计算机研究与发展
Journal of Computer Research and Development
DOI:10.7544/issn1000-1239.2020.20200614
57(10): 2027-2051, 2020

边缘计算隐私保护研究进展

周 俊 沈华杰 林中允 曹珍富 董晓蕾
(上海市高可信计算重点实验室(华东师范大学) 上海 200062)
(jzhou@sei.ecnu.edu.cn)

Research Advances on Privacy Preserving in Edge Computing

Zhou Jun, Shen Huajie, Lin Zhongyun, Cao Zhenfu, and Dong Xiaolei
(*Shanghai Key Laboratory of Trustworthy Computing* (*East China Normal University*), *Shanghai* 200062)

Abstract The wide exploitation of the theory of mobile communication and big data has enabled the flourishment of the outsourced system, where resource-constrained local users delegate batch of files and time-consuming evaluation tasks to the cloud server for outsourced storage and outsourced computation. Unfortunately, one single cloud server tends to become the target of comprise attack and bring about huge delay in response to the multi-user and multi-task setting where large quantity of inputs and outputs are respectively fed to and derived from the function evaluation, owing to its long distance from local users. To address this bottleneck of outsourced system, edge computing emerges that several edge nodes located between the cloud server and users collaborate to fulfill the tasks of outsourced storage and outsourced computation, meeting the real-time requirement but incurring new challenging issues of security and privacy-preserving. This paper firstly introduces the unique network architecture and security model of edge computing. Then, the state-of-the-art works in the field of privacy preserving of edge computing are elaborated, classified, and summarized based on the cryptographic techniques of data perturbation, fully homomorphic encryption, secure multiparty computation, fully homomorphic data encapsulation mechanism and verifiability and accountability in the following three phases: privacy-preserving data aggregation, privacy-preserving outsourced computation and their applications including private set intersection, privacy-preserving machine learning, privacy-preserving image processing, biometric authentication and secure encrypted search. Finally, several open research problems in privacy-preserving edge computing are discussed with convincing solutions, which casts light on its development and applications in the future.

Key words edge computing; privacy-preserving; secure data aggregation; secure outsourced computation; secure multiparty computation

摘 要 移动通信与大数据理论的广泛应用使得外包系统蓬勃发展,资源受限的本地用户将大批量的数据文件和开销巨大的计算任务外包给云服务器完成.然而,为了解决单一的云服务器容易成为敌手俘获

收稿日期:2020-08-14;**修回日期**:2020-08-25
基金项目:上海市自然科学基金项目(20ZR1418400);国家自然科学基金项目(61632012,61672239,U1636216);中央高校基本科研业务费专项资金(40500-20104-222196);中国博士后科学基金项目(2017M611502)
This work was supported by the Shanghai Natural Science Foundation (20ZR1418400), the National Natural Science Foundation of China (61632012, 61672239, U1636216), the Fundamental Research Funds for the Central Universities (40500-20104-222196), and the China Postdoctoral Science Foundation (2017M611502).
通信作者:曹珍富(zfcao@sei.ecnu.edu.cn)

攻击的目标导致单点失败,且在基于多输入输出的多用户、多任务场景中由于远离用户端易造成反馈延迟较大而成为外包系统瓶颈的问题,边缘计算应运而生.在边缘计算中,多个位于云服务器与用户端之间的边缘节点相互合作完成外包存储与外包计算任务,很大程度上解决了外包系统的实时性问题;但同时也带来了巨大的安全与隐私保护挑战.首先给出了边缘计算特有的网络模型与安全模型,并在此基础上从边缘计算的隐私保护数据聚合、隐私保护外包计算和包括隐私保护集合运算、隐私保护机器学习、隐私保护图像处理、隐私保护生物认证、隐私保护的密文搜索等面向应用的安全计算问题 3 方面出发,基于数据扰动、全同态加密、安全多方计算、全同态数据封装机制和可验证与可审计等密码技术,对边缘计算隐私保护领域的国内外最新研究成果进行了系统的阐述、总结与科学归类.最后,探讨了边缘计算隐私保护当前面临的挑战、未来潜在的研究方向及其解决思路,以期进一步推动边缘计算隐私保护研究的发展与应用.

关键词 边缘计算;隐私保护;安全数据聚合;安全外包计算;安全多方计算

中图法分类号 TP391

随着移动通信与大数据[1]的高速发展,信息化生活已经普及至千家万户,深刻地改变人们的生活习惯和工作模式.智能医疗、智能家居和智能交通等应用已广泛应用于日常生活中,给人们带来了极大的便利.例如,智能家居不仅能提供家电控制服务,还能实现实时的环境监测及防盗报警等功能,帮助我们构建舒适且安全的生活环境.另一方面,物联网与传感技术的蓬勃发展导致了数据的爆炸式增长,据不完全统计和预测:到 2020 年底将有 500 亿设备连入互联网,而到 2025 年这个数字将达到 5 000 亿[2-3].然而,只具备有限计算能力和存储空间的本地设备难以有效地处理这些数据.如何高效地分析利用这些海量信息成为了一个亟待解决的问题.

云计算最初被认为是一种很有前途的计算基础设施,资源受限的本地用户将其大批量的数据文件和开销巨大的计算任务外包给存储和计算资源丰富的云服务器完成[4].然而,单一的云服务器架构集中化存储和处理大量的原始数据会带来严重的带宽和能耗问题,且容易成为敌手俘获攻击的目标,导致单点失败.此外,针对一些需要实现实时响应、位置感知和上下文感知等功能的基于多输入、多输出的多用户和多任务场景,由于云服务器和用户设备的距离较远,往往会带来较大的通信延迟,从而成为外包系统的安全与性能瓶颈.

为了弥补云计算的不足,引入了边缘计算[5]的概念,用于将云计算拓展至网络的边缘.具体地说,边缘计算是一种新的分布式计算模式,由多个位于云服务器和本地用户之间的边缘节点合作完成外包存储与外包计算任务.由于其能够在靠近用户终端设备的网络边缘存储和处理数据,因此能较好地支持实时响应、环境感知等功能,从而适用于智能电网[6]、自动驾驶、虚拟现实(virtual reality, VR)等多个应用场景.

尽管边缘计算具有许多优点,但它也面临着各种安全和隐私威胁.边缘计算作为云计算的拓展,仍具有一些云计算中的安全问题:边缘节点由于其内部故障与外部攻击,通常假定与云服务器一样处于半可信或恶意敌手环境中.前者是指边缘节点会诚实执行协议并通过与协议其他参与方进行最大程度的交互来窃取其隐私信息;后者是指边缘节点可通过任意行为来破坏协议的正确执行.另一方面,由于边缘计算具有分布式部署、多元异构和低延迟等自身特性,会带来一些特有的安全与隐私保护问题.边缘节点介于云服务器与本地用户间的资源限制也使得云计算中典型的安全模型无法直接应用于边缘计算,因此,如何设计基于边缘计算的轻量级安全与隐私保护方案成为近年来国内外的研究热点.

1 边缘计算模型

本节主要介绍边缘计算的网络模型与安全模型.

1.1 网络模型

边缘计算将一些云处理过程移动至更接近终端设备的位置,从而最大限度地利用了网络边缘中未开发的计算能力[7].边缘节点是网络边缘上具有计算和存储能力的设备.它们可以是资源受限的设备,如网关、路边单元、机顶盒、路由器等,也可以是拥有丰富资源的设备,如微云等.

边缘计算的网络模型如图 1 所示.边缘计算系统包括 3 个不同的实体,即本地用户设备(local

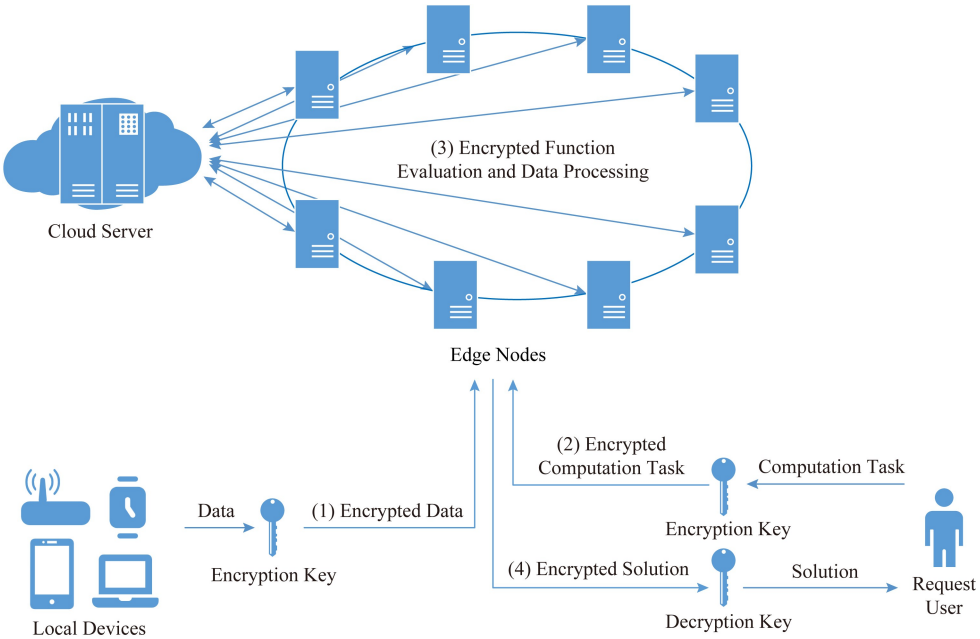

图 1　边缘计算的隐私保护网络模型

Fig. 1　Network architecture of privacy preserving in edge computing

devices/request user)、边缘节点(edge nodes)和云服务器(cloud server),本地用户设备的存储、计算和通信能力最弱,云服务器的资源最丰富,而边缘节点则处于两者之间.为了实现不同实体间的通信,边缘计算采用了各种通信技术,包括有线通信(例如以太网和光纤)、无线通信(例如蓝牙、NFC、IEEE 802.11)或两者的组合[8].这 3 个实体可以直接连接或通过权威机构(如证书机构或密钥生成中心)间接连接.如果发现网络任何威胁,权威机构将立即介入以处理事故.

具体地说,边缘计算的 3 层架构描述如下:

1) 最底层是用户设备层.由大量物联网设备组成,如传感器、智能手机、智能可穿戴设备等.其中一些设备是移动物联网对象,另一些是固定物联网对象.这些设备能够生成或感知原始数据,并发送给更高层次的设备进行进一步处理.

2) 中间层是边缘节点层.由具有一定计算能力的设备组成,如基站、路由器等.边缘节点由网络设备组成,如具有计算能力的路由器、网关、交换机和基站等.这些设备在边缘计算中称为边缘节点,可以通过网络连接部署在任何地方.边缘节点倾向于将云计算扩展到网络边缘,它具有一定的计算和存储能力和自治能力,可减少资源受限的物联网设备上的数据处理负载.除了常规通信(例如包转发和路由)之外,一些实时和需要高响应速度的应用程序可以从云服务器移至边缘节点.由于边缘节点距离设备较近,因此它们拥有有关设备及其所有者(即用户)的区域性知识,例如本地的网络情况、用户的移动方式及精确的位置信息.边缘节点能够为用户提供计算卸载、瞬态数据存储、缓存等服务,并能将来自云的服务传递给用户.为了减轻云的负担,边缘节点间可以相互合作分流计算任务.

3) 最上层是云服务器层.云服务器具有巨大的存储空间和计算资源,它能对边缘节点的预处理数据进行进一步的数据处理,并将计算任务委托给边缘节点.云服务器从各边缘节点接收数据摘要,并对其提交的数据和其他来源的数据进行全局分析,以改善各类网络应用服务[9],如智能配电[10]、电子医疗[11]等.此外,云服务器还向边缘节点发送策略,以提高边缘节点提供的服务质量.

1.2　特　性

边缘节点层的参与使得边缘计算与云计算并不完全相同,云计算与边缘计算的详细对比总结[12]如表 1 所示.

1) 位置感知[12].位置感知是指确定用户设备的地理位置的能力.云计算通常不提供位置识别服务,当云服务器需要获取用户的位置信息时,需要用户主动将位置信息发送至云服务器,这会带来巨大的通信开销,用户的位置隐私也可能泄露[13].而在边缘计算中,边缘节点能够感知自己覆盖区域内的用户

设备,因此用户不需要将自己的本地信息发送给远程的第三方.

2) 平均延迟[12].云服务器一般远离物联网设备,导致数据传输延迟较长.然而,同样拥有一定计算能力和存储空间的边缘节点距离物联网设备更近,这使得它们之间的数据传输时间更短.非实时应用程序(如离线游戏)一般不受数据延迟影响,但实时应用程序(如车载网)往往依赖于低延迟的数据传输.

3) 支持大规模物联网应用[12].由于繁重的管理和计算开销,云计算无法为大规模物联网应用提供服务.例如在广泛的环境监测系统中,大量的传感器会产生海量数据,如果在中央云服务器中管理这些传感器并执行数据处理,会带给云服务器较大的负担.而在边缘计算中,边缘节点可以以较小的开销在自己的区域内管理这些物联网设备.因此边缘计算能够有效地支持电网管理、环境监测和气候变化监测等大规模物联网应用.

4) 网络架构.在云计算中,有一个集中的服务器来管理、计算和存储资源.然而,边缘计算模式是一个分散的框架,实时的应用服务是由自组织的边缘节点所提供.

5) 移动性.在边缘计算中,具有高移动性的物联网设备通常是数据生产者,而在云计算中,数据往往由公司和企业产生,如腾讯、阿里巴巴等.由于物联网设备很容易从边缘节点覆盖的一个区域移动到另一个区域,边缘计算通常需要提供移动性支持.

Table 1 Feature Comparison Between Cloud Computing and Edge Computing

表 1 云计算和边缘计算特性比较

Features	Cloud Computing	Edge Computing
Locality Sensibility	No	Yes
Average Delay	High	Low
Enabling Large-Scale IoT Applications	No	Yes
Network Architecture	Centralized	Decentralized
Mobility	No	Yes

1.3 安全模型

边缘计算的隐私保护框架主要由 4 个步骤组成:1)存储、计算、通信资源受限的本地设备(用户)将采集的批量数据批量加密后上传至边缘节点;2)计算任务请求用户将加密的计算任务上传至边缘节点;3)边缘节点通过相互合作(必要时可与云服务器交互完成),在密文域上进行函数计算、数据分析与处理,并将密文的计算结果返回给请求用户;4)授权的请求用户解密计算结果(在不同的应用场景中,计算任务请求用户和本地设备、用户可以是同一实体或不同实体,参与边缘计算协议).

虽然边缘计算给用户提供了很大的便利,但仍存在其特有的安全与隐私保护需求.由于边缘节点往往工作在不可信的环境下,因此通常可分为半诚实(semi-trusted or honest-but-curious adversary)敌手模型和恶意(malicious adversary)敌手模型 2 类.前者是指边缘节点诚实地按照协议的规定执行计算任务,但同时通过与协议各方的交互最大限度地窃取其隐私信息;后者是指边缘节点能通过任意行为来破坏协议的执行,从而返回错误的计算结果.具体来说,我们将以基于边缘计算的电子医疗系统为例,从输入隐私、输出隐私、函数隐私、可验证性和高效性 5 方面展开阐述.

图 2 是边缘计算电子医疗系统隐私保护框架.医生用户(Physicians)的属性集合 AS 由 k 个属性子集 $AS_i(i=1,2,\cdots,k)$ 构成;k 个属性机构 $AA_i(i=1,2,\cdots,k)$ 分别为医生用户颁发对应属性子集的属性私钥.同时,d 个证书中心 $CA_j(j=1,2,\cdots,d)$ 合作为医生用户生成身份私钥.多个边缘节点采集各自负责区域病人用户的生命体征密文数据及其对应的访问控制策略,并在密文域上通过多方计算对区域的疾病发展趋势进行有效分析、预测.属性集合满足访问策略的医生用户可以成功解密分析、预测的明文结果,从而采取有效、及时与正确的干预措施.

