通信学报
Journal on Communications
主管单位：中国科学技术协会
主办单位：中国通信学会

温凤桐.基于MISTY结构的可调分组密码的设计与分析[J].通信学报,2010,(7):76~80

基于MISTY结构的可调分组密码的设计与分析

DOI：

中文关键词：

英文关键词：

基金项目：

作者 **单位**

温凤桐

中文摘要：

对如何不借助于现有的分组密码来直接设计可调分组密码进行了研究。通过在MISTY结构的不同位置添加一个标号，分析了在4轮和5轮MISTY结构上设计可调分组密码的可行性。对4轮结构提出了攻击的方法；对5轮结构提供了安全性理论证明。结果表明，在选择明文攻击下，5轮MISTY结构才能提供安全的可调分组密码。

英文摘要：

查看全文 查看/发表评论 下载PDF阅读器

关闭