前　言

网络已经完全渗透于人类社会的各个方面,形成了现代化生活必须依赖的虚拟空间——网络空间.网络空间安全治理体系早已引起各国的高度重视,目前正进入治理体系变革的关键时期.网络空间安全治理对于维护国家主权与安全、保障国家繁荣与稳定有着重要意义.网络与系统安全是网络空间安全治理的前提,密码学作为保障网络空间安全的核心与支撑技术,在网络空间安全治理中扮演关键角色.探索适应新时期网络空间安全治理需求的网络安全与密码学新理论、新技术是我们面临的重要课题.

为推动我国学者在密码学与网络空间安全治理领域的研究,及时报道我国学者在密码学与网络空间安全治理方面的最新研究成果,我们策划组织了“密码学与网络空间安全治理”专题.本专题通过公开征文共收到124篇普通投稿、4篇特邀投稿,论文分别在多个方面阐述了密码学与网络空间安全治理研究领域具有重要意义的研究成果.本专题的审稿严格按照该刊审稿要求进行,特约编委先后邀请了近百位相关领域的专家参与评审,每篇论文邀请至少3～4位专家进行评审,历经初审、复审、终审等阶段,整个流程历经一个半月,最终共录用文章25篇(含4篇特邀稿件).这25篇文章分别涵盖密码算法、网络空间安全治理与隐私保护等研究内容,在一定程度上反映了当前国内各单位在网络空间安全研究领域的主要研究方向.受刊物单期容量所限,本专题将分批刊登在2021年第10期(15篇)和第11期(10篇).

1　综　　述

本部分共收录了6篇综述.

计算机网络的快速发展与大数据的普及推动了云计算技术的进一步发展.云环境是网络与信息时代下数据交互的重要平台,为个人、企业和国家的数据高效交互提供了极大的便利,但同时也为云数据安全和隐私保护提出了新的挑战.特邀稿件“云数据安全保护方法综述”一文给出了现有云计算模型,并调研和分析了云数据安全保护中存在的威胁.在此基础上,从云数据安全的访问控制、密钥协商、安全审计和安全共享4个方面出发,对国内外云数据安全保护方案的最新研究成果进行系统分析.针对云数据安全保护方案存在访问控制过程中用户隐私易被泄露、密钥生成过程中开销难以控制、审计过程中动态操作效率低下等问题进行系统研究,并提出解决思路.为推动更加完善的云数据保护体系的建立,该文还探讨了云数据安全保护当前面临的全新挑战,指出了未来的研究方向.

区块链作为一种分布式账本,集成了分布式共识、P2P 网络、智能合约及密码学等技术,解决了“去中心化”的信任问题.区块链凭借其不可篡改、去中心化等特性,对社会各个领域产生了深远影响,掀起了区块链技术的研究应用热潮.但是,区块链技术在应用过程中面临着数据隐私泄露的问题,极大地限制了区块链的应用范围和领域,区块链数据隐私保护方案已成为研究者关注的重点问题之一.为了揭示这些安全隐患,特邀稿件“区块链数据隐私保护:研究现状与展望”基于数据隐私保护的基本概念,详细分析了区块链各技术要点面临的隐私泄露问题,探索并总结了当前区块链数据隐私保护的解决方案.该文还结合目前区块链数据隐私保护研究的最新进展,对未来区块链数据隐私保护的研究方向进行了展望.

随着信息化的不断发展,人民的生活愈加数字化、智能化,越来越多的生产生活逐渐转移到网络空间进行.自新冠疫情暴发以来,国民经济对网络空间的依赖日益凸显.互联网带来便利的同时,越来越多的犯罪从传统线下转移到网络空间中进行,威胁人民群众的生产生活.近年来研究人员持续关注各种网络犯罪及对应的防范、评估、反制技术,但目前针对网络犯罪总体综述研究较少.特邀稿件“网络犯罪的检测分析技术”一文以钓鱼、诈骗、恶意挖矿等经典网络犯罪攻击方式为切入点,深入分析包括黑帽搜索引擎优化、误植域名在内的相关支撑技术,详细揭露服务于网络犯罪的地下市场、僵尸网络和洗钱渠道等基础设施,对网络犯罪产业链进行剖析,最后讨论网络犯罪研究中仍存在的挑战,并展望未来研究方向.

