 等的全同态加密方案[31],该方案基于 RLWE 问题。RLWE 问题是 LWE 问题在交换环上的一个扩展,因此密码学界普遍认为 RLWE 问题是安全且计算上困难的。只要保证按方案进行编码和加解密,数据就是安全的。

(3)执行效率

该算法的乘法深度为 M,这受到全同态加密方案(FHE)的限制,因为过多的乘法操作会引起加密方案中噪声的增加和密文的刷新。总体来说,算法的执行效率受 M 影响,当 M 取值不大时,算法的运行时间在可接受范围内。

3.3.3 两种典型方案的对比分析

从实际效果上讲,两种方案都表现良好:在 Bost 等[29]的实验中,他们将加密决策树用于 Nursery 数据集和 Barni 等[28]的 ECG(心电图)分类数据,结果表明方案的正确性和执行效率都很高,每次预测分类仅需几秒钟;在 Aslett 等[30]的实验中,他们在 UCI 机器学习数据存储库(Lichman,2013)上测试了 20 种不同类型和尺寸数据集的方法,结果表明完全随机森林(CRF)算法在这些问题中与传统方法的性能几乎没有差别,只在少数几个问题的表现上稍落后。

从安全性上考虑,两者都使用了理论正确的同态加密方案,因此都可以保证安全。

对于执行效率,两种方案都存在问题:Bost 等[29]的方案存在着计算双方通信繁琐的问题,比较协议实际上是“走一步看一步”,另外,尽管分类预测的效率比较高,但根据他们的加密方案,模型的训练会耗费大量资源;而 Aslett 等[30]的方案则对乘法的深度仍有限制,如果乘法操作次数增多,就会导致算法运行变慢甚至出现误差,未来仍需从同态加密方案的构造上进行加强。

4　其他加密机器学习算法

Raju 等[34]提出了基于贝叶斯分类的加密机器学习算法，其可被用于多方分布式计算；刘晓红[35]提出了加密支持向量机算法；Graepel 等[36]实现了两种用于同态加密数据的二进制分类算法、线性均值和 Fisher 线性判别；Aslet 等[30]提出了对全同态加密数据进行分类的朴素贝叶斯算法和逻辑回归算法；姚禹丞等[37]提出了同态加密的分布式 K 均值聚类算法，其不但确保了聚类任务结果的正确性，还保护了数据的隐私性。还有很多国内外学者都在这个领域做出了贡献，由于篇幅所限，这里不做一一阐述。

结束语　在加密机器学习的实现中，借助同态加密方案是目前的主流观点。然而由于当前加密方案对操作数类型和操作运算的限制，导致人们寻求两种策略：1）多方计算；2）算法近似。两种策略的优缺点如下：多方计算使用的交互式信息处理可以保持复杂运算，但涉及繁琐的协议设计，影响处理效率，且要求参与的计算方必须遵守协议才能保证正确性和安全性；而算法近似无须制定协议方案，更为贴近原有的机器学习理念，但为了避免复杂运算，对原有算法做了改变，结果的正确性不免受到影响。

目前，研究人员面临的问题主要有：

1）如何在保证数据安全的前提下选择合适的同态加密方案来实现不同的数据分析；

2）如何解决全同态加密方案中存在的噪声、运算复杂、运算效率低等问题；

3）如何在确保算法安全性的前提下，使加密机器学习算法的性能准确度在可接受范围内。

当今是信息时代，因此对数据的处理格外重要。结合了机器学习算法对信息的强大分析能力和同态加密对信息的保护隐私能力的加密机器学习，具有很好的理论价值和应用前景。进一步的研究方向包括：

1）在理论上对全同态加密方案进行深入研究，降低计算复杂度，解决密文膨胀问题[38]；

2）开发出支持复杂运算且具有实际应用价值的全同态加密方案；

3）深入分析成功的机器学习算法的原理，并提出可以应用同态加密的近似算法；

4）在已有成果的基础上，扩大已有方案的适用范围并进行性能上的优化；

5）探讨多方计算执行流程上的简化，提高执行效率。

参 考 文 献

[1] LIU Q, ZHOU S, ZHU C, et al. MI-ELM[J]. Neurocomputing, 2016, 173(3): 1044-1053.

[2] LIU X, ZHOU L, WANG L, et al. An efficient radius-incorporated MKL algorithm for Alzheimer's disease prediction[J]. Pattern Recognition, 2015, 48(7): 2141-2150.

[3] RIVEST R L, ADLEMAN L, DERTOUZOS M L. On data banks and privacy homomorphisms[J]. Foundations of Secure Computation, 1978, 4(11): 169-180.

