# 中国密码学会2020年密码芯片学术会议
# （Crypto IC2020）征文通知

中国密码学会2020年密码芯片学术会议（Crypto IC2020）拟定于2020年8月（视疫情控制情况决定最终日期）在哈尔滨友谊宫举行。本次会议由中国密码学会密码芯片专业委员会主办，哈尔滨理工大学和哈尔滨工业大学联合承办。

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。为来自学术界、工业界和政府机构的专家学者、行业精英、工程技术人员和在校研究生之间搭建交流平台，共同探讨密码芯片技术在各行各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、用协同创新提供便捷的交流机会。

本次会议拟邀请2-4从事相关研究的国际知名学者做大会特邀报告，约请学术界、产业界和评测机构的知名专家2-4名做专题报告，邀约《Chinese Journal of Electronics》(SCIE)、《电子学报》(EI)和《密码学报》作为本次会议合作刊物。通过本会专家审稿录用的论文，有机会被推荐到上述刊物发表。论文一经刊物录用，作者须到会交流。

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。

将择优选取本次会议录用的学术论文须在大会进行报告。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，未曾投稿论文格式尽量按上述三个期刊模板编辑。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。

为了作者论文能尽快见刊，截稿时间安排较紧，希望大家抓紧时间踊跃投稿！

投稿方式：以附件形式用 E-mail 投稿到下面的会议联系人信箱。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）。

截稿日期：2020 年 6 月 15 日

会议审稿通知：2020 年 7 月 15 日

作者回复：2020 年 7 月 25 日

论文定稿：2020 年 7 月 31 日

刊物复审通知：（依据各刊安排）

会议时间：2020 年 8 月（视疫情控制情况决定最终日期）

会议地点：哈尔滨友谊宫

联系人：王晨旭，13573742373，wangchenxu@hit.edu.cn

中国密码学会密码芯片专业委员会

2020 年 5 月 18 日