软件的高复杂性和安全漏洞的形态多样化给软件安全漏洞研究带来了严峻的挑战.传统的漏洞挖掘方法效率低下且存在高误报和高漏报等问题,已经无法满足日益增长的软件安全性需求.目前,大量的研究工作尝试将深度学习应用于漏洞挖掘领域,以实现自动化和智能化漏洞挖掘.特邀稿件“基于深度学习的软件安全漏洞挖掘”一文对深度学习应用于安全漏洞挖掘领域进行了深入的调研和分析,通过梳理和分析基于深度学习的软件安全漏洞挖掘现有研究工作,概括其一般工作框架和技术方法,并以深度特征表示为切入点,分类阐述和归纳不同代码表征形式的安全漏洞挖掘模型.随后探讨了基于深度学习的软件安全漏洞挖掘模型在具体领域的应用,并依据对现有研究工作的整理和总结,指出该领域面临的不足与挑战,对未来的研究趋势进行了展望.

随着人工智能、大数据等技术的发展,数据采集、数据分析等应用日渐普及,隐私泄露问题越来越严重.数据保护技术的缺乏限制了企业之间数据的无法互通,导致形成“数据孤岛”.安全多方计算(MPC)技术能够在不泄露明文的情况下实现多方参与的数据协同计算,实现安全的数据流通,达到数据“可用不可见”.隐私保护机器学习是当前 MPC 技术最典型也是最受关注的应用与研究领域,MPC 技术的应用可以保证在不泄露用户数据隐私

和服务商模型参数隐私的情况下进行训练和推理.综述文章“安全多方计算及其在机器学习中的应用”一文针对 MPC 及其在隐私保护机器学习领域的应用进行全面的分析与总结.该文介绍了 MPC 的安全模型和安全目标;梳理 MPC 基础技术的发展脉络,包括混淆电路、不经意传输、秘密分享和同态加密;并对 MPC 基础技术的优缺点进行分析,提出不同技术方案的适用场景.该文还进一步对基于 MPC 技术实现的在隐私保护机器学习方案进行了介绍与分析,对未来 MPC 技术的发展和应用进行了展望.

编码计算将编码理论融于分布式计算中,利用灵活多样的编码方式降低数据洗牌造成的高通信负载,缓解掉队节点导致的计算延迟,有效提升分布式计算系统的整体性能,并通过纠错机制和数据掩藏等技术为分布式计算系统提供安全保障.鉴于其在通信、存储和计算复杂度等方面的优势,受到学术界的广泛关注,成为分布式计算领域的热门方向.综述文章“编码计算研究综述”一文介绍了编码计算的研究背景,明确编码计算的内涵与定义;随后对现有编码计算方案进行评述,从核心挑战入手,分别对面向通信瓶颈、计算延迟和安全隐私的编码计算方案展开介绍、总结和对比分析;最后指出未来可能的研究方向和技术挑战.

2 密码学

本部分共收录了 9 篇论文,主要围绕对称密码算法、密钥协商、数字签名和密文搜索等研究方向展开.

高级加密标准 AES 是一种高安全性的密钥加密系统,在实际生活中受到了多方面认可及使用,自它诞生以来对于它的安全性问题的研究一直是密码学者最感兴趣的.“基于交换等价的缩减轮 AES-128 的密钥恢复攻击”一文使用了一种新的适合于类 SPN 分组密码设计的密码分析攻击技术,基于 AES 的 5 轮自适应选择密文区分器,在恢复密钥时利用了 AES 加密算法列混合变换系数矩阵的基本性质和零差分性质,提出了一种带有秘密 S 盒的 6 轮缩减轮 AES-128 的密钥恢复攻击,通过实验结果说明了当前的对 6 轮缩减轮 AES-128 密钥恢复攻击结果比已有的对缩减轮 AES-128 的密钥恢复攻击结果更优.

密文一致性检测公钥加密方案是一种检测者能够在无需解密密文的情况下检测一对密文的一致性,即该对密文解密所得明文是否一致的公钥加密方案.已有工作中提及的细粒度授权方案和灵活授权方案在授权粒度方面对密文一致性检测公钥加密方案的功能性进行了改进,但这 2 种方案拥有各自的应用场景且在功能性方面互不包含.“标准模型下的灵活细粒度授权密文一致性检测方案”一文提出了灵活细粒度授权密文一致性检测公钥加密方案,该方案兼具细粒度授权特性与灵活细粒度特性,允许 2 名用户各自对一指定密文或所有密文进行授权操作.同时,对比依赖预言机模型的细粒度授权方案、灵活授权已有方案,该方案的安全性证明基于标准模型之上.

