嘉宾简介

王小云，清华大学高等研究院“杨振宁讲座”教授，中国科学院院士，发展中国家科学院院士，国际密码协会会士，中国密码学会理事长，中国数学会副理事长。

主要从事密码理论及相关数学问题研究。在密码分析领域，提出了密码哈希函数的碰撞攻击理论，破解了包括 MD5、SHA-1 在内的 5 个国际通用哈希函数算法；在密码设计领域，主持设计的哈希函数 SM3 为国家密码算法标准，并于 2018 年 10 月正式成为 ISO/IEC 国际标准。

代表性论文 50 余篇，3 篇获欧密会、美密会最佳论文。曾获国家科技进步一等奖，国家自然科学二等奖，陈嘉庚科学奖，求是杰出科学家奖，苏步青应用数学奖，未来科学大奖——数学与计算机科学奖等。