实验室年会特邀报告——Lattice Theory and Lattice-based Cryptography

报告人：王小云

时　间：2017 年 12 月 30 日

地　点：北京国际数学中心报告厅

嘉宾介绍：

王小云院士主要从事密码理论与密码数学问题研究。在密码分析领域，给出了包括 MD5，SHA-1 在内的系列国际通用 Hash 函数算法的碰撞攻击理论，提出了 MAC 算法 ALPHA-MAC、MD5-MAC 与 PELICAN 的子密钥恢复攻击以及 HMAC-MD5 的区分攻击思想。在密码设计领域，主持设计了 Hash 函数算法 SM3。有 4 篇论文获最佳论文，包括 2005 年度国际密码年会欧密会与美密会的最佳论文。MD5 破解的论文获得 2008 年汤姆森路透卓越研究奖（中国）。