

安全技术

改进Py区分攻击算法的计算复杂性分析

陈士伟, 金晨辉

(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 针对Crowley P提出的一种改进的Py区分攻击算法, 利用直接计算的方法分析该算法的计算复杂性。基于以空间换时间的思想提出实现该算法的一种新的方法。结果表明, 该方法能有效地将该区分攻击的计算复杂性降为直接计算所需计算复杂性的1/14。

关键词 [Py算法](#); [区分攻击](#); [计算复杂性](#)

分类号 [TN918.1](#)

DOI:

通讯作者:

作者个人主页: 陈士伟; 金晨辉

扩展功能

本文信息

- ▶ [Supporting info](#)
- ▶ [PDF](#) (75KB)
- ▶ [\[HTML全文\]](#) (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“Py算法; 区分攻击; 计算复杂性”的 相关文章](#)
- ▶ [本文作者相关文章](#)