量子计算技术快速发展带来的新挑战使得后量子密码成为当前密码学界研究热点.基于格的密码方案因其安全高效的特性,已经成为后量子公钥密码的主流之一.Aigis 密钥封装算法(Aigis-enc)是我国学者自主设计的基于模格上非对称错误学习(A-MLWE)问题的后量子密码算法,是中国密码学会举办的全国密码算法设计竞赛公钥密码算法一等奖获奖算法之一."Aigis 密钥封装算法多平台高效实现与优化"一文重点关注 Aigis-enc 算法在不同平台的实现优化,包含高性能平台的快速并行实现与嵌入式低功耗平台的紧凑实现,使用裁剪层数的数论变换并优化指令流水调度,加速多项式乘法运算,减少了预计算表存储需求,并提供了多项式序列化与反序列化的并行汇编指令实现,加快了编码解码与加解密过程.

自从属性基签名(ABS)的概念被提出后,ABS 因其匿名性特征而受到广泛关注.ABS 可以隐藏签名者的真实身份从而保护用户隐私,但其匿名性可能导致签名者滥用签名而无法进行追踪.同时在特定的应用场景,如在电子医疗或电子商务中需要保护一些敏感信息(如医疗技术、转账细节等)防止客户隐私信息泄露.为了解决数据传输中的敏感信息隐藏以及签名者滥用签名问题,"标准模型下证明安全的可追踪属性基净化签名方案"一文提出了一种可追踪身份的属性基可净化签名方案,该方案不仅解决了敏感信息隐藏,保证了签名者的隐私,而且防止了签名者对签名的滥用.

近年来,全球移动通信数量成爆发性增长,越来越多的用户对通信服务质量提出更高的要求,而物联网、人工智能、大数据等领域的不断创新也对通信技术的带宽、速率、延迟等方面提出了新的目标,第 5 代移动通信技术(5G)应运而生.针对目前 5G 车联网中车辆之间通信的认证与密钥协商方案算法复杂、时延高的问题,"基于 PUF 的 5G 车联网 V2V 匿名认证与密钥协商协议"一文提出了一种基于物理不可克隆函数的 5G 车联网 V2V 匿名认证与密钥协商协议,该协议通过引入轻量级 PUF 避免了 V2V 认证中的数字签名操作,并精简通信步骤,成功减轻车辆的计算和通信开销,还借助 PUF 实现了车辆的车载单元和 5G SIM 卡的绑定,解决了身份假冒问题.

适配器签名方案是标准数字签名的一种扩展形式,它可以创建一个隐含困难关系(例如离散对数)状态的"预签名",并通过困难关系证据将该预签名转换为一个完整签名,且转换后的完整签名可以通过一个标准签名方案的验证算法验证其有效性.适配器签名方案能够在区块链中提供很好的原子交换性质,并已在实践中被证明应用非常广泛."基于 SM2 数字签名算法的适配器签名方案"一文以 SM2 数字签名算法为基础,构造了一个新的适配器签名方案 SM2-AS.该方案能够有效地衔接 SM2 签名方案的密钥生成、签名生成和签名验证算法,通过理论分析和实验测试,SM2-AS 方案的性能与 ECDSA 适配器签名方案相当,但明显弱于 Schnorr 适配器签名方案.

动态对称可搜索加密在近年来已经成为数据隐私保护方面至关重要的原语,它能够允许客户端对保存于云服务器的加密数据执行高效的检索和更新操作,而仅向服务器泄露少量经过严格定义的信息,如搜索模式,访问模式、更新模式和容量泄露.然而,一些强大的敌手能够利用动态对称可搜索加密的泄露执行特定攻击,从而破坏数据和检索的隐私性.为了实现更好的安全和效率平衡,“基于差分隐私的多模式隐藏动态对称可搜索加密方案”一文提出了一种新的填充方法——差分隐私填充(DPP),在保证安全性的同时降低了存储负载.随后在多服务器模式下提出了一种称为“ MDSSE”的动态搜索更新方案,通过对 DPP 的动态运用实现容量、更新以及搜索模式隐藏,保证了前向安全和后向安全.

在后量子数字签名方案中,基于哈希函数的签名方案是高效和可证明安全的. 然而,过长的密钥和签名是基于哈希函数的签名方案最主要的问题.“SOTS:一个基于哈希函数更短的后量子数字签名方案”一文在已有签名方案的基础上,提出了一个新的一次签名方案,该方案不仅减少了签名的数量,同时减少了每个签名的长度.该方案和近 2 年的方案相比,在密钥和签名长度上都有显著减少,密钥生成、签名生成和签名验证所需时间也有所缩短.

