计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.200500003

面向边缘计算环境的密码技术研究综述

程庆丰[1,2]　李钰汀[1,2]　李兴华[3]　姜　奇[3]
1 战略支援部队信息工程大学网络空间安全学院　郑州 450001
2 数学工程与先进计算国家重点实验室　郑州 450001
3 西安电子科技大学网络与信息安全学院　西安 710071
(qingfengc2008@sina.com)

摘　要　边缘设备数量的急剧增加导致数据量的爆炸式增长,以云计算模型为代表的集中式数据处理模型因其存储特点与传输带宽的限制已经无法满足数据处理的实时性和高效性需求。在此背景下,边缘计算模型开始进入公众视野。由于设备轻量化、架构异构性等新特点,边缘计算在发展过程中面临着安全方面的巨大挑战。密码技术作为保护信息安全的关键手段,对应对边缘计算安全挑战有重要意义。传统的较为成熟和完备的密码技术方案,需要针对边缘计算的特点做出相应调整以适应新架构的需求。文中从边缘计算架构面临的安全挑战入手,重点分析了可应用于数据安全领域和应用安全领域的密码技术,通过与已有的研究方案进行比较,展示了不同密码技术在边缘计算安全保护中的优势,为面向边缘计算的密码技术应用提供了新的思路。

关键词:边缘计算;密码技术;安全防护;身份认证;密钥协商
中图法分类号　TP309.2

Research on Application of Cryptography Technology for Edge Computing Environment

CHENG Qing-feng[1,2],LI Yu-ting[1,2],LI Xing-hua[3] and JIANG Qi[3]
1 School of Cybersapce Security,Strategic Support Force Information Engineering University,Zhengzhou 450001,China
2 State Key Laboratory of Mathematical Engineering and Advanced Computing,Zhengzhou 450001,China
3 School of Cyber Engineering,Xidian University,Xi'an 710071,China

Abstract　The sharp increase in the number of edge devices has led to an explosive growth in the amount of data. The centralized data processing model,represented by cloud computing model,has been unable to meet the real-time and high-efficiency requirements of data processing due to its storage characteristics and transmission bandwidth limitations. As the amount of data grows,the importance of edge computing is recognized. Edge computing faces huge security challenges in the development process due to the new features of the edge computing model such as lightweight equipment and heterogeneous architecture. As an important means of protecting information security,cryptography is of great significance for dealing with the security challenges of edge computing. Traditional mature and complete cryptography technologies require corresponding adjustments to the characteristics of edge computing,in order to meet the needs of the new architecture. This paper starts with the security challenges that edge computing model faces,analyzes the corresponding cryptographic technical solutions in the data security field and the application security field,and compares existing research schemes to show the advantages of different technologies in edge computing security protection,which provides new ideas for the application of cryptographic technologies for edge computing.

Keywords　Edge computing,Cryptography technologies,Security protection,Identity authentication,Key agreement

1　引言

物联网技术的迅速发展使社会生产以及生活方式发生了巨大变化,小到医院患者身上佩戴的智能检测手环,大到地球之外的航天卫星系统,随处可见的智能终端设备通过互联网连接在一起,架起了网络资源和信息传递的便捷通道,全新的"万物互联(Internet of Everything,IoE)"[1]时代已经到来。

边缘设备数量的急剧增加导致了数据量呈爆炸式增长,以云计算为代表的集中式数据处理模型因其存储特点与传输带宽限制已经无法满足数据处理的实时性和高效性需求。在此背景下,边缘计算模型开始进入公众视野,并逐渐成为学术界和业界热议的新话题。

到稿日期:2020-05-06　返修日期:2020-08-12　本文已加入开放科学计划(OSID),请扫描上方二维码获取补充信息。
基金项目:国家自然科学基金(61872449,U1708262,U1736203,61672413)
This work was supported by the National Natural Science Foundation of China (61872449,U1708262,U1736203,61672413).
通信作者:李钰汀(1006150850@qq.com)

边缘计算作为一种新的计算范式，近些年受到了研究者的广泛关注，不同的研究者从不同的角度描述边缘计算。美国韦恩州立大学的 Shi 等[2-3]把边缘计算定义为："边缘计算是指在网络边缘执行计算的一种新型计算模式，边缘计算中边缘的下行数据表示云服务，上行数据表示万物互联服务，而边缘计算的边缘指从数据源到云计算中心路径之间的任意计算和网络资源"。美国卡内基梅隆大学的 Satyanarayanan 教授[4]则将其描述为："边缘计算是一种新的计算模式，这种模式将计算与存储资源部署在更贴近移动设备或传感器的网络边缘"。

无论哪一种定义，强调的理念都是"将计算资源迁移至更贴近数据的源头"[5]，以达到减轻数据中心处理和存储的压力、缓解网络带宽资源紧缺和提高实时服务响应能力的目的。"边缘"是一个较连续的概念，它包括了从数据产生源头到云计算中心之间路径上所有的计算资源、存储资源和网络资源。"边缘"的存在促进了传统云计算模型的实时交互性和可扩展性，"边缘"和"云"共同形成更适合物联网应用的计算模型。

2 边缘计算结构与安全挑战

为了更加形象地展示边缘计算的基本结构，按照功能将其划分为 4 个部分：云计算中心、核心网络设施、边缘计算中心与边缘网络以及边缘设备。云计算中心是存储能力与计算能力最强大的计算中心，负责综合性的分析与处理任务；核心网络设施具备动态的网络拓扑结构，能够根据实时情况改变边缘计算中心的部署策略；边缘计算中心与边缘网络在地理位置上和网络位置上都更加贴近数据产生源头，其计算资源可根据需求进行动态变化；边缘设备种类众多，可根据其应用领域划分为不同类别。

新计算模型的出现为数据处理提供了便利，也带来了更多的安全隐患。本节详细描述了边缘计算结构 4 个层次各自面临的安全挑战，如图 1 所示。

(1)云计算中心

云计算中心以其强大的存储资源和计算资源为互联网用户提供相关服务，用户根据自己的需求通过网络获得所需服务。与传统的集中式数据处理模型相同，云计算中心主要面临数据安全与网络安全。

(2)核心网络设施

在边缘计算模型中，参与通信的网络设备数量众多，网络环境开放，这些都增加了网络安全方面的不确定因素。分布式拒绝服务攻击、流量注入攻击、中间人攻击、恶意网关攻击等传统网络攻击方式依然存在，此外，一些新的恶意网络干扰(如伪基站的设置)也对网络安全造成了极大的威胁。

在核心网络设施的建设中常有第三方机构(如移动网络运营商)参与，这会带来数据篡改、隐私泄露、拒绝服务等问题。首先，用户的个人信息在核心网络中传输时，可能面临数据篡改与隐私泄露的风险；其次，当核心网络中出现"内部攻击者"时，可能出现服务劫持从而遭受拒绝服务攻击的情况；此外，用户设备在不同网络运营商管理的不同信任域间切换时，如何建立一个合理的授权机制来保证只有合法运营商才能获取用户的位置信息和行为信息等敏感信息，也是需要考虑的问题。

