边缘计算安全技术综述

凌捷，陈家辉，罗玉，张思亮
广东工业大学计算机学院，广东 广州 510006

摘要
随着物联网应用的不断展开，大量移动终端设备参与服务计算，传统的云计算模型已经不能满足网络边缘设备产生数据的速度，边缘计算模型应运而生，并成为近几年的研究热点。介绍了边缘计算的概念和物联网的边缘计算参考模型，分析总结了边缘设备容易遭受的攻击，综述了边缘计算中密码安全技术的主要研究成果，并指出：对称密码技术不适用于边缘设备之间的通信，基于身份标识的密码技术较适用于边缘设备到边缘设备的通信，基于配对的密码技术较适用于边缘设备到基站的通信。讨论了两种后量子密码技术在边缘设备中的应用，提出了边缘计算安全技术研究的几个建议。

关键词
边缘计算；物联网；边缘设备；云计算；密码技术

中图分类号：TP309　　文献标识码：A　　doi: 10.11959/j.issn.2096-0271.2019012

A survey on the security technology of edge computing

LING Jie, CHEN Jiahui, LUO Yu, ZHANG Siliang
School of Computers, Guangdong University of Technology, Guangzhou 510006, China

Abstract
With the continuous development of Internet of things applications, a large number of mobile terminal devices participate in service computing. Traditional cloud computing models cannot adapt to the rapid growth of data generated by network edge devices, and edge computing models emerge and become a research hotspot in recent years. The concept of edge computing and the reference model of edge computing in the Internet of things were introduced, the vulnerabilities of edge devices and the main research results of cryptographic security technology in edge computing were summarized, and that symmetric cryptography technology is not suitable for communication between edge devices, and identity-based cryptography technology is more suitable for communication between edge devices and edge devices was pointed out. Paired-based cryptography is more suitable for the communication between edge devices and base stations. The application of two post-quantum cryptography technologies in edge devices was discussed. Finally, some suggestions on the research of edge computing security technology were put forward.

Key words
edge computing, Internet of things, edge device, cloud computing, cryptography technology

1 边缘计算的概念

随着智慧城市、智能交通等物联网应用的不断推进和空间位置服务、移动支付服务等新型服务模式的快速发展，物联网设备连接数量和产生的数据呈海量增长趋势。传统的云计算模型采用集中处理方式，将所有数据通过网络传输到云计算中心，利用云计算中心强大的计算能力集中式地解决计算和存储问题。在万物互联的物联网应用背景下，云计算中心负载、传输带宽和数据安全等云计算局限性问题越来越突出，各种接入设备感知产生的海量数据使云计算的网络带宽变得更加有限，让云端不堪重负，造成更大的数据瓶颈。譬如云计算对时延敏感的业务系统不能很好地奏效[1]。这些时延敏感的业务往往处于数据中心边缘，可以利用附近的计算设备完成计算，并减少时延；对于高实时性要求的智能交通中的联网车辆[2]、火灾探测与消防系统[3]、高度分布架构的在线移动视频内容交付[4]等，集中于数据中心的云计算模型已难以满足需求。因此，边缘计算模型应运而生，并成为近几年的研究热点[5-8]。

边缘计算是在网络边缘执行计算的一种新型计算模型，边缘计算的边缘是指从数据源到云计算中心之间的任意计算资源和网络资源[9]。边缘计算面向的对象包括来自物联网的上行数据和来自云服务的下行数据。边缘计算允许终端设备将存储和计算的任务迁移到网络边缘节点中，既可满足终端设备的计算能力扩展需求，又能有效地节约计算任务在终端设备与云服务器之间的传输链路资源。

物联网的边缘计算参考模型可分为7层[10]，如**图1**所示，其安全涉及模型的所有层。

● 边缘设备层通常包括计算边缘设备，如传感器、智能控制器、可穿戴设备、射频识别（radio frequency identification，RFID）阅读器以及不同版本的RFID标签等。边缘设备层的安全主要考虑边缘设备的物理安全和内容安全。

● 通信层由所有能够传输信息或命令的组件组成，包括第一层设备之间的通信、第二层组件之间的通信、第一层和第三层之间的信息传输。通信层的安全主要考虑安全接入，包括通信设备安全和协议安全。

● 边缘计算层也称雾计算层，在这一层中启动基本的数据处理，包括数据元分析、数据过滤、数据清洗、数据集成和事件生成等，对于在更高层级上减少计算负载以及提供快速响应而言非常重要，因为大多数实时应用程序需要在尽可能靠近网络边缘的地方执行计算。该层通常使用简单的信号处理和学习算法，处理量取决于服务提供者、服务器和计算边缘设备的计算能力。边缘计算层的安全主要考虑协议安全和加解

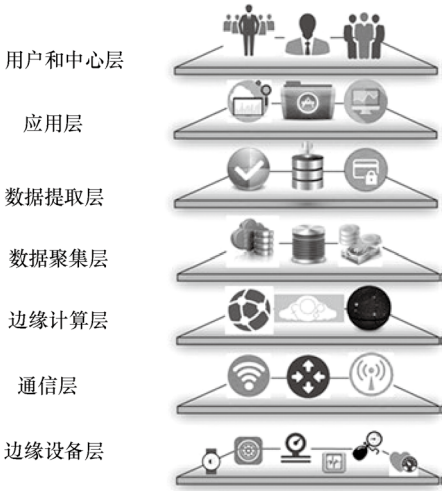


图1 物联网的边缘计算参考模型

密技术。

● 数据聚集层通常考虑事件抽样、事件集成和数据存储等。这一层的安全主要考虑防数据篡改等攻击。

● 数据提取层通常考虑数据渲染抽取和数据的存储，这一层的安全主要考虑数据安全存储。

● 应用层包括控制应用、移动应用、商业智能与分析展示等，这一层的安全主要考虑认证安全。

● 用户和中心层包括用户和云计算中心，这一层的安全主要考虑身份安全管理。

边缘计算模型拥有一些明显的优点，具体如下。

● 实时或更快速的数据处理和分析：数据处理更接近数据来源，而不是在云端或外部数据中心进行，可以减少延迟时间。

● 较低的成本：企业在本地设备的数据管理解决方案上的花费比在云和数据中心网络上的花费少。

● 网络流量较少：网络边缘设备产生的大量数据在网络边缘处理，不需要上传到云计算中心，减轻了网络带宽的负载。

● 更高的应用程序运行效率：随着时延减少，应用程序能够以更快的速度更高效地运行。

边缘计算的数据处理实时性、数据多源异构性、终端资源受限性和接入设备复杂性，使得传统云计算环境的安全机制不再适用于边缘设备产生的海量数据的安全防护，边缘计算的数据存储安全、共享安全、计算安全、传输和隐私保护[11]等问题成为边缘计算模型必须面对的挑战性问题。

本文介绍了物联网的7层边缘计算参考模型，分析总结了边缘计算参考模型中的边缘设备层、通信层和边缘计算层容易遭到的安全攻击，综述了边缘计算中密码安全技术的研究成果，最后给出了边缘计算安全技术研究的几个建议。

2 边缘计算的安全攻击

与传统的信息安全属性相似，边缘设备的安全性包括机密性、完整性和可用性。机密性需要应用一组规则来限制对某些信息进行未经授权的访问，这对于边缘设备而言至关重要，因为它们可能处理敏感的个人信息，如医疗记录和处方，若未经授权访问个人健康设备，可能会泄露个人健康信息，甚至导致生命危险；完整性也是必要的，边缘设备必须确保接收到的命令和采集到的信息是合法的，例如针对医疗设备（如糖尿病的胰岛素泵[12]或心脏起搏器[13]）的完整性攻击，可能会导致危及生命的后果；边缘设备的可用性对于提供功能齐全的物联网连接环境而言至关重要，它确保设备可用于采集数据，并防止服务中断。

