隐私保护机器学习的密码学方法

蒋 瀚[①] 刘怡然[①] 宋祥福[①] 王 皓[②] 郑志华[②] 徐秋亮*[①]

[①](山东大学软件学院 济南 250101)

[②](山东师范大学信息科学与工程学院 济南 250358)

摘 要：新一代人工智能技术的特征，表现为借助GPU计算、云计算等高性能分布式计算能力，使用以深度学习算法为代表的机器学习算法，在大数据上进行学习训练，来模拟、延伸和扩展人的智能。不同数据来源、不同的计算物理位置，使得目前的机器学习面临严重的隐私泄露问题，因此隐私保护机器学习(PPM)成为目前广受关注的研究领域。采用密码学工具来解决机器学习中的隐私问题，是隐私保护机器学习重要的技术。该文介绍隐私保护机器学习中常用的密码学工具，包括通用安全多方计算(SMPC)、隐私保护集合运算、同态加密(HE)等，以及应用它们来解决机器学习中数据整理、模型训练、模型测试、数据预测等各个阶段中存在的隐私保护问题的研究方法与研究现状。

关键词：隐私保护机器学习；安全多方计算；同态加密；隐私保护集合求交

中图分类号：TN918; TP309 **文献标识码**：A **文章编号**：1009-5896(2020)05-1068-11

DOI: 10.11999/JEIT190887

Cryptographic Approaches for Privacy-Preserving Machine Learning

JIANG Han[①] LIU Yiran[①] SONG Xiangfu[①] WANG Hao[②]

ZHENG Zhihua[②] XU Qiuliang[①]

[①](*School of Software*, *Shandong University*, *Jinan* 250101, *China*)

[②](*School of Information Science and Technology*, *Shandong Normal University*, *Jinan* 250358, *China*)

Abstract: The characteristics of the new generation of artificial intelligence technology are shown as follows: with the help of GPU computing, cloud computing and other high-performance distributed computing capabilities, machine learning algorithms represented by deep learning algorithms are used for learning and training on big data to simulate, extend and expand human intelligence. Different data sources and computing physical locations make the current machine learning face serious privacy leakage problem, so the Privacy Protection of Machine (PPM) Learning has become a widely concerned research area. Using cryptography technology to solve the problem of privacy in machine learning is an important technology to protect the privacy of machine learning. Cryptographic tools used in privacy-preserving machine learning are introduced, such as general Secure Multi-Party Computing (SMPC), privacy protection set operation and Homomorphic Encryption (HE), describes the status and developments applying the tools to solving the problems of privacy protection in various stages of machine learning, such as data processing, model training, model testing, and data prediction.

Key words: Privacy-Preserving Machine (PPM) learning; Secure MultiParty Computation(SMPC); Homomorphic Encryption(HE); Private Set Intersection(PSI)

收稿日期：2019-11-06；改回日期：2020-03-08；网络出版：2020-04-03

*通信作者： 徐秋亮 xql@sdu.edu.cn

基金项目：国家自然科学基金(61632020, 61572294)；山东省自然科学基金(ZR2017MF021)；山东省科技重大创新工程项目(2018CXGC0702)；山东半岛国家自主创新示范区发展建设项目(S190101010001)

Foundation Items: The National Natural Science Foundation of China (61632020, 61572294); The Natural Science Foundation of Shandong Province (ZR2017MF021); The Major Innovation Project of Science and Technology of Shandong Province (2018CXGC0702); The Funds Project of National Independent Innovation Demonstration Zone in Shandong Peninsula (S190101010001)

1　引言

近年来，人工智能得到空前的发展与应用，我们在生产生活中，也越来越直观地感受到人工智能产生的影响。有观点将人工智能技术看作一种战略性技术，是新一轮科技革命和产业变革的关键力量，是引领第4次工业革命的核心技术，人工智能技术成为信息技术研究中最为炙手可热的领域。

从1956年，人工智能的概念在达特茅斯会议(Dartmouth Conferences)上被提出，人工智能技术经历了几十年的发展。美国国防高级研究计划局(Defense Advanced Research Projects Agency, DARPA)将人工智能的发展分为了3个阶段。

人工智能第1阶段的特点是基于人类已有的知识，使用逻辑推理法则来解决特定的和狭义的问题或任务。这些系统需要特定领域的规则，这些规则首先由金融、物流或科学应用等特定领域的人类专家创建，然后输入计算机进行处理和理解。当涉及到例如学习新知识，或根据早期获得的数据进行抽象的能力时，第1代人工智能技术并不能胜任。

人工智能发展的第2阶段的核心要素是统计学习的应用。这一代人工智能技术有更好的分类和预测能力：针对大数据进行训练得到统计模型，然后利用统计模型来解决未知问题。经过适当的训练，它们可以学习并适应不同的情况。这一代的人工智能技术不依赖精确的规则进行推理，而是通过统计规律寻求“通常工作得足够好”的解决方案。

人工智能发展的第3阶段，也是人工智能的未来，DARPA定义它们的特征为情境适应：人工智能系统本身将构建模型来解释世界是如何运作的，换言之，它们会自己发现影响它们决策过程的逻辑规则。

当前，我们正处在人工智能发展的第2阶段。深度学习是第2代人工智能的典型代表，它通过开发特定类型的机器学习模型，基于海量数据形成智能获取能力。这其中，获得高质量的大数据和高性能的计算能力成为算法成功的关键要素。而当前大数据技术、高性能计算技术已经有了突破性的发展，正是这些技术的成熟与发展，推动了目前人工智能技术的飞跃发展。以谷歌、百度、阿里为代表的，既拥有大数据及丰富大数据处理技术，同时具备高性能计算能力的公司纷纷看好人工智能产业的前景，在人工智能领域加大投入，极大促进人工智能在医疗诊断、智能驾驶、图像识别、自然语言理解等领域的应用发展。

人工智能火热的同时，也带来了严重的隐私问题。由于这一代人工智能技术是建立在大数据技术和高性能计算之上的，而大数据一定来源多样，本身存在隐私范围扩大、隐私权利归属复杂、隐私保护难度大的问题。高性能计算一般以云计算和分布式计算为特征，用户数据脱离本地计算，数据的访问控制、隐私保护难度增大。

为了解决人工智能中的隐私保护问题，研究者提出了各种隐私保护机器学习的方法，这其中，密码学技术在其中扮演了至关重要的角色。本文将介绍一些基础的隐私保护的密码学方法，并介绍基于这些密码学工具的隐私保护机器学习的现状与发展。本文剩余章节安排如下：第2节介绍机器学习算法及其面临的隐私保护问题；第3节介绍隐私保护的密码学工具，包括通用安全多方计算(general Secure MultiParty Computation, SMPC)、隐私保护集合运算、同态加密(Homomorphic Encryption, HE)等；第4节介绍这些密码学工具在各类机器学习算法中的应用现状和发展，包括数据整理、模型训练、数据预测等各个阶段；第5节总结全文，并展望了隐私保护机器学习的未来方向。