(3)边缘计算中心与边缘网络

边缘计算设施大多部署在开放的环境中，其由于具有特殊的地理分布特征，在物理安全方面更易受到威胁，主要分为能源供应与设备损耗两个方面。由于边缘计算设备通常不在具备安全措施的固定场所下运行，因此保证基础设施的能源供应至关重要。同时，物联网的高速实时更新导致构建基础设施的硬件设备长期处于高负荷状态，如何保证设备在到达使用年限前得到更换、更换设备的同时如何保持兼容性与数据恢复能力也是值得关注的问题。

由于边缘计算设施的分布式部署特点，边缘计算中的数据防泄漏与传统的数据防泄漏有所不同。其中最关键的问题是，某个边缘节点被攻破后，其他节点的相关信息是否会泄露。此外，攻击者还可以截获节点之间传输的数据流以获取用户隐私。

边缘网络高度动态灵活的环境使网络更易受到攻击。传统的网络攻击对边缘网络的攻击虽不会像对核心网络的攻击那样造成大范围的危害，但仍会造成整体环境的不稳定性，进而影响正常的网络服务。

(4)边缘设备

在边缘计算模型中，源数据的产生与预处理都可以在边缘设备端实现。兼顾数据生产者、数据收集者和数据所有者 3 种身份，边缘设备端的数据安全问题需要引起重视。边缘设备存在被盗的可能性，为保护用户隐私数据，应在边缘设备中删除高度隐私的数据，完善数据备份机制，以保证被盗设备中的关键数据能够及时恢复。

应用安全也是边缘设备层的一个高发安全隐患。公共 WiFi 热点绝大多数不具备可靠性，当用户的摄像头、健康监测手环等边缘设备接入公共网络时，很容易被恶意攻击者操纵以窥探用户的隐私信息。此外，边缘设备间的数据交互、边缘设备与边缘服务器之间的响应与回复中也普遍存在着网络安全问题。

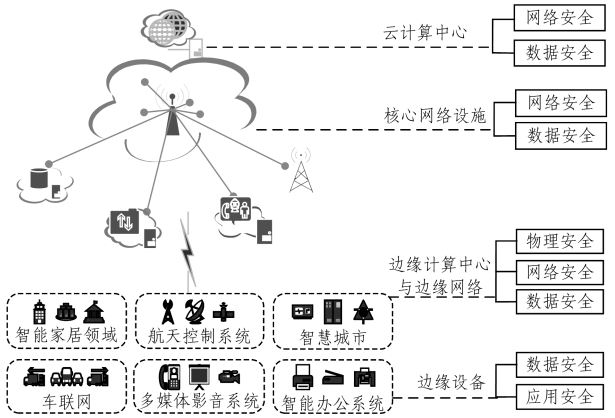

图 1 边缘计算不同层次面对的安全挑战

Fig. 1 Security challenges faced by different levels of edge computing

3 面向边缘计算环境的密码技术应用

由前文分析可知，边缘计算模型面临的安全挑战主要分为 4 个方面，即物理安全、网络安全、数据安全和应用安全，如

图 2 所示。如今，云计算模型下已有的较为成熟和完备的安全保护方案与技术体系，由于边缘计算模型中设备轻量化、架构异构性等新特点，已变得不再适用。其中，密码技术在边缘计算环境中的应用对解决数据安全问题与应用安全问题具有重要意义。本节针对边缘计算环境中的数据安全和应用安全，总结了相应的密码技术应对方案。

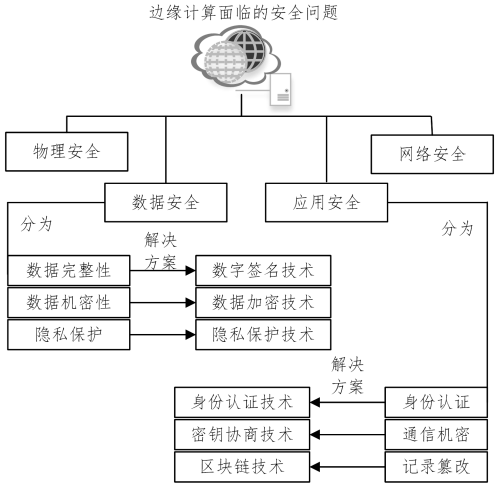

图 2 密码技术在边缘计算中的应用

Fig. 2 Application of cryptography in edge computing

数据安全问题包括数据完整性问题、数据机密性问题和隐私保护问题，这几乎涵盖了边缘计算结构的每个层面，如边缘设备端产生数据过程中的隐私保护、边缘网络通信过程汇总的数据加密、边缘计算中心读取和处理数据时的数据完整性校验等。面对数据安全问题，密码技术的应用可以有效防范风险，如数字签名技术可以保护数据完整性和隐私性、数据加密技术(如全同态加密技术、可搜索加密技术)可以保护数据机密性、隐私保护技术(如生物识别技术、多方安全计算技术)可以保护数据隐私等。

应用安全问题指在通信过程中某些环节可能存在的安全隐患，主要归结为进行身份认证、通信机密性保护和通信节点的记录篡改问题。身份认证是边缘计算安全的最基本要求，也是安全保护机制的第一道关卡。无论是边缘节点之间的通信，还是边缘节点与云服务器的通信，被传输的信息都不能以明文形式出现，这就需要密钥协商技术的保驾护航。新兴的区块链技术则能够有效防范节点记录篡改问题。

对于应用安全问题的这两方面，身份认证协议和密钥协商协议都能够有针对性地降低风险。然而，边缘计算架构中，多种安全域和网络结构并存，如何让传统的身份认证协议和密钥协商协议适应边缘计算环境的新特点，是需要重点关注的话题。此外，区块链技术作为一种新兴信息处理技术，可利用其独有的分布式结构特点为边缘计算建立完整的信任保障体系，为解决边缘计算面临的应用安全问题提供了新的思路。

3.1 身份认证技术

身份认证是边缘计算应用安全的基本要求之一。身份认证技术能够在传输机密信息之前验证各通信方的身份，与密钥交换机制互为有益补充。本节根据边缘计算环境中用户的高移动性特点，重点阐述了身份认证方案在高效性和灵活性方面的要求，并通过阐述其在车联网和智能穿戴设备两个领域中的应用，补充说明了边缘计算环境下身份认证方案的特点。