2.1 边缘设备层的安全攻击

(1) 硬件木马

硬件木马对边缘设备的集成电路进行恶意修改，使攻击者能够利用该电路或利用其功能获取边缘设备上运行的数据或软件[14-18]。硬件木马已经成为边缘设备的主要安全隐患之一。为了在原始电路中插入硬件木马，攻击者在制作过程中恶意改变集成电路的设计，设定触发机制和激活木马的恶意行为[19]。硬件木马根据其触发机制分为两类：外部激活的木马，可以通过天线或传感器与外界交互触发；内部激活的木马，在集成电路内部满足一定条件后被激活，当它从攻击者添加的倒计时电路接收到触发信号时，木马会在特定时间被唤醒。

(2) 侧信道攻击

每个边缘设备在正常运行时，即使不使用任何无线通信传输数据，也可能会泄

露关键信息，因为通过分析边缘设备发出的电磁波，就可以获取设备状态的有价值的信息。Vuagnoux M等人[20]研究的基于电磁信号的攻击和美国国家安全局解密的风暴文件都展示了非网络侧信道威胁的存在。参考文献[21]的研究人员能够从医疗设备泄漏的声波/电磁信号中获取关于患者或设备的有价值的信息，正如该工作所述，检测已知信号或协议的存在可能危及用户的安全。此外，这种类型的攻击可能会在医疗系统中导致严重的隐私问题。例如，对于一个佩戴医疗设备的人，若该设备表明他患有某种带有社会污名的疾病，发现这个装置的存在会使病人感到尴尬。另外，来自设备的特定侧通道信息可能提供有关个人健康状况的重要信息，如血糖水平和血压等。

(3) 拒绝服务攻击

针对边缘设备的拒绝服务 (denial of service, DoS) 攻击有3种类型：电池耗尽攻击、睡眠剥夺攻击和宕机攻击。

- 电池耗尽攻击：受尺寸限制，边缘设备通常携带能量有限的小电池，这使得电池耗尽攻击成为一种非常强大的攻击，可能会间接导致边缘设备中断或无法报告紧急情况的严重后果。例如，若攻击者找到耗尽烟雾探测器电池的方法，就能够禁用火灾探测系统[22]。如果边缘设备充电困难，这种攻击可能会破坏网络。电池耗尽攻击的一个例子是，攻击者向边缘设备发送大量随机数据分组，迫使边缘设备不间断地运行其检查机制。参考文献[23-24]讨论了几种电池耗尽攻击的方式。
- 睡眠剥夺攻击：睡眠剥夺是DoS攻击的一种特殊类型，受害者是一个电池供电的边缘设备，能量有限，攻击者试图发送一组看似合法的请求，刺激边缘设备。检测这类攻击比检测电池耗尽攻击困难得多。睡眠剥夺的概念最初是由Stajano F提出的[25]。
- 宕机攻击：当边缘设备停止正常运行时，一组设备或管理员设备可能会停止工作，该情况可能是由制造过程中的意外错误、电池耗尽、睡眠不足、代码注入或对边缘设备的未经授权物理访问等导致的结果。宕机攻击的著名例子之一是伊朗布什尔核电站的进程控制系统被注入震网病毒[26]，使得受感染的工业控制系统丧失了检测异常行为的能力。

(4) 物理攻击

物理攻击中，攻击者通过对设备的物理访问提取有价值的加密信息，进而篡改电路、修改编程或者更改操作系统[27-28]。对边缘设备的物理攻击可能导致永久性破坏。因为它们的主要目的是提取信息供将来使用，如查找固定的共享密钥。在参考文献[29]介绍的智能巢式恒温器事件中，攻击者用恶意固件替换了默认固件，从而使攻击者能够永久地控制恒温器，即使他不能够再物理访问该设备。

(5) 应答攻击

攻击者通过复制边缘设备的标识号，将一个新的边缘设备添加到现有的边缘设备集中。这种攻击会导致网络性能的显著降低。此外，攻击者很容易破坏或误导到达副本的数据分组[30]。应答攻击的攻击者通过获得加密/共享密钥所需的访问权限，对系统实施破坏[31]，边缘设备副本通过执行边缘设备撤销协议来撤销授权边缘设备[32]。

(6) 伪装攻击

攻击者插入伪造的边缘设备或攻击授权的边缘设备，以便其在边缘设备层隐匿。修改/伪造的边缘设备可以作为普通边缘设备来获取、处理、发送或重定向数据分组[29]，这些边缘设备也可以在被动模式下工作，只进行流量分析。

(7) 恶意边缘设备攻击

恶意边缘设备攻击的主要目标是获得对其所属网络的未授权访问或者破坏网络。

恶意边缘设备可以获得对其所属网络的其他边缘设备的访问权，进而代表攻击者控制网络、向系统中注入虚假数据或阻止传递真实消息[33]。

(8) RFID标签攻击

针对物联网RFID标签的攻击主要包括追踪、复制、物理、干扰阻塞、DoS、窃听、中间人等攻击。

● 追踪攻击：通过未经授权的阅读器隐形读取标签信息，当标签标识符与个人信息结合时，可提供很强的跟踪信息能力[34]，导致敏感信息或隐私信息泄露。

● 复制攻击：攻击者复制标签的所有信息，制造出与合法标签完全相同的电子标签[35]。

● 物理攻击：获取标签的访问权限，对标签进行物理操作和修改，包括探针攻击、Kill命令、电路操作和时钟故障[36]，可用于从标签中提取信息、修改或删除标签。

● 干扰阻塞：通过静电屏蔽和主动干扰无线电信号等方法，阻止阅读器读取标签[37]。

● DoS攻击：当阅读器收到来自标签的认证信息时，会将认证信息与数据库后端的信息进行对比，攻击者通过看似合法的手段阻塞射频通道，使得标签阅读器无法读取标签。阅读器和后端数据库都容易遭受DoS攻击。参考文献[38]分析了RFID认证协议对DoS攻击的附加漏洞。

● 窃听攻击：通过拦截标签和读写器之间传输数据的电磁波获得传输内容。美国国家标准与技术研究院 (National Institute of Standards and Technology, NIST) 的RFID指南[39]以及参考文献[40-41]发表的研究结果都提到了RFID环境中的窃听攻击风险。

● 中间人攻击：无源RFID系统标签会在收到读写器的信号后主动响应，发送联络信号。攻击者先伪装成一个阅读器靠近标签，在标签携带者毫无知觉的情况下读取标签信息，然后将从标签中偷到的联络信号发送给合法的阅读器，达到攻击的目的[42]。

2.2 通信层的安全攻击

边缘计算的通信层容易遭受的主要攻击如下。

(1) 窃听攻击

窃听攻击是指有意地监听通信链接上的私密通话[43]。若通信数据分组未加密，攻击者可以直接获得有价值的信息；在加密的情况下，攻击者也有可能获取用户名和密码。当数据分组包含访问控制信息时，如边缘设备配置、共享网络密码和边缘设备标识符，通过窃听可以捕获关键信息。攻击者可以使用这些捕获的信息设计其他定制的攻击，例如如果攻击者能够成功提取信息，将某个伪造的新边缘设备添加到授权边缘设备集中，那么它就能够轻松地把一个恶意边缘设备添加到系统中。

(2) 侧信道攻击

尽管侧信道攻击[44]不易实现，但它们是针对加密系统的强大攻击，能对加密系统的安全性和可靠性构成严重威胁。如前文所述，侧信道攻击也可以在边缘设备层启动。与边缘设备层的攻击不同，通信层的侧信道攻击通常是非侵入性的，它们只提取无意泄漏的信息。该攻击的一个重要特征是它们是难以检测的，因此，除了最小化泄漏或为泄漏的信息添加噪声之外，目前对侧信道攻击没有简单可行的防御方法。

