

摘要

密码是网络空间安全的基础，是保障数据与通信安全，构建各类安全协议、安全机制与安全系统的核心技术。随着移动互联、云计算等新型应用的发展，密码算法的运行环境发生了巨大变化，现实应用的多元化需求对密码算法提出了更多更高的要求。同时，开放融合环境下层出不穷的多元化攻击手段，以及量子计算等新型计算技术的出现，也对传统密码算法的安全性提出了严峻的挑战。本报告将从密码面临的现实需求和威胁出发，探讨密码技术在网络空间安全中的前沿应用以及未来的发展趋势。