专题：数据流通与隐私计算

Data Circulation and Privacy Computing

客座编辑

杜跃进（1972- ），男，博士，360集团首席安全官、大数据协同安全技术国家工程研究中心常务副主任。曾任阿里巴巴集团技术副总裁、高级研究员、首席安全专家，网络安全应急技术国家工程实验室主任，亚太地区计算机应急响应组织（APCERT）副主席，国家互联网应急中心副总工程师等。从事网络安全领域的研究和工作20余年，获得国家科学技术进步奖一等奖2项，以及新世纪百千万人才工程国家级人才、全国青年岗位能手、亚太区信息安全领袖成就奖、中国计算机学会杰出会员和杰出演讲者等荣誉。

罗圣美（1971- ），男，博士，中孚信息股份有限公司规划研究院副院长，江苏省产业教授，哈尔滨工业大学和南京邮电大学兼职教授，中国计算机学会杰出会员。获得国家科学技术进步奖二等奖1项，省部级科学技术进步奖一等奖4项，参与制定6项行业标准，授权30多项发明专利，在国内外核心期刊发表40多篇学术论文。多年从事通信网络、云计算、大数据、人工智能等技术研究和产品规划工作，围绕信息化、数字化、智能化产业升级，提供创新、灵活、稳定和有竞争力的解决方案。

导读

数字经济时代，数据要素的获取与开发利用已成为全球竞争的新战场。2022年1月，国务院发布《“十四五”数字经济发展规划》，提出充分发挥数据要素作用，强化高质量数据要素供给，加快数据要素市场化流通，创新数据要素开发利用机制。如何在安全合规的前提下有效利用数据，推动数据的流通共享与开发利用，实现数据价值的最大化，成为数字经济发展的当务之急。国家发展和改革委员会、中共中央网络安全和信息化委员会办公室等联合印发的《全国一体化大数据中心协同创新体系算力枢纽实施方案》提出试验隐私计算等技术模式，明确了以隐私计算为代表的数据流通技术作为当前突破数据流通瓶颈的技术路径。

“数据可用不可见”的隐私计算技术为数据流通与共享提供了新方式，为打破“数据孤岛”、实现机构间的业务协同与数据共享提供了可行性。但当前，隐私计算技术仍存在理论研究突破难、计算效率低等问题，特别是在实际场景中的落地应用已经成为数据资源共享迫切需要解决的关键问题。隐私计算如何兼顾安全与效率？如何突破算法与性能瓶颈？如何实现技术理论向产品的转化？这些都是需要进一步研究与探讨的核心问题。

为了促进隐私计算的理论研究和应用探索，本刊组织了“数据流通与隐私计算”专题。经过专家评审，最终录用6篇文章，文章主题涵盖隐私计算技术、数据流通、数据共享、隐私保护、数据治理等多个方面，本专题按照技术研究和实践探索两个部分来组织。

第一部分探讨数据流通与隐私计算领域的关键技术研究。阮雯强等人从隐私保护和数据利用的角度，提出了数据租赁技术，为数据流通提供了新思路、新方式。吴建汉等人系统性地梳理了联邦学习可能受到的攻击及相应的防御措施，全面详实地总结了各种类别的攻击方法。李懿等人结合区块链及零知识证明技术，提出了一种隐私数据安全共享模型，并验证了模型的可行性。尹虹舒等人针对纵向联邦学习在线推理过程中的用户隐私泄露问题，提出一种针对成员推断攻击的隐私保护方法，进一步提高了纵向联邦学习在线推理过程中用户隐私的安全性。

第二部分从具体应用与实际场景的角度对隐私计算进行了实践探索。张燕等人提出的数据质量治理框架对于金融风控、联合医疗等领域具有参考意义。李明等人介绍了YITA-TFL平台在车路协同场景下的落地应用，为其在交通行业的应用提供了参考。

隐私计算这一新兴技术正逐渐被大众接受与熟知，但关于隐私计算的实践探索仍需进一步加强，需结合具体应用场景考虑技术落地的可行性。希望本专题能够引起读者的兴趣，推动隐私计算相关领域技术研究与产业实践的发展。