(3) DoS攻击

通信层的DoS攻击的作用是阻塞无线电信号的传输[45]。参考文献[46]定义了两种类型的有源干扰攻击：持续干扰，即对所有

传输进行完全干扰；间歇性干扰，边缘设备可以周期性地发送/接收数据分组。持续干扰的目标是阻断所有的通信传输，而间歇性干扰的目标是降低通信的性能。例如一个火灾探测系统原本可以探测到环境中气体水平的异常变化，并在紧急情况下呼叫消防队。攻击者通过间歇性地干扰边缘设备到边缘设备、边缘设备到基站的传输，使系统变得不可靠，在这种情况下，如果攻击者使用持续干扰，系统将停止服务。有些文献研究针对各种传输协议（包括蓝牙）发起DoS攻击的可能性和有效性[47-48]。除了主动干扰攻击外，攻击者还可能使用恶意边缘设备或路由器启动DoS攻击，攻击者插入故意违反通信协议的边缘设备或路由器，以产生冲突或干扰通信。恶意路由器或边缘设备也可能拒绝路由消息或试图误导它们，这种DoS攻击可以间歇地或持续地进行。持续的DoS攻击通常较容易被检测到，而间歇性攻击的检测则需要精确和高效的监视设备。

(4) 注入欺骗分组攻击

攻击者可以使用插入、操纵和重播3种不同的攻击方式，将欺诈性数据分组注入通信链路。在插入攻击中，攻击者能够生成并发送看似合法的恶意数据分组；操纵攻击是指捕获数据分组，然后对其进行修改（如更新报头信息、校验和、数据），并发送操纵的数据分组；在重播攻击中，攻击者捕获之前两个对象之间交换的数据分组，并在通信过程中重播相同的数据分组。

(5) 路由攻击

影响消息路由方式的攻击被称为路由攻击。攻击者可以使用此类攻击在通信层欺骗、重定向、误导或删除数据分组。最简单的路由攻击类型是更改攻击，攻击者通过生成路由循环或错误消息更改路由信息。

(6) 未授权对话攻击

每个边缘设备都需要与其他边缘设备通信，以便共享数据或访问它们的数据。但是，每个边缘设备应该只与需要其数据的边缘设备子集进行通信，这是物联网系统的基本要求，特别是对于由不安全边缘设备和安全边缘设备组成的物联网系统。未授权对话攻击是获取未授权的边缘设备与边缘设备之间的对话信息的一种攻击。例如在智能家居场景中，为了在紧急情况下关闭供暖系统，恒温器需要烟雾探测器的数据。然而，如果不安全的烟雾探测器可以共享每一个其他边缘设备的信息，攻击者可能通过入侵烟雾探测器的方式控制整个家庭自动化系统。

(7) 其他攻击

除了上述攻击方式外，还有一些通信层的攻击方式，如黑洞、灰洞、蠕虫洞、泛洪和女巫（sybil）等攻击[49-52]。

- 黑洞攻击：黑洞攻击是利用一个恶意边缘设备发起的，该边缘设备通过在网络中宣称它有到目标的最短路径的方式吸引网络中的流量。结果大部分的数据分组被发送到恶意边缘设备中，攻击者可以利用这些数据分组，也可以直接丢弃它们。
- 灰洞攻击：灰洞攻击是黑洞攻击的一个变体，在分组丢失过程中，灰洞攻击让边缘设备有选择地丢弃数据分组。
- 蠕虫洞攻击：蠕虫洞攻击是一种严重的攻击，即便通信中的所有实体都保证了真实性和保密性，这种攻击也可以发起。在这种攻击中，攻击者在两个合谋恶意节点间建立一条私有通道，将在网络中某个位置记录的数据分组通过此私有通道传递到网络的另一个位置。
- 泛洪攻击：假设接收边缘设备在发送方的通信范围内，泛洪攻击的基础是边缘设备必须广播“Hello packet”以向邻居显示其存在。在这种攻击中，攻击者使用具有

高传输能力的恶意边缘设备，发送“Hello packet”到网络中的每个其他边缘设备，并声称是它们的邻居。

● 女巫攻击：在女巫攻击中，攻击者添加或使用Sybil边缘设备，这些边缘设备均具有合法的假身份，如果Sybil边缘设备足够多，在系统中进行投票时，Sybil边缘设备就可以胜过“诚实的”边缘设备。

2.3 边缘计算层的安全攻击

边缘计算模型是一种新兴的技术，其脆弱性尚未得到充分的探索。少数针对边缘计算攻击的研究主要集中在对传感器网络可能的威胁上[53-54]。本节讨论针对边缘计算的一些攻击场景。

(1) 恶意注入攻击

对输入数据的验证不足可能导致恶意注入攻击。攻击者可以注入恶意输入，导致服务提供者代表攻击者执行攻击操作。例如攻击者可能会向下层（通信或边缘设备层）添加未经授权的组件，这些层随后会将恶意输入注入服务器，之后攻击者就可以窃取数据、破坏数据库完整性或绕过身份验证。数据库返回的标准错误消息也可以帮助攻击者获取信息，如在攻击者不知道数据库表的情况下，强制执行返回的错误消息可能会揭示关于每个表及其字段名称的更多细节[55]。

(2) 基于机器学习的完整性攻击

针对物联网系统中使用的机器学习方法，可以发起两类攻击：因果攻击和探索性攻击[56]。在因果攻击中，攻击者通过操纵训练数据集改变训练过程，而在探索性攻击中，攻击者利用漏洞获取数据的信息，但不改变训练过程。参考文献[57]公布了一种新型的致因性攻击，称为中毒攻击，攻击者将精确选择的无效数据点添加到训练数据集中。在基于边缘计算的系统中，攻击者可以启动这个攻击的学习算法，直接访问服务器或各种边缘设备，或者将恶意数据添加到拥有足够数量恶意边缘设备的低水平的物联网数据集中，其目的是通过操纵训练数据集使分类算法偏离对有效模型的学习。

(3) 侧信道攻击

前文提到的针对边缘设备层和通信层的几种侧信道攻击，在边缘计算层侧信道攻击也会奏效[58]。此外，攻击者可能会使用从其他组件（如服务提供者和服务器）泄露的信息发起侧信道攻击。例如生成详细的错误警告的方法可以为设计人员和开发人员提供有用的信息，但在实际环境中，相同的警告可能提供过多的信息，从而可能被实施侧信道攻击者利用。

(4) 非标准框架和不充分测试的攻击

非标准框架缺陷会引起严重的隐私和安全问题。由于边缘设备通常需要连接到中间服务器，边缘设备被挟持的后果可能会被放大。基于边缘计算的系统的开发是一个复杂的过程，因为它需要将不同厂商生产的异构资源和设备结合起来[59]，若开发的系统测试不充分，会遗留一些安全漏洞。另外基于边缘计算的系统的实现没有普遍接受的框架，也没有标准的策略集，因此这些系统未经过充分的测试，一些隐私和安全漏洞可能仍未被发现。

3 边缘计算的密码安全技术

3.1 公钥基础设施

密码安全技术可分为对称密码（SKC）技术[60]、公钥密码（PKC）技术[61]和无密钥密码技术[62]几类（如**图2**所示）。其中，对称密码技术也称为单密钥模式，公钥密码技术称为双密钥模式，无密钥密码技术也称为随机密钥模式。随机密钥模式下

通信双方不使用固定的密钥，每次通信时双方都随机产生一个密钥进行加密通信。

对称密码技术在低通信和计算开销方面具有优势，但应用于边缘计算时需要分发共享密钥。密钥的预分发方法有以下3种类型。

● 单个网络密钥：可能会导致单点故障，即如果一个边缘设备的密钥被泄露，则整个网络会被破坏。

● 边缘设备与基站之间或两个边缘设备之间的密钥对：密钥对的管理较困难且效率低下，每个边缘设备必须共享$n(n-1)/2$个密钥，其中n为边缘设备的个数。如果某个边缘设备的密钥被泄露，具有相同密钥的另一个边缘设备也会受到威胁。

● 一组边缘设备之间的组密钥：组密钥管理比密钥对管理效率更低，因为它需要大量的计算开销和边缘设备之间的交互。如果一个边缘设备组中的组密钥被暴露，那么整个边缘设备组都将被破坏。

