软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2018,29(7):1827−1829 [doi: 10.13328/j.cnki.jos.005366]

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel: +86-10-62562563

面向隐私保护的新型技术与密码算法专题前言*

薛 锐[1], 彭长根[2], 黄欣沂[3], 刘吉强[4], 禹 勇[5]

[1](信息安全国家重点实验室(中国科学院 信息工程研究所),北京 100093)

[2](贵州大学 计算机科学与技术学院,贵州 贵阳 550025)

[3](福建师范大学 数学与计算机科学学院,福建 福州 350108)

[4](北京交通大学 计算机与信息技术学院,北京 100044)

[5](陕西师范大学 计算机科学学院,陕西 西安 710119)

通讯作者: 薛锐, E-mail: xuerui@iie.ac.cn

中文引用格式: 薛锐,彭长根,黄欣沂,刘吉强,禹勇.面向隐私保护的新型技术与密码算法专题前言.软件学报,2017,28(7):1827−1829. http://www.jos.org.cn/1000-9825/5366.htm

随着云计算、大数据、物联网、移动互联网等新兴技术的快速发展和社交网络、在线购物、位置服务、医疗服务、移动服务和云存储等应用的广泛普及,隐私安全问题有愈演愈烈之势.近年来,学术界和产业界一直在探索保护隐私的方法,匿名算法、模糊算法、同态密码算法、安全多方计算、差分隐私算法、访问控制等隐私保护方法相继被提出并在现实生活中得到广泛应用.然而,现有的隐私保护技术难以应对大数据环境下多源数据融合的关联分析,隐私保护面临新的严峻挑战,隐私泄露风险已成为大数据开放、共享等应用的主要瓶颈.目前,隐私保护的研究主要集中于两方面:一是继续研究更有效的隐私保护算法;二是探索风险可控的隐私保护机制.本专题的目的就是针对以上两个研究方向,一方面探讨更有效的隐私保护算法,另一方面研究隐私风险评估机制和模型.

本专题主要围绕“面向隐私保护的新型技术与密码算法”这一主题,与 2017 年第 2 届中国隐私保护学术会议(ChinaPrivacy 2017)合作展开征稿,共征得投稿 43 篇.这 43 篇论文通过特约编辑形式审查,有 41 篇论文进入到评审阶段.上述稿件研究内容涉及隐私保护算法和风险评估的方方面面,特约编辑先后邀请了 110 位隐私保护相关领域的专家参与审稿工作,每篇投稿邀请 2~3 位专家进行评审.稿件评审历经 4 个月,经初审、复审、ChinaPrivacy 2017 会议宣读和终审 4 个阶段,最终有 12 篇论文入选本专题.

《同态加密技术及其在云计算隐私保护中的应用》介绍了近年来同态加密技术和云计算隐私保护技术的研究进展,重点介绍同态加密技术在云计算隐私保护中的应用情况,并且指出了未来同态加密技术在云计算隐私保护领域的可能应用场景.

《基于用户分布感知的移动 P2P 快速位置匿名算法》观察到移动点对点(P2P)结构下位置隐私保护匿名区的形成存在着通信开销大、匿名效率低以及成功率低等问题.因此提出了一种移动 P2P 结构下用户分布感知方案.该算法通信开销小,在满足网络移动设备节能需求的同时,匿名区平均生成时间较短且成功率较高.

《面向工业物联网环境下后门隐私泄露感知方法》关注后门隐私信息的泄露对工业控制系统及物联网环境的安全性及稳定性所造成的严重威胁和挑战.因此,基于工业物联网环境下后门隐私的数据特征定义了若干基本属性,根据静态及动态数据流安全威胁抽取上层语义,并基于多属性决策方法聚合生成静态与动态泄露度,最终结合灰色关联分析计算安全级与安全阈值,实现了后门隐私信息在静态二进制结构及动态数据流向中的泄露场景感知.

《格上基于身份哈希证明系统的新型构造》关注具有后量子安全隐私保护特性的密码学方案和协议的设计.因此,首先在标准模型下构造了一个格上的光滑哈希证明系统;再在随机谕言机模型下,得到一个光滑且密

收稿时间: 2017-10-10

文尺寸较小的基于身份哈希证明系统.作为对新型光滑哈希证明系统的扩展,在标准模型下提出第一个格上可更新的哈希证明系统.

《基于字符串排序的高效保密数据库查询》关注利用字符串排序的方法实现对保密数据库的快速查询.因此,首先设计了一种新的编码方法和一种基于 ElGamal 加密算法的云外包计算下的同态加密方案,在此基础上提出了一个简单、高效的保密字符串排序协议.进一步利用该协议提高了保密数据库查询的效率,并且从根本上解决了大数据情况下的百万富翁问题.