1) 输入隐私.诚实的本地设备(用户)采集的数据隐私能抵抗由边缘节点、被俘获的本地设备与计算任务请求用户发起的合谋攻击.如在基于边缘计算的电子医疗系统中,输入数据表现为从本地用户(病人)身体采集的多类型生命体征数据,是本地用户的隐私.

2) 输出隐私.边缘计算结果隐私能抵抗由边缘节点、本地设备与恶意计算任务请求用户发起的合谋攻击,即边缘计算的结果仅能由被授权的请求用户访问.如:在基于边缘计算的电子医疗系统中,输出隐私表现为以本地用户(病人)生命体征数据、医检报告为输入的诊疗结果,是本地用户的隐私.

3) 函数隐私.即计算任务隐私,是指由诚实计算任务请求用户提交给边缘节点进行外包计算的函数隐私能保护由边缘节点、本地设备与恶意请求者发起的合谋攻击.如:在基于边缘计算的电子医疗系统中,边缘计算函数体现了医务人员对从病人身体

采集的生命体征数据、医检报告等进行分析诊疗的方法或医疗科研人员对医疗大数据进行分析和预测的处理方法,具有知识产权保护的需要;从而其函数隐私保护显得尤为必要.

4) 可验证性.可验证性是指边缘计算输入、输出数据的正确性可验证、可追责与可审计.该安全性需求是针对恶意敌手模型设计的,主要包括2方面:一是本地设备提交数据的合法性验证,如:在基于边缘计算的联邦学习系统中,如何有效甄别本地用户提交的数据集的合法性,从而避免恶意本地设备提交假数据而导致模型训练结果错误;二是对边缘计算结果实现正确性可验证,要求边缘节点在返回外包函数密文计算结果的同时提交计算结果正确性验证证据;计算任务请求用户在正确性验证通过的前提下,进一步解密得到边缘计算结果.

5) 高效性.边缘计算的隐私保护要求在密文域上处理数据,因此需要广泛利用(全)同态加密、安全多方计算等具有较高计算开销和通信开销的密码原语来实现.因此,如何构建轻量化的边缘计算隐私保护技术,以满足本地设备存储、计算、通信资源受限的客观性能需求是一个亟待解决的、具有挑战性的公开问题.否则,虽然在理论上能实现边缘计算隐私保护需求,但如果本地设备或计算任务请求用户用于隐私保护的计算开销大于其自己计算外包函数的计算开销,边缘计算就失去了外包的意义.

构建边缘计算隐私保护新理论和新方法需要在正确性(即边缘计算结果的可验证性)、安全性(输入隐私和输出隐私)、高效性3方面实现平衡.

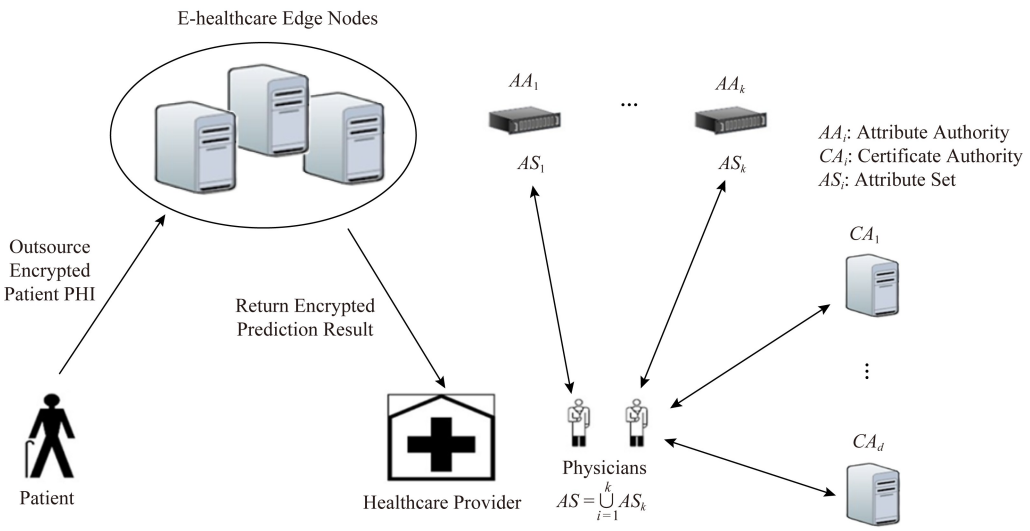

图2　边缘计算电子医疗系统隐私保护框架

Fig. 2　Framework of privacy preserving in edge-based e-healthcare system

2　边缘计算的隐私保护方案

本节从边缘计算的隐私保护数据聚合、隐私保护外包计算和面向应用的安全计算3方面,基于数据扰动、同态加密和安全多方计算等密码技术,对边缘计算隐私保护领域的国内外最新研究成果进行了系统的阐述、总结与科学归类.

2.1　隐私保护数据聚合

边缘计算的隐私保护数据聚合是指每个本地设备从周围采集并加密数据,再将加密数据发送给边缘节点,边缘节点相互合作在密文数据上进行分布式的多方聚合计算,在必要的情况下将聚合结果发送给云服务器做进一步的分析处理,或将聚合结果发送给授权接收方解密.在这个过程中,安全的数据聚合能够防止本地用户数据泄漏并且减少通信开销.

图3是基于边缘计算的智能电网隐私保护框架.在智能电网中,作为社区网关或地区网关的边缘节点可对隶属于该社区或地区的用户实时用电量在密文域上进行聚合,并将汇总后的密文提交到电力公司运营监测中心进行负荷监控.与由本地用户设备(智能电表)将所有实时用电量直接向电力公司传输相比,这种方式使得通信开销大大降低,且更易于社区网关与地区网关及时发现所在区域的用电负荷问题并加以实时控制.同时,本地用户的实时用电数据隐私和区域用电量聚合结果隐私都得到有效保护.

图4是基于边缘计算的智能交通系统隐私保护框架.在基于群智感知的车联网中,由路侧单元(road

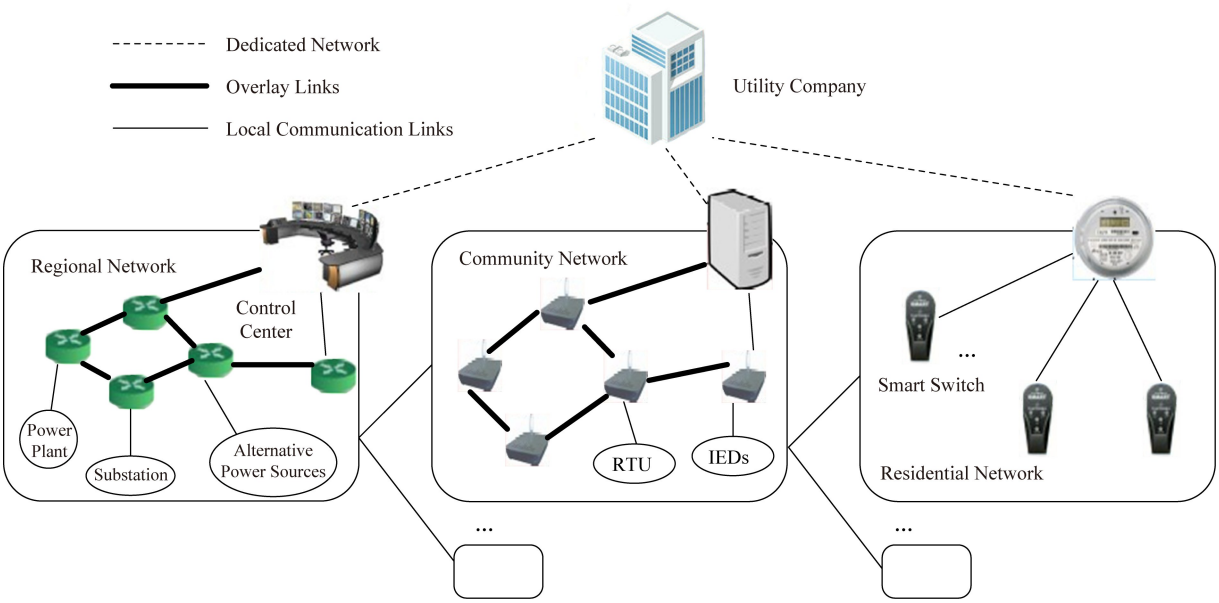

图 3 边缘计算智能电网隐私保护框架

Fig. 3 Framework of privacy preserving in edge-based smart grid

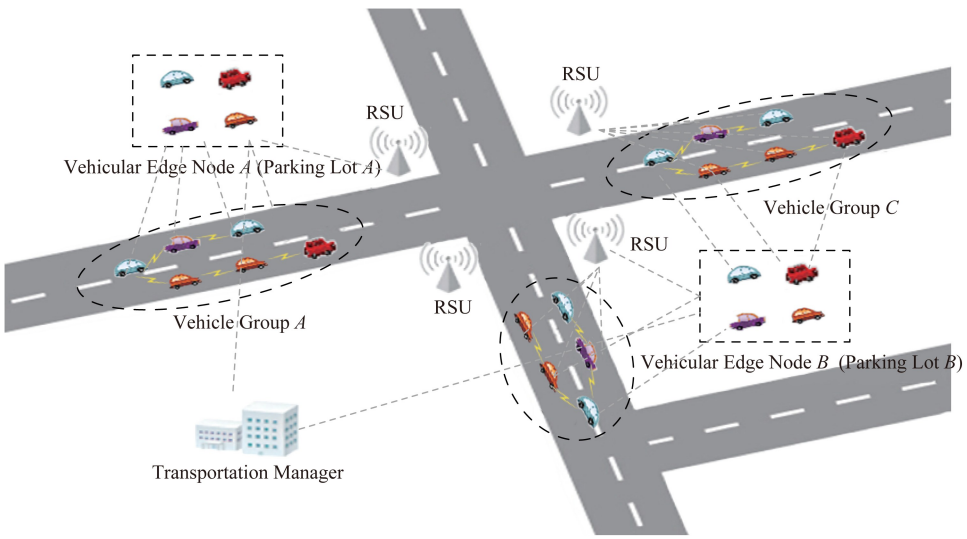

图 4 边缘计算智能交通系统隐私保护框架

Fig. 4 Framework of privacy preserving in edge-based intelligent transportation system

side unit, RSU)或处于临时闲置状态的车载设备(on board unit, OBU)担任的边缘节点从多个车辆收集并预处理加密后的交通流数据发送给云服务器,用于隐私保护的智能导航或各类基于位置的服务.因此,在边缘计算中实现基于不同安全需求和性能需要的隐私保护数据聚合就显得尤为重要.

目前,同态加密[14-16]和差分隐私[17-18]已广泛应用于智能电网以实现数据聚合,这些加密方案都支持加法同态.因此,边缘节点可以将本地设备采集的数据在密文上进行聚合.同态加密方案也能用于实现用户隐私保护[19],支持移动社交网络中的加法同态操作[20].

Lu 等人[14]利用同态加密为边缘计算中的异构物联网设备开发了一种轻量级数据聚合方案,保证了数据机密性和数据完整性,然而该方案没有考虑身份隐私、可追踪性、可拓展性和移动性.

Lyu 等人[17]提出了一种基于差分隐私和秘密共享技术的隐私保护数据聚合方案.具体来说,为了保证总体统计量的差分隐私,该方案利用高斯分布噪声对私有数据进行扰动.双层聚合可以减轻隐私泄露风险,从而保证数据的实用性.这篇文章使用公钥加密实现认证,为了保证方案的可拓展性还考虑了

节点的更新问题.然而,在提供数据聚合服务的同时,边缘节点可能会窃取用户的位置隐私并交给恶意第三方.此外,该方案并没有考虑数据完整性、身份隐私、可追踪性和移动性.

虽然上述边缘计算的隐私保护数据聚合方案[14,17]都具有容错功能,但未考虑到身份隐私保护问题.为了解决该问题,Wang 等人[15]引入了一种边缘计算场景下使用假名技术的匿名数据聚合方案.云服务器在注册阶段对边缘节点和用户设备进行认证,保证了所有参与边缘计算实体的真实性.该方案使用同态加密技术,既保护了本地设备的身份隐私,又保证了数据机密性.在该方案中,边缘节点和云服务器会对接收到的消息进行验证,保证了数据完整性.此外,该方案也考虑了本地设备和边缘节点的撤销问题,但移动性仍然没有被考察.与文献[14]不同,文献[15]和[17]的隐私保护数据聚合并未考虑边缘计算中数据的异构性.

为了同时保护数据隐私和身份隐私,Guan 等人[16]提出了一种将假名证书与 Paillier 同态加密相结合的方案,适用于增强的边缘计算物联网环境中的隐私保护数据聚合.在该方案中,每个边缘节点所负责的区域拥有一个本地证书颁发机构(local certificate authority, LCA)和一个可信证书颁发机构(trusted certificate authority, TCA).为了防止伪造证书,它将与用户设备一同生成和更新假名证书.此外,所有实体都可以在数据传输期间使用摘要来验证数据完整性,同时该方案还考虑了假名证书的更新和撤销,具有较强的灵活性.然而,上述所有数据聚合方案都不支持可追溯性,也无法验证聚合结果的正确性.

值得注意的是,国内外现有的大多数边缘计算隐私保护数据聚合方案[14-16,19-20]是利用公钥同态加密技术实现的;然而从效率方面看,直接将公钥加密算法作用在数据上违背了混合加密的基本原则,为资源受限的本地设备带来了巨大的计算和通信负担;从安全性方面看,无论是单用户、多数据聚合还是多用户、多数据聚合,都是用聚合结果接收方的公钥对本地数据进行同态加密,以保证密文域上的聚合计算;因此,本地设备数据对聚合结果接收方无法实现隐私保护;对除了聚合接收方以外的其他协议实体而言,加法同态加密仅能保证选择明文安全.另一方面,用数据扰动方法对本地数据加噪,又会对聚合结果的准确性产生一定程度的影响.

因此,如何在隐私保护数据聚合的准确性、安全性和性能 3 方面实现最优化是一个具有挑战性的公开研究问题,近年来受到了国际密码安全研究人员的广泛关注.边缘计算的另一个重要应用领域是认知无线电网络(cognitive radio network).认知无线电网络能通过频谱聚合与共享实现有效的频谱管理,从而解决极具增加的移动用户和有限的频谱带宽之间的供求矛盾.二级用户可以在与一级用户不产生地理位置冲突的前提下,发现和共用同一个频谱.然而,其中仍存在许多安全问题未能解决,其中最为重要的是用户位置隐私泄露问题.国内外现有工作或未能完全解决用户位置隐私保护问题,或依赖计算开销巨大的公钥同态加密技术实现,不适用于资源受限的移动用户的客观性能需求.Zhou 等人[21]不利用公钥同态加密技术,基于任意单向陷门置换提出了一个高效的隐私保护多用户数据聚合协议 PPMDA,并在此基础上构造了认知无线电网络中的轻量级隐私保护频谱聚合与拍卖协议 PPSAS.尤其值得指出的是,为了抵抗合谋攻击,还将 PPMDA 协议进行了分布式扩展设计,并且在密文域上实现了一个扩展的完美稳定婚姻匹配协议,从而在保护用户位置隐私的前提下,灵活实现了二级用户(竞拍者)利益最优化和拍卖方利益最优化.

2.2　隐私保护外包计算

在隐私保护数据聚合的基础上,在边缘计算中,资源受限的本地设备可将基于大批量输入数据的各类复杂多元函数计算任务外包给具备一定存储、计算和通信资源的边缘节点完成.本节将从 4 类适用于边缘计算隐私保护的外包计算技术,即:数据扰动、公钥全同态加密、安全多方计算和全同态数据封装技术出发,对国内外最新的研究成果进行阐述与归类.最后,我们小结了恶意敌手环境下,边缘计算结果正确性可验证与可审计方面的最新研究进展.