安全的密码方案应该保证，无论捕获多少个边缘设备，从受损边缘设备提取的秘密信息都不会影响非受损边缘设备的安全，即非受损边缘设备之间的通信仍然安全。但是对称密码技术的以上3种类型都不能满足这个要求，公钥密码技术则可以做到。

公钥密码技术在安全广播和身份验证方面具有优势，它可以在以前未知的伙伴之间安全地交换密钥。公钥密码中的公钥必须经过认证，一般通过公钥基础设施（public key infrastructure，PKI）使用由认证机构（CA）发出的公钥证书解决公钥认证问题。

公钥密码技术使许多边缘计算应用程序需要的安全属性和功能（如具有不可抵赖性的身份验证、同态属性、聚合、批处理验证、带有消息恢复的签名等）成为可能。公钥密码的计算成本阻碍了它在资源受约束的边缘设备上的应用。如果没有加密硬件的加速，公钥密码对于小型设备来说计算成本过高，但有许多研究表明[63-65]，将公钥密码算法应用于资源有限的小型无线设备是可行的。

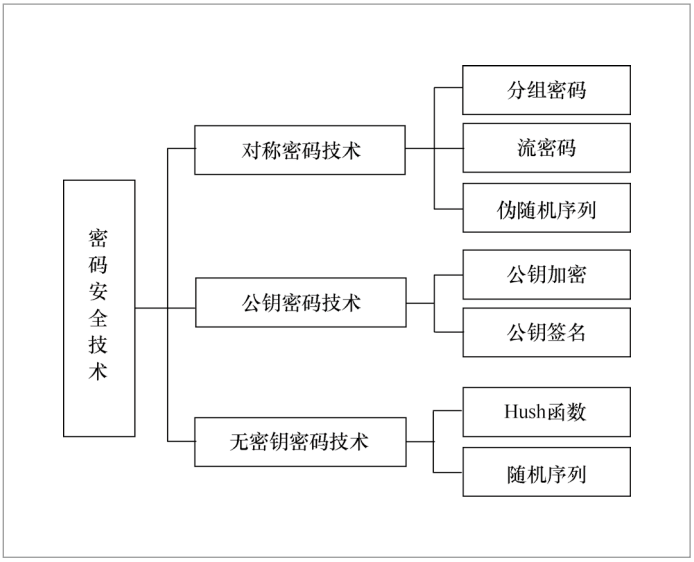


图2 密码安全技术的分类

为了在边缘计算中应用PKC，需将PKI部署到边缘设备中，并选择适当的层次结构模型。在大多数情况下，边缘设备层的边缘设备架构比较简单：一个基站（base station，BS）作为成百上千个边缘设备的接口，与属于同一网络的边缘设备通信。因此，大多数边缘计算网络使用一个根CA的简单分层PKI体系结构就足够了。PKI的注册、初始化、密钥生成、认证和认证检索等基本功能在边缘设备中的实现过程如下：基站创建边缘设备的公共/秘密密钥对，为边缘设备分配唯一标识，并创建一个证书，该证书将该唯一标识与边缘设备公钥链接起来。然后初始化边缘设备的内容（如配置数据和内部编程），包括其证书和根CA的证书（即BS本身）。当边缘设备检索其邻居的证书

时，它将能够使用根CA的证书检查邻居的证书的有效性。

在一些固定基站的边缘计算应用中，公钥密码方案适用于边缘设备到基站通信中的端到端的保密。因为边缘计算的引导程序可以在预部署阶段将公钥预加载到每个边缘设备。每个边缘设备通过BS公钥下的PKC方案对检测到的数据进行加密，然后将加密后的数据发送到BS或邻近设备进行中继传输。但是，在特定的边缘计算中，如果需要边缘设备到边缘设备通信中的逐跳认证，这种公钥密码方案就不适合了。因为，为了相互验证，边缘设备应该交换它们的公钥证书，然后验证证书中CA的签名，证书传输的通信开销和验证CA签名的计算开销在每个边缘设备中都很大。在这种情况下，更好的替代方案是基于身份标识的密码（identity-based cryptograph，IBC）技术。

3.2 基于身份标识的密码技术

基于身份标识的密码技术是Shamir A提出的[66]，它使用户的公钥可以很容易地从已知的身份标识信息（如电子邮件地址或移动电话号码）中派生出来，解决了对公钥证书的需求，减少了证书开销。一个私钥生成器（private key generator，PKG）有一个主公共/秘密密钥对，负责为用户生成私钥。因此，在边缘计算中，可以只交换边缘设备的身份，而不发送公钥及其证书，为通信节省了能源。

在PKI的应用[67]中，每个边缘设备都将自己的公钥/私钥对与CA颁发的相应公钥证书存储在一起，任何希望与节点交互的外部方都需要节点的公钥证书。由于需要交换设备的公钥证书，PKI适用于边缘设备到BS的通信，但不适用于边缘设备到边缘设备的通信。而基于身份标识的密码方案则更适合如下场景：每个边缘设备都有其唯一的标识信息（如序列号），并能从PKG中获取相应的私钥。为了相互验证，只需要交换身份标识信息，不需要额外的公钥数据。身份标识的长度比公钥及其证书的长度短得多，在验证与身份相关的签名时，要确定身份信息的有效性，如果签名验证成功，则身份信息的合法性也能得到保证。特别是，IBC技术可以在不进行任何交互的情况下建立会话密钥，双方只知道对方的身份而不进行通信，因此可以派生任何其他方不知道的秘密信息，并使用与该秘密信息计算用于安全通信相同的加密密钥。在设备到BS的通信中，BS只存储节点的身份ID，而不是数据量相对较大的公钥。因此，基于身份标识的方案更适合这些边缘计算场景，它不需要设备和设备间通信的公钥和证书。

3.3 RSA和ECC密码技术

Gura N等人[64]证明了在没有硬件加速的小型设备上实现RSA和ECC的可行性，他们分别实现了针对secp160r1、secp192r1和secp224r1上的160位、192位和224位NIST/SECG曲线的椭圆曲线标量乘法以及RSA-1024和RSA-2048在8位单片机平台上的汇编代码。Chu D等人[68]实现了ECC和两个不同家族的椭圆曲线方案。Gouvea C P L等人[69]在ECDSA中测试了这些单片机上的ZSS短签名方案[70]的签名验证时间，并在ZSS的配对实现中，选取了158位(BN-158)和254位(BN-254)的素数域上的两条BN（Barreto-Naehrig）曲线[71]进行了实现。有学者提出一种在具有有效计算自同态的椭圆曲线上加速标量乘法的方法[72]，改进了椭圆曲线方案，并给出了具体的改进实例GLV-GLS。

3.4 基于配对的密码技术

基于配对的公钥密码 (pairing-based cryptography, PBC) 技术方案更适用于边缘设备到基站的通信, 因为PBC的签名长度小于无配对公钥密码的长度 (如ZSS的签名长度是ECDSA的一半) 。但是PBC方案不太适合边缘设备到边缘设备的通信, 因为设备的公钥证书是交换的, 设备端的计算量非常大, 所以设备端的通信开销和签名验证开销会变大。比较有影响的方案是基于Weil配对的基于身份的加密 (identity-based encryption, IBE) 方案[73], 该方案促进了短签名方案[74]、三方密钥协议[75]、非交互式基于身份的密钥协议[76]、高效广播加密方案[77]、关键字可搜索加密方案[78]的完善。在实现方面, 计算配对的标准算法是Miller算法[79]。第一个配对是定义在超奇异曲线上的Weil配对和Tate配对。TinyTate需要大约31 s计算使用TinyECC的RSA-512的安全级别的Tate配对[80]。在NanoECC中[81], MSP430平台可以分别在5.25 s和11.82 s完成二进制域和素数域下80位安全级别 (RSA-1024) 的配对计算。研究表明 (参考文献[7]) , 根据参数的选择和系统硬件平台的不同, 椭圆曲线组上的标量乘法比配对计算的时间快2~7倍。为了实现配对, 大多数研究使用MIRACL (multiprecision integer and rational arithmetic C/C++ library) 库[82], 该库提供了在椭圆曲线上执行操作所需的所有工具。

