

安全技术

叛逆者追踪方案的密码学分析

张建中¹, 王永峰¹, 王翠玲²

(1. 陕西师范大学数学与信息科学学院, 西安 710062; 2. 哈尔滨理工大学测控技术与通信工程学院, 哈尔滨 150080)

收稿日期 修回日期 网络版发布日期 接受日期

摘要 对一种叛逆者追踪方案提出安全性分析, 指出它存在的安全缺陷有被撤销的叛逆者可以在合法用户的帮助下继续解密新密文及合法用户可以合谋伪造有效的解密密钥。提出伪造攻击方案, 并给出方案被攻击的原因。指出方案的一个设计错误, 说明该方案在实际操作上是不可行的。

关键词 [叛逆者追踪](#); [RSA算法](#); [合谋攻击](#)

分类号 [TN918](#)

DOI:

通讯作者:

作者个人主页: [张建中¹](#); [王永峰¹](#); [王翠玲²](#)

扩展功能

本文信息

- ▶ [Supporting info](#)
- ▶ [PDF\(74KB\)](#)
- ▶ [\[HTML全文\]\(0KB\)](#)
- ▶ [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“叛逆者追踪; RSA算法; 合谋攻击”的 相关文章](#)
- ▶ [本文作者相关文章](#)