2.2.1　数据扰动

数据扰动(data perturbation)是在边缘计算中实现隐私保护的一类常用技术.通常,数据拥有者通过执行线性运算或非线性运算,以某些特定方式对原始数据进行盲化,然后将盲化后的数据外包给服务器用于数据分析与处理[22].具体的数据扰动方法包括交换记录值[23-24]、随机化[25]、几何扰动[26]、旋转扰动[27-28]、同分布样本替换[29-30]等.

Lin 在文献[31]中设计了一个保护隐私的内核 k 均值聚类外包方案,对向量中的所有值进行扰动运算.Yang 等人[32]采用了一种可检索的数据扰动

方法来进行隐私保护的外包计算.他们的方案通过添加噪声矩阵来保护私有数据,该矩阵具有被扰动的数据具有与原始数据相同的均值和协方差的特性.此外,几何数据扰动(geometric data perturbation)是一种组合技术,包括乘法变换、平移变换和噪声加法运算.这些子变换的集成在计算中展现出了良好的性能以及隐私保护能力[33-34].另一种是基于置换函数的数据扰动技术,在不改变原始数据值的情况下对其进行无序置换.较为常见的有矩阵置换,即置换矩阵的行和列.置换函数可以表示为 $\pi(i)=p_i$ $(i=1,2,\cdots,n)$,其中 i 是原始索引,而 $\pi(i)$ 是置换后索引.换句话说,第 1 个由 i 标记的元素将被 p_i 标记的元素替换.Duan 等人[35]提出了一种用于非负矩阵分解的安全可靠的外包方案.输入矩阵通过执行置换操作实现盲化,并且 2 个置换矩阵由 Knuth shuffle 算法生成[36].基于置换的方法已应用于许多特定的外包方案中,例如线性代数[37-38]、图像处理[39]和数据挖掘[40].

在基于数据扰动的方案中,随机值或置换的随机性被视为用户的秘密密钥.与基于密码方法的技术相比,扰动方法由于其相对简单的操作而通常导致较低的计算开销与通信开销.然而,其隐私保护的能力通常不如基于密码学的方法,某些重要信息经过线性(逆)变换还是会泄露一部分的数据,且对外包计算结果的准确性会带来一定程度的影响.

2.2.2 全同态加密

全同态加密可以在密文域上实现与明文域上相同的加法和乘法运算,并由于加法和乘法运算在有限域上功能是完整的,因此可实现使用这 2 个原子运算来构造的任意函数的同态计算.表 2 总结了具有代表性的公钥全同态加密方案(其中前 2 种 BGN 方案[41]和 Armknecht 等人提出的方案[42]是一定程度的同态加密方案 SWHE).

首先,一定程度同态加密(somewhat homomorphic encryption, SWHE)可以对密文执行有限次的加法和乘法运算,可认为是一种功能受限的全同态加密.如 BGN 密码系统[41]支持有限数量的加法同态运算,并且仅支持一次乘法同态运算.Armknecht 等人[42]基于编码理论问题提出了一种 SWHE 方案,它允许在任意有限域上进行任意次数的加法和固定次数的乘法运算.但是,该方案的密文大小随预期的加密总数呈指数增长.尽管 SWHE 同时支持加法和乘法,但是所允许的运算数量是有限的,因此只能用于小规模的程序/电路运算场景.

作为安全计算的高级解决方案,公钥全同态加密(fully homomorphic encryption, FHE)允许对密文进行无限次数的任意操作(包括任意次数的加法和乘法运算).2009 年,Gentry [43]首次提出了 FHE,他先构造了 SWHE 方案,并使它可引导.也就是说,该方案在解密之后还可以执行至少一次的同态操作.但是 Gentry 和 Halevi 的文献[44]中指出,基于文献[43]的全同态加密方案需要对明文消息逐位加密,计算开销非常巨大,所以无法直接用于边缘计算底层资源受限的本地设备.尽管随后提出了几种改进和优化方法[45-46],但就计算开销和密文扩张而言,这些方案对于边缘计算隐私保护应用仍然不切实际.此外,Gentry 等人[47]还提出了一种新的近似特征向量方法,以使同态加法和乘法运算更加有效.之后由 Brakerski 等人[48]根据带错误的学习(learning with errors, LWE)问题构造了另一种 FHE 方案.近年来,Halevi 等人[49]建立了一个名为 HElib 的 FHE 算法库,以实现上述的密码系统和自引导方法[50].Brakerski 等人[51]建立了一个新的有效工具来减少密文噪声.为了更有效地存储数据,Smart 等人[52]构造了一种 FHE 新技术,该技术允许将多个密文值打包为单个密文,并以单指令多数据(SIMD)方式对这些值进行操作.

为了进一步提高 FHE 的计算和通信效率,Ducas 等人[53]构建了具有有效自引导功能的 FHE 方案.Chillotti 等人[54-55]给出了 2 种改进的自引导方法,以使 FHE 方案切实可行.Meaux 等人[56]结合分组密码和流密码评估的优势,设计了一种有效的 FHE 方案,该方案具有密文的低噪声性质.Brakerski[57]提出了一种量子 FHE(quantum FHE, QFHE)方案,该方案提出在量子多项式时间内可计算的函数.在多项式量子电路中,同态计算的误差会成倍地减小.Boneh 等人[58]基于带错误的学习假设构造了阈值 FHE(threshold FHE, ThFHE)方案,此外 ThFHE 还给出了阈值密码系统的通用框架.由于 FHE 的天然优势(所有计算都可以在某个半可信的服务器中执行),因此许多基于 FHE 算法的应用程序都被设计出来,例如关联规则挖掘[59]、私有信息检索[60]和临床决策支持系统[61].虽然上述国内外关于公钥全同态加密(FHE)的轻量化工作取得了显著成效,但其高计算、存储和通信开销仍然无法满足边缘计算系统中资源受限的本地设备的客观性能需求,成为基于 FHE 的隐私保护外包计算获得广泛应用的严重障碍.

Table 2　Typical HE Schemes and Their Security Assumptions

表 2　代表性的同态加密以及他们的安全假设

Schemes	Homomorphism	Security Assumptions
BGN[41]	SWHE	Sub-group decision assumption
Armknecht et al[42]	SWHE	Decisional synchronized polynomial reconstruction assumption
Gentry[43]	FHE	Sparse subset sum assumption
Brakerski et al[48]	FHE	Learning with errors assumption
Ducas et al[53]	FHE	Learning with errors assumption
Chillotti et al[54]	FHE	Learning with errors assumption
Méaux et al[56]	FHE	Learning with errors assumption
Brakerski[57]	FHE	Learning with errors assumption for polynomial modulus

2.2.3　安全多方计算

安全多方计算(secure multi-party computation, MPC)是指一种在多用户间进行的安全计算的协议,其中多个参与方共同对他们的输入数据进行计算,同时保持各个输入数据为私有.MPC 是密码学中的一个热门话题,自 Yao 提出百万富翁协议[62]以来,它已经被研究了二十多年.Yao 的百万富翁问题描述了这样一种情况:假设有 2 个整数 a(来自参与方 A)和 b(来自参与方 B),目的是获得这 2 个整数之间的大小关系,但不向对方透露各自拥有整数的实际值.

Yao[63]首先描述了基于混淆电路(garbled circuit)的 MPC 的思想,通过门电路的组合来构造通用的 MPC.在这种设计中,参与方 A 首先创建了一个"混淆电路",并将该电路发送给另一方 B.然后 B 将他的输入放入电路中计算并将结果返回给 A.通过这样交换一些信息,双方会知道计算结果,但不知道另一方的输入.然而 Yao 的论文没有提供有关如何构建该通用电路的详细信息.后来,在双参与方的情况下高效的混淆电路技术被提出[64],以节省运行时间和存储空间.尽管双参与方的混淆电路取得了成功,但多方安全计算进度却比两方的情况要慢得多.减少多方计算中的轮复杂度一直是 MPC 研究中的重点.Beaver 等人[65]设计了一种用于常数轮的多方安全功能计算的方案(由 n 个参与方($n\geqslant 2$)组成,每个方都具有私有输入 $x_i(1\leqslant i\leqslant n)$).$n$ 个参与方希望在不暴露输入值的同时共同计算函数 $f(x_1, x_2, \cdots, x_i)$.Ben-Efraim 等人的研究[66]表明,通过多方混淆电路,对于半诚实的敌手,可以在常数轮的安全多方计算达到较好的表现.然后这项工作提出了一种构建混淆电路的新方法,对于大量参与方而言,每个门仅需进行常数次的操作即可对其进行运算.

Wang 等人[67]通过一个计算方预处理消息的方法实现了一个常数轮的多方计算协议,且在恶意敌手模型下安全.Zhu 等人[68]在 Wang 的方案的基础上运用动态规划进一步提升了安全多方计算的效率.Ananth 等人[69]基于 DDH 假设提出了一个 5 轮的多方计算协议,并基于混淆电路提出了一个 4 轮的多方安全计算协议.Badrinarayanan 等人[70]通过单项函数来实现了无状态令牌模型下的 3 轮的多方计算,并证明了在 UC 模型下安全.Mukherjee 等人[71]在随机字符串模型下提出了一个通用的 2 轮多方计算协议的构造.在有错误学习(LWE)假设下达到了半可信参与方模型下安全,在非交互式零知识证明的假设下达到了恶意敌手模型下安全.Boyle 等人[72]使用了逐位的不经意传输,提出了一个 2 轮的交换群内的多方计算协议.Garg 等人[73]通过减少使用不经意传输,用更多的单项陷门来代替,以减少公钥密码使用次数,来构造了高效的 2 轮多方安全计算协议,且在半可信和恶意敌手模型下都保证了安全性.Benhamouda 等人[74]通过提出了一个交互式混淆电路,构造了通用的方法来使用 k 轮的不经意传输构造 k 轮的多方计算.

除了减少轮复杂度,很多工作关注于安全多方计算的安全等级,比如在不同敌手的门限数量的情况下保证安全性以及可用性.Coretti 等人[75]优化了异步传输中的多方安全计算的轮数,在恶意敌手模型下达到了 $t<n/3$ 门限的敌手数量.Hazay 等人[76]构造了一个半诚实模型下的多方计算协议,可以达到敌手门限数量为 $n-1$.在此基础上,他们又将方案转化为恶意敌手模型下安全[77].Lindell 等人[78]提出了一种通用框架,可以将算数电路中的半诚实模型下安全的多方计算协议转化为恶意敌手模型下安全的多方计算协议.Benhamouda 等人[79]构造了一个非交互式的多方计算协议,可以在恶意敌手模型下抵抗常数大小的敌手腐化攻击.Garay 等人[80]

分析了多方计算要达到次线性级的通信开销所需要牺牲的安全性.在具有静态腐化能力的敌手条件下能容忍的恶意用户数量为 $t<(1/2)n$. Damgard 等人[81]构造了一个任意环内的多方安全计算,并将被动安全的多方计算方案转换成了主动安全的多方计算方案,代价是减少能容忍的敌手的门限数量. Chida 等人[82]构造了恶意敌手模型下的大规模多方计算协议,且只比半可信模型的协议开销高一倍,但代价是牺牲了多方计算中的公平性.Cohen 等人[83]研究了具有自适应腐化能力的恶意敌手模型在不同敌手数量门限下保证多方计算的安全性所需要的开销,最高安全性可达的敌手数量为 $n-1$,最快的效率可达到次线性级别的通信开销.Patra 等人[84]得出结论,n 个参与方的多方安全计算最少需要 $\lceil n/2\rceil+1$ 轮交互来保证公平性并抵抗主动/被动攻击.Cohen 等人[85]分析了不同安全等级下参与需进行的最少的广播轮次.

由于很多现实应用都需要多参与方共同进行计算,大量参考文献使用混淆电路方法来设计用于实际应用的协议,例如生物识别[86]、私有线性分支程序[87]、保护隐私的远程诊断[88]和人脸识别[89].但是,这些方案仍然需要很高的计算量和多轮的通信复杂度[90].

MPC 的另一种构造方法是基于秘密共享的协议,该协议使用秘密共享(secret sharing)技术生成随机份额,并将份额分配给不同的参与者,并且参与者共同交互地计算目标函数.秘密共享(由 Shamir[91]和 Blakley[92]首先提出)可以将机密信息分割并分配给一定数量的拥有者,只有在聚集了足够多的拥有者的情况下,才可以联合执行解密.Ben-Or 等人[93]和 Chaum 等人[94]提出了安全计算任何函数的协议.他们都设计了以(可验证的)秘密共享形式对秘密值进行加法和乘法(XOR 和 AND)运算.依靠每个门上的加法和乘法运算,就可以逐个门计算任何函数.基于通用秘密共享的 MPC 协议往往比解决专门函数的多方计算协议的效率低,这有 2 个原因.首先,通用电路通常很大;其次,乘法子协议效率很低,因为它需要大量的交互.因此,一系列研究集中于为特定函数开发有效的 MPC 协议.Damgård 等人[95]提出了基于通用秘密共享机制的用于比较、相等性测试和位分解操作的通用协议.Nishide 和 Ohta[96]构建了更高效的协议,用于求解 2 个数的大小关系,而无需依赖位分解协议.后来 Dinur 等人[97]通过分布式离散对数问题构造了一个同态的秘密分享协议.除此之外,很多拥有特定安全属性的多方计算方案被提出,比如隐藏输入输出大小[98]、威慑合谋的敌手[99]、隐藏网络拓扑结构[100].很多工作聚焦于方便其他学者设计的 MPC 方案,比如 Eldefrawy 等人[101]设计了一套代码 EasyCrypt,可以让机器自检多方安全计算的安全性及效率,Agarwal 等人[102]提出了一组叫做 CPS 的代数结构来更方便地进行多方安全计算.还有很多针对特定功能的更有效的 MPC 协议也被提出了,例如安全的多方乘积[103]、标量乘积[104]、排序[105]、矩阵分解[106]和集合求交[107]等.这些协议已用于隐私保护的多方数据挖掘[108]、多方科学计算[109]、数据库查询[110]、几何计算[111]等.

2.2.4 全同态数据封装机制

基于数据扰动的边缘计算隐私保护方案虽然采用了较高效的盲化技术,但无法保证外包计算结果的准确性.在基于公钥全同态加密技术实现的边缘计算隐私保护中,存储、计算、通信资源受限的本地设备需要用公钥全同态加密去加密其采集的每一个数据,违背了混合加密的基本原则,且本地设备执行公钥全同态加密运算的次数与数据量的大小 n 成线性关系(计算复杂度为 $O(n)$);其数据安全(包括本地设备采集的输入数据隐私和计算结果隐私)仅达到选择明文安全(公钥全同态加密由于其密文具有延展性,无法达到适应性选择密文安全).在基于安全多方计算的方案中,多个边缘节点间较高的通信开销与轮复杂度又成为了边缘计算隐私保护轻量化的瓶颈.

为了解决上述问题,Cao 和 Zhou 等人[112]提出了不依赖传统的公钥全同态加密技术,通过减少公钥加密使用次数构造轻量级安全外包计算新理论构想、总体实现思路和方法.具体而言,依据边缘计算节点存储、计算资源受限、自组织和通信范围有限等特点,形式化刻画了基于边缘计算的物联网中的隐私保护外包计算的安全模型.在此基础上,不利用公钥全同态加密技术,通过离线状态下一次任意单项陷门置换与在线状态下仅包含简单加法、乘法运算的对称加法同态映射,设计了高效的安全外包数据聚合方案.

在安全性方面,该方案中由于本地设备提交给边缘节点的数据密文中包含了对随机数(该随机数用于带密钥的对称全同态映射加密数据本身)的任意单向陷门置换这一密文项,由于该密文项是不具有全同态性质的,而边缘计算是在针对数据加密的对称全同态映射上进行,因此其外包计算结果可达到

适应性选择密文安全.在性能方面,本地设备仅在离线状态下执行了一次任意单向陷门置换(其计算开销相当于一次任意公钥加密),对大批量的 n 个数据实现批量加密,因此其公钥加密使用次数复杂度为 $O(1)$,与本地设备采集的数据大小无关.该方案解决了国际著名密码学家 Gentry[113] 团队在国际三大顶级密码会议之一美密会上提出的"如何利用比全同态加密更高效的密码原语设计可验证安全计算(our work leaves open several interesting problems. It would be desirable to devise a verifiable computation scheme that used a more efficient primitive than fully homomorphic encryption.)"这一挑战性公开问题.同时,进一步将上述理论与方法应用到基于边缘计算的物联网中,解决了轻量级数据包安全传输与高效的隐私保护认证两大问题.

