计算机工程　2009 35 (20): 165-166　ISSN: 1000-3428　CN: 31-1289/TP　首页　当期目录　上一期

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