[4] GENTRY C. Fully homomorphic encryption using ideal lattices [C]// ACM Symposium on Theory of Computing(STOC 2009). Bethesda, MD, USA, BLP, 2009: 169-178.

[5] BRAKERSKI Z, VAIKUNTANATHAN V. Fully homomorphic encryption from ring-LWE and security for key dependent messages[C] // Annual Cryptology Conference. Springer, Berlin, Heidelberg, 2011: 505-524.

[6] CORON J S, BASTIEN, MANDAL A, et al. Fully homomorphic encryption over the integers with shorter public keys[C]// Conference on Advances in Cryptology. Springer-Verlag, 2011: 487-504.

[7] BRAKERSKI Z, GENTRY C, VAIKUNTANATHAN V. (Leveled) fully homomorphic encryption without bootstrapping [C]// Innovations in Theoretical Computer Science Conference. ACM, 2012: 309-325.

[8] ZHANG W K, YANG Y, YANG Y. Research of Secure Multiparty Computation [J]. Information Security and Communications Privacy, 2014(1): 97-99. (in Chinese)
张文科，杨勇，杨宇. 安全多方计算研究[J]. 信息安全与通信保密，2014(1)：97-99.

[9] BARNI M, ORLANDI C, PIVA A. A privacy-preserving protocol for neural-network-based computation[C]// Proceedings of the 8th Workshop on Multimedia and Security. ACM, 2006: 146-151.

[10] ORLANDI C, PIVA A, BARNI M. Oblivious neural network computing via homomorphic encryption[J]. EURASIP Journal on Information Security, 2007, 2007(1): 037343.

[11] BARNI M, FAILLA P, LAZZERETTI R, et al. Privacy-Preserving ECG Classification With Branching Programs and Neural Networks[J]. IEEE Transactions on Information Forensics & Security, 2011, 6(2): 452-468.

[12] DOWLIN N, GILAD-BACHRACH R, LAINE K, et al. Cryptonets: Applying neural networks to encrypted data with high throughput and accuracy[C]// International Conference on Machine Learning(ICML). 2016: 201-210.

[13] PAILLIER P. Public-key cryptosystems based on composite degree residuosity classes[C]// International Conference on the Theory and Applications of Cryptographic Techniques. Springer Berlin Heidelberg, 1999: 223-238.

[14] DAMG, RD I, JURIK M. A Generalisation, a Simplification and Some Applications of Paillier's Probabilistic Public-Key System [C]// International Workshop on Practice and Theory in Public Key Cryptography: Public Key Cryptography. Springer-Verlag, 2001: 119-136.

[15] BOS J W, LAUTER K, LOFTUS J, et al. Improved security for a ring-based fully homomorphic encryption scheme[C]// IMA International Conference on Cryptography and Coding. Springer, Berlin, Heidelberg, 2013: 45-64.

[16] GOLDREICH O. Secure multi-party computation (working draft) version 1[J]. Multimodal Output Generation, 2008, 2(3): 1-10.

[17] LIVNI R, SHALEV-SHWARTZ S, SHAMIR O. On the computational efficiency of training neural networks[C]// Advances in

Neural Information Processing Systems. 2014:855-863.

[18] QI Y, ATALLAH M J. Efficient Privacy-Preserving k-Nearest Neighbor Search[C]// International Conference on Distributed Computing Systems. IEEE, 2008:311-319.

[19] ZHAN J Z, CHANG L W, MATWIN S. Privacy preserving k-nearest neighbor classification[J]. IJ Network Security, 2005, 1(1):46-51.

[20] KUMAR P, SINGH M D, SAXENA A. HEMIN: A cryptographic approach for private k-NN classification[C]// International Conference on Data Mining. Las Vegas, USA, 2008:500-505.

[21] ZHU J. A New Scheme to Privacy-Preserving Collaborative Data Mining[C]// International Conference on Information Assurance and Security. IEEE, 2009:468-471.

[22] UTSUNOMIYA Y, TOYODA K, SASASE I. LPCQP: Light-weight Private Circular Query Protocol with Divided POI-table and Somewhat Homomorphic Encryption for Privacy-Preserving k-NN Search [J]. Journal of Information Processing, 2016, 24(1):109-122.

[23] BREIMAN L. Random Forests[J]. Machine Learning, 2001, 45(1):5-32.

[24] GEURTS P, ERNST D, WEHENKEL L. Extremely randomized trees[J]. Machine Cncrypted Data, 2006, 63(1):3-42.

[25] CUTLER A, ZHAO G. Pert-perfect random tree ensembles[J]. Computing Science and Statistics, 2001, 33:490-497.