3.5 格密码技术

格密码是一种抗量子计算攻击的公钥密码技术 (也称后量子密码) , 具有简单的可加性和可并行化的结构, 容易构建同态密码方案。Hoffstein J等人[83]提出了一种公钥密码的方案NTRUEncrypt (number theory research unit) , 该方案的实现基于一种特别设计的卷积模格类, 称为NTRU格。Goldreich O等人[84]提出了一种基于网格约简问题计算难度的公钥密码方案——ACVP (approximate closest vector problem) 。Hoffstein J等人[85]提出了一种基于求解特殊NTRU格中ACVP的公钥密码签名方案——NTRUSign。这些方案用卷积多项式环进行构建, 由于其加密和签名操作简单, 仅仅是多项式乘法, NTRUEncrypt和NTRUSign比其他非对称密码方案的加密速度和签名速度更快。用于NTRUEncrypt的密钥由一个良好的基组成一个2n维NTRU格的n维子格, 但是为了有效地求解任意消息摘要点的ACVP, 必须知道这个格的一个完整的好基。使用Tumbler得到NTRU加密、解密和创建密钥的计算结果, NTRU的最大优势是密钥创建时间快[86]。

参考文献[87]在NTRUSign-251上进行了一次成功的、与IEEE的NTRU标准[88]相关的、不受干扰的密钥恢复实验, 在实验中由于存在对称性, 400个签名足以公开NTRUSign-251密钥NTRU格。文中实验结果表明, 使用NTRUSign-251的8 000个签名, 可以在几个小时内恢复密钥。参考文献[89]中提出的80位安全参数集只需5 000个签名就可以恢复。NTRUEncrypt有解密失败的问题: 使用NTRU标准参数, 有效生成的密文可能无法解密。Howgrave-Graham N等人[90]的研究表明, 解密失败是不可忽视的, 因为解密失败发生的频率远远高于人们的预期。如果严格遵循NTRU标准的建议, 当参数N=139时, 每212条的消息就会发生一次解密失败; 当参数N=251时, 每225条消息就会发生一次解密失败。在任何情况下, 即使在NTRU产品中, 解密失败发生的频率也足够高, 以至于不能忽略它们。Howgrave-Graham N等人[91]考虑了填充方案的安全性证明中解密失败的可能的影响因素, 认为这些失败与消息和密钥密切相关。参考文献[92]给出了一种用于NTRUEncrypt的CCA2安全填充方案,

但该证明没有考虑解密失败，说明在使用当前的NTRUEncrypt参数集实例化时存在缺陷。这些问题在参考文献[93]中有进一步的探讨。Buchmann J等人[94]将标准草案中提出的SVES-3称为NTRUSVES，它们为IEEE P1363.1-D9提出的所有参数集提供了时间测量和密钥大小分析。

3.6 多变量公钥密码技术

多变量公钥密码系统（multivariate public key cryptosystem，MPKC）的安全性取决于求解有限域上随机产生的多元非线性方程组（一般为多元二次，称MQ问题，相应的系统为MQPKC）的困难程度，已证明有限域上的MQ问题在系数随机选取时是NP难的问题，目前还没有有效求解该问题的量子算法，因此，MQPKC也是抗量子计算攻击的候选密码技术之一。多变量公钥密码系统的公钥由两个仿射变换和一个中心映射组成，私钥为随机生成的仿射变换。MQPKC的优点是计算在较小的有限域上实现，计算效率高，缺点是密钥长度大。

Czypek P等人[95]在32 MHz的8位单片机上实现了MQ签名方案，其中包括UOV、Rainbow和enTTS等签名算法。Yang B Y等人[96]将enTTS(20,28)在MSP430上以8 MHz运行，平均签名时间为71 ms、平均验证时间为726 ms，以开源操作系统TinyOS提供的1/32 768 s的粒度进行测量，平均运行超过1 000次。与Tmote Sky上的二元Koblitz曲线相比[97]，enTTS(20,28)的签名速度比ECDSA快1.8倍左右，而ECDSA的验证速度比enTTS(20,28)快2.84倍左右。然而，若要在实际的边缘计算应用程序中使用MQPKC方案，PKI或基于身份标识的基础方案也要被应用。与简化的ECC-160证书相比，MQ模式中用于验证公钥的PKI中所需的公钥证书的大小（长度）非常大。在无线通信中，一般来说，数据传输的能耗是非常昂贵的。在这一点上，其高性能可以抵消这些沉重的传输。另外，为了减少与公钥证书相关的开销，可以考虑基于身份标识的MQ模式。已有人研究基于身份的签名方案IBS（identity-based signature）的一般构造[98]，它可以将两个公钥签名方案PKS（public key signature）方案转换为一个IBS方案，方法是通过发送公钥和PKG主秘密签名的公钥上的签名以及消息上的签名实现一个基于身份的MQ签名。基于身份标识的MQ签名的大小是一个公钥的长度加上两个MQ签名的长度，且不减少公钥和私钥的长度。因此，构造一个高效的基于身份标识的MQ签名方案很有必要，但目前尚未见到这样的方案。若要在边缘计算环境中采用多变量公钥密码安全技术，系统参数的大小和存储在其中的公钥和签名的大小必须足够小，同时，公钥加密和签名生成/验证的时间和能量消耗也必须最小化。MQPKC由于密钥长度和通信开销较大，应用于边缘计算仍需进行深入的研究和优化。

4 结束语

本文总结了边缘计算7层参考模型中边缘计算设备层、通信层和边缘计算层的安全攻击技术，综述了边缘计算中的密码安全技术（包括基于身份标识的密码技术、RSA和ECC密码技术、基于配对的密码技术、格密码技术、多变量公钥密码技术）在边缘计算中的应用现状，分析指出了对称密码技术不适合于边缘设备与边缘设备或边缘设备与基站之间的通信，基于身份标识的密码技术较适合于边缘设备到边缘设备的通信，基于配对的密码技术较适合于边缘设备到基站的通信，并讨论了

格密码和多变量公钥密码这两种后量子密码技术在边缘设备中的应用。边缘计算的安全涉及边缘设备层的设备安全、通信层的协议安全、边缘计算层的计算安全、数据聚集层的防篡改安全、数据抽取层的存储安全、应用层的认证安全、用户和云计算中心层的身份管理安全，由于应用场景众多，接入设备繁杂，数据结构不同，安全需求各异，有很多边缘计算的安全问题需要深入探索，建议进一步的研究工作可以围绕以下几个方面展开。

● 边缘设备的安全，包括边缘设备的信任评估机制、恶意边缘设备的检测方法和边缘设备的可信证书更新管理机制。

● 边缘计算的隐私安全，包括边缘计算中对象的位置隐私、边缘设备生成的敏感数据的数据隐私、边缘设备及数据的使用隐私。

● 无证书公钥密码技术（如PBC）的优化，要将PBC加密算法嵌入内存和处理速度有限的边缘设备中，极富挑战性。

● 后量子密码技术（如MQPKC）的优化，考虑融合IBC和MQPKC方案，使加密/签名的效率和密钥的长度能适应资源受限的边缘设备。

参考文献:

[1] JIAO L, FRIEDMAN R, FU X M. Cloud-based computation offloading for mobile devices: state of the art, challenges and opportunities[C]//2013 Future Network & Mobile Summit, July 3-5, 2013, Lisbon, Portugal. Piscataway: IEEE Press, 2013: 1-11.

[2] STOJMENOVIC I. Fog computing: a cloud to the ground support for smart things and machine-to-machine networks[C]//2014 Australasian Telecommunication Networks and Applications Conference, November 26-28, 2014, Southbank, Australia. Piscataway: IEEE Press, 2014: 117-122.

[3] YANGUI S, RAVINDRAN P, BIBANI O, et al. A platform as-a-service for hybrid cloud/fog environments[C]// 2016 IEEE International Symposium on Local and Metropolitan Area Networks, June 13-15, 2016, Rome, Italy. Piscataway: IEEE Press, 2016: 1-7.