身份认证技术几乎遍布边缘计算架构的每一个层级，Almajali 等[6]评估了移动边缘计算架构下现有的认证协议。边缘用户设备的身份认证是边缘计算安全机制的第一道防线，目前已有许多针对移动设备的身份认证方案。Tsai 等[7]为移动设备设计了一种可用于访问云计算中心的认证方案，并声称此方案能抵抗重放攻击和伪装攻击。然而，Jiang 等[8]却指出 Tsai 等[7]提出的方案不支持设备和云计算中心之间的相互认证，易受到用户伪装攻击。为此，研究者们针对文献[7]的方案提出了一系列改进方案。Irshad 等[9]选择了双线性对操作，设计了一种用于移动边缘计算环境中多服务器机制下的身份认证方案，但是 Xiong 等[10]指出该方案缺少用户注册和撤销功能。为解决上述问题，Xiong 等[10]提出了一种可证明安全的身份验证方案。此外，Li 等[11]提出了一种基于椭圆曲线的移动设备认证方案，并表示此方案能够保护用户隐私并提供完美前向保密性。Yang 等[12]基于椭圆曲线密码(Elliptic Curve Cryptography，ECC)设计了一种用于移动设备的认证方案，然而，Yoon 等[13]指出该方案不仅无法抵抗模拟攻击，也不能提供完美的前向保密性。

这些方案虽然能在一定程度上为移动边缘计算中的用户提供安全保护，但伴随着高昂的通信和计算开销。在万物互联中，数量众多的资源受限设备不具备足够的计算能力与存储资源，因此仍然需要进一步探索轻量级身份认证技术。Kaur 等[14]提出了一种用于移动边缘计算环境的高效轻量级认证协议。该协议的设计基于椭圆曲线和单向散列函数，还利用了离散对数等难解问题和随机数、时间戳的随机性来抵御伪装攻击、重放攻击、中间人攻击等。该协议所需的通信代价和计算开销相对较小，更适用于资源受限的边缘计算设备。

在身份认证技术的应用中，另一个需要关注的问题是跨域认证。移动设备因其灵活便携等特点，工作区域并不是一成不变的。随着地理位置、网络环境及所需服务的更换，不同安全域的身份标识可能会发生改变，身份认证机制也会随之改变。在不同的信任域间，如何快速进行身份认证机制的切换是需要解决的关键问题。Zeng 等[15]提出了一种基于 ECC 问题的切换认证协议。该协议能够在无线网络中的多个接入点之间进行身份认证机制的切换，同时保护了移动设备的身份匿名性，并能够进行周期性的更新。

车联网也是移动边缘计算应用的重要领域。边缘计算技术提高了网络边缘的计算能力，增大了系统的存储空间，从而增强了通信可靠性，降低了时延，满足车联网的通信需求。消息认证环节是车联网通信过程的第一个步骤。Cui 等[16]基于移动边缘计算设计了一种消息认证方案，引入过滤器，向车辆广播合法的消息。车辆仅需要通过查询过滤器来确定消息是否有效，而不需要单独地验证所接收的消息，避免了对冗余信息的认证，提高了消息认证的效率。

集成了传感器和无线通信等技术的可穿戴设备广泛应用于运动、医疗、保健等领域，可提供收集个人数据、监视患者状况等服务。可穿戴设备在为人们的生活带来便利的同时，也带来了重大的安全隐患，例如隐私泄露问题和对可穿戴设备

的未授权访问。为了确保敏感数据的私密性和安全性，设计适用于可穿戴设备的有效身份验证协议至关重要。目前，研究者们对可穿戴设备的身份认证协议的研究主要集中在基于双因素(Two-factor)的认证协议上。

为了避免因智能设备丢失而导致用户隐私数据泄露，有学者提出在认证环节中加入生物识别特征作为第三种身份认证凭证，设计了基于三因素(Three-factor)的认证协议。2018年，Das等[17]提出了基于三因素的轻量级认证协议，并声称该协议实现了可穿戴设备和移动终端之间的安全通信。但是，Jiang等[18]发现该协议易受到离线情况下的密码猜测攻击。因此，他们提出了以用户为中心的三要素认证方案，可在云服务器的辅助下，保护智能可穿戴设备的密钥协商与身份认证过程。2020年，Kong等[19]采用了多因素身份认证方案来弥补边缘设备安全认证的弱点。此外，采用软件定义网络(Software Defined Network，SDN)技术来实现对大量边缘设备部署和应用的全局管理，从而实现万物互联的有效安全保护。最后，对设计框架的身份认证过程进行了形式化验证。

综上所述，边缘计算中身份认证方案的设计应当以轻量级为基本原则，兼顾敏感数据的隐私保护与多安全域切换认证的效率问题。表1列出了本节所述的主要研究成果。

表1 边缘计算环境下身份认证技术的研究成果

Table 1 Research results of identity authentication schemes in edge computing environment

应用领域	文献	主要内容
服务器与用户设备间的认证	[9]	设计了一种多服务器机制下的认证方案
	[10]	在认证方案中增加了用户注册、撤销功能
	[11]	保护用户隐私，提供完美前向保密性
	[12]	设计了一种用于移动设备的认证方案
轻量级算法	[14]	设计了轻量级认证协议，可抵抗伪装攻击、重放攻击、中间人攻击，通信开销低
跨域认证	[15]	设计了一种无线匿名切换认证协议
车联网	[16]	提出了避免冗余认证的方法，提高了认证的效率
可穿戴设备	[17]	设计了一种基于三因素的认证协议
	[18]	完善了基于三因素认证协议的安全缺陷，提出以用户为中心的三要素认证方案
	[19]	采用软件定义网络技术(SDN)来实现对大量边缘设备的部署和应用的全局管理

3.2 密钥协商技术

密钥协商技术广泛应用于有保密要求的通信场景中，密钥的安全性很大程度上影响着系统的安全性。在边缘计算架构中，云服务器、边缘服务器和用户对密钥信息有不同的所有权和控制权，这使得面向边缘计算环境的密钥协商变得更为复杂。无论是边缘节点之间的通信，还是边缘节点与云服务器的通信，都需要密钥协商技术的保驾护航。除通信过程外，边缘计算模型中的任何一个环节都需要安全密钥作为保护，例如设备层需要认证密钥，通信层需要会话密钥，一个完整安全的密钥体系是至关重要的[20]。

密钥协商技术通常与身份认证技术结合使用。例如，Jia等[21]为MEC(Mobile Edge Computing)环境设计了一个基于身份的匿名认证密钥协商协议，声称协议仅在单个消息交换回合中即可完成双方的身份验证过程，并保证了用户匿名性和不可追溯性。他们在该协议设计中采用了代价较高的双线性配对操作，虽然运算时间与其他方案相比具有明显优势，但协议的具体实施仍受到设备计算能力的限制。经分析发现，该协议在安全性方面仍存在不足[22]，无法保证用户匿名性和前向安全。

如何使密钥协商机制同时保证匿名性和高效率，是研究者们一直在探索的课题。以智能电网为例，2011年，Wu等[23]基于对称密码和ECC问题构建了一个用于智能电网环境的密钥分配方案，该方案需要可信机构(Trusted Authority，TA)和另一台服务器的参与以组成公钥基础设施。他们声称这种方案可以抵抗重放攻击和中间人攻击，但随后被Xia等否认[24]。Xia等[24]提出了一种新的AKA(Authenticated Key Agreement)方案，用轻量级目录访问服务器充当TA。同样，该方案也被指出不能抵抗伪造攻击和未知密钥共享攻击，且TA的参与限制了方案的执行效率。