[26] ZHAN J. Using Homomorphic Encryption For Privacy-Preserving Collaborative Decision Tree Classification[C]// IEEE Symposium on Computational Intelligence and Data Mining, 2007 (CIDM 2007). IEEE, 2007:637-645.

[27] ZHAN J. Privacy-preserving collaborative data mining[J]. IEEE Computational Intelligence Magazine, 2008, 3(2):31-41.

[28] BARNI M, FAILLA P, LAZZERETTI R, et al. Privacy-Preserving ECG Classification with Branching Programs and Neural Networks[J]. IEEE Transactions on Information Forensics & Security, 2011, 6(2):452-468.

[29] BOST R, POPA R A, TU S, et al. Machine Learning Classification over Encrypted Data[C]// Network and Distributed System Security Symposium. 2014.

[30] ASLETT L J M, ESPERANCA P M, HOLMES C C. Encrypted statistical machine learning: new privacy preserving methods [J]. arXiv preprint arXiv:1508.06845, 2015.

[31] FAN J, VERCAUTEREN F. Somewhat Practical Fully Homomorphic Encryption[J]. IACR Cryptology ePrint Archive, 2012, 2012:144.

[32] GOLDWASSER S, MICALI S. Probabilistic encryption & how to play mental poker keeping secret all partial information[C]// Fourteenth ACM Symposium on Theory of Computing. ACM, 1982:365-377.

[33] SHAI HALEVI. Helib-an implementation of homomorphicen cryption[OL]. https://github.com/shaih/HElib.

[34] RAJU R, KOMALAVALLI R, KESAVAKUMAR V. Privacy maintenance collaborative data mining-a practical approach[C]// 2009 2nd International Conference on Emerging Trends in Engineering and Technology (ICETET). IEEE, 2009:307-311.

[35] LIU X H, Research on Algorithms for privacy-preserving Support Vector Machines[D]. Qingdao: University of Science and Technology in Shandong Province, 2011. (in Chinese)
刘晓红. 隐私保护支持向量机的算法研究[D]. 青岛:山东科技大学, 2011.

[36] GRAEPEL T, LAUTER K, NAEHRIG M. ML confidential: machine learning on encrypted data[C]// International Conference on Information Security and Cryptology. Springer-Verlag, 2012:1-21.

[37] YAO Y C, SONG L, E C. Research on Homomorphic Encryption based distributed K-means Clustering Algorithm[J]. Computer Technology and Development, 2017, 27(2):81-85. (in Chinese)
姚禹丞, 宋玲, 鄂驰. 同态加密的分布式 K 均值聚类算法研究[J]. 计算机技术与发展, 2017, 27(2):81-85.

[38] LI S D, DOU J W, WANG D S. Homomorphic Encryption Algorithm and its Application in Cloud Security[J]. Journal of Computer Research and Development, 2015, 52(6):1378-1388. (in Chinese)
李顺东, 窦家维, 王道顺. 同态加密算法及其在云安全中的应用[J]. 计算机研究与发展, 2015, 52(6):1378-1388.

(上接第 24 页)

[27] CAO Y, GUO S, HE T. Robust multi-pipeline scheduling in low-duty-cycle wireless sensor networks[C]// Proceedings of the 31st IEEE International Conference on Computer Communications. IEEE, 2012:361-369.

[28] ZHU C, YANG L T, SHU L, et al. A geographic routing oriented sleep scheduling algorithm in duty-cycled sensor networks [C]// Proceedings of IEEE International Conference on Communications. IEEE, 2012:5473-5477.

[29] CHEN L Y, YAN B S, ZHANG J Y, et al. Neighbor discovery algorithm in Mobile Low-Duty-Cycle Wireless Sensor Networks [J]. Journal of Software, 2014, 25(6):1352-1368. (in Chinese)
陈良银, 颜秉姝, 张靖宇, 等. 移动低占空比传感网邻居发现算法[J]. 软件学报, 2014, 25(6):1352-1368.

[30] HUANG T, CHEN H, ZHANG Y, et al. EasiND: Effective Neighbor Discovery Algorithms for Asynchronous and Asymmetric-Duty-Cycle Multi-channel Mobile WSNs[J]. Wireless Personal Communications, 2015, 84(4):3031-3055.

[31] RAZAQUE A, ELLEITHY K M. Low duty cycle, energy-efficient and mobility-based boarder node—MAC hybrid protocol for wireless sensor networks[J]. Journal of Signal Processing Systems, 2015, 81(2):265-284.

[32] CHEN L, SHU Y, GU Y, et al. Group-based Neighbor Discovery in Low-duty-cycle Mobile Sensor Networks[J]. IEEE Transactions on Mobile Computing, 2016, 15(8):1996-2009.