现代密码学基础理论研究

关 键 词：现代密码学　基础理论

所属年份：1993	成果类型：应用技术
所处阶段：	成果体现形式：
知识产权形式：	项目合作方式：
成果完成单位：北京邮电大学	

成果摘要：

该成果研究了现代密码学的两个主要分支（序列密码和分组密码）内的若干基础问题。在序列密码方面采用布尔函数方法和序列分析技术研究密钥流，通过有限域中的迹变换和序列递归与连分式展开的迫近关系研究序列的线性复杂度曲线及随机统计特性，为序列密码的安全性分析和实用系统的设计提供了理论依据。在分组密码方面将高维矩阵和编码理论中的若干方法引入分组密码的设计与分析，破译了一些密码，同时也设计出了一些新的密码体制，将正交变换方法和快速卷积方法和神经网络方法等引入分组码的研究，为研究现代密码学与人工神经网络等新兴科学之间的内在联系提供了潜在的可行性。

成果完成人：杨义先;林须端;潘新安

完整信息

推荐成果

· 空间飞行器SPACEWIRE高速数据... 04-23
· Adhoc网络中的QoS保证(Wirel... 04-23
· 基于正交多载波传输的高速无... 04-23
· 光因特网体系结构与管理技术 04-23
· 一种光因特网中不同网络结构... 04-23
· 40Gbit/s DWDM软件仿真系统 04-23
· 移动互联网服务质量控制工程... 04-23
· 数字图像处理系统研究 04-23
· IPv6核心路由器 04-23

行业资讯

QH3792S腔式双工器
数字微波传输关键设备研制
2.4G无线接入系统设备
VSAT卫星通信系统
码分多址卫星数据通信地球站
WSD-1卫星数据通信单收站
1560点对多点微波通信系统
M2000 6GHz 155Mb/s SDH微波...
2×155Mbit/s SDH微波通信系统
M1000型2×34Mb/s数字微波接...

成果交流