

摘要

密码学是保障网络和信息安全的核心技术与基础支撑。本报告简要介绍了现代密码学以及相关密码数学理论的发展，介绍了格密码作为一类抗量子计算攻击的密码具备的优势及其研究的重要性、格密码数学困难问题及格密码设计的研究现状，并对格密码的发展与应用进行了展望。