2　机器学习及其面临的隐私风险

2.1　机器学习的定义

早在1959年，Arthur Samuel就给出机器学习的一个非正式的定义：机器学习是一门给予计算机不需要显式编程而获得学习能力的领域。1998年，Tom Mitchell提出一个关于机器学习的定义：对于一个计算机程序来说：给它一个任务T和一个性能测量方法P，如果在经验E的影响下，P对T的测量结果得到了改进，那么就说程序从经验E中学习而得到提升。

机器学习的一般过程，如图1所示，一般由数据收集，数据预处理，模型训练与测试，预测几个阶段构成，并且模型的生成是一个反复迭代优化的过程。

2.2　机器学习中的隐私保护问题

在目前大数据与高性能计算为特征的机器学习中，由于用户自有资源脱离用户的物理控制，也就是资源的所有权和控制权相互分离，导致了在机器学习的每一个步骤中，都存在着隐私泄漏的危险。

(1) 在数据收集阶段，用户数据在多个数据集之间存在着一定的关联性，大数据的多样性带来的多源数据融合，使得隐私泄露风险大大增加。此阶段面临的最大隐私挑战在于如何保护用户原始数据，避免因数据挖掘而导致隐私泄露。

(2) 在数据预处理阶段，在某些场景之下，不同数据集的所有者，可能需要共同完成数据清洗、集成、转换等操作，还要保证参与数据处理的各方

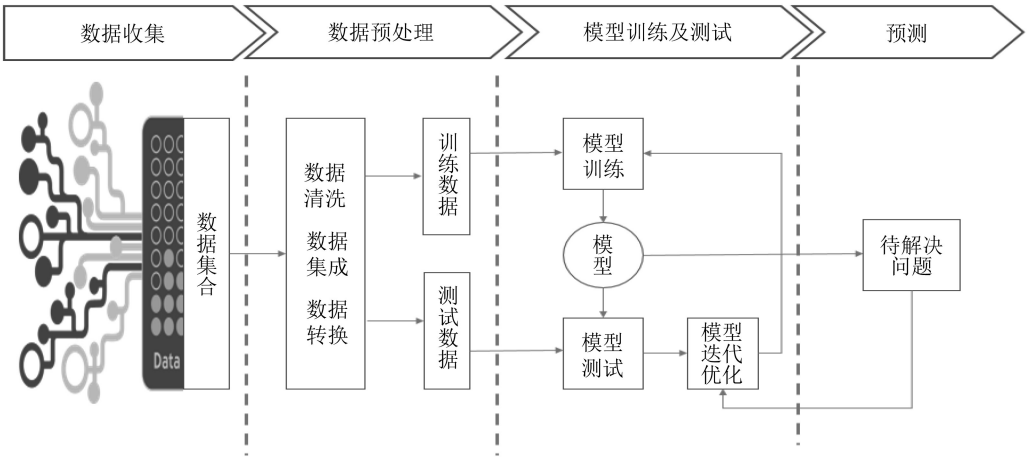


图 1 机器学习的一般过程

及彼此之间不能泄露数据的隐私。此阶段最主要的任务是隐私保护的集合运算，包括集合求交、并、差等运算。

(3) 在模型训练和测试阶段，鉴于训练数据、测试数据，以及训练所使用的计算资源，可能分属不同参与方，因此，此阶段的隐私分为训练数据隐私、模型隐私和模型输出隐私。此阶段的主要挑战在于如何在多个参与方之间安全地完成各类不同的机器学习计算任务。

(4) 在预测阶段，由于预测所使用的模型是在大数据集上经过高性能计算而得到，一般由服务器端拥有，而用户希望利用服务器端的模型，来计算自己的私有数据，并且仅有自己可以得到预测结果。此阶段需要保护模型的隐私性及输出结果的隐私性。

对于机器学习中的隐私保护，目前已经存在各种不同种类的方法，这些方法中，不可避免地使用到了密码技术，其中通用安全多方计算、同态加密、隐私保护的集合计算是最为常用的密码学方法。

3 常用隐私保护密码技术

3.1 通用安全多方计算及其相关技术

安全多方计算协议最早是由Yao[1]在1982年提出的。在安全多方计算中，两个或多个持有私有输入的参与者，想要联合计算某些(事先协定的)计算任务，得到他们的输出，并达到正确性、隐私性、输出可达性、公平性等安全特性。多方参与的计算任务可抽象为理想功能(functionality)，为方便，在下文中“functionality”将广义地称为“函数”。

由安全多方计算的定义可以看出，保护用户隐私是安全多方计算在处理多参与方交互的计算任务时最基本的动机和要求。

安全多方计算的研究大致可以划分为两个类别：通用安全多方计算，以及特定的安全多方计算。

对于任意的函数f，都存在一个等价的电路C，使得对于任意的输入，电路C和函数f的输出一致，即$C(x_1,x_2,\cdots,x_n)=f(x_1,x_2,\cdots,x_n)$。事实上，任意的函数，只要能够利用编程语言实现，那么，它一定是转化为电路在计算机中完成计算的。因而，对任意函数f的安全多方计算，可转换为对等价的电路C的安全多方计算。这类研究讨论可以用于任意计算任务的通用方法，被称为通用安全多方计算。而另一类安全多方计算，针对某一个具体的问题，根据问题特点，设计专门算法来解决，被称为特定的安全多方计算，包括隐私保护集合求交(Private Set Intersection, PSI)等等。

本节主要介绍通用安全多方计算协议。

通用安全多方计算协议中，与函数f等价的电路C，可能是一个逻辑电路，也可能是一个计算电路。安全多方计算协议需要依次对电路中的每一个电路门进行计算，从而完成整个电路的计算。对于逻辑电路来说，原则上由于“与门”、“或门”和“非门”组成完备集(当然存在冗余)，因此针对逻辑电路设计安全多方计算协议，只需要解决“与门”、“或门”和“非门”的计算就足够了。但在实际计算中，往往引入更多的电路门直接进行安全多方计算，从而获取较高的效率。对于算术电路来说，“加法门”与“乘法门”就是完备的，因此针对算术电路设计安全多方计算协议，只需要解决“加法门”与“乘法门”的计算就足够了。

通用安全多方计算协议的安全性分为半诚实模型安全和恶意敌手模型安全，在安全多方计算协议的设计中，一般先设计半诚实模型安全的协议，然后利用承诺、茫然传输(Oblivious Transfer, OT)协议、零知识证明及一些固定的范式转化为恶意敌手模型安全的协议。

通用安全多方计算协议主流的构造方法有两

类：基于Yao[2]混乱电路(garbled circuits)的构造和基于秘密分享(secret sharing)的构造[3,4]。早期的通用安全多方计算协议只是解决了通用安全多方计算协议的存在性问题，效率较低。而近年来，安全多方计算协议的实用化技术得到了飞速的发展，恶意敌手模型下，基于Yao混乱电路的安全两方计算协议，以及基于秘密分享的安全多方计算协议，都有了高效实现方案。

