第十八届亚洲密码学年会在京召开

文章来源：信息工程研究所 发布时间：2012-12-11 【字号： 小 中 大 】

12月2日至6日，第十八届亚洲密码学年会（International Conference on Theory and Application of Cryptology and Information Security，简称Asiacrypt 2012）在北京国际会议中心召开。本次会议由国际密码学会（IACR）和中国密码学会（CACR）共同主办，中国科学院信息工程研究所信息安全国家重点实验室、上海交通大学、清华大学协办。信息安全国家重点实验室常务副主任林东岱研究员同时担任了大会程序委员会委员和组织委员会委员，并主持了安全证明小节的报告。

亚洲密码学年会是密码学专业学术年会，是国际密码学界最著名的三大学术会议(美密会、欧密会、亚密会)之一，每年一次在亚太国家轮流举办。本次会议，继1998年（北京），2006年（上海）后第三次在中国召开。

大会共分11个小节（session）进行发言报告，研究成果涵盖了当前密码学领域的前沿技术和最新发展动态，会议邀请了美国斯坦福大学的国际著名密码学家Dan Boneh教授和北京大学的国际知名数学家宗传明教授做了特邀报告。另外在Rump Session上，数名学者就最新研究进展做了简要报告、以及对明年密码和安全领域若干会议的通告，其中来自以色列Weizmann研究所的图灵奖获得者Adi Shamir教授公布了他们对于SHA-3最新的攻击结果。

此次会议受到世界各国学者的广泛关注，来自中国、美国、法国、瑞士、丹麦、澳大利亚、以色利、日本、韩国等地的知名学者300余人参加了会议。会议共收到国内外有效投稿241篇，经过由32位专家组成的程序委员会及256位外部审稿人的筛选，最终收录论文43篇，论文录用率约为17.8%。中国大陆共有3篇文章被收录，值得一提的是，信息安全国家重点实验室就占有其中2篇：刘美成博士、张寅博士和林东岱研究员在布尔函数方面的工作“Perfect Algebraic Immune Functions”；张立廷助理研究员等人在消息验证码可证明安全方面的工作“3kf9: Enhancing 3GPP-MAC beyond the Birthday Bound”。

本次会议盛况空前，为历年来参会人数最多的一届，会议促进了我国在这一领域的科学研究。会议召开期间，多名世界著名学者到信息工程研究所进行访问和交流，举办了多场学术报告，进一步加强了与国外的学术交流，同时，对于提高信息工程所在国际学术领域的知名度具有积极意义。