针对效率问题，学者提出了智能电表(Smart Meter，SM)和服务提供商(Service Provider，SP)的概念，SM和SP同时提供基于身份的加密凭据。2017年，Yan等[25]给出了一种类似结构的密钥协商认证方案。在这种结构中，SM的身份暴露在信道中，显然这违反了匿名性的要求。匿名性也是智能电网应用中不可忽视的一个重要问题。Wu等[26]提出一种基于椭圆曲线密码的密钥协商方案，用于智能电网中的密钥交换。该方案避免了以明文形式传输SM的身份信息，做到了匿名性和高效率的统一。Mahmood等[27]使用基于身份的签名，设计了用于智能电网基础设施的匿名密钥协商协议。该协议设置的可信第三方仅参与了注册阶段，并未参与密钥交换与身份认证阶段。此举不仅减小了密钥协商协议对可信第三方的依赖，还减小了计算开销与通信延迟。

边缘计算模型中主要有3种角色：边缘设备、边缘服务器和云中心服务器。这3种角色的可信密钥协商机制也是备受关注的焦点。Jia等[28]的密钥协商方案在边缘设备、边缘服务器和云服务器之间建立共享密钥。其中只有云服务器才知道边缘设备的身份并负责访问控制，以此来保护设备匿名性。但经过分析发现，该方案存在一些不足之处：首先，该方案仅限于具有智能卡的设备；其次，该方案在注册阶段要求为用户设备和受信任的云服务提供商之间提供安全通道，这在实际操作中是较难实现的；最后，该方案涉及到计算代价高昂的配对操作。文献[29]描述了一个在CK安全模型下可证明安全的三方密钥协商方案，但是该方案没有为设备和服务器提供匿名保护。出于对通信效率的考虑，文献[30]研究了在3个不同方之间建立相互认证所需的最小通信回合和消息数量。

在边缘计算应用中，为了更好地优化资源配置，云服务器往往会将部分数据外包给其他服务提供商或数据服务器。如何在数据外包的情况下确保云中存储数据的安全性成为了人们关注的焦点。文献[31-33]提出了几种方案来保护外包数据的隐私性，然而这些方案仅考虑了单个数据所有者。Shen等[34]根据对称平衡不完全块的思想提出了一种密钥协商协议，可支持多个参与者并根据块设计的结构灵活地改变参与者的数量。多个参与者根据组数据共享模型，以分组结构高效安全地共享外包数据。这种应用于多个参与者的密钥协商协议在边缘计算环境下是值得借鉴的。

云服务器将一些非核心的计算任务和存储任务迁移到不

同的边缘服务器，这个过程与 Shen 等[34]描述的数据外包过程相似，不同边缘服务器访问共享数据的方式也可以模仿文献[34]提出的组数据共享模型。

综上所述，边缘计算中密钥协商方案的设计更注重匿名性与高效性。此外，大规模异构网络中多方密钥协商机制的安全性、外包数据的隐私性，同样给面向边缘计算的密钥协商实现带来了新的挑战。表 2 列出了本节所述的主要研究成果。

表 2 边缘计算环境下密钥协商技术的研究成果

Table 2 Research results of key agreement schemes in edge computing environment

应用领域	特点	文献	时间
密钥体系	完整性、全面性	[20]	2018 年
移动边缘计算	注重安全性与匿名性	[21]	2019 年
智能电网	注重匿名性与高效性	[23]	2011 年
		[24]	2012 年
		[25]	2017 年
		[26]	2019 年
	可信第三方仅参与注册，减小了通信开销与延迟	[27]	2018 年
多方密钥协商	减小计算代价，提高通信效率	[28]	2019 年
		[29]	2018 年
		[30]	2017 年
数据外包	注重数据隐私保护，动态改变参与者的数量	[31]	2015 年
		[32]	2014 年
		[33]	2015 年
		[34]	2019 年

3.3 数据加密技术

对通信数据进行加密是密码技术在边缘计算领域最基本、最普遍的应用。与云端相比，边缘网络的数据存储量要小得多，并且边缘中存储的数据可以是多个用户共享的本地化信息。出于对密钥管理机制的复杂性和方案执行效率的考量，公钥加密机制在边缘计算框架中仍然过于复杂，资源受限的终端设备在进行解密操作时无法承受如此巨大的计算量。如何将加密算法轻量化，依然是一项重要且具有挑战性的工作。

最常见的公钥加密体制是基于身份的公钥加密体制。身份加密系统将主体的身份信息作为输入，通过密钥导出函数输出相应的公钥信息，并生成相应的私钥，这种方式解决了使用数字证书时的管理和开销问题[35]。Kim 等[36]提出了一种基于身份的广播加密技术，以支持边缘计算架构中的数据加密，通过将部分解密委托给边缘，大大减小了终端设备所需的计算和通信开销。对于资源受限的设备组成而言，这种方案能够显著延长设备的电池寿命并减轻系统的管理负担。

当边缘设备中的数据需要进一步处理分析时，边缘设备会将数据外包给第三方来获取更高级的计算资源与服务，这就造成了数据的所有权与控制权相分离的情况。若外包数据的保密级别较高，则需要某种特殊的技术来保证数据在外包过程中仍然呈现密文形态，即数据内容不被第三方所知。针对数据外包问题，全同态加密技术[37]是一种可行的方案，其特点保证了对密文执行代数运算与明文执行代数运算后再加密的结果是一致的。图 3 展示了全同态加密的特点。目前，全同态加密技术在边缘计算架构下的应用并没有具体的研究成果，尚待探索。

图 3 全同态加密

Fig. 3 Full homomorphic encryption

除此之外，可搜索公钥加密技术[38]也是一个值得关注的研究方向。第三方服务提供商可以在不解密用户数据的条件下，通过关键字搜索技术对加密数据进行搜索、管理等操作；用户可以通过搜索操作在密文数据中找到自己需要的数据。要将可搜索公钥加密技术应用于边缘计算的数据保护，首先要解决的问题是运算过程所需功耗如何与通信设备的电力储备与计算资源相适配。对于边缘计算中的外包数据安全保护问题，全同态加密技术和可搜索加密技术的应用是值得关注的研究方向。

在边缘计算中，数据在浏览、传输、中转等过程中要经历许多环节，在处理好应用服务商与用户的授权问题、协作问题的同时，确保数据的机密性与完整性是需要关注的重点。面向边缘计算的数据加密技术应用仍需要继续实践。

3.4 数据完整性保护技术

在对数据进行外包、控制权移交、格式转换等操作之前，最先进行的是对数据的完整性校验；其次，数据在存储或传输过程中，也可能会被恶意或偶然修改、删除、伪造等；此外，边缘计算的基础设施多位于网络边缘，缺少可供数据备份、恢复的存储资源，也缺乏有效的审计措施，攻击者可能修改或删除用户在边缘节点上的数据来销毁某些证据。

