“量子密码与传统密码融合性研讨会”在北京召开

由中国密码学会量子密码专业委员会主办、北京邮电大学网络与交换技术国家重点实验室网络安全研究中心承办的“量子密码与传统密码融合性研讨会之二——量子密码的安全性证明”于2012年10月13日在北京邮电大学科技大厦召开，国内高等院校、科研院所的专家学者40余人参加了会议。

开幕式由中国密码学会量子密码专委会副主任委员、中国科技大学韩正甫教授主持。北京信息科学研究院蔡吉人院士、中国密码学会强志军秘书长、中国密码学会量子密码专委会副主任委员吴令安研究员等出席了会议。

近年来，量子密码的研究取得了丰硕的成果，越来越受到各国学者和相关机构的重视。量子密码的安全性基于基本物理原理，其证明方法与传统密码大不相同。如何正确认识量子密码的安全性证明思路、探讨借鉴传统密码分析技术的可行性以及如何融合量子密码和传统密码的优势，是大家广泛关注的问题。此次研讨会以“量子密码的安全性证明”为主题，特别邀请了中国科学院武汉物理与数学研究所的蔡庆宇教授做了题为“量子密码安全性的物理基础与BB84协议”的报告；清华大学的马雄峰博士做了题为“QKD安全与纠缠”的报告；中国科技大学的李宏伟博士做了题为“基于BELL不等式的量子密码安全性”的报告。三场报告从最初的物理基础开始，延伸到目前最新的理论和实验进展，介绍了一些深受关注的前沿热点问题。报告引起了参会者的极大兴趣，每场报告的结束都伴随着与会者热烈的交流和讨论。西安电子科技大学的王育民教授、王新梅教授，陕西师范大学的王国俊教授，清华大学的龙桂鲁教授，中国科学院物理研究所的吴令安研究员，武汉大学的张焕国教授，上海交通大学的来学嘉教授等积极发言，他们从不同的角度阐述和分析了量子密码的安全性和实用性，为量子密码的进一步研究提出了很多建设性的建议。现场气氛活跃，学术讨论自由而深入，整个会议为所有的参会者创造了一个良好的学术交流平台。

闭幕式上，韩正甫教授对本次研讨会进行了总结，充分肯定了会议取得的成果，认为会议加速了量子密码和传统密码研究的融合，传统密码的专家们对量子密码的安全性有了更深层的理解，双方也在量子密码的理论安全性方面达成了共识。除此之外，与会专家的思维碰撞也为今后量子密码的研究提供了一些创新性的思路。他希望与会专家学者共同努力，促进量子密码在研究中取得更多更好的科研成果。

本次研讨会作为量子密码专委会举办的“量子密码与传统密码融合性”系列讨论会的第二期会议，得到广大密码研究专家的关注和支持，会议为我国量子密码的学术研讨提供了一个良好的平台，促进了量子密码学术研讨和交流。会议取得圆满成功。