中国科学院数学与系统科学研究院

量子论与信息论

学术报告

报告题目： **后量子密码(格密码)的数学基础**

报 告 人： **宗传明 教授**

天津大学

时　　间： **2022 年 12 月 15 日 (星期四) 下午 14:00--15:00**

地　　点： **腾讯会议 310-882-617**

摘　　要： 1831 年，高斯提出了格(lattice)的概念。历经 Hermite, Minkowski, Siegel, Lovasz 等数学家的深入研究, 格理论已发展成为数论，代数与几何交叉领域的一个重要数学分支。2021 年，Lovasz 由于 LLL 算法荣获 Abel 奖。2022 年，Viazovska 由于 8 维空间和 24 维空间的堆球成就荣获 Fields 奖。上世纪末，格理论被意想不到地用于现代密码学，特别是由 Shor, Ajtai, Pipher 等人进行的抗量子攻击密码体系的研究。2022 年 7 月 5 日，美国国家标准与技术研究院(NIST)公布了四项后量子密码标准，其中三项基于格理论。这样，格理论成了未来量子科技时代信息安全的“保护神”。本报告将介绍格理论的历史及其在后量子密码中基础作用。