根据边缘计算架构的特点，对数据完整性的要求主要集中在批量审计、动态审计和低复杂度 3 个方面。边缘网络用户众多，数据完整性保护方案应当支持大量用户在不同的边缘节点同时发送请求的操作；面向物联网的数据是不断更新的，数据完整性保护方案应当具备动态审计功能；除此之外，数据完整性保护方案还应具备低复杂度的特点，包括低通信开销、低存储代价和低计算成本。

在众多密码技术中，数字签名技术在保证数据完整性方面有重要作用。数字签名的不可伪造性使得数据接收者能够验证数据的可靠性与完整性。下面以无人机为例来阐述数字签名技术在边缘计算中的具体应用。

无人机在远离指挥中心执行任务时，在传达和接收命令的过程中会经历较长的传播延迟，甚至还可能因天气和地形的限制而无法接收命令。移动边缘计算技术可以将这些命令带到更靠近无人机的网络边缘，以减少传播延迟。在这种情况下，引入代理签名方案可以实现边缘计算在无人机任务中的应用。指挥中心可以将指挥权临时授权给更靠近无人机的指挥站（如地面控制站等），地面控制站计算出用于代理签名的私钥，就可以代表命令中心进行签名，从而对无人机发出命令。

若无人机租赁公司将无人机出租给用户，用户不希望租赁公司知道租赁无人机执行的具体任务以保护隐私，则需要使用盲签名方案。He 等[39]提出了一种基于移动边缘计算技术的代理盲签名方案，其主要贡献是缩短了网络时延。

由此可见，数字签名技术不仅能够满足对数据完整性的要求，还能在一定程度上避免敏感数据的隐私泄露，实现安全高效的授权控制。目前，面向边缘计算环境设计的数字签名方案并不多，尚待进一步聚焦和关注。

3.5 隐私保护技术

隐私保护主要指的是边缘用户的隐私保护。边缘节点获取边缘用户的第一手数据，其中包含大量的敏感隐私数据，且相对于传统的云中心来说，边缘节点缺少有效的加密或脱敏措施，更容易遭受恶意攻击者的嗅探与腐蚀。在用户隐私保护方面，本节首先用 3 个典型的应用场景来阐明其重要性。

车联网领域面临着车辆的资源管控问题。公安部门等第三方有时会利用车辆的定位系统或监控系统抓捕罪犯或寻找丢失老人，即把车辆上的某些资源变成开源，在此情况下如何保证车辆自身数据的安全是亟待解决的重要问题。另一个流行的应用领域是智能医疗领域。大量监视用户健康的嵌入式和可穿戴设备被用于诊断或治疗。这些设备连接到附近的边缘服务器处，在边缘服务器处数据将被进一步处理和存储，随后转发[40]。检测患者身体状况的设备数据不可外泄，尤其是针对保险公司等一些身份敏感的机构。在这两种应用情况下，设备对边缘节点的匿名性都是至关重要的。

除了用户的位置信息、健康信息之外，用户的行为信息隐私保护也是一个重要的问题。例如，在智能家居中，只需观察智能电表的读数就可以获知家中何时无人、何时用电量高等信息。在智能家居中，同样存在位置隐私保护问题，即用户卸载计算任务或者将数据上传到附近的边缘节点上，第三方可以推断出终端的大致位置。

生物识别技术目前已成为最受欢迎的身份验证技术之一。与传统的基于密码的身份验证相比，生物识别技术具有独特性、可移动性、用户友好性等不可替代的优势[41]。其中，人脸识别是生物识别技术中最流行的技术，在身份验证系统中得到了广泛的应用[42]。在验证过程中，必须将面部图像上传到服务提供商的云服务器端。而人脸图像是非常敏感的信息，如果不加密就上传人脸图像，则会出现未获得授权者在未经用户许可的情况下收集、分析和滥用人脸信息等问题。

在人脸识别技术的应用中，隐私数据保护是一个至关重要的环节。安全多方计算技术是一个很好的选择。顾名思义，安全多方技术中通常不止使用一个云服务器。Ma 等[43]提出了一种基于全同态加密算法，使用深度神经网络提取面部特征的安全验证系统，由数据服务器存储用户的加密面部特征，通过验证服务器来执行面部验证。所有数据均以密文传输，除了验证服务器外，其他任何人都无法对其进行解密。这种引入多服务器的思想与边缘计算的思想在某种程度上相似。

因此，与传统的云服务器模型相比，在基于人脸识别技术的身份验证系统中引入边缘计算可以更轻松地满足隐私保护的需求。针对这个问题，Wang 等[44]提出了基于安全近邻算法的隐私保护方案，该方案可直接使用加密后的面部特征向量进行面部验证，并引入了边缘计算服务器，通过减少用户与云服务器之间的交互次数来提高验证效率。

研究者们还根据分类的思想提出了一些隐私保护方案。Chi 等[45]使用一种基于二分拓扑威胁模型和交互式对抗深度网络的分类算法来实现隐私保护，提出了“隐私分区”的概念，将资源分为可信分区和不可信分区，并进行隔离；Tramanan-da 等[46]设计了一种应用于智能家居场景的隐私保护方法——Vigilia，通过对设备进行分类，限制不同类设备的网络访问来增强系统的防御力，在保持很小资源开销的同时，对网络实现有效的通信限制；Wang 等[47]通过分析移动智能终端内主要的两种不同的隐私数据，提出了边缘计算下对移动智能终端内隐私数据的保护方法。分类的思想基于数据的多源性、异构性，这不仅能实现对不同类隐私数据的不同保护级别，还大大提高了具体实施过程中的执行效率。

此外，Xiao 等[48]重点针对移动卸载和缓存过程，研究了移动边缘计算系统中的攻击模型，并提出了一种基于应用强化学习（Reinforcement Learning，RL）技术的安全解决方案，可以向边缘节点提供安全的卸载服务，以防止攻击者从中干扰。这个协作缓存方案能够保证边缘设备的身份验证安全，从而进一步保护数据隐私。

由于边缘计算服务模式的复杂性、实时性，以及数据的多源异构性、感知性以及终端资源受限特性，传统环境下的数据安全和隐私保护机制不再适用于边缘设备产生的海量数据防护。表 3 列出了本节提到的主要研究成果，除此之外，对敏感数据处理和监测等也是一个值得关注的研究方向。

表 3 边缘计算环境下隐私保护技术的研究成果

Table 3 Research results of privacy protection technologies in edge computing environment

应用领域	文献	主要内容
生物特征识别	[43]	设计了多服务器机制下的人脸识别系统，由深度神经网络、数据服务器、验证服务器完成验证
	[44]	设计了基于安全近邻算法的隐私保护方案，减少用户与云服务器间的交互次数，提高验证效率
资源保护	[45]	提出“隐私分区”的思想，将资源分为可信分区和不可信分区，设计一种基于二分拓扑威胁模型和交互式对抗深度网络的分类算法
智能家居	[46]	设计了应用于智能家居场景的隐私保护方法——Vigilia
移动边缘计算	[47]	分析移动终端内的主要两种隐私数据，提出保护方法
	[48]	研究移动卸载和缓存过程的攻击模型，提出基于应用强化学习的协作缓存方案

