中国密码学会2024年密码芯片学术会议（CryptoIC2024）征文通知

由中国密码学会密码芯片专业委员会主办，电子科技大学和成都三零嘉微电子有限公司承办的“中国密码学会2024年密码芯片学术会议（CryptoIC 2024）”于2024年8月9日至11日在四川成都举行。会议旨在聚焦密码芯片软硬件设计、安全分析和实现及其工程应用的最新科学研究和技术开发成果，共同探讨密码芯片技术在各行业应用中存在的主要理论和现实问题、学术热点、工程实现和发展趋势，为安全芯片产、学、研协同创新提供便捷的交流平台。

本次会议拟邀请多位从事相关研究的国际知名学者作大会主旨报告，邀请学术界、产业界和测评机构的知名专家作特邀报告，邀约《密码学报》、《电子与信息学报》(EI)作为本次会议合作刊物。欢迎各位同行踊跃投稿。

一、征文内容

征稿范围包括但不限于以下议题的新思想、新方法、新技术、新问题和学科综述：

1.密码算法的集成电路实现技术。包括各种密码算法实现的电路设计、低功耗设计、安全设计、密码处理器、协处理器设计；硬件随机数生成器；物理不可克隆技术等。

2. 密码算法集成电路的攻击和防范技术。包括侧信道攻击与防范、故障攻击与防范、硬件篡改及防篡改技术、白盒密码和代码混淆、硬件及软件逆向工程技术等。

3. 芯片安全标准及测评技术、评估设备。包括评估标准分析、研究、问题和建议，密码算法集成电路的渗透性安全评测，评估方法、评估工具、集成电路探测方法和装置等。

4. 工具和方法论。计算机辅助密码工程实现、安全设计证明方法和工具、嵌入式系统安全指标、安全编程技术、FPGA 设计安全等。

5. 密码理论与抗攻击实现的综合安全技术。包括免泄露密码学、针对嵌入式系统的新型密码算法、代码侧信息泄露、密码芯片安全实现的系统架构、版图、算法、电路以及真随机数（数字物理噪声源）、伪随机数电路设计等。

6. 密码及安全芯片应用技术。物联网应用密码与安全（包括 RFID、传感器网络、智能器件和智能装置等）、硬件 IP 保护及防伪、可重构密码硬件、智能卡处理器及系统，信息物理系统安全（智能家庭网络、医疗植入、工业控制等）、安全存储设备（存储器、磁盘等）、可信计算平台、汽车安全（无人驾驶）、内容保护硬件与技术等等。

7. 芯片硬件安全。硬件木马、漏洞、后门和前门等相关硬件安全技术。

二、重要日期

征文提交截止时间：2024 年 7 月 15 日

征文采纳通知时间：2024 年 7 月 25 日

三、征文要求

大会将邀请部分被本次会议录用的学术论文作者在会议上做报告。投稿论文可以是已向重要学术刊物或国际会议投稿，或新近发表的研究成果，论文不限长度，已发表或已投稿论文格式不限，未曾投稿论文格式按《密码学报》模板编辑。对特邀报告、约稿报告和其他录用论文，大会拟编纂为内部交流资料（不出版正式论文集，无版权声明）。对通过本会评审且未曾发表的论文，经作者同意，将择优推荐到上述合作刊物。

投稿方式：以附件形式用 Email 投稿到下面的会议联系人信箱。邮件标题请注明论文标题及投稿单位，邮件正文中请注明作者基本信息（隶属单位、职称、学历学位、研究兴趣）和文章联系人联系方式、是否为已在其他刊物或会议出版或投稿的论文（并注明对应的刊物或会议）。

四、联系方式

联 系 人：刘老师

征稿邮箱：crypto_ic_2024@163.com

中国密码学会密码芯片专业委员会

2024 年 6 月 7 日