可修正区块链的实现所依赖的关键密码学工具是变色龙哈希函数.“一次变色龙哈希函数及其在可修正区块链中的应用”一文提出了称为一次变色龙哈希函数的新密码学原语:同一哈希值的 2 个原像(一次碰撞)不会暴露任何陷门信息,而同一哈希值的 3 个原像(二次碰撞)则会暴露部分陷门信息,但足以导致严重的安全危害.该文基于 RSA 困难问题构造了简单高效的一次变色龙哈希函数方案,并在随机预言模型下证明了其安全性.该文所提出的可修正区块链方案具有高效和修正权限契合实际需求的两大特点,有望为区块链监管提供有力的技术参考.

3 网络空间安全治理

本部分共收录了 10 篇论文,主要围绕攻击检测、身份识别、联邦学习数据安全与隐私保护等研究方向展开.

社交网络是一个有效的信息传播平台,使得人们的生活更加便捷.同时,在线社交网络也不断提高了社交网络账号的价值.然而,为了获取非法利益,犯罪团伙会利用社交网络平台隐秘地开展各种诈骗、赌博等犯罪活动.为了保护用户的社交安全,各种基于用户行为、关系传播的恶意账号检测方案被提出.“微信恶意账号检测研究”一文提出了一种基于账号注册属性的恶意账号检测方案.该方案首先通过分析恶意账号和正常账号在不同属性值上的分布,设计并提取了账号的相似性特征和异常特征,然后基于此计算两两账号的相似度构图以聚类挖掘恶意注册团体,从而有效实现注册阶段的恶意账号检测.

面向工控网的攻击策略多种多样,其最终目的是导致系统进入临界状态或危险状态,因此,基于设备状态异常的攻击检测方式相较于其他检测方法更为可靠.然而,状态异常检测中存在攻击结束时刻难以准确界定的问题,“工业控制网络多模式攻击检测及异常状态评估方法”一文构建了攻击策略及系统异常状态描述模型,并提出基于状态转移概率图的异常检测方案.针对语义攻击对系统状态影响的定量评估难题,该文提出了基于异常特征和损害程度指标融合分析的攻击影响定量评估方法,实现系统所处不同阶段时状态的定量评估与分析.

目前针对说话人识别的攻击需要对音频注入长时间的扰动,因此容易被机器或者管理人员发现.“基于单‘音频像素’扰动的说话人识别隐蔽攻击”一文提出了一种新颖的基于单“音频像素”扰动的针对说话人识别的隐蔽攻击,该攻击利用了差分进化算法不依赖于模型的黑盒特性和不依赖于梯度信息的搜索模式,克服了已有攻击中扰动时长无法被约束的问题,实现了使用单“音频像素”扰动的有效攻击.该文还提出了分别基于去噪器、重建算法和语音压缩的防御思路.

联邦学习使用户在数据不出本地的情形下参与协作式的模型训练,降低了用户数据隐私泄露风险,广泛地应用于智慧金融、智慧医疗等领域.但联邦学习对后门攻击表现出固有的脆弱性,攻击者通过上传模型参数植入后门,一旦全局模型识别带有触发器的输入时,会按照攻击者指定的标签进行误分类.“基于生成式对抗网络的联邦学习后门攻击方案”一文提出了一种新型后门攻击方案 Bac_GAN,通过结合生成式对抗网络技术将触发器以水印的形式植入干净样本,降低了触发器特征与干净样本特征之间的差异,提升了触发器的隐蔽性,并通过缩放后门模型,避免了参数聚合过程中后门贡献被抵消的问题,使得后门模型在短时间内达到收敛,从而显著提升了后门攻击成功率.

无线网络利用开放性的无线信道传输数据,因此容易遭受设备假冒攻击和通信数据伪造攻击,而防范此类攻击需要精准的设备识别.基于信道状态信息(CSI)指纹的设备识别技术利用无线信道特征来识别设备.由于 CSI 提供细粒度的信道特征,并且可以从 OFDM 无线设备中轻松获取,因此该技术受到广泛的关注.“基于混合特征指纹的无线设备身份识别方法”一文提出了一种基于混合特征指纹的设备身份识别方法,包含终端接入时和通信时的设备识别.在接入时,引入了与终端外界因素无关的数据包时间间隔分布(PAID)指纹进行识别,以弥补 CSI 指纹的缺陷.该文还提出了一种计算复杂度较低的指纹匹配方案,以保证在计算能力有限的设备中也能快速且准确地识别终端.

