电子与信息学报 2005 27 (2): 235-238 ISSN: 1009-5896 CN: 11-4494/TN

论文

两种群签名方案的安全性分析

陈艳玲, 陈鲁生, 符方伟

南开大学数学科学学院, 天津 300071

收稿日期 2003-10-9 修回日期 2004-3-9 网络版发布日期 2008-4-18 接受日期

摘要
群签名允许群成员以匿名的方式代表整个群体对消息进行签名。而且, 一旦发生争议, 群管理员可以识别出签名者。该文对Posescu(2000)群签名方案和Wang-Fu(2003)群签名方案进行了安全性分析, 分别给出一种通用伪造攻击方法, 使得任何人可以对任意消息产生有效群签名, 而群权威无法追踪到签名伪造者。因此这两个方案都是不安全的。

关键词 群签名 伪造攻击 不关联性

分类号 TN918

Security Cryptanalysis of Two Group Signature Schemes

Chen Yan-ling, Chen Lu-sheng, Fu Fang-wei

College of Mathematical Science Nankai University Tianjin 300071 China

Abstract
Group signature schemes allow a group member to anonymously sign on group’s behalf. Moreover, in case of anonymity misuse.a group manager can recover the issuer of a signature. This paper analyzes the security of two group signature schemes recently proposed respectively by Posescu (2000) and Wang Xiaoming (2003), and shows that both schemes are universally forgeable, that is, anyone (not necessarily a group member) is able to produce a valid group signature on an arbitrary message, which cannot be traced by the group manager. So both schemes are insecure.

Key words Group signature Forgery attack Unlinkability

DOI:

通讯作者

作者个人主页 陈艳玲; 陈鲁生; 符方伟