(1) 高效的基于Yao混乱电路的安全两方计算协议：基于Yao混乱电路的安全两方计算协议的效率提升，主要从3个方面入手。第一个技巧是采用Free-XOR/Flex-XOR/Half-Gate等技术，避免混乱电路中的XOR门的加解密计算。第2个技巧是应用茫然传输扩展技术。基于Yao混乱电路的安全两方计算协议中的主要计算开销是OT协议，此类协议只能基于公钥密码体制设计，效率较低，而茫然传输扩展技术，可以使用少量的基础茫然传输(数百个)协议，加以大量的高效的对称加密运算，达到大量(数百万个)茫然传输的效果。第3个技巧是利用剪切-选择技术(cut-and-choose)，实现半诚实敌手下的协议到恶意敌手下协议的转换，避免了大量使用低效的零知识证明及承诺。关于恶意敌手下高效的基于Yao混乱电路的安全两方计算协议，在文献[5]中给出了全面的综述。

(2) 高效的基于秘密分享的安全多方计算协议：在基于秘密分享的安全多方计算协议中，以GMW87[3]为代表的基于加法秘密分享的方法，在计算加法门时，各参与方将自己的共享份额相加即可，不需要交互，效率很高。而在计算乘法门时，原生的GMW87方法需要在参与方之间使用茫然传输协议来完成，交互次数及计算量都很高，无法用于实际计算。

1992年，Beaver[6]提出一种方法，利用一种随机选取的Beaver 3元组，可以将乘法门计算分为预计算与在线计算两个阶段，大量的交互操作都转移到预计算过程中，在线计算过程中只需要1次交互即可。

在半诚实敌手下的协议到恶意敌手下的协议的编译过程中，原生GMW编译器使用零知识证明和承诺，使得参与方每一步操作都必须遵守协议，从而保证协议的安全性。但零知识证明的效率较低，导致协议整体效率低下。加法秘密分享的秘密份额具备加法同态的特征，基于这一特性，2011年，Bendlin等人[7]提出一种信息论安全的1次消息认证码协议，称为BDOZ，可以用于保证参与方输入正确的秘密分享份额。BDOZ方法中参与方本地保存的秘密份额需要记录所有其它参与方的消息认证码，其数量与秘密份额线性相关。2012年，Damgård等人[8]提出一种称为SPDZ的机制，每一参与方只需要保留常数数量的份额即可。目前SPDZ算法也已经提供了开源代码，是一种广为认可的高效实现方法。

3.2 同态加密技术

从抽象代数的角度来讲，同态(映射)指的是不同代数系统之间保持运算关系的映射。以带有一个二元运算的代数系统为例，对于两个代数系统$<X, *>$和$<Y, \Diamond>$，如果映射f: $X \to Y$，满足$f(a*b) = f(a) \Diamond f(b)$，称$f$为$<X, *>$到$<Y, \Diamond>$的同态，并称$f$把$<X, *>$同态映射到$<Y, \Diamond>$。如果一个加密算法能够把明文空间及其运算形成的代数系统同态映射到密文空间及相对应运算形成的代数系统，则称该加密算法为同态加密算法。当然，明文空间带有的运算一般不止1个，比如常用的模n剩余环$\boldsymbol{Z}_n$带有模n加法和乘法两种运算。从定义上可以看到，同态加密算法不需要对密文解密，而可直接对密文进行运算，得到的运算结果，等同于对应明文所作相应运算计算结果的密文。不解密而进行计算，对于隐私保护，具备得天独厚的优势。

如果加密算法可以保持明文空间上的一种运算，称之为部分同态(partial homomorphic)加密算法，相应地，如果加密算法可以保持明文代数系统上的加法运算，称之为加法同态加密。典型的加法同态加密算法有Paillier加密[9]。如果加密算法可以保持明文空间上的乘法运算，称之为乘法同态加密，典型的乘法同态加密算法有RSA加密算法，以及ElGamal加密等。

我们期望的目标是通过密文运算，可以等价实现对明文的任意运算。通常需要的明文运算是加法和乘法。如果同态加密算法可以同时保持明文的加法及乘法运算，称之为全同态加密算法。全同态加密的构造比较困难，直到2009年，Gentry等人[10]首次基于理想格构造了全同态加密算法，之后相继出现了一些全同态加密算法[11–13]。

尽管全同态加密算法具备优良的性质，但目前所有算法的效率太低，不足以在实际中应用。因此使用部分同态加密算法来解决实际中的部分问题，是目前不得已的选择。特别值得提出的是，Paillier加密不但是一个加法同态算法，满足性质$\mathrm{Enc}(a + b) = \mathrm{Enc}(a) \times \mathrm{Enc}(b)$，同时它也保持常数的倍乘，即$\mathrm{Enc}(a \times b) = (\mathrm{Enc}(a))^b$。这个性质有时为明密文计算的转换带来很大便利，在实际应用中被大量采用。

3.3 隐私保护的集合运算

隐私保护的集合运算在隐私保护机器学习的数据预处理阶段非常有用，它可以使持有私有数据集合的参与方合作产生集合运算的结果，而不泄露各自私有数据集的隐私。

基础的集合运算包括集合求交和集合求并。

隐私保护集合求交协议(Private Set Intersection, PSI)是安全多方计算领域的特定应用，也是一个被大量研究的、具有广泛应用的问题。PSI协议允许持有各自私有集合的两方共同计算两个集合的交集，协议完成后，一方或者两方得到正确的交集，且不会得到交集以外的另一方集合中的任何信息。PSI协议可以通过通用安全多方计算协议来实现，如文献[14]，但更多的是采用特殊的算法来实现。

最早的PSI协议基于Hash算法构造，其原理是双方不比较元素本身，而比较集合元素的Hash值，Hash值相等的元素属于集合的交集。由于Hash函数具备单向性(求原像困难)，因此协议可以得到交集中的元素，而不泄露非交集中的元素。该方法的主要弱点是当集合元素的范围较小时(例如年龄等)，明显存在穷举攻击。要解决这一问题，直觉上，只要使用一个受限的单向函数来替代Hash函数，并且要求这个单向函数只能在有限制的点上计算(比如只能计算自己集合中的元素的函数值)，这样就避免了穷举攻击。或者将这个概念弱化一些，单向函数要求拿到集合求交结果的一方只能计算受限点上的函数值，而另外一方可以计算所有点。

2016年Kolesnikov等人[15]基于OT协议设计了一种称为茫然伪随机函数(Oblivious Pseudo Random Function, OPRF)的协议，实现了上述弱化的受限单向函数的概念。该协议涉及两个参与方，协议结束后，一个参与方获得某个伪随机函数的种子s，另一个参与方获得该伪随机函数在某一特定值上(即只能计算一个点的函数值)的输出但不知道种子s的信息，即以茫然的方式计算出该伪随机函数的特定输出。Kolesnikov将OPRF用于PSI，得到一个高效的隐私保护集合求交方案。

集合求并集虽然在功能是集合求交集的补运算，但隐私保护集合求并集(Private Set Union, PSU)无法直接利用已有的PSI技术，即无法直接使用OPRF技术实现。2019年，Kolesnikov等人[16]以OPRF为基础，利用多项式表示集合元素，提出了反向成员检测(Reverse Private Membership Test, RPMT)原语，利用RPMT高效实现了PSU。