《基于离线密钥分发的加密数据重复删除方法》观察到对冗余数据的安全删除在云存储等工业界的迫切性和重要性,因此,通过利用双线性对和广播加密技术,提出一种基于离线密钥分发的加密数据重复删除方案.从而在没有第三方参与的情况下,实现云服务器对加密数据的重复删除.

《基于恶意读写器发现的 RFID 空口入侵检测技术》利用无源感知技术对 RFID 信号的信道状态信息进行分析与计算,提取并建立可以描述无线信道状态信息的参数.利用提取的参数建立基于有限状态机的 RFID 信号感知数据推断模型,结合自适应算法得出稳态作为依据,分析判断 RFID 信号的具体变化,实现基于恶意读写器的 RFID 空口入侵检测.

《对三个多服务器环境下匿名认证协议的分析》关注多服务器环境下匿名身份认证协议的安全性.基于广泛接受的攻击者模型,对多服务器环境下的 3 个代表性匿名认证协议进行了安全性分析.指出相关协议不安全的深层原因,并提出保证协议安全的相应修正方法.

《公平理性委托计算协议》注意到在传统委托计算的过程中引入理性参与者的重要性.首先在委托计算中引入博弈论,给出了唯一稳定均衡解.其次,基于比特币和 Micali-Rabin 的随机向量表示技术,设计一种新的理性委托计算协议.该协议不但高效地解决了传统委托计算的验证复杂问题,同时保证了诚实者的利益.

《面向云数据的隐私度量研究进展》介绍了面向云数据的隐私度量技术的发展概况.首先提出云数据隐私保护技术的性能评价指标和一种综合评估框架;然后,提出一种云数据隐私度量抽象模型,从工作原理和具体实施的角度对基于匿名、信息熵、集对分析理论和差分隐私这 4 类隐私度量方法进行详细阐述,并且详细分析这 4 类方法的特点;最后,指出了云数据隐私度量技术的发展趋势及有待解决的问题.

《本地化差分隐私研究综述》概述了近年来本地化差分隐私保护技术的研究进展.重点总结和归纳了该技术的研究热点.并且在对已有技术深入对比分析的基础上,指出了本地化差分隐私保护技术的未来研究挑战.

《高效且可验证的多授权机构属性基加密方案》观察到已有多授权机构属性基加密云存储数据的访问控制方案不适合直接应用于电力资源有限的移动设备.因此提出了一种高效的可验证的多授权机构属性基加密方案,该方案不仅可以降低加密解密的计算开销,同时可以验证外包解密的正确性,并且保护用户的隐私.

本专题主要面向大数据安全与隐私保护、网络空间安全及相关领域的研究人员和专业工程师等,反映了我国学者在隐私保护技术方面的最新研究进展.在此,我们要特别感谢《软件学报》编委会和隐私保护专委会对专题工作的指导和帮助,感谢隐私保护专委会的各位老师从征稿启示发布、审稿专家邀请至评审意见汇总、论文定稿、修改及出版所付出的辛勤工作和汗水,感谢专题评审专家及时、耐心、细致的评审工作.此外,我们还要感谢向本专题踊跃投稿的作者对《软件学报》的信任.

最后,感谢专题的评审专家、编辑和读者们,希望本专题能够对大数据安全与隐私保护相关领域的研究工作有所促进.

薛锐(1963－),男,山西翼城人,博士,中国科学院信息工程研究所研究员、博士生导师、信息安全国家重点实验室副主任.中国密码学会安全协议专委会副主任、中国密码学会密码应用委员会副主任委员、中国保密协会隐私保护专业委员会秘书长.“智能交通数据安全与隐私保护技术”北京市重点实验室学术委员会委员.《计算机研究与发展》和《软件学报》编委.主要研究领域为密码学,安全协议,隐私保护,等.

彭长根(1963－),男,贵州锦屏人,博士,教授,博士生导师.现任中国密码学会理事、中国保密协会隐私保护专业委员会委员、贵州省计算机学会秘书长,CCF 专业会员,担任《通信学报》副主编,《网络与信息安全学报》、《信息网络安全》等学术期刊编委.主要研究领域为密码学,隐私保护.

黄欣沂(1981－),男,江苏仪征人,博士,教授,博士生导师.现任中国密码学会理事,担任 IEEE TDSC、IJIS (Springer)等学术期刊编委,CCF 专业会员.主要研究领域为安全认证技术.

刘吉强(1973－),男,山东海阳人,博士,教授,博士生导师,全国信息安全标准化技术委员会委员,中国保密协会隐私保护专业委员会委员,中国密码学会安全协议专业委员会委员、教育与科普工作委员会委员,教育部新世纪优秀人才(2011),首届网络安全优秀教师(2016).主要研究领域为隐私保护,可信计算.

禹勇(1980－),男,山东泰安人,博士,教授,博士生导师.现任中国保密协会隐私保护专业委员会委员、中国密码学会安全协议专业委员会委员,CCF 专业会员,担任 Soft Computing 等学术期刊编委.主要研究领域为公钥密码及其应用.