在有限的时空资源条件下,研究人员使用网络隐蔽通道,基于少量的水印信息来追踪攻击流,定位真实攻击源.然而,水印内容和位置的相对固定会造成追踪的流量呈现出自相似性,并且 IPv6 协议内嵌的 IPsec 加密协议限制了载体的选择范围,基于单一载体的水印

嵌入方案更容易被识别攻击.“一种面向IPv6网络空间的特征水印生成与嵌入方案研究”一文针对水印隐蔽性的优化目标,结合IPv6报文中间节点不分片的特性,考虑间断性传输网络和流速较慢网络的特征提取限制,设计目标流关联的特征水印序列提取策略,针对不同的网络传输场景,制定了包依赖的基于混合隐蔽通道和时间依赖的基于混合时隙的水印嵌入方式.

联邦学习由于可以更好地保护数据隐私,一提出即受到重视.然而当模型进行训练时,其聚合算法FedAvg容易受到拜占庭客户端的联合攻击.针对此问题,很多研究提出了不同的防御策略,但这些聚合算法存在防守能力不足、模型假设不贴合实际等问题.“基于矩阵映射的拜占庭鲁棒联邦学习算法”一文提出了一种新型的拜占庭鲁棒聚合算法——基于矩阵映射的模型异常程度检测算法,从而依据异常程度剔除每轮更新中拜占庭客户端生成的毒模型,该方案能有效防御联邦学习中的防御阻碍收敛攻击和后门攻击.

近些年基于位置服务的软件变得越来越受欢迎.但是由于轨迹数据具有规模大、纬度高、连续性等特点,因此在发布轨迹数据时存在隐私泄露的风险.针对这一问题,在现有的差分隐私机制的数据保护技术基础上,“一种满足差分隐私的轨迹数据安全存储和发布方法”一文提出一种基于噪声前缀树结构的轨迹数据发布方法.采用等差隐私预算分配方式对前缀树节点中数据添加拉普拉斯噪声,并由每层的阈值限制添加噪声量的大小,最终发布满足差分隐私模型的较高可用性的轨迹数据.通过真实数据集实验对比已有的方案,验证了该文所提出的算法在保证数据隐私性的同时,也提高了数据可用性.

端信息扩展技术使用多项端信息组成的扩展序列来表示身份信息,各项端信息与所传递的数据本身无关,从而隐藏用户的真实信息.然而,端信息扩展序列资源利用率低、自相关性弱,无法实现多用户并发安全通信.“基于SCMA的端信息扩展多用户安全通信系统研究”一文将稀疏码多址接入(SCMA)技术引入端信息扩展序列生成过程中,提出基于SCMA的端信息扩展多用户安全通信系统模型,详细阐述了模型中的码本设计分配、码字加载发送策略.采用稀疏编码后,系统具有较低误比特率,且在一定过载条件下,仍具有良好的传输性能.

针对Android恶意软件检测存在特征引入过程主观性高、特征选择过程可解释性差、训练模型检测效果不具备时间稳定性的问题,“InterDroid:面向概念漂移的可解释性Android恶意软件检测方法”一文提出了一种面向概念漂移的可解释性Android恶意软件检测方法InterDroid.该方法首先通过高质量的人工Android恶意软件分析报告引入权限、API包名、意图名、Dalvik字节码4种特征,并通过自动化机器学习算法TPOT获得InterDroid训练及对比算法,从而摒弃传统方法中繁复的模型选择与参数调整过程.随后,融入模型解释算法SHAP改进传统的特征包装方法,从而获得对分类结果具有高贡献度

的特征组合用于检测模型训练.最后,通过曼-惠特尼 U 与机器学习模型的双重检验证明概念漂移现象在 Android 恶意软件检测中的存在性.

承蒙各位作者、审稿专家和编辑部等方面的全力支持,本专题得以顺利出版.目前密码学与网络空间安全治理研究涉及领域十分广泛,这给审稿人及特邀编辑的审稿、选稿工作带来了巨大挑战.由于投稿数量大、主题广泛、时间安排紧张、专题容量有限等原因,本专题仅选择了部分有代表性的研究工作予以发表,无法全面体现该领域所有的最新研究工作.部分优秀稿件无法列入专题发表,敬请谅解.

我们要特别感谢《计算机研究与发展》编委会和编辑部,从专题的立项到征稿启事的发布,从审稿专家的邀请到评审意见的汇总,以及最后的定稿、修改和出版工作,都凝聚了他们辛勤的汗水.本专题的出版期望能给广大相关领域研究人员带来启发和帮助.在审稿过程中难免出现不尽人意之处,希望各位作者和读者包容谅解,同时也请各位同行不吝批评指正.最后,再次衷心感谢各位作者、审稿专家、编辑部和特邀编委的辛勤工作.

曹珍富 华东师范大学
徐秋亮 山东大学
张玉清 中国科学院大学
董晓蕾 华东师范大学

2021 年 9 月