



第八届信息安全与密码学国际会议在京召开

2012年11月28日至30日,信息安全国家重点实验室与中国密码学会联合主办的“第八届信息安全与密码学国际会议”(INSCRYPT 2012)在北京国际会议中心召开,来自12个国家和地区的60余人参加了会议。



会议邀请两名信息安全领域的国际知名专家作了精彩特邀报告。韩国首尔大学Jung Hee Cheon教授的特邀报告以“离散对数的公开问题”为题,介绍了关于离散对数求解相关问题的最新进展,相关的研究结果发表在最新一期的密码学顶级期刊Journal of Cryptology上;日本知名学者Goichiro Hanaoka研究员的特邀报告以“具有短密文结构的ElGamal型的CCA安全的公钥加密方案”为题,总结了ElGamal型公钥加密方案的历史发展,并提出有效的构造手段使得方案具有短密文结构。会议还安排了Junfeng Fan博士和 Miroslaw Kutylowski教授做侧信道和数字认证方面的专题培训,以及 23位论文作者作专题报告,内容涉及对称密码、公钥密码、密码学基础、安全协议、密码分析、视觉密码等多个领域。

本次大会收到来自中国、澳大利亚、日本、韩国、新加坡、德国、美国、印度、英国、法国、瑞士、西班牙等24个国家的稿件共73篇,经过程序委员会委员和外聘专家审阅,录用23篇,论文集将由国际著名出版社SPRING出版。

在为期三天的会议中,与会者对信息安全和密码学的前沿和热点问题进行广泛的讨论和交流,学术氛围浓郁。本次会议由信息安全与密码学的国际间交流提供了一个重要的平台,大力推动了国内信息安全与密码学专业的发展,提高了我国在国际密码学领域的地位和影响,会议取得圆满成功。