[4] ZHU X, CHAN D S, PRABHU M S. Improving video performance with edge servers in the fog computing architecture[J]. Intel Technology Journal, 2015, 19(1): 202-224.

[5] SUN X, ANSARI N. EdgeIoT: mobile edge computing for the Internet of things[J]. IEEE Communications Magazine, 2016, 54(12): 22-29.

[6] ALRAWAIS A, ALHOTHAILY A, HU C Q, et al. Fog computing for the Internet of things: security and privacy issues[J]. IEEE Internet Computing, 2017, 21(2): 34-42.

[7] KANG J W, YU R, HUANG X M, et al. Privacy-preserved pseudonym scheme for fog computing supported internet of vehicles[J]. IEEE Transactions on Intelligent Transportations Systems, 2018, 19(8): 2627-2637.

[8] MOURADIAN C, NABOULSI D, YANGUI S, et al. A comprehensive survey on fog computing: state-of-the-art and research challenges[J]. IEEE Communications Surveys & Tutorials, 2018, 20(1): 416-464.

[9] 施巍松, 张星洲, 王一帆, 等. 边缘计算: 现状与展望[J]. 计算机研究与发展, 2019, 56(1): 1-21.
SHI W S, ZHANG X Z, WANG Y F, et al. Edge computing: state-of-the-art and future directions[J]. Journal of Computer Research and Development, 2019, 56(1): 1-21.

[10] Cisco Systems Inc. The Internet of things reference model[C]//2014 Internet of Things World Forum, October 14-16, 2014, Chicago, USA. [S.l.:s.n.], 2014: 1-12.

[11] 张佳乐, 赵彦超, 陈兵, 等. 边缘计算数据安全与隐私保护研究综述[J]. 通信学报, 2018, 39(3): 1-21.
ZHANG J L, ZHAO Y C, CHEN B, et al. Survey on data security and privacy-preserving for the research of edge computing[J]. Journal

on Communications, 2018, 39(3): 1-21.

[12] LI C, RAGHUNATHAN A, JHA N K. Hijacking an insulin pump: security attacks and defenses for a diabetes therapy system[C]//2011 IEEE 13th International Conference on e-Health Networking, Applications and Services, June 13-15, 2011, Columbia, USA. Piscataway: IEEE Press, 2011: 150-156.

[13] HALPERIN D, HEYDTBENJAMIN T S, RANSFORD B. Pacemakers and implantable cardiac defibrillators: software radio attacks and zero-power defenses[C]// 2008 IEEE Symposium on Security and Privacy, May 18-22, 2008, Oakland, USA. Piscataway: IEEE Press, 2008: 129-142.

[14] BHUNIA S, HSIAO M S, BANGA M, et al. Hardware Trojan attacks: threat analysis and countermeasures[J]. Proceedings of the IEEE, 2014, 102(8): 1229-1247.

[15] SALMANI H, TEHRANIPOOR M M. Vulnerability analysis of a circuit layout to hardware Trojan insertion[J]. IEEE Transactions on Information Forensics and Security, 2016, 11(6): 1214-1225.

[16] WEHBE T, MOONEY V J, KEEZER D C, et al. A novel approach to detect hardware Trojan attacks on primary data inputs[C]//The WESS'15: Workshop on Embedded Systems Security, October 4-9, 2015, Amsterdam, Netherlands. New York: ACM Press, 2015: 1-10.

[17] BHASIN S, REGAZZONI F. A survey on hardware Trojan detection techniques[C]//2015 IEEE International Symposium on Circuits and Systems, May 24-27, 2015, Lisbon, Portugal. Piscataway: IEEE Press, 2015: 2021-2024.

[18] SHILA D M, VENUGOPAL V. Design, implementation and security analysis of hardware Trojan threats in FPGA[C]// 2014 IEEE International Conference on Communications, June 10-14, 2014, Sydney, Australia. Piscataway: IEEE Press, 2014: 719-724.

[19] TEHRANIPOOR M, KOUSHANFAR F. A survey of hardware Trojan taxonomy and detection[J]. IEEE Design & Test of Computers, 2010, 27(1): 10-25.

[20] VUAGNOUX M, PASINI S. Compromising electromagnetic emanations of wired and wireless keyboards[C]//The 18th Conference on USENIX Security Symposium, August 10-14, 2009, Montreal, Canada. Berkeley: USENIX Association, 2009: 1-16.

[21] NIA A M, SUR-KOLAY S, RAGHUNATHAN A, et al. Physiological information leakage: a new frontier in health information security[J]. IEEE Transactions on Emerging Topics in Computing, 2016, 4(3): 321-334.

[22] BRANDT A, BURON J. Home automation routing requirements in low power and lossy networks[R]. [S.l.]: Internet Engineering Task Force, 2010: 1-17.

[23] MARTIN T, HSIAO M, HA D, et al. Denial-of-service attacks on battery-powered mobile computers[C]//The 2nd IEEE Annual Conference on Pervasive Computing and Communications, March 17, 2004, Orlando, USA. Piscataway: IEEE Press, 2004: 309-318.

[24] VASSERMAN E Y, HOPPER N. Vampire attacks: draining life from wireless ad-hoc sensor networks[J]. IEEE Transactions on Mobile Computing, 2013, 12(2): 318-332.

[25] STAJANO F. The resurrecting duckling[M]. Heidelberg: Springer, 2000: 183-194.

[26] MATROSOV A, RODIONOV E, HARLEY D, et al. Stuxnet under the microscope[R]. Bratislava: ESET LLC, 2011.

[27] WANG X, CHELLAPPAN S, GU W, et al. Search-based physical attacks in sensor networks[C]//IEEE 24th International Conference on Computer Communications and Networks, August 3-6, 2015, Las Vegas, USA. Piscataway: IEEE Press, 2005: 489-496.

[28] ZORZI M, GLUHAK A, LANGE S, et al. From today's Intranet of things to a future Internet of things: a wireless-and mobility-related view[J]. IEEE Wireless Communications, 2010, 17(6): 44-51.

[29] HERNANDEZ G, ARIAS O, BUENTELLO D, et al. Smart nest thermostat: a smart spy in your home[R]. Orlando: University of Central

Florida, 2014.

[30] PARNO B, PERRIG A, GLIGOR V. Distributed detection of node replication attacks in sensor networks[C]// 2005 IEEE Symposium on Security and Privacy, May 8-11, 2005, Oakland, USA. Piscataway: IEEE Press, 2005: 49－63.

[31] WALTERS J P, LIANG Z, SHI W, et al. Wireless sensor network security: a survey[J]. Security in Distributed, Grid, and Pervasive Computing, 2007, 1(367).

[32] CHAN H, PERRIG A, SONG D. Random key predistribution schemes for sensor networks[C]//2003 Symposium on Security and Privacy, May 11-14, 2003, Berkeley, USA. Piscataway: IEEE Press, 2003: 197－213.

[33] PADMAVATHI G, SHANMUGAPRIYA D. A survey of attacks, security mechanisms and challenges in wireless sensor networks[J]. International Journal of Computer Science and Information Security, 2009, 4(1): 1－9.

[34] WEIS S A, SARMA S E, RIVEST R L, et al. Security and privacy aspects of low-cost radio frequency identification systems[C]//The 1st International Conference Security in Pervasive Computing, March 12-14, 2003, Boppard, Germany. Heidelberg: Springer, 2004: 201－212.

[35] LEHTONEN M, OSTOJIC D, ILIC A, et al. Securing RFID systems by detecting tag cloning[C]// The 7th International Conference on Pervasive Computing, May 11-14, 2009, Nara, Japan. Heidelberg: Springer, 2009: 291-308.

[36] WEINGART S H. Physical security devices for computer subsystems: a survey of attacks and defenses[C]// The 2nd International Workshop on Cryptographic Hardware and Embedded Systems, August 17-18, 2000, Worcester, USA. London: Springer-Verlag, 2000: 302－317.

