特约主编寄语

在万物互联时代，5G、大数据、人工智能等新技术为物联网带来了创新与活力。Gartner 公司发布的调查报告显示，2017 年全球物联网设备数量大约为 84 亿，2020 年可达 200 亿。我国“十三五”规划将物联网作为战略性新兴产业的重要组成内容，美国、欧盟、日本等国家与组织也纷纷将物联网上升到战略高度。电力物联网、能源互联网、工业物联网等是物联网应用中的新兴领域，大量智能电力终端（如 FTU、DTU、RTU、智能电表、能源路由器等）在“发电 – 变电 – 输电 – 配电 – 用电”和“源 – 网 – 储 – 荷”中起到了源端真实数据感知的关键作用，采集数据进一步有效支持系统精准调度策略。然而，物联网本身沿袭了传统互联网的安全风险，其终端规模巨大、部署环境复杂，传统安全问题会被急剧放大，如：大部分物联网终端设备的计算资源较低，使得很多适用于通用计算设备的安全防护功能无法实现，抗攻击能力较差，物联网终端时刻面临着硬件、软件以及数据等方面的安全风险。

能源互联网本质是以开放为基础的对等互联式的能量交换与分享：一方面能源互联网基于“能源互联、信息共享、业务互动”的思想，进行能量流、业务流和信息流的高度融合控制；另一方面能源互联网的新需求、新业务和新技术使得能源信息的获取方法、存储形态、传输渠道和处理方式发生了新的变化，致使能源网络结构复杂化、边界模糊化、设备类型多样化，信息安全高风险化。

能源安全离不开信息安全，但目前能源互联网的信息安全主要对网络边界进行重点防护，在系统内部的网络、设备和应用的安全系统和机制相对较少。虽然当前电力物联网、能源互联网等网络中的电力终端基本都支持网络接入和访问，但无法保障通信过程的安全，如：部分设备的加密通讯密钥可直接从注册表读出；本地管理协议没有身份认证机制；通信协议未加密或加密方式过于简单；访问系统面临多方威胁且普遍存在脆弱性，接入网络时访问数据可能会被窃取或者篡改；终端通信可能会遭到中间人攻击、DDoS 攻击等；基于电表细粒度读数的大数据分析会泄露家庭用电隐私；数据注入攻击导致电力生产和调度数据出现偏差。因此，面向电力用户的安全计算，包括电力终端安全、用户端安全、网络安全、边缘计算安全等日益成为研究者关注的研究热点。能源互联网的某一环节或者节点设备的安全故障，都可能通过多米诺骨牌效应使的整个能源互联网瘫痪，直接影响到能源电力系统安全稳定运行。因此，有必要面向电力用户安全计算领域研究开展攻防结合、里外兼顾、多维融合的能源互联网信息安全研究。

专刊征稿得到了国内外专家学者的大力支持，经过专家评审及编辑部精心优选，共收录 13 篇稿件，涵盖终端身份认证、终端协议安全、数据安全、终端流量安全检测、基于计算机视觉的电力设备安全检测、终端安全架构标准、基于大数据的设备效率分析等多个方面。期望通过汇集相关领域专家学者的最新研究成果与实践经验，为进一步推动我国面向电力用户安全计算领域的发展提供理论、方法、技术、机制等方面的支持与借鉴，并为我国从事物联网终端安全研究和应用的专家学者、物联网行业相关从业人员等提供重要参考。

衷心感谢有关专家对本专刊的大力支持，感谢《华电技术》编辑部在本专刊的策划、编辑和出版过程中的辛勤耕耘。