3.6 区块链技术

在边缘计算场景下，参与的基础设施类型多、数量大，信任关系非常复杂。一方面，攻击者可能将恶意边缘节点伪装成合法的边缘节点，诱使终端用户连接到恶意边缘节点，隐秘地收集用户数据；另一方面，边缘基础设施多位于极端网络边缘，物理攻击时有发生，为其提供安全防护非常困难；此外，边缘节点的分散特点使得各个节点存储的数据很难同步更新，各节点的数据记录易遭到恶意攻击者的篡改。在这种情况下，需要分布式节点的验证和共识机制来解决分散系统节点之间的信任建立问题。符合这一要求的区块链技术就进入了人们的视野。

区块链作为加密货币的基础技术，在智能电网和物联网中有着广泛的应用。区块链在分布式系统上具有许多安全功能。首先，它能够在网络中保留完整的历史记录，以便恢复和验证用户获得的块信息。其次，区块链旨在抵抗其记录的修改。从理论上讲，除非恶意用户拥有超过一半的计算能力，否

则块及块中包含的数据都无法更改。最后,它不需要可信第三方来验证数据,避免了系统对第三方的依赖。区块链的优势在于分散管理与安全性方面,这也正是边缘计算架构面临的巨大挑战。

有研究者提出,将区块链技术和边缘计算集成到一个系统中已经成为一种不可避免的发展趋势[49-50]。通过合并区块链技术和边缘计算架构,系统既可以在大量分布式边缘节点上部署网络资源、存储资源和计算资源,同时又能实现可靠访问和控制,以提供更安全的数据存储和计算方式。Xu等[51]提出了资源受限的分层轻量级区块链框架(Layered Lightweight Blockchain Framework, LLBF)和实现机制。该框架由资源约束层(Resource Constrained Layer, RCL)和资源扩展层(Resource Extended Layer, REL)区块链组成,重新设计了块结构和大小,以适应边缘计算设备的特点,并引入轻量级共识算法和动态信任权算法,来提高区块链的吞吐量,减少分别在新区块中验证的交易数量。该框架通过高吞吐量管理,来保证区块链的交易负载平衡。

区块链技术发展至今,仍在可扩展性方面存在较大障碍,限制了其提供频繁交易服务的能力。而这也恰是边缘计算能够弥补的不足:边缘计算结构使系统拥有大量计算资源和分布在网络边缘的存储资源,从而有效地减轻了资源受限设备的区块链存储和挖掘计算负担,能够实现更加高效且合理的资源分配机制。针对区块链的资源分配问题和工作效率问题,已有许多边缘计算环境下的解决方案。

在区块链技术的资源分配方面,已有一些较好的方案可供参考。Liu等[52]设计了一种基于组合式双向拍卖的机制,将矿工的挖掘过程转移到边缘服务器上,提出了相应的分配算法和支付方案,分别进行资源分配和交易价格计算。实验结果表明,该机制产生效用较高,且具有可扩展性。与之类似,Xia等[53]提出了一种三阶段拍卖方案来实现专为移动区块链设计的资源分配,并引入团购机制来激励移动用户。Huang等[54]在区块链中找到用于交易数据存储的最佳对等节点,可以公平有效地在边缘设备上分配资源,大大提高了系统的可扩展性。与传统的区块链系统相比,该方案平均节省了15%的时间,只需消耗原有方案64%的电池电量。

除了资源分配问题之外,区块链技术的另一障碍是工作效率问题。区块链用户需要解决预设的工作量证明难题,才能向区块链添加新数据(即区块)。但是,完成工作量证明会消耗大量的CPU运行时间和能量资源,不适用于资源受限的移动设备。为了在移动物联网系统中促进区块链应用,多路访问移动边缘计算(Multiple Access Mobile Edge Computing)可作为一种解决移动用户工作量证明难题的方案。Xiong等[55]介绍了一种基于移动边缘计算的区块链系统原型,将提供者与矿工之间的行为交互抽象成Stackelberg游戏模型,游戏的目的是找到Stackelberg平衡。Stackelberg平衡确保服务提供者选择的价格可以使利润最大化,矿工也都能获得最佳响应。

将区块链技术的分散管理和安全性优势,与边缘计算的资源分配特点相结合,这不仅能够实现更加高效且合理的资源分配机制,还能通过分布式节点的验证和共识机制来解决分散系统节点之间的信任建立问题[56]。区块链技术和边缘计算两种技术的有机结合,在信任建立、信息传递和网络资源分配方面有着不可取代的优势,帮助各个通信节点之间加强协作,推动了通信技术与信息技术的融合发展。

4 面向边缘计算环境的密码技术比较

边缘计算领域在发展过程中不仅面临着层出不穷的新想法、新技术,也面临着安全方面的巨大挑战。如今,云计算模型下已有的较为成熟和完备的安全保护方案与技术体系,由于边缘计算模型中设备轻量化、架构异构性等新特点,变得不再适用。安全问题成为边缘计算研究中一个亟待解决的重要课题。

密码技术在边缘计算环境中的应用对解决数据安全问题与应用安全问题具有重要意义。本文从身份认证技术、密钥协商技术、数据加密技术、数据完整性保护技术、隐私保护技术和区块链技术入手,比较已有的研究方案,分别展示了不同技术在边缘计算安全保护中的优势与亟待解决的问题,如表4所列。

表4 边缘计算环境下不同密码技术应用的比较

Table 4 Comparison of different cryptographic technology applications in edge computing environment

安全挑战	密码技术应用	简述	优点	需要解决的问题
数据安全	数字签名技术	数据接收者能够验证数据的可靠性与完整性	低通信开销、低存储代价和低计算成本	需要具备动态审计功能,以适应数据不断更新的情况
	加密技术	公钥加密技术、全同态加密技术等	提供安全的通信服务	加密算法要适合轻量级设备的需求,降低算法执行过程中的功耗
	隐私保护技术	生物识别技术、安全多方计算技术、基于分类思想的隐私保护方案等	保护边缘用户的隐私	对灵活性和可适应性要求较高,且工作效率有待提高
应用安全	身份认证技术	传输机密信息之前验证各通信方身份	与密钥协商技术互为补充	重点要从高效性和灵活性方面做出优化
	密钥协商技术	广泛应用于有保密要求的通信场景中	与身份认证技术互为补充	需要设计完整安全的密钥体系,保证匿名性和高效率的特点
	区块链技术	加密货币的基础技术,在智能电网和物联网中都有着广泛的应用	抵抗恶意者对记录的修改	资源分配与效率问题