4 密码技术在隐私保护机器学习中的应用

机器学习中的训练和预测问题最终转化为函数计算和数值比较问题，这些计算包括线性函数求值、线性方程组求解、非线性激活函数求值等，而前两种计算可归结为加法与乘法计算。因此隐私保护机器学习中要解决的问题，最终归结为安全数值比较，安全计算乘法、加法和安全计算非线性激活函数。

4.1 隐私保护的机器学习训练

隐私保护下的机器学习训练，涉及保护训练数据和模型两方面的隐私。这主要是通过同态加密和安全多方计算来实现的。

基于同态加密的隐私保护下的机器学习方案，Barni等人[17]在2006年提出了一种用于神经网络计算的数据隐私保护协议，在神经网络的每一层中，用户持有秘密向量$\boldsymbol{x}$，服务器持有秘密向量$\boldsymbol{y}$，双方计算向量的内积，并仅有用户端得到计算结果。用户利用Paillier同态加密来加密用户向量，然后将密文发送至云平台，云平台利用Paillier加密保持常数倍乘运算的性质计算$\boldsymbol{x}$与$\boldsymbol{y}$内积的密文，发送给用户，用户解密得到计算结果。在这个过程中用户必须保持在线，并且要共享中间的数据结果，因此大部分的权重信息会泄露给用户。因此，Orlandi等人[18]在2007年提出了另一种方法，该方法仍然利用同态加密对数据进行加密，但对权重进行模糊化处理，所以神经网络权重和激活函数等也是保密的。协议执行后，用户只知道神经网络的最终输出，所有中间计算结果都是保密的。同态加密方案虽然安全可靠，但只支持加法和乘法等多项式运算，而不支持机器学习过程中使用的非线性激活函数运算，如sigmoid和ReLu等激活函数。对于这些非线性的激活函数，如果它们是足够光滑的，那么可以使用多项式插值或分段多项式插值逼近，然后再使用同态加密机制来解决近似的多项式函数[19–21]。

基于安全多方计算协议的隐私保护下的机器学习方案，由于不同的安全多方计算协议具有不同的特性，因而适用于不同的场景，因此相应地出现了使用不同安全多方计算原语组合构建的多种机器学习隐私保护方案。其中经典的计算方案有：混乱电路 + 茫然传输[22]、同态加密 + 混乱电路[23]、同态加密 + 混乱电路 + 秘密分享 + 茫然传输[24]和混乱电路 + 秘密分享 + 茫然传输[25]等，这其中Mohassel等人[24]提出的机器学习框架SecureML具有良好的代表意义。

Mohassel等人[24]2017年在IEEE S&P上提出的安全机器学习框架SecureML，使用基于Beaver

3元组的预计算秘密分享安全多方计算的方法，将用户的数据秘密分享成两个份额后发送到两个不合谋的服务器，然后两个不合谋的服务器之间，进行安全两方计算，以训练线性回归，逻辑回归，神经网络等各种模型。

在线性回归过程中，非线性的激活函数可以直接使用多项式进行逼近。而在逻辑回归过程中，其非线性的sigmoid激活函数$y=\dfrac{1}{1+\mathrm{e}^{-x}}$，其图像如图2(a)所示，如果使用传统的方法用多项式去拟合该sigmoid函数，存在两个问题，一是需要的多项式次数较高(一般需要10次)，在自变量较大的情况下截断误差和稳定性都不理想。因此，文献[24]提出了用一个分段函数来代替sigmoid函数，如式(1)所示：

$$f(x)=\begin{cases}0, & x<-\dfrac{1}{2}\\ x+\dfrac{1}{2}, & -\dfrac{1}{2}\le x\le\dfrac{1}{2}\\ 1, & x>\dfrac{1}{2}\end{cases}\tag{1}$$

其图像如图2(b)所示。

由于在上述分段函数计算过程中使用了元素的比较，而基于算术电路的秘密分享安全多方计算，不擅长元素大小比较，而基于Yao混乱电路的安全多方计算，比较操作则较为简单。因此，在使用基于秘密分享的安全多方计算协议计算完矩阵-向量乘法之后，需要使用Demmler等人[26]引入的ABY框架，转化为Yao混乱电路来计算上述分段函数，计算完成后，再使用ABY框架，将Yao混乱电路转化为基于秘密分享的安全多方计算。

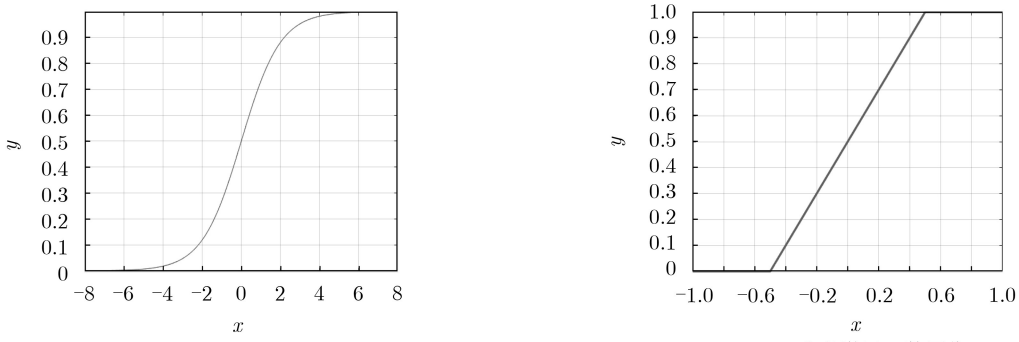
对于神经网络，文献[24]只考虑了基本的全连接的神经网络，其中的线性回归和逻辑回归操作采用了同样的方法。

4.2　隐私保护的深度机器学习预测

目前深度神经网络的机器学习算法是一大研究热点，在很多领域都得到了相当广泛的应用。为了保护机器学习中模型的参数和用户的敏感数据，最简单的想法是在密文上运行深度神经网络，这当然需要同态加密，另一方面利用多项式逼近神经网络中非线性激活函数是一个自然的思路。Xie等人[27]在2014年提出一种基于全同态加密的隐私保护神经网络模型Crypto-Nets，该模型利用多项式近似模拟神经网络非线性激活函数，直接在密文上做预测，但仅适用于小型数据集或线性模型等简单模型。2016年，微软研究院的Gilad-Bachrach等人[28]基于leveled-FHE技术(YASHE[29])提出了一种近似神经网络模型Cryptonets。该文章假设在云端已经用明文训练好神经网络模型，对该模型进行转化，使得转化后的模型可以用于密文的预测，使用此方法，用户可以将密文数据发送给云端，云端将训练好的模型进行变换后用于预测，并将加密的预测结果返回给用户，用户解密得到最终结果。虽然在转化过程中对神经网络模型的激活函数进行了近似，但该模型分类性能较高，并且中间结果不共享，泄露给数据持有者的信息更少。但是由于文中对数据使用了同态加密技术，计算复杂度大大增加。当非线性层的数目很小时，该模型的效率和准确性得到了证实，但对于较深的神经网络，模型的效果较差。

