BDLL型正形置换及其在密码学中的应用

关 键 词：正形置换　分组密码

所属年份：2000	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：中国科学院研究生院	

成果摘要：

BDLL型正形置换研究成果在理论上发现了一类密码学性质良好的非线性置换，在实践上解决了在分组密码设计中正形置换密钥控制的难题，具有知识创新的丰富内涵。该成果既有理论深度，也有很强的实用性，为设计具有我国自主知识产权的分组密码体制提供了良好的基础置换资源。在正形置换的研究上，该成果居国际领先水平。 基于BDLL型正形置换我们设计了KDCS-128P分组密码算法，该算法已经通过国密办的审批，命名为SSF18；基于该算法的密码芯片被命名为SSX01，目前正处于系统设计阶段。这些成果将广泛应用于信息安全产业中。

成果完成人：吕述望;张宝东;刘振华;张文婧;王挺;孙林红

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

Google提供的广告

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