结束语 互联网正朝着物联网方向快速发展,正如Ericsson公司预测的那样:到2025年,将有超过500亿个设备连接到互联网[57]。这些边缘设备以极高的速度生成并更新大量数据,其中部分数据还需要在一定时间内得到转发、处理与存储。线性增长的集中式云计算能力无法匹配爆炸式增长的海量边缘数据,基于云计算模型的单一计算资源不能满足大

数据处理的实时性、安全性和低能耗等需求。边缘计算正是以这个角度出发，对云计算做进一步的完善与补充。与云计算相比，边缘计算具有缓解网络带宽与压力、增强服务响应能力、保护隐私数据等优势，与云计算相辅相成，互为补充。在边缘计算模式快速发展的同时，其安全防护问题是亟待解决的关键问题。

本文先阐述了边缘计算不同结构层次面临的安全挑战；然后重点分析了数据安全领域和应用安全领域对应的密码技术应对方案；最后，列举比较了已有的研究方案，分别展示了不同密码技术在边缘计算安全保护中的优势，为面向边缘计算环境的密码技术应用提供了新的思路。

参 考 文 献

[1] CULLER D E. The Once and Future Internet of Everything [EB/OL]. http://sites. nation- alacademies. org/cs/groups/cstbsite/documents/webpage/cstb_160416. pdf.

[2] SHI W, SUN H, CAO J. Edge Computing : An Emerging Computing Model for the Internet of Everything era[J]. Journal of Computer Research and Development, 2017, 54(5): 907-924.

[3] SHI W, CAO J, ZHANG Q, et al. Edge Computing: Vision and Challenges[J]. IEEE Internet of Things Journal, 2016, 3(5): 637-646.

[4] SATYANARAYANAN M. The Emergence of Edge Computing [J]. Computer, 2017, 50(1): 30-39.

[5] VARGHESE B, WANG N, BARBHUIYA S, et al. Challenges and Opportunities in Edge Computing[C]// 2016 IEEE International Conference on Smart Cloud (SmartCloud). IEEE Computer Society, 2016: 20-26.

[6] ALMAJALI S, SALAMEH H B, AYYASH M, et al. A Framework for Efficient and Secured Mobility of IoT Devices in Mobile Edge Computing[C]// The 3rd International Conference on Fog and Mobile Edge Computing (FMEC). 2018.

[7] TSAI J L, LO N W. A Privacy-aware Authentication Scheme for Distributed Mobile Cloud Computing Services[J]. IEEE Systems Journal, 2015, 9(3): 805-815.

[8] JIANG Q, MA J, WEI F. On the Security of a Privacy-aware Authentication Scheme for Distributed Mobile Cloud Computing Services[J]. IEEE Systems Journal, 2018, 12(2): 2039-2042.

[9] IRSHAD A, SHER M, AHMAD H F, et al. An Improved Multi-server Authentication Scheme for Distributed Mobile Cloud Computing Ser-vices[J]. KSII Transactions on Internet and Information Systems, 2016, 10(12): 6092-6115.

[10] XIONG L, PENG D, PENG T, et al. An Enhanced Privacy Aware Authentication Scheme for Distributed Mobile Cloud Computing Services[J]. KSII Transactions on Internet and Information Systems, 2017, 11(12): 6169-6187.

[11] LI J, ZHANG W, DABRA V, et al. AEP-PPA: An Anonymous, Efficient and Provably-secure Privacy Preserving Authentication Protocol for Mobile Services in Smart Cities[J]. Journal of Network and Computer Applications, 2019, 134: 52-61.

[12] YANG J H, CHANG C C. An ID-based Remote Mutual Authentication with Key Agreement Scheme for Mobile Devices on Elliptic Curve Cryptosystem [J]. Computer Security, 2009, 28(3): 138-143.

[13] YOON E J, YOO K Y. Robust ID-based Remote Mutual Authentication with Key Agreement Scheme for Mobile Devices on ECC[C]// IEEE International Conference on IEEE Cse. IEEE Computer Society, 2009, 2: 633-640.

[14] KAUR K, GARG S, KADDOUM G, et al. A Lightweight and Privacy-preserving Authen-tication Protocol for Mobile Edge Computing [C] // IEEE Global Communications Conference (GLOBE-COM' 19). IEEE Computer Society, 2019: 1-6.

[15] ZENG Y, GUANG H, LI G. Performance Improvement of Wireless Handover Authen-tication Protocol [J]. Application Research of Computers, 2018, 35(3): 901-904.

[16] CUI J, WEI L, ZHANG J, et al. An Efficient Message Authentication Scheme Based on Edge Computing for Vehicular Ad Hoc Networks[J]. IEEE Transactions on Intelligent Transportation Systems, 2019, 20(5): 1621-1632.

[17] DAS A K, WAZID M, KUMAR N, et al. Design of Secure and Lightweight Authen-tication Protocol for Wearable Devices Envi-ronment[J]. IEEE Journal of Biomedical and Health Informatics, 2018, 22(4): 1310-1322.

[18] JIANG Q, QIAN Y, MA J, et al. User Centric Three-factor Authentication Protocol for Cloud-assisted Wearable Devices[J]. Interna-tional Journal of Communication Systems, 2019, 32(6): e3900.

[19] KONG Z, XUE J, WANG Y, et al. Identity Authentication Under Internet of Everything Based on Edge Computing[C]// 6th IEEE International Conference on Cloud Computing and Intelligence Systems (CCIS 2019). IEEE Computer Society, 2020, 1149: 72-85.

[20] LIU X P, LIAO Z B, WEI Z G. Lightweight Key Management Scheme for Internet of Things[J]. Journal of International Security Research, 2018, 4(9): 819-824.

[21] JIA X Y, HE D, KUAMR N, et al. A Provably Secure and Efficient Identity-Based Anonymous Authentication Scheme for Mobile Edge Computing[J]. IEEE Systems Journal, 2019, 14(1): 560-571.

[22] LI Y, CHENG Q, LIU X. A Secure Anony-mous Identity-Based Scheme in New Authen-tication Architecture for Mobile Edge Computing[J/OL]. IEEE Systems Journal, 2020. http://doi.org/10.1109/JSYST.2020.2979006.

[23] WU D, ZHOU C. Fault-tolerant and Scalable Key Management for Smart Grid[J]. IEEE Transactions Smart Grid, 2011, 2(2): 375-381.

[24] XIA J, WANG Y. Secure Key Distribution for the Smart Grid [J]. IEEE Transactions Smart Grid, 2012, 3(3): 1437-1443.

[25] YAN L, CHANG Y, ZHANG S. A Lightweight Authentication and Key Agreement Scheme for Smart Grid[J]. International Journal of Distributed Sensor Networks, 2017, 13(2): 1-7.

[26] WU F, XU L, LI X, et al. A Lightweight and Provably Secure Key Agreement System for a Smart Grid With Elliptic Curve Cryptography[J]. IEEE Systems Journal, 2019, 13(3): 2830-2838.

[27] MAHMOOD K, LI X, CHAUDHRY S A, et al. Paring Based Anonymous and Secure Key Agreement Protocol for Smart Grid Edge Computing Infrastructure[J]. Future Generation Computer Systems, 2018, 88: 491-500.

