前　言

物联网技术的广泛应用对促进社会经济绿色、智能、可持续发展起着至关重要的作用，成为了国家数字化关键基础设施中不可或缺的组成部分. 然而，物联网终端数量庞大、异构性强、拓扑多变、应用环境复杂等特性，导致其面临的安全威胁日益严峻. 同时，物联网中海量异构数据的共享需要得到隐私和完整性的保护，而其与人工智能的深度融合也带来了全新的安全风险. 加强物联网安全对维护国家主权和社会稳定，以及保护个人和企业切身利益具有至关重要的作用，这使得物联网安全成为网络空间安全不可或缺的组成部分. 为应对物联网中日益加剧的安全挑战，探索物联网安全的前沿技术成为学术界和工业界广泛关注而具有极大挑战性的研究课题.

为进一步推动我国学者在物联网安全领域的研究，及时报道我国学者在物联网安全方面的最新研究成果，我们组织策划了“物联网安全前沿与进展”专题. 本专题通过公开征文共收到 36 篇投稿，这些论文分别从多个方面阐述了物联网安全关键支撑技术研究领域具有重要意义的研究成果. 本专题严格按照《计算机研究与发展》期刊的审稿要求进行，特邀编委先后邀请了多位相关领域的专家参与评审，每篇论文邀请至少 2 位专家进行评审，历经初审、复审、终审等阶段，整个审稿流程历经一个半月，最终共录用文章 8 篇. 这 8 篇文章涵盖物联网中的安全数据共享、物联网中人工智能安全与隐私、物联网设备安全保护以及物联网应用安全等研究内容，在一定程度上反映了当前国内各单位在物联网安全领域的主要研究方向.

1. 物联网中的安全数据共享

针对物联网数据共享中存在的效率低下和隐私泄露问题，张学旺等作者的“策略隐藏的高效多授权机构 CP-ABE 物联网数据共享方案”提出了解决物联网数据安全共享问题的方案，该方案通过采用多授权机构 CP-ABE 技术实现了数据细粒度的访问控制. 在利用区块链的不可篡改特性保护了密文和密钥的安全性的同时通过 MurmurHash3 算法完全隐藏访问策略. 针对网络群聊消息在物联网设备的公开信道传输时面临窃听攻击的威胁，王后珍等作者的“基于身份的群组密钥分发方案”提出了基于身份的群组密钥分发方案，该方案基于 SM9 算法和多项式进行构造，将群组密钥嵌入到椭圆曲线点与多项式系数中后进行分发，从而实现了即时通讯群聊场景下的群组密钥分发，保障了通信安全.

2. 物联网中人工智能安全与隐私

针对人工智能技术在物联网数据处理过程中面临的抵抗推理攻击和检测投毒攻击，陈景雪等作者的“物联网环境下鲁棒的源匿名联邦学习洗牌协议”提出了一个源匿名数据洗牌方案，通过采用不经意传输协议以实现联邦学习环境中参与者模型的匿名上传，使得参数服务器能够在不知道该模型具体来自哪个参与者时获得参与者的原始本地模型，同时该方案采用秘密共享机制，在保证梯度数据原始性的同时，解决了传统洗牌协议中参与者难以退出的问题. 针对物联网设备面临来自恶意代码的威胁，刘奇旭等作者的“基于人工智能的物联网恶意代码检测综述”从物联网环境和设备的特性出发，陈述了基于人工智能的恶意代码检测工作主要动机的分类方法，从面向物联网设备限制缓解的恶意代码检测和面向性能提升的物联网恶意代码检测等方面综合分析了该领域的研究现状.

3. 物联网设备安全保护

针对嵌入式设备面临的安全威胁和嵌入式设备自身硬件资源的限制，张浩等作者在“嵌入式设备固件仿真器综述”中基于采用的仿真技术和衍生关系对嵌入式设备固件仿真器进行探索总结，在对经典固件仿真器进行评估和细化比较的基础上为用户选择固件仿真器提供了技术指导. 针对物联网设备面临安全威胁的多样性和复杂性，张妍等作者在“物联网设备安全检测综述”中对有关 IoT 设备安全威胁的法律法规、评测及认证和检测技术进行了深入分析. 该文从探讨 IoT 设备面临的安全威胁出发，逻辑层次划分攻击面的基础上分析总结了现有的安全法规和评估标准，同时该文重点关注了 IoT 安全风险检测技术，包括芯片木马、接口安全、无线协议安全、固件和应用安全.

4. 物联网应用安全

针对无人机传感器注入攻击的在线检测和恢复方法存在检测精度不高、系统状态恢复缺乏持续性、控制模型精度及检测精度受无人机硬件算力限制的问题，孙聪等作者的“基于机器学习的无人机传感器攻击在线检测和恢复方法”提出基于轻量级机器学习模型的无人机传感器攻击在线检测和恢复方法，利用机器学习模型构建各传感器对应的预测模型，从而实现对不同传感器对应的无人机系统状态进行准确预测. 针对车联网复杂的网络架构带来的安全挑战以及车辆失窃、信息泄露和驾驶故障威胁，况博裕等作者在“车联网安全研究综述：威胁、对策与未来展望”中对车联网系统安全进行了深入调研和分析，在将车联网架构划分为车内网和车外网的基础上总结了目前已有的攻击威胁及相应的安全对策，并对当前车联网安全领域的关键技术进行了梳理和总结.

物联网安全研究是一个发展迅速且活跃的领域，学科前沿的瞬息万变给特邀编辑和审稿人的审稿、选稿工作带来了巨大挑战. 由于投稿数量大、专题容量有限等原因，本专题仅选择了部分研究工作予以发表，无法全面体现该领域所有的最新研究工作，对此我们感到抱歉. 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如人意之处，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.

本专题的顺利出版离不开各位作者、审稿专家和编辑部对本专题的全力支持、无私贡献和辛勤工作，我们对此致以诚挚的感谢！

秦志光（电子科技大学）
张玉清（中国科学院大学）
熊 虎（电子科技大学）

2023 年 9 月