计算机工程与应用 2007 43 (33): 22-23 ISSN: 1002-8331 CN: 11-2127/TP

博士论坛

对一种改进的群签名方案的密码学分析

鲁荣波[1], 王常吉[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．中山大学 计算机科学系,广州 510275
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 修回日期 网络版发布日期 2007-11-9 接受日期

摘要 对司光东等人提出的一种改进的群签名方案进行安全性分析,指出该方案是不安全的：群管理员不能够打开一个群签名,该群签名是不可跟踪的;群管理员可以伪造一个能通过验证的群签名;同时该方案并不能抵抗联合攻击,两个群成员合谋后可以伪造出有效的群签名。

关键词 群签名 安全性分析 伪造攻击 联合攻击

分类号

Cryptanalysis of improved group signature scheme

LU Rong-bo[1],WANG Chang-ji[2],HE Da-ke[3]

1.College of Math. and Computer Science,Jishou University,Jishou,Hunan 416000,China
2.Dept. of Computer Science,Sun Yat-Sen University,Guangzhou 510275,China
3.Laboratory of Information Security and National Computing Gird,Southwest Jiaotong University,Chengdu 610031,China

Abstract

An improved group signature scheme proposed by G.D.Si et al has been analyzed.We have showed that the scheme is insecure.The revocation center cannot open a valid group signature,so the group signature is not tracked.Meanwhile,the group manager can forge group signatures that could be verified by a verifier.And the scheme does not satisfy the properties of against coalition attack.Two group members can conspire to generate valid group signatures.

Key words group signature security analysis forge attack coalition attack

DOI:

通讯作者 鲁荣波 E-mail：lurongbo8563@163.com