针对边缘计算的隐私保护,国内外学者更关注如何在多服务器架构下构造轻量级的隐私保护外包计算协议.Zhou 等人[114] 在合作且不合谋的双服务器架构下,提出了一个轻量级的多用户、多数据安全外包计算协议,并在此基础上研究无线车联网的高效数据包认证协议.车联网的位置服务有助于基于地理位置的社交网中的信息获取,认证保证了基于位置服务信息的有效性与不可伪造性.然而,由于车联网通信中存在大量的冗余信息与无用信息、周期性分发认证密钥导致的高认证开销、基于消息标识码过滤的不彻底性和公钥全同态加密使用等原因,使得现有的认证协议无法满足资源受限的车载设备的性能需求或不适应于车联网对实时控制的需求.作者不利用传统的公钥全同态加密技术,在不合谋的双服务器假设下,首先提出了一个高效的多密钥安全外包计算协议 MSOC.然后,基于 MSOC,在无需用户与服务器在线交互的前提下,设计了一个高效的隐私保护整数比较协议 LSCP.再次,基于 MSOC 协议,设计一个高效的隐私保护信息过滤系统,在执行位置服务消息认证前过滤了冗余和无用信息,从而构造了最终的轻量级隐私保护认证协议 LPPA.车载用户的位置隐私、兴趣隐私得到有效保护,可抵抗路侧单元和半诚实服务器(或密码服务提供商)发起的合谋攻击.尤其值得一提的是,所构造的 MSOC 方案中密文具有可重随机化性质,从而进一步保护了车载用户的兴趣模板隐私,即敌手对 2 个不同车载用户是否对同一条位置服务信息感兴趣这一事实计算不可区分.

2.2.5　可验证与可审计

在恶意敌手模型中,无论是理性的边缘节点为了从本地设备获得更多外包计算收益从节省计算资源的角度出发,还是被敌手俘获的边缘节点都可能将错误的计算结果返回给计算任务请求方.另一方面,边缘节点在网络边缘代表上层云服务器向用户提供分布式计算服务,云服务器也关心边缘节点是否向用户提供了正确可信的计算结果.因此,计算结果的正确性验证对于用户和云来说都是非常重要的.如果没有检查返回结果正确性的机制,云服务器可能不愿意将计算任务分摊给边缘节点,当用户无法访问边缘节点提供的服务时,意味着边缘计算分流失败.如何在实现边缘计算数据隐私保护的基础上保证外包计算结果的正确性可验证与可审计成为具有挑战性的研究热点.

Gennaro 等人[115] 引入了可验证计算的概念,并设计了一种基于混淆电路的非交互式可验证计算方案[116].Chung 等人[117] 利用全同态加密方案构造了一个使用较小公钥的非交互式可验证计算方案.此外,Parno 等人[118] 设计了一种基于 CP-ABE 的公开可验证计算方案,Papamanthou 等人[119] 提出了一种云环境下新的动态计算验证模型.为了支持多用户系统,Choi 等人[120] 提出了一种使用代理无关传输方案的多用户非交互式可验证计算方案.Gordon 等人[121] 利用 ABE、全同态加密和混淆电路构造了一个多用户可验证的计算方案.Elkhiyaoui 等人[122] 提出了一种有效的公开可验证的计算委托,Zhuo 等人[123] 采用可验证计算技术设计了一种保护隐私的可验证数据聚合移动众包方案.

聚合签名为实现边缘计算结果高效可验证与可审计提供了重要的研究思路.聚合签名的工作原理如下:给定来自同一用户的 n 个不同消息上的 n 个签名,可以将这 n 个签名聚合成一个签名[124].为了实现用户多个签名的聚合,目前已提出了许多聚合签名方案[125-126] 来缩短签名长度.其中,为了克服聚合签名中的 n 个签名只能来源于同一个用户这一局限性,我们引入了多签名[127]、顺序聚合签名[128] 和同态签名[128] 等密码原语,用来聚合来自 n 个不同用户对同一消息的 n 个签名.Ni 等人[129] 利用多密钥同态签名来聚合由多用户对同一消息产生的多个签名.然而,目前还没有一种在无需多用户预先共享秘密的前提下,使用多密钥同态签名来将 n 个用户对 n 个不同消息的 n 个签名实现高效聚合的方法;相信在这一方向的突破会对基于多输入、多输出

的多用户、多任务场景下的边缘计算结果正确性高效可验证与可审计问题提供有力的理论支撑.

上述边缘计算结果的正确性可验证方案主要通过 Yao 的混淆电路(garbled circuit)、双线性配对或聚合签名技术实现,因此计算开销巨大.如果计算结果验证的开销大于外包计算任务请求方自身计算外包函数的计算开销,则外包计算将违背其初衷.另一方面,在边缘计算中,边缘节点以分布式的方式协同执行用户的计算任务.一个边缘节点所得出的错误(中间)计算结果会扩散到邻近的其他边缘节点,从而导致错误结果的迅速累积直至最终外包计算结果正确性验证失败.因此,如何对边缘计算的所有中间结果和最终结果进行及时验证,以保证结果的正确性,并对输出错误结果的边缘节点进行快速有效追踪与审计,仍然是值得关注的研究问题.

2.3 面向应用的隐私保护边缘计算

本节将从 2 类基本函数、人工智能神经网络、图像处理、生物认证和密文搜索等应用场景出发,具体阐述边缘计算的隐私保护在各类新兴智能网络服务中的应用密码学研究.

2.3.1 基本函数的边缘外包计算

基本函数是指解决基本算术问题的一些简单操作,如集合运算、矩阵运算等.

1) 集合运算.集合通常被用作不同对象的容器.集合上的主要操作包括集合求交、集合求并,它们已作为基础模块应用于许多程序中,例如数据挖掘、图形算法和推荐服务.本节主要讨论集合交集、并集及其变体的外包方案.由于集合内的数据有时会涉及用户隐私,因此需要保证集合元素运算结果正确性以及安全性.

集合求交是指在计算出多个集合之间的共同元素.在边缘计算环境中,一个或多个客户端共同计算并获得交集结果,而其各自的集合保持私有状态.边缘节点有效地执行预设的相交操作,但无法得知集合中的任何信息.

Freedman 等人[130]讨论了半诚实和恶意对手模型中的安全的两方集合相交协议,想法是将集合元素映射到多项式中,然后依靠同态加密方案在密文上进行运算.基于文献[130]的思想,Dachman-Soled 等人[131]描述了一种用于集合相交的鲁棒协议,对恶意敌手的行为具有验证能力.该算法还采用 Shamir 秘密共享技术,通过 k 阶多项式共享服务器的集合,其中 k 是安全参数.为了验证最终结果的正确性,服务器和客户端在服务器集合上共同运行了一个切割选择协议.最终,客户端正确地获得自己集合和服务器集合的交集.

除隐私和正确性要求外,效率也是集合运算中要考虑的重要因素.Yang 等人[132]利用 RSA 密码系统的乘法同态性质提出了一种高效的集合相交协议,在半诚实模型下安全.该协议假设 2 个不同的参与方(即 A 和 B)拥有各自的私有集,这些私有集已加密并外包到云中.当一方 A 尝试获取其集合的交集结果时,他向另一方 B 发送请求信号.如果 B 同意参与该集合交集,则他将向云发送许可消息和一些必要的信息.由于具有同态属性,云服务器对加密的集合进行操作,并将交集结果(也是加密形式)返回给 A.最后 A 解密结果并恢复交集,而不会知道 B 的私有集的信息.客户端上的计算仅涉及几个简单的模块化乘法.如果有多个客户端(每个客户端都拥有一个秘密集合),则云服务器将在从客户端那里接收到许可消息后,在所涉及的加密集合之间执行集合相交操作.Chen 等人[133]利用分层的 FHE 方案构造了一个私有集求交协议.通过组合各种优化技术(例如批处理和散列技术),大大降低了通信和计算成本,并证明了在半诚实模型下安全.除了用多项式来表示集合,Ruan 等人[134]将集合表示为向量,集合相交运算由此转换为向量运算.Zhu 等人[135]基于 GM 密码系统构造了另一个基于 Bloom 过滤器的集合表示形式.该协议允许多个客户端外包其集合并获得集合相交结果,而无需透露其私有集合.

2) 矩阵运算.矩阵乘法是 2 个矩阵之间的运算,无论在特定应用程序中还是其他矩阵运算中,矩阵乘法通常被用作构造块.在矩阵乘法的外包方案中,假设矩阵 $\boldsymbol{A}$ 和矩阵 $\boldsymbol{B}$ 是输入矩阵,则在服务器端进行计算之后,客户端将以最小的开销得到 $\boldsymbol{C}=\boldsymbol{AB}$ 的结果.服务器将永远不会知道原始输入矩阵或最终的乘法结果.当对 $n\times n$ 维矩阵进行运算时,矩阵乘法公认的理论上限为 $O(n^{\omega})(\omega\geqq 2.38)$.但是,在实际运用中,计算复杂度通常接近 $O(n^3)$.

在许多工作中都研究了具有可验证属性的矩阵乘法外包方案.Mishra 等人[136]采用了一种新颖的矩阵包装方法,提出了一种高效的安全矩阵乘法方案.在该协议中,将输入矩阵的条目打包为一个多项式,并使用 SWHE[137]方案进行加密.在该协议中,2 个矩阵之间的乘法只需要对密文进行一次同态乘法运算.由于文献[136]仅支持 2 个矩阵之间的乘法运算,为了改进这一点,Mishra 等人[138]基于 BGV 密码系统,进一步提出了多矩阵乘法.另外,该方法

是在 HElib 下实现的,具有很高的效率.Lu 等人[139]也提出了一种具有更高效率的安全矩阵乘法协议.为了减少计算和通信的开销,引入了几种优化方法.一方面,使用中国剩余定理(Chinese Remainder Theorem, CRT)设计了一种高效的打包技术,以单次同构运算为代价来计算一批内积.另一方面,在协议的开头构造了一个预先计算的表,并由客户端多次重用,从而大大减少了客户端的工作量.实践证明,该方案并发性也很高.Benjamin 等人[140]设计了将矩阵乘法分配给 2 个云服务器的协议.每个输入矩阵都随机分成 2 个份额,分别外包给 2 个服务器.为了保持强大的可验证性,Atallah 等人[141]通过扩展 Shamir 的秘密共享和语义安全的 AHE 方案的组合技术,提出了一种仅使用一个服务器的改进解决方案.Mohassel[142]基于不同的 HE 方案分析了委托同态矩阵乘法的有效性.他们的工作证明了如果采用的 HE 方案满足 2 个属性(即关联性和独特性),则可以用 $O(n^2)$复杂度验证计算结果.

上述隐私保护的基本函数计算协议[136-142]大多利用公钥(全)同态加密技术实现,其巨大的计算开销和密文扩张无法满足边缘计算场景中存储、计算和通信资源受限的本地设备的性能需求和适应性选择密文安全性.为了解决该问题,Zhou 等人[143]构造了各类轻量级隐私保护外包信号处理协议.密文域上的信号处理使得外包计算环境中,在保持大规模信号分析与处理结果精确性的前提下,对不可信的云服务器和未授权用户保护敏感的信号消息.国内外现有工作大多采用 Paillier 公钥加法同态加密技术对输入信号逐一进行加密,为资源受限的用户本地带来了巨大的计算开销,且无法对信号处理结果的授权接收方有效保护每一个输入信号的隐私.该方案不利用公钥同态加密算法,提出了一个高效的隐私保护外包离散小波变换协议 PPDWT(包括 PPDWT-1 和 PPDWT-2 两个子协议).具体而言,PPDWT-1 协议中的信号输入隐私能有效抵抗半诚实的云服务器和未授权用户发起的合谋攻击;PPDWT-2 协议中的信号输入隐私和小波变换系数隐私均能有效抵抗上述合谋攻击.所构造的协议 PPDWT 利用离线状态下一次任意单向陷门置换运算对输入信号进行批量加密,并实现密文域上的信号处理.仅授权用户(即小波变换外包计算任务请求方)能成功解密离散小波变换的结果.国内外现有的利用公钥同态加密技术实现的协议在用户端的计算复杂度是 $O(|l|)$(其中 l 是输入信号的大小),而该协议在用户端的计算复杂度为 $O(1)$.此外,作者还进一步讨论了隐私保护信号处理中扩张因子对结果精确度影响的上限,以及在隐私保护离散傅里叶变换与余弦变换上的方案扩展,并在 UC 通用组合安全模型下形式化证明了所构造协议 PPDWT 的安全性.

2.3.2　人工神经网络

机器学习(machine learning)极大地推动了人工智能的发展.机器学习的框架模拟生物大脑中的神经系统,包含一组连接的单元或节点.在输入和输出层之间具有多个隐藏层的神经网络被称作深度神经网络(deep neural network, DNN).递归神经网络(recursive neural network, RNN)和卷积神经网络(convolutional neural network, CNN)是 DNN 的两大类型.为了降低本地设备用户的计算开销与通信开销,通常在边缘节点和云服务器进行模型训练和分类、回归等各种预测评估.如果说基于单一云服务器的外包计算可应用于传统的隐私保护机器学习,则基于边缘计算的外包计算模型则与隐私保护的联邦学习存在天然对应关系.

图 5 表明了边缘计算场景下的隐私保护联邦学习(Edge-AI)框架,主要由 4 个步骤组成:1)本地用户将加密数据集发送给负责本区域数据处理的边缘节点;2)边缘节点在密文域上执行本地训练过程,获得并将加密的局部参数发送给上层云服务器;3)云服务器聚合加密的局部参数,获得加密的全局参数并返回至各边缘节点;4)各边缘节点重复多轮密文域上的模型训练,直到满足训练目标为止(如满足特定的预设损失函数要求).虽然联邦学习与传统的机器学习相比,由于本地用户的数据集并未直接上传到云服务器,实现了一定程度的隐私保护;然而,敌手仍可以通过窃听信道中传输的模型参数来推导用户数据集的构成,从而发起成员推理攻击.此外,恶意本地用户还企图上传恶意数据来破坏模型训练的准确性.最终,由于边缘节点和云服务器通常工作在半可信或恶意敌手环境中,用户的数据集隐私及其合法性、模型参数隐私和预测评估结果隐私均应实现有效保护.

Xie 等人[144]和 Gilad-Bachrach 等人[145]实现了加密数据上神经网络的隐私保护预测.在该协议中,客户端将加密的样本特征(通过 HE 算法)发送到云中,以根据训练后的模型进行预测.输入数据和预测结果均对云服务器保密.Ma 等人[146]提出了第一个完全非交互的(在云服务器和客户端之间)神经网络

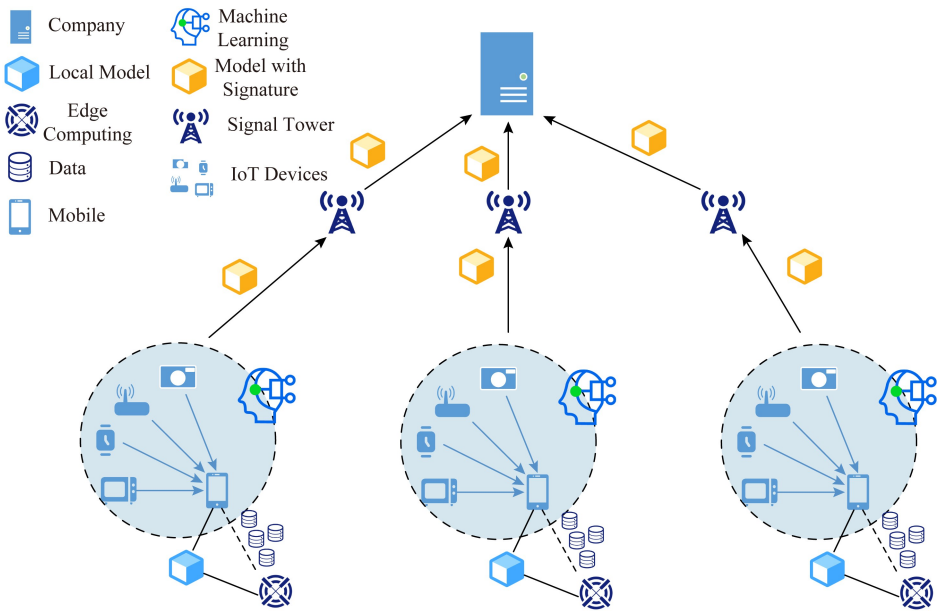

图 5 边缘计算联邦学习隐私保护框架

Fig. 5 Framework of privacy preserving in edge-based federated machine learning

预测方案.在协议中,使用秘密共享技术将训练后的模型分为 2 个随机部分,然后分别将其发送到 2 个非竞争服务器.由于加法同态性,服务器在客户端的输入数据(通过 Paillier 方案加密)上交互地应用神经网络,并将加密的预测份额返回给客户端.最后,客户端通过组合结果份额来解密并恢复其数据样本的相应预测.他们的方案中,客户端的计算与通信开销是独立的,与模型的大小无关.

