

# 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](mailto:weihr168@yahoo.com.cn)

## 扩展功能

### 本文信息

- ▶ [Supporting info](#)
- ▶ [PDF\(243KB\)](#)
- ▶ [\[HTML全文\]\(0KB\)](#)
- ▶ [参考文献](#)

### 服务与反馈

- ▶ [把本文推荐给朋友](#)
- ▶ [加入我的书架](#)
- ▶ [加入引用管理器](#)
- ▶ [复制索引](#)
- ▶ [Email Alert](#)

### 相关信息

- ▶ [本刊中 包含“分组密码” 的相关文章](#)
- ▶ 本文作者相关文章
- [卫宏儒](#)