Chabanne等人[30]在2017年提出了一种将Relu激活函数用多项式逼近与批量归一化(batch normalization)相结合的深度神经网络分类模型。该方案基于全同态加密技术，与Cryptonets相比，可应用于更深的神经网络，同时保持了较高的精度。在分类阶段用多项式逼近Relu函数与批量归一化操作相结合，减少了实际训练模型与转换模型之间的精度差距。缺点是存在与Cryptonets同样的问题，客户端需要根据模型的结构生成加密参数，泄露了模型隐私。

2017年Hesamifard等人[31]提出了CryptoDL，它是一种可以对密文数据进行分类的深度神经网



(a) Sigmoid函数图像　　(b) 分段激活函数图像

图 2 Sigmoid函数与分段激活函数图像

络。其主要思想在于利用已用明文训练好的模型对Leveled-FHE加密的数据进行分类，采用低阶多项式逼近神经网络(Cellular Neural Networks, CNNs)中常用的激活函数。同时采用单指令多数据(Single Instruction, Multiple Data, SIMD)批处理技术，有效提高了数据分类效率。2017年CCS上Liu等人[32]提出了基于茫然神经网络(Oblivious Neural Networks, ONN)的两方计算框架MiniONN。在离线预计算阶段引入了同态加密，而在在线预测阶段使用秘密共享和混乱电路，确保了模型和数据隐私。该框架直接计算Relu激活函数，并且用多项式较为精确地逼近了sigmoid函数，提高了神经网络预测的准确性。下面详细介绍一下本文主要的思想和方法。通过MiniONN框架可以将现有的神经网络转化成“茫然的神经网络”，这样就可以实现隐私保护下的机器学习的预测。场景是用户想要获得服务器的预测服务，但是又不想泄露自身的输入数据；服务器端拥有神经网络的模型，并且也不想向客户端泄露自己的模型(实际上就是一些参数，比如说线性回归中w和激活函数等)。总之，想要实现的就是在预测服务结束后，用户只得到最终的结果，并不知道关于模型的信息；同时服务器端也得不到任何关于用户输入的信息。首先，神经网络是由输入层，隐藏层和输出层组成的。隐藏层的操作一般包括：线性层计算输入数据和权重值之间的乘法，而后将结果输入到非线性层，也就是将乘法结果代入到一个非线性的激活函数中去计算，然后可能再经过池化层(就是一些求均值或求最大值的一些操作)。下面用具体的参数举例说明，在神经网络中用户输入数据通过隐藏层的线性操作和非线性操作后得到最终结果的过程(以2次线性操作1次非线性操为例)。在下面的式子中，x表示用户输入数据，$\boldsymbol{W}\cdot\boldsymbol{x}+\boldsymbol{b}$表示一次线性操作，然后经过一个函数$f$(可能是激活函数或者池化函数)运算后，又进行了一次线性操作，这样得到一个最终结果

$$
\begin{aligned}
&\boldsymbol{z}\sim=\boldsymbol{W'}\cdot f\left(\boldsymbol{W}\cdot\boldsymbol{x}+\boldsymbol{b}\right)+\boldsymbol{b'}\\
&\boldsymbol{x}=\begin{bmatrix}x_1\\x_2\end{bmatrix},\boldsymbol{W}=\begin{bmatrix}w_{1,1}&w_{1,2}\\w_{2,1}&w_{2,2}\end{bmatrix},\boldsymbol{b}=\begin{bmatrix}b_1\\b_2\end{bmatrix},\\
&\boldsymbol{W'}=\begin{bmatrix}w'_{1,1}&w'_{1,2}\\w'_{2,1}&w'_{2,2}\end{bmatrix},\boldsymbol{b'}=\begin{bmatrix}b'_1\\b'_2\end{bmatrix}
\end{aligned}\tag{2}
$$

MiniONN的思想还是秘密分享，将用户数据和服务器参数都分成两个份额分给服务器和用户进行安全计算。线性层的乘法操作可以通过前面介绍的Beaver 3元组的方式实现，该文基于同态生成这些乘法3元组。对于激活层和池化层的操作，也就是函数f的计算，实际上和线性操作类似，也是将线性操作层输出的结果分成两个份额，客户端拥有y^{C}，服务器端拥有y^{S}，将这两个份额作为输入得到函数f计算结果的各方份额。最终的预测结果也是分享到两方的，服务器端将自己的份额发送给客户端，客户端加和后就能得到最终的预测结果。MiniONN对于激活函数的操作，具体来说，对Relu函数$(y)=\max(0,y)$，通过两方执行一个混乱电路的比较协议实现这个函数的安全计算；对于其余的非线性的激活函数，则采用多项式逼近，通过算术电路进行计算。类似地，对于池化操作，如果是平均池化操作，也就是求平均值，只要让服务器和客户端分别计算各自份额的和，然后求均值即可。如果是最大池化操作，也就是求最大值，则采用混乱电路的比较协议实现。这样，在服务器半诚实的假设下，神经网络中的基本操作就都可以转化成一个半诚实模型下的安全两方计算的协议去执行了。MiniONN在数据集MNIST及CIFAR10上的运行效率如表1所示。

2016年Courbariaux等人[33]提出了二值化神经网络(Binary Neural Network, BNN)，它可用来对数据进行高效和准确的预测，主要用来在有限的内存和计算资源的设备上训练和测试深度学习模型。在此基础上，2018年Bourse等人[34]提出FHE-DiNN模型，利用神经网络的带符号整数权值和二进制激活函数执行加密预测，但目前预测的准确性一般。由于加密方案参数依赖于模型的结构，所以服务提供者如果更新模型，那么用户将需要重新加密数据。为了解决这个问题并且提高预测的准确率，2018年Sanyal等人[35]提出了TAPAS系统，主要研究了对全同态加密数据的机器学习模型的预测，将权重二值化，并且采用二值化和稀疏化技术，对加密数据进行加速和并行计算，准确率非常高。

对于现有神经网络如何转化为二值化网络进行高效预测，2019年USENIX上，Sadegh等人[36]提出了基于混乱电路的茫然神经网络的预测框架XONN，它可以在保护客户输入隐私的情况下，服务器端将正确的预测结果返回给用户。它将现有的神经网络首先转化为二值化神经网络，此时神经网络中，除了第1层的用户输入为常数外，此层的乘

表 1 MiniONN效率实验结果

数据集	MNIST	CIFAR10
精确度(%)	99.52	91.5
运行时间(s)	320	11686
数据传输(MB)	336.7	1803
#p/h	163840	2524

法操作可以用OT来实现，从第2层开始权重值和激活值都为+1或者–1。这样，从第2层开始神经网络中的乘法操作就可以通过混乱电路中的XONR操作来实现，利用混淆网络中的Free-XOR操作，可以极大提高神经网络的效率和预测的准确率。