[37] JUELS A, BRAINARD J. Soft blocking: flexible blocker tags on the cheap[C]//The 2004 ACM Workshop on Privacy in the Electronic Society, October 28, 2004, Washington DC, USA. New York: ACM Press, 2004: 1-7.

[38] DUC D N, KIM K. Defending RFID authentication protocols against DoS attacks[J]. Computer Communications, 2011, 34(3): 384－390.

[39] KARYGIANNIS T, EYDT B, BARBER G, et al. Guidelines for securing radio frequency identification systems[R]. Gaithersburg: National Institute of Standards & Technology Special Publication, 2007.

[40] JUELS A. RFID security and privacy: a research survey[J]. IEEE Journal on Selected Areas in Communications, 2006, 24(2): 381－394.

[41] HANCKE G. Eavesdropping attacks on high-frequency RFID tokens[C]//The 4th Workshop on RFID Security, July 11, 2008, Budapest, Hungary. [S.l.:s.n.], 2008: 100－113.

[42] YANG J, PARK J, LEE H, et al. Mutual authentication protocol for low-cost RFID[C]// Workshop on RFID and Lightweight Crypto, July 14, 2005, Durham, USA. Durham: WRLC, 2005: 17-24.

[43] MUKHERJEE A. Physical-layer security in the Internet of things: sensing and communication confidentiality under resource constraints[J]. Proceedings of the IEEE, 2015, 103(10): 1747-1761.

[44] FAN J, XU G, ELKE D, et al. State-of-the-art of secure ECC implementations: a survey on known side-channel attacks and countermeasures[C]//2010 IEEE International Symposium on Hardware-Oriented Security and Trust, June 13-14, 2010, Anaheim, USA. Piscataway: IEEE Press, 2010: 76-87.

[45] NOUBIR G, LIN G. Low-power DoS attacks in data wireless LANs and countermeasures[J]. ACM SIGMOBILE Mobile Computing and Communications Review, 2003, 7(3): 29－30.

[46] SARHAN Q. Security attacks and countermeasures for wireless sensor networks: survey[J]. International Journal of Current Engineering and Technology, 2013, 3(2): 628－635.

[47] WILHELM M, MARTINOVIC I, SCHMITT J B, et al. Short paper: reactive jamming in wireless networks: How realistic is the threat [C]//The 4th ACM Conference on Wireless Network Security, June 14-17, 2011, Hamburg, Germany. New York: ACM Press, 2011: 47－52.

[48] MPITZIOPOULOS A, GAVALAS D, KONSTANTOPOULOS C, et al. A survey on jamming attacks and countermeasures in WSNs[J]. IEEE Communications Surveys and Tutorials, 2009, 11(4): 42-56.

[49] REVATHI B, GEETHA D. A survey of cooperative black and gray hole attack in MANET[J]. Journal of Computer Science and Management Research, 2012, 1(2): 205-208.

[50] GARCIA-MORCHON O, KUMAR S, STRUIK R, et al. Security considerations in the IP-based Internet of things[R]. [S.l.]: IETF, 2013.

[51] WALLGREN L, RAZA S, VOIGT T. Routing attacks and countermeasures in the RPL-based Internet of things[J]. International Journal of Distributed Sensor Networks, 2013: 1-11.

[52] DOUCEUR J R. The Sybil attack[C]//The 1st International Workshop on Peer-to-Peer Systems, March 7-8, 2002, Cambridge, USA. London: Springer-Verlag, 2002: 251-260.

[53] STOJMENOVIC I, WEN S. The fog computing paradigm: scenarios and security issues[C]//2014 Federated Conference on Computer Science and Information Systems, September 7-10, 2014, Warsaw, Poland. Piscataway: IEEE Press, 2014: 1-8.

[54] STOJMENOVIC I, WEN S, HUANG X, et al. An overview of fog computing and its security issues[J]. Concurrency and Computation: Practice and Experience, 2016, 28(10): 2991-3005.

[55] BOYD S W, KEROMYTIS A D. SQLrand: preventing SQL injection attacks[C]//The 2nd International Conference on Applied Cryptography and Network Security, June 8-11, 2004, Huangshan, China. Heidelberg: Springer, 2004: 292-302.

[56] BARRENO M, NELSON B, SEARS R, et al. Can machine learning be secure [C]//The 2006 ACM Symposium on Information, Computer and Communications Security, March 21-24, 2006, Taipei, China. New York: ACM Press, 2006: 16-25.

[57] BIGGIO B, NELSON B, LASKOV P. Poisoning attacks against support vector machines[C]// The 29th International Conference on Machine Learning, June 26-July 1, 2012, Edinburgh, Scotland. Athens: OmniPress, 2012: 1807-1814.

[58] BAZM M, SAUTEREAU T, LACOSTE M, et al. Cache-based side-channel attacks detection through intel cache monitoring technology and hardware performance counters[C]//2018 3rd International Conference on Fog and Mobile Edge Computing (FMEC), April 23-26, 2018, Barcelona, Spain. Piscataway: IEEE Press, 2018: 7-12.

[59] HONG K, LILLETHUN D, RAMACHANDRAN U, et al. Mobile fog: a programming model for large-scale applications on the Internet of things[C]//The 2nd ACM SIGCOMM Workshop on Mobile Cloud Computing, August 16, 2013, Hong Kong, China. New York: ACM Press, 2013: 15-20.

[60] AGRAWAL M, MISHRA P. A comparative survey on symmetric key encryption techniques[J]. International Journal on Computer Science and Engineering, 2012, 4(5): 877.

[61] CHEN X F, WANG Y M. A survey of public key cryptography[J]. Journal of China Institute of Communications, 2004, 25(8): 109-118.

[62] BAKHTIARI S, SAFAVI-NAINI R, PIEPRZYK J. Cryptographic hash functions: a survey[R]. Wollongong: University of Wollongong, 1995.

[63] GROBAUER B, WALLOSCHEK T, STOCKER E. Understanding cloud computing vulnerabilities[J]. IEEE Security and Privacy, 2011, 9(2): 50-57.

[64] GURA N, PATEL A, WANDER A, et al. Comparing elliptic curve cryptography and RSA on 8-bit CPUs[C]// International Workshop on Cryptographic Hardware and Embedded Systems, August 11-13, 2004, Boston, USA. Heidelberg: Springer, 2004: 119-132.

[65] CZYPEK P, HEYSE S, THOMAE E. Efficient implementations of MQPKS on constrained devices[C]//The 14th International Conference on Cryptographic Hardware and Embedded Systems, September 9-12, 2012, Leuven, Belgium. Heidelberg: Springer, 2012: 374-389.

[66] SHAMIR A. Identity-based cryptosystems and signature schemes[C]//CRYPTO 84 on Advances in Cryptology, August 19-22, 1984, Santa Barbara, USA. New York: Springer-Verlag New York, Inc., 1984: 47－53.

[67] MALAN D J, WELSH M, SMITH M D. A public-key infrastructure for key distribution in TinyOS based on elliptic curve cryptography[C]//The 1st Annual IEEE Communications Society Conference on Sensor and Ad Hoc Communications and Networks, October 4-7, 2004, Santa Clara, USA. Piscataway: IEEE Press, 2004: 71-80.

[68] CHU D, GROßSCHÄDL J, LIU Z. Twisted Edwards-form elliptic curve cryptography for 8-bit AVR-based sensor nodes[C]//The 1st ACM Workshop on Asia Ppublic-Key Cryptography, May 8, 2013, Hangzhou, China. New York: ACM Press, 2013: 39-44.

[69] GOUVÊA C P L, LÓPEZ J. Efficient software implementation of public-key cryptography on sensor networks using the MSP430X microcontroller[J]. Journal of Cryptographic Engineering, 2012, 2(1): 19－29.

