计算机工程与应用 2008 44 (15): 124-126 ISSN: 1002-8331 CN: 11-2127/TP

网络、通信、安全

对一种向前安全群签名体制的密码学分析

鲁荣波[1], 杨兴萍[2], 何大可[3]
1．吉首大学 数学与计算机科学学院，湖南 吉首 416000
2．吉首大学 网络中心，湖南 吉首 416000
3．西南交通大学 信息安全与国家计算网格实验室，成都 610031

收稿日期 2007-11-5 修回日期 2007-12-24 网络版发布日期 2008-5-16 接受日期

摘要 对陈少真等提出的一种有效取消的向前安全群签名方案进行了密码学分析，首先指出该群签名体制存在错误的模运算及冗余数据，效率不高。其次，指出该群签名体制是不安全的，群管理员可以伪造能够通过验证的群签名。

关键词 群签名 向前安全 可取消性 密码学分析 冗余数据
分类号

Cryptanalysis of efficient revocable group signature scheme with forward security

LU Rong-bo[1],YANG Xing-ping[2],HE Da-ke[3]

1.College of Math. and Computer Science，Jishou University，Jishou，Hunan 416000，China
2.Center of Network，Jishou University，Jishou，Hunan 416000，China
3.Laboratory of Information Security and National Computing Gird，Southwest Jiaotong University，Chengdu 610031，China

Abstract
The efficient revocable group signature scheme with forward security proposed by Chen Shao-Zhen et al is analyzed.First，its shortage in the module and there is redundancy data in the scheme，so，it is low in efficiency.At the same time，it is insecure.The group manager can forge group signatures that can be verified by a verifier.

Key words group signature forward security revocable cryptanalysis redundant data

DOI:

通讯作者 鲁荣波 lurongbo8563@163.com