4.3 联邦学习

传统机器学习中，一般是用户将数据上传服务器，由服务器在收集到的用户数据集合上进行学习，无法保护用户数据的隐私。2016年谷歌提出的一种隐私保护的机器学习框架：联邦学习。在联邦学习框架下，客户端不需要将自己的数据统一上传到服务器，而由各个终端用户训练出本地模型后，将各模型参数发送至各自服务器，各个服务器通过数据聚合得到整体模型。由于所有的本地模型都是各个终端用户利用本地数据训练后得到，因此可以比较易于实现整体数据隐私。具体过程见图3。

在文献[37–40]中，每一轮中具有参与资格的各终端用户从服务器获得某一整体模型的参数，然后将所获得的参数作为局部模型的初值进行本地训练并得到训练结果，训练结果可以看作是通过局部更新后的整体模型参数，最后将这些局部训练结果返回给服务器，服务器根据终端用户返回的结果聚合得到更新后整体模型，并进行多轮迭代。在联邦学习中，每一轮中终端用户和服务器之间的通信内容仅仅与模型参数有关，即终端用户的本地存储的原始数据并不会上传至服务器或发送给其它终端用户，但是需要说明的是，服务器端保存的终端用户局部训练得到的模型参数，虽然不会直接泄露用户的数据信息，但是也有可能存在某些攻击手段(比如说模型推断攻击)导致用户数据信息的泄露。

在联邦学习中，参数聚合一直是其训练中的核心的问题，也是隐私保护所要处理的主要问题。在最开始的方法中，参数服务器直接将明文形式的参数聚合在一起(求加权平均值)，这样的方法虽然能防止数据的直接泄露，但还是会给恶意敌手通过攻击手段获得客户端私密数据的机会。

为了解决这个问题，Google的Keith Bonawitz等人[41]在CCS2017上提出了一种高效安全的聚合方法：mask-then-encrypt，之后有许多研究扩展了这个方法，提升了其性能。在此本文沿着上述脉络介绍相关结果。

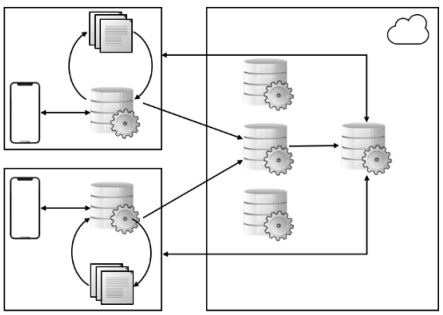


图 3 联邦学习

文献[41]中的方法适用于大规模数量的终端(例如手机)通过一个服务器，安全计算各输入之和的情形，即在计算中，无论是对服务器还是对其他的终端，都不能泄露任何特定终端的输入。例如，现在系统中有m个客户端$C_1, C_2, \cdots, C_m$，其中C_i持有隐私数据x_i，现在所有的客户端和服务器联合起来，共同求出所有隐私数据x_i的和$\sum_{i=1}^{m} x_i$，但是每个x_i都不能泄露给其他的客户端，并且也不能泄露给服务器端S。为说明文中采取的处理方法，先看一个简单的例子。对于任意两个数a, b，如果要求$c = a + b$，选取随机数r，令$a' = a + r$, $b' = b - r$，那么$a' + b' = a + r + b + r = a + b$。利用这个原理，让任意两个客户端$i$与$j$之间共享一个随机数$s_{ij}$，以此来盲化真实的数据$x_i$。而在所有被盲化的数据求和的时候，所有$s_{i,j}$就会抵消。聚合过程如式(3)

$$y_i = x_i + \sum_{j \in U, i<j} s_{i,j} - \sum_{j \in U, i>j} s_{j,i} \bmod R \tag{3}$$

聚合后的结果为

$$z = \sum_{i \in U} y_i = \sum_{i \in U} \left(x_i + \sum_{j \in U, i<j} s_{i,j} - \sum_{j \in U, i>j} s_{j,i} \right) = \sum_{i \in U} x_i \bmod R \tag{4}$$

两两之间共享的随机数可以通过DH密钥协商协议来实现，协商的密钥也作为伪随机数发生器PRG的种子，利用伪随机发生器的输出进行盲化。

然而，此时的聚合协议是在假设没有用户掉线的情况下进行的，如果在协议的执行阶段存在用户掉线，随机数就可能不能够抵消，这时客户端就得不到最后的聚合结果。为了防止客户端掉线以及服务器端不诚实的情况，文献[41]中提出了一个新的方法来解决这个问题，这种方法叫做double-masking。这种方法引入了一个新的随机数b_i，这个随机数产生的伪随机值直接加到盲化数据y_i上。现在的求和公式变为

$$y_i = x_i + \mathrm{PRG}(b_i) + \sum_{j \in U, i<j} \mathrm{PRG}(s_{i,j}) - \sum_{j \in U, i>j} \mathrm{PRG}(s_{j,i}) \bmod R \tag{5}$$

同时，C_i将对b_i和$s_{i,j}$进行秘密分享，将份额分

发给其余的客户端。这样，只要t个客户端在线就可得到正确的计算结果。

文献[41]中的方法存在一些待改进的问题。第一，密钥协商阶段的开销巨大，第二，秘密分享和秘密恢复的时间开销很大。为了优化这两个问题，2018年Mandal等人[42]提出了新的方案。针对第1个问题，文中引入了两个不合谋的“秘密提供者”，实际上是两个不合谋的服务器。这两个服务器在离线阶段生成后面计算过程中的主密钥，分发给用户，这样用户之间就不需要进行协商来产生密钥了；针对第2个问题，文中引入了正则图和邻居用户的概念，每个用户只和邻居协商盲化原始数据的随机数，并且其中一部分秘密分享用(3, 2)门限方案代替了(m, t)门限方案，大大减小了秘密分享的开销。整个聚合协议的效率提高了1.5倍到3倍。该方案的效率分析如表2所示。其中m表示用户数量，l表示通讯网络中节点的数量，r表示梯度向量的维度，$(k$–1)是秘密分享多项式的次数，$c(r, n)$是伪随机发生器的计算耗费，μ=$|q|$, λ=$|N|$, γ是DH群元素比特长度，ζ是中途退出用户的数量。

最近，在2019年CCS workshop上，Mandal等人[43]结合文献[42]中高效的安全聚合协议，面向线性回归和逻辑回归，解决联邦学习下的训练和预测问题。文中主要的场景和两方机器学习的场景类似，客户端要求输入数据保密，服务器端要求输入的模型保密。具体见图4。

