

安全技术

不可能差分攻击中的明文对筛选方法

张庆贵

(解放军信息工程大学电子技术学院, 郑州 450004)

收稿日期 修回日期 网络版发布日期 接受日期

摘要 基于快速排序原理, 提出用于筛选明文对的基本算法和改进算法, 改进算法的计算复杂性可以将由直接检测方法的 $O(n^2)$ 降为 $O(n \log n)$ 。基于上述结果以改进算法分析对ARIA等分组密码算法的几个不可能攻击的计算复杂性, 证明ICISA2008上发表的某个针对对ARIA的不可能攻击的数据筛选过程的计算复杂性远高于密钥求解过程的计算复杂性。

关键词 [密码学](#); [密码分析](#); [不可能差分攻击](#); [明文对筛选](#); [计算复杂性](#); [ARIA算法](#)

分类号 [TN918.1](#)

DOI:

通讯作者:

作者个人主页: 张庆贵

扩展功能

本文信息

▶ [Supporting info](#)

▶ [PDF](#) (86KB)

▶ [\[HTML全文\]](#) (0KB)

▶ [参考文献\[PDF\]](#)

▶ [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](#)

▶ [引用本文](#)

▶ [Email Alert](#)

▶ [文章反馈](#)

▶ [浏览反馈信息](#)

相关信息

▶ [本刊中 包含“密码学; 密码分析; 不可能差分攻击; 明文对筛选; 计算复杂性; ARIA算法”的相关文章](#)

▶ [本文作者相关文章](#)