[70] ZHANG F, SAFAVI-NAINI R, SUSILO W. An efficient signature scheme from bilinear pairings and its applications[C]//The 7th International Workshop on Theory and Practice in Public Key Cryptography, March 1-4, 2004, Singapore. Heidelberg: Springer, 2004: 277－290.

[71] BARRETO P S L M, NAEHRIG M. Pairing-friendly elliptic curves of prime order[C]//The 12th International Workshop on Selected Areas in Cryptography, August 11-12, 2005, Kingston, Canada. Heidelberg: Springer, 2006: 319－331.

[72] BROWN D. Sec 2: Recommended elliptic curve domain parameters[J]. Standards for Efficient Cryptography, 2010.

[73] BONEH D, FRANKLIN M. Identity-based encryption from the weil pairing[J]. SIAM Journal on Computing, 2003, 32(3): 586－615.

[74] BONEH D, LYNN B, SHACHAM H. Short signatures from the weil pairing[C]//The 7th International Conference on the Theory and Application of Cryptology and Information Security: Advances in Cryptology, December 9-13, 2001, Gold Coast, Australia. Heidelberg: Springer, 2004: 297－319.

[75] JOUX A. A one round protocol for tripartite Diffie-Hellman[C]//The 4th International Symposium on Algorithmic Number Theory, July 2-7, 2000, Leiden, Netherlands. London: Springer-Verlag, 2000: 385－394.

[76] SAKAI R, OHGISHI K, KASAHARA M. Cryptosystems based on pairings[C]//The Symposium on Cryptography and Information Security, January 25, 2000, Okinawa, Japan. [S.l.:s.n.], 2000: 26－28.

[77] BONEH D, GENTRY C, WATERS B. Collusion resistant broadcast encryption with short ciphertexts and private keys[C]//The 25th Annual International Conference on Advances in Cryptology, August 14-18, 2005, Santa Barbara, USA. Heidelberg: Springer, 2005: 258－275.

[78] BONEH D, CRESCENZO G D, OSTROVSKY R, et al. Public key encryption with keyword search[C]// International Conference on the Theory and Applications of Cryptographic Techniques, May 2-6, 2004, Interlaken, Switzerland. Heidelberg: Springer, 2004: 506－522.

[79] MILLER V S. The weil pairing, and its efficient calculation[J]. Journal of Cryptology, 2004, 17(4): 235－261.

[80] OLIVEIRA L B, ARANHA D F, MORAIS E, et al. TinyTate: computing the tate pairing in resource constrained nodes[C]//The 6th IEEE International Symposium on Network Computing and Applications, July 12-14, 2007, Cambridge, USA. Piscataway: IEEE Press, 2007: 318－323.

[81] SZCZECHOWIAK P, OLIVEIRA L B, SCOTT M, et al. NanoECC: testing the limits of elliptic curve cryptography in sensor networks[C]//The 5th European Conference on Wireless Sensor Networks, January 30-February 1, 2008, Bologna, Italy. Heidelberg: Springer, 2008: 305－320.

[82] Shamus Software Ltd. Multiprecision integer

and rational arithmetic C/C++ library[R]. 2008.

[83] HOFFSTEIN J, PIPHER J, SILVERMAN J H. NTRU: a ring-based public key cryptosystem[C]// International Algorithmic Number Theory Symposium, June 21-25, 1998, Portland, USA. Heidelberg: Springer, 1998: 267-288.

[84] GOLDREICH O, GOLDWASSER S, HALEVI S. Public-key cryptography from lattice reduction problems[C]// CRYPTO 1997, August 17-21, 1997, Santa Barbara, USA. Heidelberg: Springer, 1997: 112-131.

[85] HOFFSTEIN J, GRAHAM N A H, PIPHER J, et al. NTRUSIGN: digital signatures using the NTRU lattice[C]//2003 RSA Conference on the Cryptographers' Track, April 13-17, 2003, San Francisco, USA. Heidelberg: Springer, 2003: 122-140.

[86] HOFFSTEIN J, LIEMAN D, PIPHER J, et al. NTRU: a ringbased public key cryptosystem[C]//International Algorithmic Number Theory Symposium, June 21-25, 1998, Portland, USA. Heidelberg: Springer, 1998: 267-288.

[87] NGUYEN P Q, REGEV O. Learning a parallelepiped: cryptanalysis of GGH and NTRU signatures[J]. Journal of Cryptology, 2009, 22(2): 139-160.

[88] Consortium for Efficient Embedded Security. Efficient embedded security standards, EESS#1: Implementations Aspects of ETRUEncrypt and NTRUSign[S]. [S.l.]: Consortium for Efficient Embedded Security, 2003.

[89] HOFFSTEIN J, HOWGRAVE-GRAHAM N, PIPHER J, et al. Practical lattice-based cryptography: NTRUEncrypt and NTRUSign[M]//The LLL Algorithm. Heidelberg: Springer, 2010: 349-390.

[90] HOWGRAVE-GRAHAM N, SILVERMAN J H, SINGER A, et al. NAEP: provable security in the presence of decryption failures[R]. [S.l.]: IACR, 2003.

[91] HOWGRAVE-GRAHAM N, SILVERMAN J H, WHYTE W. Choosing parameter sets for NTRUEncrypt with NAEP and SVES-3[C]// The 2005 International Conference on Topics in Cryptology, February 14-18, 2005, San Francisco, USA. Heidelberg: Springer, 2005: 118-135.

[92] NGUYEN P, POINTCHEVAL D. Analysis and improvements of NTRU encryption paddings[C]//Annual International Cryptology Conference, August 18-22, Santa Barbara, USA. Heidelberg: Springer, 2002: 210-225.

[93] MESKANEN T, RENVALL A. A wrap error attack against NTRUEncrypt[J]. Discrete Applied Mathematics, 2006, 154(6): 382-391.

[94] BUCHMANN J, DÖRING M, LINDNER R. Efficiency Improvement for NTRU[R]. Darmstadt: Technische Universität Darmstadt, 2007.

[95] CZYPEK P, HEYSE S, THOMAE E. Efficient implementations of MQPKS on constrained devices[C]//The 14th International Conference on Cryptographic Hardware and Embedded Systems, September 9-12, 2012, Leuven, Belgium. Heidelberg: Springer, 2012: 374-389.

[96] YANG B Y, CHEN J M, CHEN Y H. TTS: High-speed signatures on a low-cost smart card[C]// International Workshop on Cryptographic Hardware and Embedded Systems, August 11-13, 2004, Cambridge, USA. Heidelberg: Springer, 2004: 371-385.

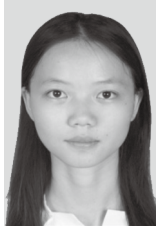
[97] OLIVEIRA L B, KANSAL A, PRIYANTHA B, et al. Secure-TWS: authenticating node to multi-user communication in shared sensor networks[J]. Computer Journal, 2012, 55(4): 384-396.

[98] BELLARE M, NAMPREMPRE C, NEVEN G. Security proofs for identity based identification and signature schemes[C]// International Conference on the Theory and Applications of Cryptographic Techniques, May 2-6, 2004, Interlaken, Switzerland. Heidelberg: Springer, 2004: 268-286.

作者简介

凌捷 (1964-) , 男, 博士, 广东工业大学计算机学院二级教授, 主要研究方向为网络信息安全、智能视频处理技术等。

陈家辉 (1986-) , 男, 博士, 广东工业大学计算机学院讲师, 主要研究方向为后量子密码学、区块链技术及云安全。



罗玉 (1991-) , 女, 博士, 广东工业大学计算机学院讲师, 主要研究方向为人工智能、计算机视觉等。

张思亮 (1996-) , 男, 广东工业大学计算机学院硕士生, 主要研究方向为网络与信息安全技术。

收稿日期: 2019-01-18

基金项目: 国家自然科学基金资助项目 (No.61702112) ; 广州市科技计划基金资助项目 (No.201802010043, No.201807010058)

Foundation Items: The National Natural Science Foundation of China (No. 61702112), Science and Technology Project of Guangzhou (No.201802010043, No.201807010058)