文献[144-146]这 3 个工作假设神经网络模型是已经训练好的,仅关注预测阶段.而 Hesamifard 等人[147]主要考虑神经网络的训练阶段,实现了安全地对加密数据运行 CNN 算法的方案.为了突破 HE 算法的局限性,该协议使用低阶多项式来近似激活函数,并使用近似多项式来训练 CNN 模型.然后,在加密数据上运行训练后的模型以进行预测.Tang 等人[148]提出了一种具有安全保证和高精度的分布式深度学习方案.在该协议中,数据请求者将加密的梯度外包给数据服务提供商,以进行新一轮的模型权重更新.采用新的参与者(即密钥变换服务器)对加密的梯度进行重加密.同时,数据服务提供商使重新加密的梯度具有加法同态性,并对密文执行更新计算.最后,每个数据请求者获得更新的权重并将其解密.在该算法中,为了实现隐私性,增加了额外的通信成本.Shamsabadi 等人[149]使用全同态加密以及多方安全计算方案提出了一种分布式的隐私保护的机器学习训练及预测方案.

国内外现有的隐私保护机器学习工作大多利用公钥全同态加密或安全多方计算技术完成,导致高额的计算开销与密文扩张,且要求用户与服务器之间进行多轮在线交互.为了解决该问题,Zhou 等人[150]首先提出了一个高效的单密钥全同态数据封装机制 SFH-DEM;然后基于该机制,设计了一系列可用于隐私保护机器学习模型训练与计算的原子计算协议,如密文域上的多元多项式计算协议、非线性激活函数计算协议、梯度函数计算协议和最大值计算协议等;最终,在离散神经网络中提出了一个轻量级隐私保护的模型训练与计算协议 LPTE,同时还进一步给出了扩展到加密域上卷积神经网络的具体方法.形式化安全性证明表明所构造协议在半诚实敌手模型下能有效保护用户的数据集隐私、模型训练隐私和模型计算结果隐私;在 MNIST 数据集上的实验结果表明,其所构造的 LPTE 协议用于离散神经网络中隐私保护的手写数字识别时,比同类方案相比,具有更高的准确性与高效性.

2.3.3 图像特征提取与匹配

图像特征提取与匹配在图像分析、处理和识别过程中都必不可少.它的主要目的是从原始图像数据中提取有用的特征,以作为分析图像的重要依据.图像提取算法已经发现了广泛的应用场景,如基于云的电子医疗系统[151]和生物识别系统[152].国内外隐私保护的图像特征提取算法主要集中在 4 类特征:尺度不变特征变换(SIFT)[153]、加速鲁棒特征

(SURF)[154]、定向梯度直方图(HOG)[155]和位置上下文描述子(shape-context)等.

SIFT[162]是一种用于检测和描述图像局部特征的算法,具有强大的抗攻击特征点检测能力.Hsu 等人[156]利用 Paillier 加法同态加密算法,提出了安全可靠的 SIFT 计算外包协议,实现了 SIFT 特征在加密域中的提取和表示.该算法包括 4 个主要部分:高斯差分(DoG)变换、特征点检测、特征描述和描述子匹配.在这基础上,Hsu 等人[157]进一步探索了一个类似的基于公钥同态加密的安全 SIFT 外包方案.该算法基于离散对数问题和 RSA 问题,对纯密文攻击(cybertext only attack, COA)和已知明文攻击(known plaintext attack, KPA)是安全的.然而,文献[156-157]从隐私角度引入了很大的计算复杂性和一定的不安全性[158].为了消除这些限制,Hu 等人[159]提出了一种高级协议.与用 Paillier 密码系统加密初始图像不同,该工作将原始图像分成 2 个随机共享串,并将加密后的子图像上传到 2 个独立的云服务器上.采用 SWHE 方案和 SIMD 批处理技术对比较过程进行了改进.此外,隐私保护 SIFT 方案很好地保留了原始明文上 SIFT 方案在显著性和鲁棒性方面的重要特性.为提供更强的隐私,Li 等人[160]利用文献[161]的部分解密 Paillier 密码体制,提出了另一种安全的 SIFT 特征提取方案.为了进一步减少公钥(全)同态加密给资源受限的本地设备带来的巨大开销,Zhou 等人[151]基于任意单向陷门置换提出了隐私保护的整数比较协议,并在此基础上构造了密文域上轻量级的基于 SIFT 的图像特征提取与匹配协议.

SURF[162]被认为是 SIFT 的增强版.与 SIFT 相比,它可以更快地执行,并且对不同的图像变换更加健壮.SURF 算法的步骤和原理与 SIFT 算法基本一致,但在尺度空间、特征点检测和方向确定、特征描述符等方面存在一些差异.比如说,SIFT 算法通过找到 DoG 域中的极值点来作为特征点提取,而 SURF 算法通过计算所构造的 Hessian 矩阵的行列式进行特征检测.Bai 等人[163]提出了一种在加密域中执行的 SURF 特征提取外包解决方案.通过 Paillier 密码系统的性质来进行密文上的计算.但是,由于操作需要客户端和服务器之间的多个交互,因此会产生相当大的通信开销.除此之外,它也很难保存原始 SURF 的主要特征.基于这些观察结果,Wang 等人[164]设计了一个实用的 SURF 计算外包协议,它使用 2 个非共谋服务器来共同计算输入图像的加密特征描述符.在该算法中,基于 SWHE 和 SIMD 技术设计了高效的乘法和比较操作交互子协议,不仅支持安全计算,而且降低了整体通信开销.

HOG 是计算机视觉和图像处理中广泛应用的另一种图像特征描述子,它是通过计算局部区域的梯度方向直方图而形成的.Wang 等人[165]为 HOG 计算设计了安全的外包方案.该工作介绍了加密域中 HOG 计算的 2 种不同模式下的隐私保护协议:单服务器和双服务器设置.在单服务器模式下,利用 SWHE 与 SIMD 技术相结合对原始图像进行加密,达到了安全和高效的双重要求.加密的特征描述符被安全地计算并返回给客户端.对于双服务器模型,首先将图像随机分成 2 个共享,然后将加密的共享分别发送到 2 个独立的服务器.之后,2 台服务器共同计算各自的加密特征描述符.在最后一步中,客户机解密并恢复组合从服务器返回的这 2 部分的功能描述符.利用一种更有效的同态方法(即向量同态加密(VHE)[166]),Yang 等人[167]还提出了一种隐私保护的 HOG 特征提取方案.直接对图像矢量进行加密,可以很好地应用于图像处理.基于一个 FHE 方案,Shortell 和 Shokoufandeh[168]还设计了一个安全框架,使 SURF 和 HOG 计算能够在加密域中进行.在协议中,SURF 和 HOG 任务分别在有理数和固定点二进制数上实现.实验评估表明,这些解决方案[165-167]达到了与原始 HOG 解决方案相当的性能.

位置上下文描述子(shape-context)是一种侧重于图像中各组成元素相对位置的特征描述符.国内外的一部分研究工作利用公钥(全)同态加密实现可验证的隐私保护图像特征提取与匹配,在资源受限的移动用户本地带来了巨大的计算和通信开销;另一部分已有工作未能实现加密域上的图像去噪,或仅研究基于尺度不变特征变换描述子的外包图像处理,无法满足位置敏感的图像特征提取要求.为了解决上述问题,Zhou 等人[169]首先基于任意单向陷门置换,提出了一个高效的隐私保护可验证图像去噪协议,提高了加密域上图像匹配的精度,并在此基础上,构造了安全高效的整数比较协议与计数协议;最终设计了一个基于位置上下文描述子的、轻量级隐私保护可验证图像特征提取与匹配协议.该协议有效保护了用户的图像隐私与图像匹配结果隐私,同时利用轻量级的同态消息认证码技术实现了图像匹配结果的高效可验证,使得用户端的计算开销由 $O(Nn)$降低到 $O(1)$,云服务器端的计算开销由 $O(n_M^2)$降低到 $O(n_M)$,云服务器的通信开销由

$O(n_M)$降低到$O(1)$,其中N,n和n_M分别代表图像数、每个图像中的像素点个数和去噪匹配函数中所需乘法运算次数.

2.3.4 生物认证

生物特征认证是一种利用人类固有的生理和行为特征进行身份识别或访问控制的技术.通过比较目标样本和数据库中样本之间的生物特征,如果比较结果在一定阈值范围内,系统就可以成功地识别出对应个体.

Chun等人[170]利用加法同态加密与Yao混淆电路混合方法提出了一种隐私保护方案,将生物特征认证的任务外包.这项工作使用云服务器存储加密的生物特征数据,并使用另一个独立服务器保存解密密钥.这2个服务器在协议期间交互操作,它们都不会学习敏感的生物特征信息和中间结果.然而,由于2台服务器之间的通信成本昂贵,该方案并不实用.Yasuda等人[171]利用公钥SWHE提出了隐私保护的模式匹配协议,并在DNA序列上实现了安全的通配符模式匹配(即可以在查询的模式中包含通配符),该协议具有良好的性能和较低的通信复杂度.

Sedenka等人[172]引入了另一种生物特征认证外包方案,该方案使用可扩展的Manhattan和Euclidean验证器,首先提出了一种基于Yao混淆电路方法的算法,然后将其改进为一种基于加法同态加密的隐私保护方案.为了提高认证的准确性,作者采用了主成分分析(principal component analysis, PCA)的思想,但增加了计算和通信的开销.为了获得更好的效率表现,Hu等人[173]分别针对单服务器和双服务器(假设2个服务器是非共谋)模型描述了2种不同的外包生物识别任务的解决方案.单服务器协议使用对称密钥加密方案和数学变换来盲化数据.在协议的末尾,服务器对输入记录和数据库记录之间的欧几里德距离进行排序,并将最近的记录返回给客户端.而双服务器协议采用了与SIMD模型相结合的公钥SWHE方案,实现了更高的安全标准.在同态计算完距离后,服务器将索引转换为带有输入记录最小距离的置换索引返回给客户端.因此,结果的实际索引及其相关距离对于服务器来说是未知的.对于半诚实模型,前者在已知样本攻击(known sample attack, KSA)下是安全的,而后者在已知明文攻击(KPA)下实现安全.Salem等人[174]提出了一种保护隐私的生物识别系统,能同时满足数据安全和验证能力的要求.根据加法同态的性质,对加密后的特征进行识别.此外,客户端还增加了一项真假生物特征数据检测任务,增强了系统结果的完整性和正确性.

在体域网(body area network)中基于生物特征的轻量级隐私保护可认证密钥协商协议是近年来国内外的研究热点之一.体域网已被广泛采用于电子医疗服务中,用于有效地实时监测病人的健康状况和各类应急处理.具有即插即用和透明性的密钥协商协议是在人体传感器之间建立安全通信信道不可或缺的重要密码原语.现有的工作主要利用模糊保险库技术,允许部署在同一个人体上的传感器节点间以较高的概率建立安全的密钥对.其中真实的生物特征点数据和为了隐私保护加入的噪声点数据从概率多项式时间能力的敌手的角度不可区分,但同时因处理大批量的噪声冗余数据带来了巨大的额外开销.为了解决该问题,Zhou等人[175]设计了轻量级的隐私保护集合求交集协议,并在次基于上构建了一个体域网中安全高效的基于生物特征的确定性密钥协商协议.其安全性可归约至单向陷门函数求逆的困难问题,而不依赖于其他方案中采取的模糊保险箱的大小.与同类方案相比,该方案具有更强的容侵性,以及更少的存储空间、计算和通信开销.

2.3.5 密文搜索

密文搜索是我们日常生活中经常使用的加密数据库最为重要的应用之一,它能在保护用户查询隐私和数据文件隐私的前提下返回包含特定关键词的数据文件.

图6是边缘计算密文搜索隐私保护框架.通常,一个密文搜索协议包含4个步骤:1)数据拥有者将加密后的数据文件上传至边缘节点或云服务器;2)查询

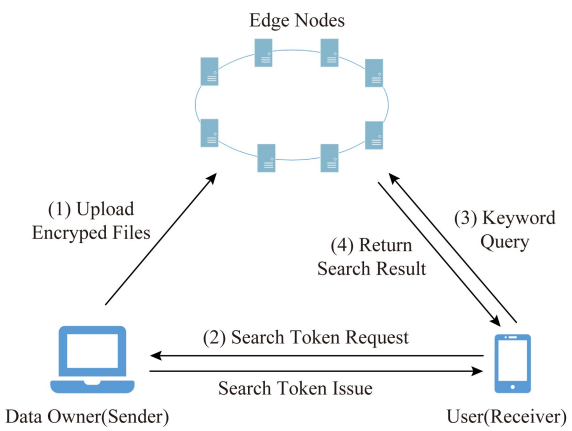

图6 边缘计算密文搜索隐私保护框架

Fig. 6 Framework of privacy preserving in edge-based encrypted search

用户向数据拥有者申请并获得针对指定关键词的搜索令牌;3)边缘节点或云服务器收到搜索令牌后,在密文域上进行相应文件查询并返回查询结果;4)查询用户验证搜索结果的正确性并解密相应文件.

Hou 等人[176]为了保护数据的隐私性,基于同态加密方案构造了 2 个搜索方案.但是系统只能查找与某个关键字匹配的数据,而不能同时查找多个关键字.在此基础上,Hou 等人[177]又提出了改进的协议版本,使服务器能够匹配多个关键字.该工作利用同态加密技术设计了析取和合取的多关键字搜索算法.Yang 等人[178]以隐私保护的方式实现了联合关键字搜索,支持有限时间内的有效搜索授权.该系统能够抵抗选择关键字的时间攻击和离线的关键字猜测攻击.由于大多数方案只支持精确搜索或模糊搜索,Yang 等人[179]从关键词语义的角度描述了一个更实用的安全搜索解决方案.根据语义信息,系统将相关结果和语义相关关键字返回给用户.

Yu 等人[180]提出了一种 2 轮 top-k 多关键字检索方案,该方案采用向量空间模型(VSM)表示文件,并采用改进的 FHE 方案[181]对索引/陷门进行加密.当接收到多关键字查询时,服务器计算文件关联分数(取决于术语频率反向文档频率(TF-IDF)[182]的规则),并将加密后的分数返回给客户端.然后,客户端解密分数并在本地执行 top-k 排序算法.最后,客户机将 k 个得分最高的标识符发送到服务器,并访问它们相应的标识符.然而,由于 FHE 的效率限制,该系统不适用于大规模加密数据的实际应用.Strizhov 等人[183]也实现了一个多关键字搜索系统,返回的结果按分数排序.该方案达到了最优的次线性搜索时间,并且对自适应选择关键字攻击(CKAs)是安全的.Zhang 等人[184]设计了一个具有验证能力的安全排名关键字搜索方案,一旦服务器行为异常,很可能会被检测到.Yang 等人[185-187]利用带门限解密的 Paillier 密码体制,提出了多关键字搜索的安全 top-k 排名系统.在文献[186]中,查询的关键字中允许使用通配符.此外,关键字可以由逻辑运算符 AND 或 OR 连接.通过使用标准编码技术(即 Unicode[188]),文献[185]的系统能够以任意语言搜索加密数据.此外,客户可以设置查询关键字的偏好分数,以获得更满意的结果.对于更具表现力的查询,文献[187]支持不同的查询模式,例如单/合取关键字查询和混合布尔查询.在文献[185-187]方案中,搜索多个数据所有者的数据只需要一个陷门.此外,还实现了可执行的搜索授权和撤销.

