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

赵新杰,王 韬,王素贞,吴 杨.MIBS深度差分故障分析研究[J].通信学报,2010,(12):82~89

MIBS深度差分故障分析研究

DOI：

中文关键词：

英文关键词：

基金项目：

作者	单位
赵新杰	
王 韬	
王素贞	
吴 杨	

中文摘要：

给出了MIBS算法及故障分析原理，基于不同深度的故障模型，提出了3种针对MIBS差分故障分析方法，并进行实验验证。实验结果表明，由于其feistel结构和S盒差分特性，MIBS易遭受深度差分故障攻击，最好的实验结果为在第30轮左寄存器导入1次4bit故障，故障位置和值未知，可将64bit主密钥降低到24bit，经1min暴力破解恢复完整主密钥。此外，该故障分析方法也可为其他使用S盒的分组密码差分故障分析提供一定思路。

英文摘要：

查看全文 查看/发表评论 下载PDF阅读器

关闭