《计算机学报》“硬件安全”征稿

集成电路是构建安全信息系统的基石，在日常生活、军事安全等领域广泛应用，从民用智能电器到军方武器系统，小到手机、优盘，大到卫星、飞船，概莫能外。同时，集成电路还是程序与数据的载体，如果集成电路芯片存在安全隐患，其运行的软件、存储的数据及其关联的一切，便再无安全可言。IEEE Spectrum 曾报道 2007 年以色列导弹袭击叙利亚时，叙利亚的防御雷达系统并没有做出必要的预警，科学家分析其原因是由于叙利亚雷达系统使用的商业芯片在制造过程中被植入了的“木马”或者“后门”。2018 年爆发的史诗级 CPU 漏洞 Meltdown 和 Spectre 导致 Intel 市值蒸发近 110 亿美元。2020 年 4 月，德国研究人员纰漏的一个名为“StarBleed”的漏洞又把 FPGA 芯片的安全问题带入了大众视野。近年日益增多的这些硬件安全问题表明集成电路硬件已成为发起跨层和远程攻击的有效界面，亟需学术界和工业界提出有效的方案解决芯片的安全问题。

为了进一步推动硬件安全的研究，《计算机学报》拟征集“硬件安全”方面的研究型论文，并结集出版。征稿内容包括以下但不局限于以下方向：

（1）硬件安全原语：物理不可克隆函数、真随机数发生器等
（2）硬件木马与后门
（3）硬件辅助系统安全
（4）侧信道攻击与防御
（5）故障注入攻击与防御技术
（6）逆向工程与防御技术
（7）IP 保护技术
（8）可信执行环境
（9）FPGA、SOC 安全
（10）物联网安全
（11）物理层安全
（12）车载/自动驾驶安全
（13）后量子密码
（14）AI 软硬件安全
（15）嵌入式系统安全
（16）计算机微体系结构安全
（17）侵入式攻击与防御
（18）硬件增强云安全
（19）存储芯片安全

征稿对象为高等院校师生、科研院所及企业科研人员，稿件类型为研究型或综述类论文。稿件提交后将经同行评议，择优录用，正刊结集发表（预计会在 2022 年第 1 季度）。

投稿截止时间为 2021 年 08 月 30 日。

本次活动责任专家为：王兴伟、张吉良、谷大武、贾杰

注意事项：

（1）《计算机学报》唯一网址为：http://cjc.ict.ac.cn/index.htm

（2）投稿方法：请访问学报网址--〉在线投稿；投稿时，投稿领域，请选择热点话题“硬件安全”。

（3）为便于审读，要求稿件符合学报征稿指南要求，可读性强，条理清楚，无中英文语法错误。为了便于快速处理稿件，投稿论文应符合计算机学报论文模板要求（可在学报网站 http://cjc.ict.ac.cn/index.htm 下载）。