应用数学学报 2008 31 (31卷2): 193-198 ISSN: 1439-8516 CN: 11-2039/O1

RAINBOW分组密码的线性密码分析

卫宏儒

北京科技大学应用科学学院, 北京 100083

收稿日期 修回日期 网络版发布日期 2008-11-16 接受日期

摘要 本文在对RAINBOW分组密码的基础模块深入研究和测试后,
利用扩散层的特点, 对RAINBOW分组密码进行了线性密码分析, 攻击的数据复杂度为2^{94},
计算复杂度小于2^{18}。
此结果显示RAINBOW分组密码对线性密码分析是不免疫的.

关键词 分组密码 线性密码分析 复杂度 安全性 S-盒

分类号 11A55 11B37 11J70 11T71

Abstract

Key words

DOI:

通讯作者 weihr168@yahoo.com.cn