北京大学前沿计算研究中心
Center on Frontiers of Computing Studies, Peking University

静园5号院
科 研 讲 座

安全性归约与密码协议的轮复杂性

Dr. Yi Deng (邓燚)
中国科学院信息工程研究所

Host：刘天任 助理教授
2022年04月28日 星期四 15:00-16:00
北京大学静园五院102室

Abstract

安全性归约在整个公钥密码学中扮演着重要的角色。已知的普适性（universal）/黑盒安全性归约方法在许多场合下被证明具有很大局限性，无法将一些目标密码算法/协议通过黑盒归约建立在一些标准困难假设上。这一报告里我们将介绍一种依赖敌手计算结构特征的新型安全性归约技术--个体化安全归约（individual reductions），以及怎样利用这种归约技术来突破一些基础性密码协议--如承诺，零知识证明和不经意传输等--的轮复杂度黑盒下界，构造更低轮数的密码协议。

Biography

邓燚，中国科学院信息工程研究所研究员。2008年获中国科学院软件所信息安全国家重点实验室博士学位。曾先后在英国伦敦大学学院和新加坡南洋理工大学从事博士后研究工作。他的主要研究方向为密码学，特别是零知识证明和密码协议，以及它们在金融科技中的应用。曾在一些密码学和计算机科学领域旗舰会议--如 FOCS，Eurocrypt，Asiacrypt，PKC上发表多篇论文。2011年获中国密码学会首届优秀青年奖，2014年获中国密码学会首届创新奖一等奖，2019年获中国电子学会自然科学奖一等奖。