隐私保护的模式匹配是密文搜索的重要功能之一.外包模式匹配是指资源受限的设备将“从文本 T 中找出所有模板 P 出现的所有位置”这一任务外包给云服务器完成.然而,它带来了一系列安全与隐私问题.国内外现有的部分安全外包模式匹配协议仅能保护文本隐私或模板隐私;另一部分则利用计算开销巨大的公钥全同态加密、承诺协议和零知识证明协议实现文本隐私、模板隐私和匹配结果的可验证,效率较低而不实用.为了解决该问题,Zhou 等人[189]首先基于任意单向陷门置换和同态消息认证码提出了一个高效的隐私保护可验证外包离散傅里叶变换协议 OVFT;基于 OVFT,进一步设计了安全高效的可验证外包多项式乘法协议 OPVML;最终在此基础上构造了轻量级可验证的隐私保护外包模式匹配协议 PVOPM.不利用传统的公钥全同态加密,给出的外包模式匹配协议对恶意云服务器和接收方/发送方发起的合谋攻击实现了文本隐私和查询模板隐私,同时实现了模式匹配结果的正确性可验证.所生成的匹配结果正确性验证证据的大小和任意单项陷门置换的计算复杂度均为常数,与文本的长度 n 和查询模板长度 m 均无关.

尤其需要指出的是,到目前为止国内外关于隐私保护数据聚合、隐私保护外包计算和面向应用的安全计算具体方案构造仍多基于云计算环境构建[190],如何刻画边缘计算的隐私保护新安全模型与设计可证明安全的轻量级隐私保护边缘计算协议仍是一个亟待解决的、具有挑战性的研究课题.

3　总结与展望

本文首先介绍边缘计算隐私保护的网络模型与安全模型,并在此基础上从边缘计算的隐私保护数据聚合、隐私保护外包计算和包括隐私保护集合运算、隐私保护机器学习、隐私保护图像处理、隐私保护生物认证、隐私保护的密文搜索等面向应用的安全计算问题 3 方面出发,基于数据扰动、同态加密和安全多方计算等密码技术,对边缘计算隐私保护领域的国内外最新研究成果进行了系统的阐述、总结与科学归类.提出了在轻量化密码原语的基础上,通过减少公钥密码使用次数构造边缘计算轻量级隐私保护的新理论和新方法,从而达到“一次加密、多次使用”和“一次验证、多次有效”的轻量化目标.虽然,目前国内外基于传统云服务的安全外包计算隐私保护已取得一系列重要研究成果,但针对边缘计算的

隐私保护仍有若干具有挑战性的公开问题值得进一步研究.

1) 边缘计算场景下敏感数据的识别问题.对特定边缘场景中各类数据的隐私性进行有效甄别和度量,确定"哪些数据是敏感的,哪些数据是可以公开使用的"是实现边缘计算轻量级隐私保护的前提和基础.有些数据被认为是隐私数据,如位置信息、健康状况和社会关系等;而有些则不是,如社会事件、道路交通状况等.如何利用机器学习技术对用户数据的敏感性进行智能分类与识别,成为边缘计算中实现高效、安全的数据分析的关键问题.

2) 刻画边缘计算隐私保护的形式化安全模型.与传统单一的云服务器场景不同的是,边缘计算要求多个边缘节点合作完成外包计算任务.因此,不可避免地存在多个边缘节点合谋以及部分被俘获的边缘节点与恶意本地用户设备间合谋的敌手模型.需要结合已有的安全多方计算成果,对其进行形式化地刻画与建模.

3) 在传统的云计算场景中,设计安全外包计算协议往往更侧重于考虑本地资源受限用户的性能需求,而较少考察资源丰富的云服务器端的存储、计算与通信开销.然而,地理位置部署于本地设备和云服务器之间的边缘节点所具备的资源往往远不如云服务器丰富.因此,如果一个边缘节点执行过多复杂的运算,如双线性配对和模幂运算等,必将导致较高的反馈延迟,从而违背了边缘计算可实现实时控制的初衷.特别是对于实时性要求较高的应用,效率成为安全数据处理的关键问题.因此,设计一种能兼顾本地设备与边缘节点的轻量级的边缘计算隐私保护新方法实现数据的安全高效处理迫在眉睫.

4) 可验证与可审计能有效保证恶意敌手环境下边缘计算结果的正确性.然而,在边缘计算中实现可验证性比云计算中更具挑战.一方面,外包计算的可验证可能给边缘计算带来高延迟;另一方面,由于每个边缘节点有自己的管理区域,移动用户可能会频繁地从一个区域移动到另一个区域,这导致不同区域的多个边缘节点一起工作为用户服务.因此,这些边缘节点中的任何一个出错,最终的结果都是不正确的.因此,如何及时对边缘节点的中间计算结果进行高效验证,并有效追踪和删除恶意边缘节点是重要的研究问题.国内外研究者对属性基加密中如何有效追踪恶意私钥泄露源以及在群签名中如何有效追踪签名用户已经有了一系列重要研究成果.因此,如何借鉴上述已有成果,设计高效可追踪、可验证的隐私保护边缘计算协议是一个亟待解决的重要研究问题.

5) 边缘计算的外包存储与密文搜索问题是重要的研究课题.与传统单一云服务器环境不同的是,同一份数据文件可能在多个边缘节点存储多个备份,因此如何实现高效的安全数据文件同步更新、添加、删除等操作是值得考察的;此外,查询用户在本区域发起特定关键字密文搜索失败时,如何设计多个边缘节点间的联合密文搜索也是一个具有重要理论意义与实际应用价值的问题.

6) 在轻量化密码原语的基础上,通过减少公钥密码使用次数构造边缘计算轻量级隐私保护的新理论和新方法,在基于多输入、多输出模型的多用户、多任务边缘计算模型下设计轻量化隐私保一般性构造,从而达到"一次加密、多次使用"和"一次验证、多次有效"的轻量化目标;实现边缘计算的轻量级隐私保护理论在各类新兴智能网络服务中的多态化应用方法,提出满足不同安全性和性能要求的个性化轻量级隐私保护边缘计算新方案是一个极具挑战的重要研究课题.

参 考 文 献

[1] Al-Fuqaha A, Guizani M, Mohammadi M, et al. Internet of things: A survey on enabling technologies, protocols and applications [J]. IEEE Communications Surveys and Tutorials, 2015, 17(4): 2347-2376

[2] Evans D. The Internet of things: How the next evolution of the Internet is changing everything [OL]. [2020-07-20]. http://wenku.baidu.com/view/9fd28fd40242a8956aece428.html

[3] Camhi J. Former cisco CEO John chambers predicts 500 billion connected devices by 2025 [OL]. [2020-07-20]. https://www.cisco.com

[4] Roman R, Lopez J, Mambo M. Mobile edge computing, Fog et al: A survey and analysis of security threats and challenges [J]. Future Generation Computer Systems, 2016, 78(2): 680-698

[5] Satyanarayanan M. The emergence of edge computing [J]. Computer, 2017, 50(1): 30-39

[6] Stojmenovic I, Wen S. The fog computing paradigm: Scenarios and security issues [C] //Proc of 2014 Federated Conf on Computer Science and Information Systems. Piscataway, NJ: IEEE, 2014: 1-8

[7] Want R, Schilit B N, Jenson S. Enabling the Internet of things [J]. Computer, 2015, 48(1): 28-35

[8] Khan A R. Access control in cloud computing environment [J]. Journal of Engineering and Applied Sciences, 2012, 7(5): 613-615

[9] Bonomi F, Milito R, Natarajan P, et al. Fog computing: A platform for Internet of things and analytics [C] //Proc of Conf on Big Data and Internet of Things: A Roadmap for Smart Environments. Berlin: Springer, 2014: 169-186

[10] Sharma V, You I, Jayakody D N K, et al. Cooperative trust relaying and privacy preservation via edge-crowdsourcing in social Internet of things [J]. Future Generation Computer Systems, 2017, 92(3):758-776

[11] Bonatti P, Duma C, Olmedilla D, et al. An integration of reputation-based and policy-based trust management [J]. Networks, 2005, 10(2): 1-6

[12] Bonomi F, Milito R, Zhu Jiang, et al. Fog computing and its role in the Internet of things [J]. Proceedings of the MCC Workshop on Mobile Cloud Computing. New York: ACM, 2012: 13-16

[13] Paul W, Zhang Heng, Saurabh B, et al. Dependability in edge computing [J]. Communications of the ACM, 2020, 63 (1): 58-66

[14] Lu Rongxing, Heung K, Lashkari A H, et al. A lightweight privacy-preserving data aggregation scheme for fog computing-enhanced IoT [J]. IEEE Access, 2017, 5: 3302-3312

[15] Wang Huaqun, Wang Zhiwei, Domingo-Ferrer J. Anonymous and secure aggregation scheme in fog-based public cloud computing [J]. Future Generation Computer Systems, 2017, 78(2): 712-719

[16] Guan Zhitao, Zhang Yue, Wu Longfei, et al. APPA: An anonymous and privacy preserving data aggregation scheme for fog-enhanced IoT [J].Journal of Network and Computer Applications, 2019, 125: 82-92

[17] Lyu Lingjuan, Nandakumar K, Rubinstein B, et al. PPFA: Privacy preserving fog-enabled aggregation in smart grid [J]. IEEE Transactions on Industrial Informatics, 2018, 14(8): 3733-3744

[18] Yang Mengmeng, Zhu Tianqing, Liu Bo, et al. Machine learning differential privacy with multifunctional aggregation in a fog computing architecture [J]. IEEE Access, 2018, 6: 17119-17129

[19] Zhang Rui, Zhang Yanchao, Sun Jinyuan, et al. Fine-grained private matching for proximity-based mobile social networking [C] //Proc of Conf on Computer Communications. Piscataway, NJ: IEEE, 2012: 1969-1977

[20] Liang Xiaohui, Li Xu, Zhang Kuan, et al. Fully anonymous profile matching in mobile social networks [J]. IEEE Journal on Selected Areas in Communications, 2013, 31(9): 641-655

[21] Zhou Jun, Zhang Yifang, Cao Zhenfu, et al. PPSAS: Lightweight privacy-preserving spectrum aggregation and auction in cognitive radio networks [C] //Proc of Int Conf on Distributed Computing Systems. Piscataway, NJ: IEEE, 2019: 1127-1137

[22] Yang Yang, Huang Xindi, Liu Ximeng, et al. A comprehensive survey on secure outsourced computation and its applications [J]. IEEE Access, 2019,7: 159426-159465

[23] Denning D E R. Cryptography and data security [J]. Journal of Clinical Computing, 1982, 15(1): 11-14

[24] Reiss S P. Practical data-swapping: The first steps [C] // Proc of Practical Data-Swapping: The First Steps. Piscataway, NJ: IEEE, 1980: 20-37

[25] Agrawal R, Srikant R. Privacy-preserving data mining [C] // Proc of the 2000 ACM SIGMOD Int Conf on Management of Data. New York: ACM, 2000: 439-450

[26] Liu Jie, Xu Yifeng. Privacy preserving clustering by random response method of geometric transformation [C]//Proc of Conf on Internet Computing for Science and Engineering. Piscataway, NJ: IEEE, 2009: 181-188

[27] Oliveira S, Zaiane O, Zaane O, et al. Data perturbation by rotation for privacy-preserving clustering, TR04-17 [R]. Edmonton: University of Alberta, 2004

[28] Chen Keke, Liu Ling. A random rotation perturbation approach to privacy preserving data classification, TR GIT-CC-05-12 [R]. Dayton: Wright State University, 2005

[29] Lefons E, Silvestri A, Tangorra F. An analytic approach to statistical databases [C]//Proc of Int Conf on Very Large Data Bases. New York: ACM, 1983: 260-274

[30] Liew C K, Choi U J, Liew C J. A data distortion by probability distribution [J]. ACM Transactions on Database Systems, 1985, 10(3): 395-411

[31] Lin K P. Privacy-preserving kernel k-means outsourcing with randomized kernels [J]. Knowledge and Information Systems, 2016, 49(3): 885-908

[32] Yang Pan, Gui Xiaolin, An Jian, et al. A retrievable data perturbation method used in privacy-preserving in cloud computing [J]. Communications, 2014, 11(8): 73-84

[33] Balasubramaniam S, Kavitha V. Geometric data perturbation-based personal health record transactions in cloud computing [J]. Science World Journal, 2015: No. 927867

[34] Reddy V S, Rao B T. A combined clustering and geometric data perturbation approach for enriching privacy preservation of healthcare data in hybrid clouds [J]. International Journal of Intelligent Engineering and Systems, 2018, 11(1): 201-210

[35] Duan Jia, Zhou Jiantao, Li Yuanman. Secure and verifiable outsourcing of nonnegative matrix factorization [C] //Proc of ACM Workshop on Information Hiding and Multimedia Security. New York: ACM, 2016: 63-68

[36] Knuth D. The Art of Computer Programming [M]. New Jersey: Addison-Wesley Professional, 1981: 59-60

[37] Chen Fei, Xiang Tao, Yang Yuanyuan. Privacy-preserving and verifiable protocols for scientific computation outsourcing to the cloud [J]. Journal of Parallel and Distributed Computing, 2014, 74(3): 2141-2151

[38] Yu Yunpeng, Luo Yuchao, Wang Dongsheng, et al. Efficient, secure and non-iterative outsourcing of large-scale systems of linear equations [C] //Proc of IEEE Int Conf on Communications. Piscataway, NJ: IEEE, 2016: 1-6

[39] Xia Zhihua, Ma Xiaohe, Shen Zixuan, et al. Secure image LBP feature extraction in cloud-based smart campus [J]. IEEE Access, 2018, 6: 30932-30401

[40] Wu Wei, Parampalli U, Liu Jian, et al. Privacy preserving k-nearest neighbor classification over encrypted database in outsourced cloud environments [J]. World Wide Web, 2019, 22(1): 101-123

[41] Boneh D, Goh E J, Nissim K. Evaluating 2-DNF formulas on ciphertexts [C] //Proc of Int Conf on Theory of Cryptography. Berlin: Springer, 2005: 325-341

[42] Armknecht F, Sadeghi A R. A new approach for algebraically homomorphic encryption, TR422 [R/OL]. IACR Cryptol ePrint Arch, 2008 [2020-08-01]. https://eprint.iacr.org/20081/422.pdf

[43] Gentry C. A Fully Homomorphic Encryption Scheme [M]. San Francisco: Stanford University, 2009

[44] Gentry C, Halevi S. Implementing Gentry's fully-homomorphic encryption scheme [C] //Proc of Annual Int Conf on the Theory and Applications of Cryptographic Techniques. Berlin: Springer, 2011: 129-148

[45] Stehlé D, Steinfeld R. Faster fully homomorphic encryption [C] //Proc of Annual Int Conf on the Theory and Applications of Cryptographic Techniques. Berlin: Springer, 2010: 377-394

[46] Smart N P, Vercauteren F. Fully homomorphic encryption with relatively small key and ciphertext sizes [C] //Proc of Workshop Public Key Cryptography. Berlin: Springer, 2010: 420-443

[47] Gentry C, Sahai A, Waters B. Homomorphic encryption from learning with errors: Conceptually-simpler, asymptotically-faster, attribute-based [C] //Proc of Annual Int Cryptology Conf. Berlin: Springer, 2013: 75-92