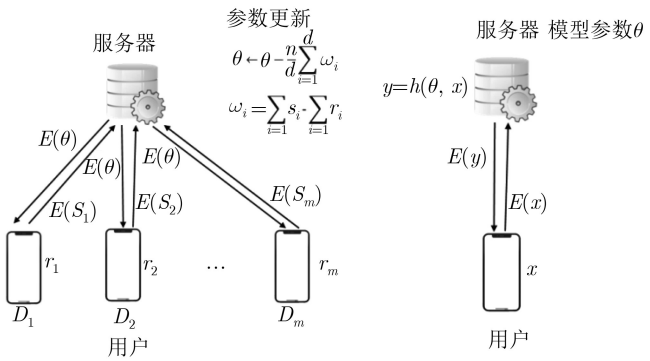
每次训练的时候，服务器通过同态加密将模型参数进行加密，然后将加密的模型参数传给用户，用户用自己的输入和这些参数执行安全计算协议之后得到两个份额：$E(s_i)$和r_i，且满足$\omega_i = s_i - r_i$，其中，$E(s_i)$表示s_i的密文。然后用户将$E(s_i)$返回给服务器，服务器解密得到s_i，并将s_i聚合得到$s = \sum_i s_i$。而对于r_i，用户将r_i发送给服务器端，服务器端可以通过聚合得到$r = \sum_i r_i$，这样服务器就能得到最后的ω_i。其中与之前的方案的最大不同点在于在每次计算梯度进行训练的时候不用事先确定在线的用户，只需要在共享数据恢复阶段确定在线的用户即可。而对于逻辑回归的训练，则会牵扯到非线性函数sigmoid。在此，Mandal采用了惯用的手段：多项式近似。近似用的多项式是$\sigma_3(x) = q_0 + q_1 x + q_2 x^2 + q_3 x^3$，具体协议和线性回归没有太大区别。对于茫然预测的功能，则是用户将数据进行同态加密之后发送给服务器，服务器使用模型进行计算，得到一个加密的标签之后返回给用户，用户解密就可以得到最终结果。

5 结束语

机器学习中的隐私保护问题，得到了研究者越来越多的关注。越来越多的研究者开始使用密码学工具来解决这一类问题。但是，受到现有密码学工具在效率及安全性上的局限，目前的解决方案只能在一些小规模的问题上进行应用。隐私保护的机器学习目前处在发展初期，许多问题亟待解决。在隐私保护下的机器学习模型训练时，高效的安全计算工具和适合安全计算的准确的激活函数逼近是目前面临的主要挑战。安全高效性与训练模型准确性的

表 2 文献[42]效率分析

	通信	计算	存储
用户端	$O((\lambda+\mu)m+nr)$	$O\left(m(\lg(m))^2+(l+1)\cdot c(r,n)\right)$	$O\left(4k\lambda+\mu\left(m+3\left\lceil\frac{l}{2}\right\rceil\right)+nr\right)$
服务器端	$O\left(m^2\mu+nmr+\frac{ml}{2}\right)$	$O\left(m^2+(m-\zeta)\cdot l\cdot c(r,n)\right)$	$O\left(mnr+m^2\mu+\frac{ml\mu}{2}\right)ght)$



(a) 训练预测模型 (b) 为用户提供预测服务

图 4 安全数据聚合协议

平衡是实现隐私保护下机器学习的一个长期课题。在进行隐私保护下机器学习预测时，特别是利用神经网络的带符号整数权值和二进制激活函数进行加密预测时，目前所提出一些方案其预测的准确性不能令人满意，有待改善。在机器学习的各阶段，提取数据、模型参数或其统计特征的攻击也是值得注意的一个安全性问题。对于联邦学习来说，其聚合阶段的隐私保护需求是一个典型的安全多方计算场景，针对这种聚合的特殊性质，构造更加有效的安全多方计算协议，或者对更复杂的聚合函数进行讨论的成果，目前较少见到。在安全性方面，现在大多数可行方案都是半诚实模型安全的，恶意模型下安全的较为实用的模型不多，事实上这类模型具有更大需求。

参 考 文 献

[1] YAO A C. Protocols for secure computations[C]. The 23rd Annual Symposium on Foundations of Computer Science, Chicago, USA, 1982: 160–164.

[2] YAO A C C. How to generate and exchange secrets[C]. The 27th Annual Symposium on Foundations of Computer Science, Toronto, Canada, 1986: 162–167.

[3] GOLDREICH O, MICALI S, and WIGDERSON A. How to play ANY mental game[C]. The 19th Annual ACM Symposium on Theory of Computing, New York, USA, 1987: 218–229.

[4] BEN-OR M, GOLDWASSER S, and WIGDERSON A. Completeness theorems for non-cryptographic fault-tolerant distributed computation[C]. The 20th Annual ACM Symposium on Theory of Computing, Chicago, USA, 1988: 1–10.

[5] 蒋瀚, 徐秋亮. 实用安全多方计算协议关键技术研究进展[J]. 计算机研究与发展, 2015, 52(10): 2247–2257. doi: 10.7544/issn1000-1239.2015.20150763.
JIANG Han and XU Qiuliang. Advances in key techniques of practical secure multi-party computation[J]. *Journal of Computer Research and Development*, 2015, 52(10): 2247–2257. doi: 10.7544/issn1000-1239.2015.20150763.

[6] BEAVER D. Efficient multiparty protocols using circuit randomization[C]. Annual International Cryptology Conference, Santa Barbara, USA, 1992: 420–432.

[7] BENDLIN R, DAMGÅRD I, ORLANDI C, *et al*. Semi-homomorphic encryption and multiparty computation[C]. The 30th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Tallinn, Estonia, 2011: 169–188.

[8] DAMGÅRD I, PASTRO V, SMART N, *et al*. Multiparty computation from somewhat homomorphic encryption[C]. The 32nd Annual International Cryptology Conference, Santa Barbara, USA, 2012: 643–662.

[9] PAILLIER P. Public-key cryptosystems based on composite degree residuosity classes[C]. International Conference on the Theory and Applications of Cryptographic Techniques, Prague, Czech Republic, 1999: 223–238.

[10] GENTRY C. A fully homomorphic encryption scheme[D]. [Ph.D. dissertation], Stanford University, 2009.

[11] VAN DIJK M, GENTRY C, HALEVI S, *et al*. Fully homomorphic encryption over the integers[C]. The 29th Annual International Conference on the Theory and Applications of Cryptographic Techniques, French Riviera, France, 2010: 24–43.

[12] BRAKERSKI Z, GENTRY C, and VAIKUNTANATHAN V. (Leveled) fully homomorphic encryption without bootstrapping[J]. *ACM Transactions on Computation Theory*, 2014, 6(3): No.13.

[13] DUCAS L and MICCIANCIO D. FHEW: Bootstrapping homomorphic encryption in less than a second[C]. The 34th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Sofia, Bulgaria, 2015: 617–640.

[14] 孙茂华, 胡磊, 朱洪亮, 等. 布尔电路上保护隐私集合并集运算的研究与实现[J]. 电子与信息学报, 2016, 38(6): 1412–1418. doi: 10.11999/JEIT150911.
SUN Maohua, HU Lei, ZHU Hongliang, *et al*. Research and implementation of privacy preserving set union in Boolean circuits[J]. *Journal of Electronics & Information Technology*, 2016, 38(6): 1412–1418. doi: 10.11999/JEIT150911.

[15] KOLESNIKOV V, KUMARESAN R, ROSULEK M, *et al*. Efficient batched oblivious PRF with applications to private set intersection[C]. 2016 ACM SIGSAC Conference on Computer and Communications Security, Vienna, Austria, 2016: 818–829.

[16] KOLESNIKOV V, ROSULEK M, TRIEU N, *et al*. Scalable private set union from symmetric-key techniques[EB/OL]. https://eprint.iacr.org/2019/776, 2019.

