完善保密密码体制的研究

关 键 词：密钥协商　无条件安全　完善保密

所属年份：2004	成果类型：基础理论
所处阶段：	成果体现形式：论文
知识产权形式：	项目合作方式：
成果完成单位：西安电子科技大学	

成果摘要：

研究了窃听者在信息协调阶段获得的边信息对保密增强阶段所能提取出的秘密钥长度的影响；研究了在不安全且非认证的公共信道上根据部分保密的密钥实现认证的方法；研究了随机变量的Rényi熵与该随机变量的概率分布到均匀分布的随机变量的概率分布之间的距离的关系；假定敌手的存储容量有限，研究了通信双方所能提取的秘密钥的长度；研究了基于平滑熵进行无条件安全秘密钥协商时的密钥速率；研究了防主动攻击的无条件安全的秘密钥协商；研究了基于阶大于1小于2的任意阶Rényi熵的保密增强在实现不经意传输协议时的安全性条件；提出了新的优先提取/退化协议、不经意传输协议、信息协调协议；推导出针对一般分布的通用上界；提出了新的用纠错码构造认证码的方法。

成果完成人：杨波;王卫卫;胡予濮;吴振强;刘胜利;张彤;秦兴成

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