[48] Brakerski Z, Vaikuntanathan V. Efficient fully homomorphic encryption from (standard) LWE [C] //Proc of IEEE Symp on Foundations of Computer Science. Piscataway, NJ: IEEE, 2011: 97-106

[49] Halevi S, Shoup V. HElib-An implementation of homomorphic encryption, 2014/039 [R]. New York: IBM Thomas J. Waston Research Center, 2014

[50] Halevi S, Shoup V. Bootstrapping for HElib [C] //Proc of Annual Int Conf on the Theory and Applications of Cryptographic Techniques. Berlin: Springer, 2015: 641-670

[51] Brakerski Z, Gentry C, Vaikuntanathan V. (Leveled) fully homomorphic encryption without bootstrapping [J]. ACM Transactions on Computation Theory, 2014, 6(3): 1-36

[52] Smart P, Vercauteren F. Fully homomorphic SIMD operations [J]. Designs Codes and Cryptography, 2014, 71(1): 57-81

[53] Ducas L, Micciancio D. FHEW: Bootstrapping homomorphic encryption in less than a second [C] //Proc of Annual Int Conf on the Theory and Applications of Cryptographic Techniques. Berlin: Springer, 2015: 617-640

[54] Chillotti I, Gama N, Georgieva M, et al. Faster fully homomorphic encryption: Bootstrapping in less than 0.1 seconds [C] //Proc of Annual Int Conf on the Theory and Application of Cryptology and Information Security. Berlin: Springer, 2016: 3-33

[55] Chillotti I, Gama N, Georgieva M, et al. Faster packed homomorphic operations and effcient circuit bootstrapping for TFHE [C] //Proc of Int Conf on the Theory and Application of Cryptology and Information Security. Berlin: Springer, 2017: 377-408

[56] Méaux P, Journault A, Carlet C, et al. Towards stream ciphers for efficient FHE with low-noise ciphertexts [C] //Proc of Advances in Cryptology (EUROCRYPT 2016). Berlin: Springe, 2016: 311-343

[57] Brakerski Z. Quantum FHE (almost) as secure as classical [C] //Proc of Annual Int Cryptology Conf. Berlin: Springer, 2018: 37-95

[58] Boneh D, Gennaro R, Goldfeder S, et al. Threshold cryptosystems from threshold fully homomorphic encryption [C] //Proc of Annual Int Cryptology Conf. Berlin: Springer, 2018: 565-596

[59] Kaosar M G, Paulet R, Yi Xun. Fully homomorphic encryption based two-party association rule mining [J]. Data and Knowledge Engineering, 2012, (76/77/78): 1-15

[60] Yi Xun, Kaosar M G, Paulet R, et al. Single-database private information retrieval from fully homomorphic encryption [J]. IEEE Transactions on Knowledge and Data Engineering, 2013, 25(5): 1125-1134

[61] Liu Ximeng, Deng R, Choo K K R, et al. Privacy-preserving outsourced clinical decision support system in the cloud [J/OL]. IEEE Transactions on Services Computing, 2017 [2020-08-01]. https://ieeexplore.ieee.org/document/8110695

[62] Yao A C. Protocols for secure computation [C] //Proc of Foundations of Computer Science. Piscataway, NJ: IEEE, 1982: 160-164

[63] Yao A C. How to generate and exchange secrets [C] //Proc of Symp on Foundations of Computer Science. Piscataway, NJ: IEEE, 1986: 162-167

[64] Asharov G, Lindell Y, Schneider T, et al. More efficient oblivious transfer extensions [J]. Journal of Cryptology, 2017, 30(3): 805-858

[65] Beaver D, Micali S, Rogaway P. The round complexity of secure protocols [C] //Proc of ACM Symp on Theory of Computing. New York: ACM, 1990: 503-513

[66] Ben-Efraim A, Lindell Y, Omri E. Optimizing semi-honest secure multiparty computation for the Internet [C] //Proc of ACM SIGSAC Conf on Computer and Communications Security. New York: ACM, 2016: 578-590

[67] Wang Xiao, Ranellucci S, Katz J. Global-scale secure multiparty computation [C] //Proc of the 2017 ACM SIGSAC Conf. New York: ACM, 2017: 39-56

[68] Zhu Ruiyu, Cassel D, Sabry A, et al. NANOPI: Extreme-scale actively-secure multi-party computation [C] //Proc of the 2018 ACM SIGSAC Conf. New York: ACM, 2018: 862-879

[69] Ananth P, Choudhuri A R, Jain A. A new approach to round-optimal secure multiparty computation [C] //Proc of Int Cryptology Conf. Berlin: Springer, 2017: 468-499

[70] Badrinarayanan S, Jain A, Ostrovsky R, et al. UC-secure multiparty computation from one-way functions using stateless tokens [C] //Proc of the 5th Int Conf on the Theory and Application of Cryptology and Information Security. Berlin: Springer, 2019: 577-605

[71] Mukherjee P, Wichs D. Two round multiparty computation via multi-key FHE [C] //Proc of Annual Int Conf on the Theory and Applications of Cryptographic Techniques. Berlin: Springer, 2016: 735-763

[72] Boyle E, Gilboa N, Ishai Y. Group-based secure computation: Optimizing rounds, communication, and computation [C] //Proc of Annual Int Conf on the Theory and Applications of Cryptographic Techniques. Berlin: Springer, 2017: 163-193

[73] Garg S, Miao P, Srinivasan A. Two-round multiparty secure computation minimizing public key operations [C] //Proc of Annual Int Cryptology Conf. Berlin: Springer, 2018: 273-301

[74] Benhamouda F, Lin Huijia. k-round multiparty computation from k-round oblivious transfer via garbled interactive circuits [C] //Proc of Annual Int Conf on the Theory and Applications of Cryptographic Techniques. Berlin: Springer, 2017: 500-532

[75] Coretti S, Garay J, Zikas V, et al. Constant-round asynchronous multi-party computation based on one-way functions [C] //Proc of Int Conf on the Theory and Application of Cryptology and Information Security. Berlin: Springer, 2016: 998-1021

[76] Hazay C, Orsini E, Scholl P, et al. TinyKeys: A new approach to efficient multi-party computation [C] //Proc of Annual Int Cryptology Conf. Berlin: Springer, 2018: 3-33

[77] Hazay C, Orsini E, Scholl P, et al. Concretely efficient large-scale MPC with active security (or, tinykeys for tinyot) [C] //Proc of Int Conf on the Theory and Application of Cryptology and Information Security. Berlin: Springer, 2018: 86-117

[78] Lindell Y, Nof A. A framework for constructing fast MPC over arithmetic circuits with malicious adversaries and an honest-majority [C] //Proc of the 2017 ACM SIGSAC Conf on Computer and Communications Security. New York: ACM, 2017: 259-276

[79] Benhamouda F, Krawczyk H, Rabin T. Robust non-interactive multiparty computation against constant-size collusion [C] //Proc of Annual Int Cryptology Conf. Berlin: Springer, 2017: 391-419

[80] Garay J, Ishai Y, Ostrovsky R, et al. The price of low communication in secure multi-party computation [C] //Proc of Annual Int Cryptology Conf. Berlin: Springer, 2017: 420-446

[81] Damgard I, Orlandi C, Simkin C. Yet another compiler for active security or: Effcient MPC over arbitrary rings [C] //Proc of Annual Int Cryptology Conf. Berlin: Springer, 2018: 799-829

[82] Chida K, Genkin D, Hamada K, et al. Fast large-scale honest-majority MPC for malicious adversaries [C] //Proc of Annual Int Cryptology Conf. Berlin: Springer, 2018: 34-64

[83] Cohen R, Shelat A, Wichs D. Adaptively secure MPC with sublinear communication complexity [C] //Proc of Annual Int Cryptology Conf. Berlin: Springer, 2019: 30-60

[84] Patra A, Ravi D. Beyond honest majority: The round complexity of fair and robust multi-party computation [C] //Proc of Int Conf on the Theory and Application of Cryptology and Information Security. Berlin: Springer, 2019: 456-487

[85] Cohen R, Garay J, Zikas V. Broadcast-optimal two-round MPC [C] //Proc of Annual Int Conf on the Theory and Applications of Cryptographic Techniques. Berlin: Springer, 2020: 828-858

[86] Huang Yan, Malka L, Evans D, et al. Efficient privacy-preserving biometric identification [C] //Proc of Network and Distributed System Security Symp. Reston: ISOC, 2011: 1-40

[87] Barni M, Failla P, Kolesnikov V, et al. Secure evaluation of private linear branching programs with medical applications [C] //Proc of European Symp on Research in Computer Security. Berlin: Springer, 2009: 424-439

[88] Brickell J, Porter D E, Shmatikov V, et al. Privacy-preserving remote diagnostics [C] //Proc of ACM Conf on Computer and Communications Security. New York: ACM, 2007: 498-507

[89] Sadeghi A R, Schneider T, Wehrenberg I. Efficient privacy-preserving face recognition [C] //Proc of Information, Security and Cryptology (ICISC 2009). Berlin: Springer, 2009: 229-244

[90] Bellare M, Hoang V T, Rogaway P. Foundations of garbled circuits [C] //Proc of ACM Conf on Computer and Communications Security. New York: ACM, 2012: 784-796

[91] Shamir A. How to share a secret [J]. Communications of the ACM, 2011, 22(11): 612-613

[92] Blakley G R. Safeguarding cryptographic keys [C] //Proc of IEEE Computer Society. Piscataway, NJ: IEEE, 1979: 1-6

[93] Ben-Or M, Goldwasser S, Wigderson A. Completeness theorems for non-cryptographic fault-tolerant distributed computation [C] //Proc of ACM Symp on Theory of Computing. New York: ACM, 1988: 1-10

[94] Chaum D, Crépeau C, Damgard I. Multiparty unconditionally secure protocols [C] //Proc of ACM Symp on Theory of Computing. New York: ACM, 1988: 11-19

[95] Damgård I, Fitzi M, Kiltz E, et al. Unconditionally secure constant-rounds multi-party computation for equality, comparison, bits and exponentiation [C] //Proc of Theory of Cryptography Conf. Berlin: Springer, 2006: 285-304

[96] Nishide T, Ohta K. Multiparty computation for interval, equality, and comparison without bit-decomposition protocol [C] //Proc of Int Workshop on Public Key Cryptography. Berlin: Springer, 2007: 343-360

[97] Dinur I, Keller N, Klein O. An optimal distributed discrete log protocol with applications to homomorphic secret sharing [C] //Proc of Annual Int Cryptology Conf. Berlin: Springer, 2018: 824-873

[98] Shinagawa K, Nuida K, Nishide T, et al. Size-hiding computation for multiple parties [C] //Proc of Int Conf on the Theory and Application of Cryptology and Information Security. Berlin: Springer, 2016: 937-966

[99] Wang Zhaohong, Luo Ying, Cheung S S, et al. Information-theoretic secure multi-party computation with collusion-deterrence [J]. IEEE Transactions on Information Forensics and Security, 2016, 12(4): 980-995

[100] Hirt M, Maurer U, Tschudi D, et al. Network-hiding communication and applications to multi-party protocols [C] //Proc of Cryptology Conf. Berlin: Springer, 2016: 335-365

[101] Eldefrawy K, Pereira V. A high-assurance evaluator for machine-checked secure multi-party computation [C] //Proc of the 26th ACM Conf on Computer and Communications Security. New York: ACM, 2019: 851-868

[102] Agarwal N, Anand S, Prabhakaran M. Uncovering algebraic structures in the MPC landscape [C] //Proc of Advances in Cryptology (EUROCRYPT 2019). Berlin: Springer, 2019: 381-406

[103] Atallah M J, Du Wenliang. Secure multi-party computational geometry [C] //Proc of Workshop Algorithms Data Struct. Berlin: Springer, 2001: 165-179

[104] Huang Haiping, Gong Tianhe, Chen Ping, et al. Secure two-party distance computation protocol based on privacy homomorphism and scalar product in wireless sensor networks [J]. Tsinghua Science and Technology, 2016, 21(4): 385-396

[105] Yao Yifei, Yu Fanhua. Privacy-preserving similarity sorting in multi-party model [J]. International Journal of Network Security, 2017, 19(5): 851-857

[106] Ioannidis E, Weinsberg E, Taft N A, et al. A method and system for privacy preserving matrix factorization. U.S., 14771534 [P]. 2016-01-05

[107] Freedman M J, Nissim K, Pinkas B. Efficient private matching and set intersection [C] //Proc of Annual Int Conf on the Theory and Applications of Cryptographic Techniques. Berlin: Springer, 2004: 1-19

[108] Lu Rongxing, Zhu Hui, Liu Ximeng, et al. Toward efficient and privacy-preserving computing in big data era [J]. Network IEEE, 2014, 28(4): 46-50

[109] Du Wenliang, Atallah M J. Privacy-preserving cooperative scientific computations [C] //Proc of the 14th IEEE Computer Security Foundations Workshop. Piscataway, NJ: IEEE, 2001: 273-282

[110] Chow S S M, Lee J H, Subramanian L. Two-party computation model for privacy-preserving queries over distributed databases [C] //Proc of Network and Distributed System Security Symp. Reston: ISOC, 2009: 1-16

[111] Wang Rui, Wang Xiaofeng, Li Zhou, et al. Privacy-preserving genomic computation through program specialization [C] //Proc of ACM Conf on Computer and Communications Security. New York: ACM, 2009: 338-347

[112] Zhou Jun, Cao Zhenfu, Dong Xiaolei, et al. Security and privacy for cloud-based IoT: Challenges [J]. IEEE Communications Magazine, 2017, 55(1): 26-33

[113] Gennaro R, Gentry C, Parno B. Non-interactive verifiable computing: Outsourcing computation to untrusted workers [C] //Proc of Annual Cryptology Conf. Berlin: Springer, 2010: 465-482

[114] Zhou Jun, Cao Zhenfu, Qin Zhan, et al. LPPA: Lightweight privacy-preserving authentication from efficient multi-key secure outsourced computation for location-based services in VANETs [J]. IEEE Transactions on Information Forensics and Security, 2020, 15(99): 420-434

[115] Gennaro R, Gentry C, Parno B. Non-interactive verifiable computing: Outsourcing computation to untrusted workers [C] //Proc of Int Cryptology Conf. Berlin: Springer, 2010: 465-482

[116] Yao A C. Protocols for secure computation [C] //Proc of the 23rd Annual Symp on Foundations of Computer Science (SFCS'08). Piscataway, NJ: IEEE, 1982: 160-164

[117] Chung K M, Kalai Y, Vadhan S. Improved delegation of computation using fully homomorphic encryption [C] //Proc of Advances in Cryptology (CRYPTO 2010). Berlin: Springer, 2010: 483-501

[118] Parno B, Raykova M, Vaikuntanathan V. How to delegate and verify in public: Verifiable computation from attribute-based encryption [C] //Proc of Theory of Cryptography Conf. Berlin: Springer, 2012: 422-439

[119] Papamanthou C, Shi E, Tamassia R. Signatures of correct computation [C] //Proc of Theory of Cryptography Conf. Berlin: Springer, 2013: 222-242

[120] Choi S G, Katz J, Kumaresan R, et al. Multi-client noninteractive verifiable computation [C] //Proc of Theory of Cryptography Conf. Berlin: Springer, 2013: 499-518

[121] Gordon S D, Katz J, Shi E, et al. Multiclient verifiable computation with stronger security guarantees [C] //Proc of Theory of Cryptography Conf. Berlin: Springer, 2015: 144-168

[122] Elkhiyaoui K, Melek Önen, Azraoui M, et al. Efficient techniques for publicly verifiable delegation of computation [C] //Proc of the 11th ACM Conf on Computer and Communications Security. New York: ACM, 2016: 119-128

[123] Zhuo Gaoqiang, Jia Qi, Guo Linke, et al. Privacy-preserving verifiable data aggregation and analysis for cloud-assisted mobile crowdsourcing [C] //Proc of IEEE Conf on Computer Communications. Piscataway, NJ: IEEE, 2016: 1-9