[17] BARNI M, ORLANDI C, and PIVA A. A privacy-preserving protocol for neural-network-based computation[C]. The 8th Workshop on Multimedia and Security, Geneva, Switzerland, 2006: 146–151.

[18] ORLANDI C, PIVA A, and BARNI M. Oblivious neural network computing via homomorphic encryption[J]. *EURASIP Journal on Information Security*, 2007, 2007(1): 037343. doi: 10.1186/1687-417X-2007-037343.

[19] GRAEPEL T, LAUTER K, and NAEHRIG M. ML confidential: Machine learning on encrypted data[C]. The 15th International Conference on Information Security and Cryptology, Seoul, Korea, 2012: 1–21.

[20] ZHANG Qingchen, YANG L T, and CHEN Zhikui. Privacy preserving deep computation model on cloud for big data feature learning[J]. *IEEE Transactions on Computers*, 2016, 65(5): 1351–1362. doi: 10.1109/TC.2015.2470255.

[21] HESAMIFARD E, TAKABI H, GHASEMI M, *et al*. Privacy-preserving machine learning in cloud[C]. 2017 ACM

Cloud Computing Security Workshop, Dallas, USA, 2017: 39–43.

[22] ROUHANI B D, RIAZI M S, and KOUSHANFAR F. DeepSecure: Scalable provably-secure deep learning[C]. The 55th ACM/ESDA/IEEE Design Automation Conference, San Francisco, USA, 2018: 1–6.

[23] NIKOLAENKO V, WEINSBERG U, IOANNIDIS S, *et al*. Privacy-preserving ridge regression on hundreds of millions of records[C]. 2013 IEEE Symposium on Security and Privacy, Berkeley, USA, 2013: 334–348.

[24] MOHASSEL P and ZHANG Yupeng. SecureML: A system for scalable privacy-preserving machine learning[C]. 2017 IEEE Symposium on Security and Privacy, San Jose, USA, 2017: 19–38.

[25] CHANDRAN N, GUPTA D, RASTOGI A, *et al*. EzPC: Programmable, efficient, and scalable secure two-party computation for machine learning[EB/OL]. https://eprint.iacr.org/2017/1109, 2017.

[26] DEMMLER D, SCHNEIDER T, and ZOHNER M. ABY-A framework for efficient mixed-protocol secure two-party computation[C]. 2015 Network and Distributed System Security, San Diego, USA, 2015: 1–15.

[27] XIE Pengtao, BILENKO M, FINLEY T, *et al*. Crypto-nets: Neural networks over encrypted data[EB/OL]. https://arxiv.org/abs/1412.6181, 2014.

[28] DOWLIN N, GILAD-BACHRACH R, LAINE K, *et al*. CryptoNets: Applying neural networks to encrypted data with high throughput and accuracy[C]. The 33rd International Conference on Machine Learning, New York, USA, 2016: 201–210.

[29] BOS J W, LAUTER K, LOFTUS J, *et al*. Improved security for a ring-based fully homomorphic encryption scheme[C]. The 14th IMA International Conference on Cryptography and Coding, Oxford, England, 2013: 45–64.

[30] CHABANNE H, DE WARGNY A, MILGRAM J, *et al*. Privacy-preserving classification on deep neural network[EB/OL]. https://eprint.iacr.org/2017/035, 2017.

[31] HESAMIFARD E, TAKABI H, and GHASEMI M. CryptoDL: Deep neural networks over encrypted data[EB/OL]. https://arxiv.org/abs/1711.05189, 2017.

[32] LIU Jian, JUUTI M, LU Yao, *et al*. Oblivious neural network predictions via MiniONN transformations[C]. 2017 ACM SIGSAC Conference on Computer and Communications Security, Dallas, USA, 2017: 619–631.

[33] COURBARIAUX M, HUBARA I, SOUDRY D, *et al*. Binarized neural networks: Training deep neural networks with weights and activations constrained to +1 or –1[EB/OL]. https://arxiv.org/abs/1602.02830, 2016.

[34] BOURSE F, MINELLI M, MINIHOLD M, *et al*. Fast homomorphic evaluation of deep discretized neural networks[C]. The 38th Annual International Cryptology Conference, Santa Barbara, USA, 2018: 483–512.

[35] SANYAL A, KUSNER M J, GASCÓN A, *et al*. TAPAS: Tricks to accelerate (encrypted) prediction as a service[EB/OL]. https://arxiv.org/abs/1806.03461, 2018.

[36] SADEGH RIAZI M, SAMRAGH M, CHEN Hao, *et al*. XONN: XNOR-based oblivious deep neural network inference[C]. The 28th USENIX Conference on Security Symposium, Santa Clara, USA, 2019: 1501–1518.

[37] MCMAHAN H B, MOORE E, RAMAGE D, *et al*. Communication-efficient learning of deep networks from decentralized data[C]. The 20th International Conference on Artificial Intelligence and Statistics, Fort Lauderdale, USA, 2017: 1272–1282.

[38] KONEČNÝ J, MCMAHAN B, and RAMAGE D. Federated optimization: Distributed optimization beyond the datacenter[EB/OL]. https://arxiv.org/abs/1511.03575, 2015,

[39] KONEČNÝ J, MCMAHAN H B, YU F X, *et al*. Federated learning: Strategies for improving communication efficiency[EB/OL]. https://arxiv.org/abs/1610.05492, 2016.

[40] 杨立君, 丁超, 吴蒙. 一种同时保障隐私性与完整性的无线传感器网络可恢复数据聚合方案[J]. 电子与信息学报, 2015, 37(12): 2808–2814. doi: 10.11999/JEIT150208.
YANG Lijun, DING Chao, and WU Meng. A recoverable privacy-preserving integrity-assured data aggregation scheme for wireless sensor networks[J]. *Journal of Electronics & Information Technology*, 2015, 37(12): 2808–2814. doi: 10.11999/JEIT150208.

[41] BONAWITZ K, IVANOV V, KREUTER B, *et al*. Practical secure aggregation for privacy-preserving machine learning[C]. 2017 ACM SIGSAC Conference on Computer and Communications Security, Dallas, USA, 2017: 1175–1191.

[42] MANDAL K, GONG Guang, and LIU Chuyi. NIKE-based fast privacy-preserving high-dimensional data aggregation for mobile devices[R]. CACR Technical Report, CACR 2018–10, 2018.

[43] MANDAL K and GONG Guang. PrivFL: Practical privacy-preserving federated regressions on high-dimensional data over mobile networks[EB/OL]. https://eprint.iacr.org/2019/979, 2019.

蒋 瀚：男，1974年生，讲师，研究方向为密码学与信息安全.
刘怡然：女，1996年生，博士生，研究方向为密码学与信息安全.
宋祥福：男，1992年生，博士生，研究方向为密码学与信息安全.
王 皓：男，1984年生，副教授，研究方向为密码学与信息安全.
郑志华：女，1962年生，副教授，研究方向为密码学与信息安全.
徐秋亮：男，1960年生，教授，研究方向为密码学与信息安全.