[28] JIA X, HE D, KUAMR N, et al. Authenticated Key Agreement Scheme for Fog-driven IoT Healthcare System [J]. Wireless Networks, 2019, 25(8): 4737-4750.

[29] LIU C, TSAI W J, CHANG T Y, et al. Ephemeral-secret-leakage Secure ID-based Three-party Authenticated Key Agreement Protocol for Mobile Distributed Computing Environments[J]. Symmetry, 2018, 10(4): 84.
[30] LEE T F, HWANG T. Three-party Authenticated Key Agreements for Optimal Communication[J]. PLoS ONE, 2017, 12(3): e0174473.
[31] ZHOU L, VARADHARAJAN V, HITCHENS M. Cryptographic Role-based Access Control for Secure Cloud Data Storage Systems[C]// 10th International Conference on IEEE Security and Cryptography (SECRYPT). IEEE Computer Society, 2013, 10(11): 2381-2395.
[32] CHEN F, XIANG T, YANG Y, et al. Secure Cloud Storage Meets with Secure Network Coding[C] // IEEE INFOCOM. IEEE Computer Society, 2014: 673-681.
[33] HE D, ZEADALLY S, WU L. Certificateless Public Auditing Scheme for Cloud-assisted Wireless Body Area Networks[J]. IEEE Systems Journal, 2015, 12(1): 64-73.
[34] SHEN J, ZHOU T, HE D, et al. Block Design-based Key Agreement for Group Data Sharing in Cloud Computing[J]. IEEE Transactions on Dependable and Secure Computing, 2019, 16(6): 996-1010.
[35] SHAMIR A. Identity-based Cryptosystems and Signature Schemes[C] // Advances in Cryptology-Crypto'84. Springer-Verlag, 1984, 196: 47-53.
[36] KIM J, CAMTEPE S, SUSILO W, et al. Identity-Based Broadcast Encryption with Outsourced Partial Decryption for Hybrid Security Models in Edge Computing[C]// 2019 AsiaCCS. 2019: 55-66.
[37] RIVEST R L, ADLEMAN L, DERTOUZOS M L. On Data Banks and Privacy Homo-morphisms[M]// Foundations of Secure Computation. New York: Academic Press, 1978: 169-179.
[38] KAMARA S, PAPAMANTHOU C, ROEDER T. Dynamic Searchable Symmetric Encryption[C] // The 19th ACM Conference on Computer and Communications Security. 2012: 965-976.
[39] HE L, MA J, MO R, et al. Designated Verifier Proxy Blind Signature Scheme for Unmanned Aerial Vehicle Network Based on Mobile Edge Computing[J]. Security and Communication Networks, 2019, 8583130: 1-12.
[40] OGBANUFE O, KIM D J. Comparing Fingerprint-based Biometrics Authentication Versus Traditional Authentication Methods for E-payment[J]. Decision Support Systems, 2018, 106: 1-14.
[41] BLANTON M, GASTI P. Secure and Efficient Protocols for Iris and Fingerprint Identification[C] // European Symposium on Research In Computer Security. 2011: 190-209.
[42] HSIEH C T, HAN C C, LEE C H, et al. Person Authentication Using Nearest Feature Line Embedding Transformation and Biased Discriminant Analysis[C]// International Carnahan Conference on Security Technology. 2017: 1-5.
[43] MA Y, WU L, GU X, et al. A Secure Face Verification Scheme Based on Homomorphic Encryption and Deep Neural Networks [J]. IEEE Access, 2017, 5: 16532-16538.
[44] WANG X, XUE H, LIU X, et al. A Privacy-preserving Edge Computation-Based Face Verification System for User Authentication[J]. IEEE Access, 2019, 7: 14186-14197.
[45] CHI J, OWUSU E, YIN X, et al. Privacy Partition: A Privacy-preserving Framework for Deep Neural Networks in Edge Networks[C] // IEEE/ACM Symposium on Edge Computing (SEC). 2018: 378-380.
[46] TRAMANANDA R, YOUNIS A, WANG B J, et al. Vigilia: Securing Smart Home Edge Computing[C]// IEEE/ACM Symposium on Edge Computing (SEC). 2018: 74-89.
[47] WANG F, WEN H, CHEN S, et al. Privacy Data Protection Method for Mobile Intelligent Terminal Based on Edge Computing[J]. Cyberspace Security, 2018, 9(2): 47-50.
[48] XIAO L, WAN X, DAI C, et al. Security in Mobile Edge Caching with Reinforcement Learning[J]. IEEE Wireless Communications, 2018, 25(3): 116-122.
[49] YANG R, YU F R, SI P, et al. Integrated Blockchain and Edge Computing Systems: A Survey, Some Research Issues and Challenges [J]. IEEE Communications Surveys & Tutorials, 2019, 21(2): 1508-1532.
[50] SHARMA K, SINGH S, JEONG Y S, et al. Distblocknet: A Distributed Blockchains-based Secure SDN Architecture for IoT Networks[J]. IEEE Communications Maga zine, 2017, 55(9): 78-85.
[51] XU X, ZENG Z, YANG S, et al. A Novel Blockchain Framework for Industrial IoT Edge Computing[J]. Sensors, 2020, 20(7): 2061.
[52] LIU X, WU J, CHEN L, et al. Efficient Auction Mechanism for Edge Computing resource Allocation in Mobile Blockchain[C]// IEEE 21st International Conference on High Performance Computing and Communications; IEEE 17th International Conference on Smart City; IEEE 5th International Conference on Data Science and Systems (HPCC/SmartCity/DSS). 2019: 1-10.
[53] XIA C, CHEN H, LIU X, et al. ETRA: Efficient Three-Stage Resource Allocation for Mobile Blockchain in Edge Computing [C]// IEEE 24th International Conference on Parallel and Distributed Systems (ICP-ADS). 2018: 701-705.
[54] HUANG Y, ZHANG J, DUAN J, et al. Resource Allocation and Consensus on Edge Blockchain in Pervasive Edge Computing Environments[C]// IEEE 39th International Conference on Distributed Computing Systems (ICDCS). 2019: 1476-1486.
[55] XIONG Z, ZHANG Y, NIYATO D, et al. When Mobile Blockchain Meets Edge Computing[J]. IEEE Communications Magazine, 2018, 56(8): 33-39.
[56] Chinese Mobile 5G Innovation Center. White Papers for Blockchain and Edge Computing[R]. Innovation Research Report of Chinese Mobile 5G Innovation Center, 2020.
[57] Ericsson Inc. Ceo to Shareholders: 50 Billion Connections 2020 [EB/OL]. http:// www. ericsson. com/thecom-pany/press/releas- es/2010/04/1403231.

CHENG Qing-feng, born in 1979, Ph.D, associate professor, Ph. D supervisor. His main research interests include cryptography and information security.

LI Yu-ting, born in 1996, postgraduate. Her main research interests include cryptography and edge computing.