

摘要

密码函数在密码算法的设计中起到至关重要的作用。密码函数的选取直接影响密码算法的安全性和实现效率。报告今年来在密码函数研究中主要的进展和主要的公开问题。