混沌理论及其在密码学中的应用研究

关 键 词：密码学　混沌理论　分组密码置换网络

所属年份：2003	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：哈尔滨商业大学	

成果摘要：

提出了一种新的二维混沌映射—平面方体上的帐篷映射，平面方体上帐篷映射的输出序列具有均匀的分布函数和良好的相关特性，用该映射产生的混沌序列构造二进制密钥流，具有良好的随机特性和符合密码学特性的线性复杂度和非线性复杂度；利用构造的平面方体上帐篷映射作为混沌序列产生器，在平面方体上帐篷映射的迭代过程中改变其初值和结构参数，并利用混沌二进制密钥流设计了随机非线性组合密钥产生器，它产生的序列能有效抵抗相关攻击和一次逼近攻击；利用Logistic-Map混沌序列的遍历性及其良好的相关特性，提出了一种二维置换网络，并对置换网络的时间复杂度和其置换性质做了分析，利用混沌序列的遍历性来产生分组密码置换网络，克服了以往用简单的移位、取模、线性变换等实现置换网络的缺点。

成果完成人：

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