[124] Boneh D, Gentry C, Lynn B, et al. Aggregate and verifiably encrypted signatures from bilinear maps [C] //Proc of European Cryptology Conf. Berlin: Springer, 2003: 416-432

[125] Zhang Lei, Zhang Futai. Security model for certificateless aggregate signature schemes [C] //Proc of Int Conf on Computational Intelligence and Security. Piscataway, NJ: IEEE, 2008: 364-368

[126] Bellare M, Neven G. Identity-based multi-signatures from RSA [C] //Proc of RSA Conf on Cryptographers' Track. Berlin: Springer, 2006: 145-162

[127] Lu S, Ostrovsky R, Sahai A, et al. Sequential aggregate signatures and multisignatures without random oracles [C] //Proc of European Cryptology Conf. Berlin: Springer, 2006: 465-485

[128] Derler D, Slamanig D. Key-homomorphic signatures and applications to multiparty signatures, 792 [R/OL]. Cryptol ePrint Arch, 2016 [2020-07-20]. https://eprint.iacr.org/2016/792.pdf

[129] Ni Jianbing, Lin Xiaodong, Zhang Kuan, et al. Secure and deduplicated spatial crowdsourcing: A fog-based approach [C] //Proc of Global Communications Conf. Piscataway, NJ: IEEE, 2016: 1-6

[130] Freedman M J, Nissim K, Pinkas B. Efficient private matching and set intersection [C] //Proc of Int Conf on the Theory and Applications of Cryptographic Techniques. Berlin: Springer, 2004: 1-19

[131] DachmanSoled D, Malkin T, Dachman-Soled D, et al. Efficient robust private set intersection [J]. Lecture Notes in Computer Science, 2009, 2(4): 289-303

[132] Yang Xiaoyuan, Luo Xiaoshuang, Raykova M, et al. Improved outsourced private set intersection protocol based on polynomial interpolation [J]. Concurrency and Computation Practice & Experience, 2018, 30(1): No.4329

[133] Chen Hao, Laine K, Rindal P. Fast private set intersection from homomorphic encryption [C] //Proc of ACM SIGSAC Conf. New York: ACM, 2017: 1243-1255

[134] Ruan O, Wang Zihao, Mi Jing, et al. New approach to set representation and practical private set-intersection protocols [J]. IEEE Access, 2019, 7: 64897-64906

[135] Zhu Hongliang, Chen Meiqi, Sun Maohua, et al. Outsourcing set intersection computation based on Bloom filter for privacy preservation in multimedia processing [J]. Security and Communication Networks, 2018, 2018: 1-12

[136] Mishra P K, Duong D H, Yasuda M. Enhancement for secure multiple matrix multiplications over ring-LWE homomorphic encryption [C] //Proc of Int Conf on Information Security Practice and Experience. Berlin: Springer, 2016: 69-83

[137] Brakerski Z, Vaikuntanathan V. Fully homomorphic encryption from ring-LWE and security for key dependent messages [C] //Proc of Annual Int Cryptology Conf. Berlin: Springer, 2011: 505-524

[138] Mishra P K, Rathee D, Yasuda M. Fast secure matrix multiplications over ring-based homomorphic encryption, 663 [R]. Fukuoka: Kyushu University, 2018 [2020-08-01]. https://eprint.iacr.org/2018/663.pdf

[139] Lu Wenjie, Sakuma J. More practical privacy-preserving machine learning as a service via efficient secure matrix multiplication [C] //Proc of the 6th ACM Workshop Encrypted Computer Application Homomorphic Cryptography. New York: ACM, 2018: 25-36

[140] Benjamin D, Atallah M J. Private and cheating-free outsourcing of algebraic computations [C] //Proc of Privacy, Security and Trust. Piscataway, NJ: IEEE 2008: 240-245

[141] Atallah M J, Frikken K B. Securely outsourcing linear algebra computations [C] //Proc of the 5th ACM Symp Information, Computer Communications Security. New York: ACM, 2010: 48-59

[142] Mohassel P. Efficient and secure delegation of linear algebra, 605 [R/OL]. IACR Cryptol ePrint Arch, 2011 [2020-08-01]. http://pages.cpsc.ucalgary.ca/~pmohasse/OutLin.pdf

[143] Zhou Jun, Cao Zhenfu, Dong Xiaolei, et al. Efficient privacy-preserving outsourced discrete wavelet transform in the encrypted domain [J/OL]. IEEE Transactions on Cloud Computing, 2019 [2020-08-01]. https://ieeexplore.ieee.org/document/8873671

[144] Xie Pengtao, Bilenko M, Finley T, et al. Crypto-Nets: Neural networks over encrypted data [J/OL]. Computer Science, 2014 [2020-08-01]. https://arxiv.org/abs/1412.6181

[145] Gilad-Bachrach R, Dowlin N, Laine K, et al. CryptoNets: Applying neural networks to encrypted data with high throughput and accuracy [C] //Proc of IEEE Int Conf on Machine Learning. Piscataway, NJ: IEEE, 2016: 201-210

[146] Ma Xu, Chen Xiaofeng, Zhang Xiaoyu. Non-interactive privacy-preserving neural network prediction [J]. Information Sciences, 2019, 481: 507-519

[147] Hesamifard E, Takabi H, Ghasemi M. CryptoDL: Deep neural networks over encrypted data [J/OL]. arXiv: 1711.05189, 2017 [2020-07-20]. https://arxiv.org/abs/1711.05189

[148] Tang Fengyi, Wu Wei, Liu Jian, et al. Privacy-preserving distributed deep learning via homomorphic re-encryption [J]. Electronics, 2019, 8(4): 411-431

[149] Shamsabadi A, Gascon A, Haddadi H, et al. PrivEdge: From local to distributed private training and prediction [J]. IEEE Transactions on Information Forensics and Security, 2020, 15: 3891-3831

[150] Chen Jialu, Zhou Jun, Cao Zhenfu, et al. Lightweight privacy-preserving training and evaluation for discretized neural networks [J]. IEEE Internet of Things Journal, 2020, 7(4): 2663-2678

[151] Zhou Jun, Cao Zhenfu, Dong Xiaolei, et al. PPDM: A privacy-preserving protocol for cloud-assisted e-healthcare systems [J]. IEEE Journal of Selected Topics in Signal Processing, 2015, 9(7):1332-1344

[152] Choras R S. Image feature extraction techniques and their applications for CBIR and biometrics systems [J]. International Journal of Biol Biomed Engineering, 2007, 1(1): 6-16

[153] Lowe D G. Object recognition from local scale-invariant features [C] //Proc of Int Conf on Computer Vision. Piscataway, NJ: IEEE, 1999: 1150-1157

[154] Bay H, Ess A, Tuytelaars T, et al. Speeded-up robust features (SURF) [J]. Computer Vision and Image Understanding, 2008, 110(3): 346-359

[155] Dalal N, Triggs B. Histograms of oriented gradients for human detection [C] //Proc of IEEE Conf on Computer Vision and Pattern Recognition. Piscataway, NJ: IEEE, 2005: 886-893

[156] Hsu Chaoyun, Lu Chunshien. Homomorphic encryption-based secure SIFT for privacy-preserving feature extraction [J]. Proceedings of Spie the Int Society for Optical Engineering, 2010, 7880(2): 1-17

[157] Hsu Chaoyun, Lu Chunshien, Pei Soochang, et al. Image feature extraction in encrypted domain with privacy-preserving SIFT [J]. IEEE Transactions on Image Processing, 2012, 21(11): 4593-4607

[158] Schneider M, Schneider T. Notes on non-interactive secure comparison in image feature extraction in the encrypted domain with privacypreserving SIFT [C] //Proc of the 2nd ACM Workshop Information Hiding Multimedia Security. New York: ACM, 2014: 135-140

[159] Hu Shengshan, Wang Qian, Wang Jingjun, et al. Securing SIFT: Privacy-preserving outsourcing computation of feature extractions over encrypted image data [J]. IEEE Transactions on Image Process, 2016, 25(7): 3411-3425

[160] Li Dongmei, Dong Xiaolei, Cao Zhenfu, et al. Privacy-preserving outsourced image feature extraction [J]. Journal of Information Security and Applications, 2019, 47: 59-64

[161] Liu Ximeng, Deng R H, Ding Wenxiu, et al. Privacy-preserving outsourced calculation on floating point numbers [J]. IEEE Transactions on Information Forensics and Security, 2017, 11(11): 2513-2527

[162] Liu Dan, Yan Zheng, Ding Wenxiu, et al. A survey on secure data analytics in edge computing [J]. IEEE Internet of Things Journal, 2019, 6(3): 4946-4967

[163] Bai Yu, Zhuo Li, Cheng Bo, et al. Surf feature extraction in encrypted domain [C] //Proc of 2014 IEEE Int Conf on Multimedia and Expo (ICME). Piscataway, NJ: IEEE, 2014: 1-6

[164] Wang Qian, Hu Shengshan, Wang Jingjun, et al. Secure surfing: Privacy-preserving speeded-up robust feature extractor [C] //Proc of IEEE Int Conf on Distributed Computing Systems. Piscataway, NJ: IEEE, 2016: 700-710

[165] Wang Qian, Hu Shengshan, Wang Jingjun, et al. SecHOG: Privacypreserving outsourcing computation of histogram of oriented gradients in the cloud [C] //Proc of ACM Conf on Computer and Communications Security. New York: ACM, 2016: 257-268

[166] Zhou Hongchao, Wornell G. Efficient homomorphic encryption on integer vectors and its applications [C] //Proc of 2014 Information Theory and Applications Workshop (ITA). Piscataway, NJ: IEEE, 2014: 1-9

[167] Yang Haomiao, Huang Yunfeng, Yu Yong, et al. Privacy-preserving extraction of HOG features based on integer vector homomorphic encryption [C] //Proc of Information Security Practice and Experience. Berlin: Springer, 2017: 102-117

[168] Shortell T, Shokoufandeh A. Secure feature extraction in computational vision using fully homomorphic encryption [C] //Proc of the Future Technologies Conf. Berlin: Springer, 2018: 189-213

[169] Zhou Jun, Zheng Meng, Cao Zhenfu, et al. PVIDM: Privacy-preserving verifiable shape context based image denoising and matching with efficient outsourcing in the malicious setting [J]. Computers and Security, 2020, 88(1): 1-15

[170] Chun Hu, Elmehdwi Y, Li Feng, et al. Outsourceable two-party privacy-preserving biometric authentication [C] //Proc of the 9th ACM Symp on Information, computer and Communications Security. New York: ACM, 2014: 338-353

[171] Yasuda M, Shimoyama T, Kogure J, et al. Privacy-preserving wildcards pattern matching using symmetric somewhat homomorphic encryption [C] //Proc of Australasian Conf on Information Security and Privacy. Berlin: Springer, 2014: 338-353

[172] Sedenka J, Govindarajan S, Gasti P, et al. Secure outsourced biometric authentication with performance evaluation on smartphones [J]. IEEE Transactions on Information Forensics and Security, 2017, 10(2): 384-396

[173] Hu Shengshan, Li Minghui, Wang Qian, et al. Outsourced biometric identification with privacy [J]. IEEE Transactions on Information Forensics and Security, 2018, 13(10): 2448-2463

[174] Salem M, Taheri S, Yuan J S. Utilizing transfer learning and homomorphic encryption in a privacy preserving and secure biometric recognition system [J]. Computers, 2018, 8(1): 3-26

[175] Zhou Jun, Cao Zhenfu, Dong Xiaolei. BDK: Secure and efficient biometric based deterministic key agreement in wireless body area networks [C] //Proc of Int Conf on Body Area Networks. Berlin: Springer, 2013: 488-494

[176] Hou Shuhui, Uehara T, Yiu S, et al. Privacy preserving confidential forensic investigation for shared or remote servers [C] //Proc of the 7th Int Conf on Intelligent Information Hiding and Multimedia Signal Processing. Piscataway, NJ: IEEE, 2011: 378-383

[177] Hou Shuhui, Uehara T, Yiu S, et al. Privacy preserving multiple keyword search for confidential investigation of remote forensics [C] //Proc of the 3rd Int Conf on Multimedia Information Networking and Security. Piscataway, NJ: IEEE, 2011: 595-599

[178] Yang Yang, Ma Maode. Conjunctive keyword search with designated tester and timing enabled proxy re-encryption function for e-health clouds [J]. IEEE Transactions on Information Forensics and Security, 2016, 11(4): 746-759

[179] Yang Yang, Zheng Xianghan, Tang Chunming, et al. Lattice assumption based fuzzy information retrieval scheme support multi-user for secure multimedia cloud [J]. Multimedia Tools and Applications, 2017, 77(8): 9927-9941

[180] Yu Jiadi, Lu Peng, Zhu Yanmin, et al. Toward secure multikeyword top-k retrieval over encrypted cloud data [J]. IEEE Transactions on Dependable & Secure Computing, 2013, 10(4): 239-250

[181] Dijk M V, Gentry C, Halevi S, et al. Fully homomorphic encryption over the integers [C] //Proc of Annual Int Conf on Theory and Applications of Cryptographic Techniques. Berlin: Springer, 2010: 24-43

[182] Salton G, Buckley C. Term-weighting approaches in automatic text retrieval [J]. Information Processing Management, 1988, 24(5): 513-523

[183] Strizhov M, Ray I. Multi-keyword similarity search over encrypted cloud data [C] //Proc of IFIP Int Information Security Conf. Berlin: Springer, 2014: 52-65

[184] Zhang Wei, Lin Yaping, Gu Qi. Catch you if you misbehave: Ranked keyword search results verification in cloud computing [J]. IEEE Transactions on Cloud Computing, 2018, 6(1): 74-86

[185] Yang Yang, Liu Ximeng, Deng R H. Multi-user multi-keyword rank search over encrypted data in arbitrary language [J]. IEEE Transactions on Dependable and Secure Computing, 2017, 5(4): 320-334

[186] Yang Yang, Liu Ximeng, Deng R H, et al. Flexible wildcard searchable encryption system [J]. IEEE Transactions on Services Computing, 2020, 13(3): 464-477

[187] Yang Yang, Liu Ximeng, Robert D, et al. Expressive query over outsourced encrypted data [J]. Information Sciences: An Int Journal, 2018, 442: 33-53

[188] Needleman M. The unicode standard [J]. Serials Review, 2000, 26(2): 51-54

[189] Zhou Jun, Choo K K R, Cao Zhenfu, et al. PVOPM: Verifiable privacy-preserving pattern matching with efficient outsourcing in the malicious setting [J]. IEEE Transactions on Dependable and Secure Computing, 2019. DOI: 10.1109/TDSC.2019.2947436

[190] Ni Jianbing, Zhang Kuan, Lin Xiaodong, et al. Securing fog computing for Internet of things applications: Challenges and solutions [J]. IEEE Communications Surveys and Tutorials, 2018, 20(1): 601-628

Zhou Jun, born in 1982. Received his PhD in the Department of Computer Science and Engineering, Shanghai Jiao Tong University. Currently associate professor in East China Normal University. Member of IEEE and ACM. His main research interests include public key cryptography, secure multiparty computation, key theories for secure edge computing, privacy preserving, and applied cryptography in big data security, AI security, IoT security, 5G security and blockchain security.

Shen Huajie, born in 1997. Master candidate in the Department of Cryptography and Network Security, East China Normal University. His main research interests include blockchain security and secure computing. (adijeshen@gmail.com)

Lin Zhongyun, born in 1999. Undergraduate student in the Department of Cryptography and Network Security, East China Normal University. His main research interests include secure multiparty computation and IoT security. (zylin829@126.com)

Cao Zhenfu, born in 1962. PhD, distinguished professor in East China Normal University. Senior member of IEEE. His main research interests focus on number theory and new theories for cryptography and network security, including blockchain security, AI security, 5G security and privacy preserving.

Dong Xiaolei, born in 1971. PhD, distinguished professor in East China Normal University. Her main research interests include number theory, cryptography, network security, big data security and privacy preserving. (dongxiaolei@sei.ecnu.edu.cn)