计算机工程与应用 2010 46 (6): 96-97 ISSN: 1002-8331 CN: 11-2127/TP

网络、通信、安全

一种新的基于身份的动态群签名方案

欧海文[1]，王佳丽[1，2]

1.北京电子科技学院 信息安全与保密重点实验室，北京 100070
2.西安电子科技大学 通信工程学院，西安 710071

收稿日期 2008-9-1 修回日期 2008-11-3 网络版发布日期 2010-2-23 接受日期

摘要 为了解决在基于身份的群签名中KGC不可信的问题，提出了一种新的基于身份的动态群签名方案。新的验证和打开算法确保了该方案可以抵抗伪造攻击。另外该方案可以简单有效地删除群成员，而不改变群公钥和其他群成员的密钥，签名和密钥的长度不依赖于群成员的个数。

关键词 群签名 基于身份 动态

分类号 TN918.1

New ID-based dynamic group signature scheme

OU Hai-wen[1]，WANG Jia-li[1，2]

1.Key Lab of Information Security and Secrecy，Beijing Electronic Science and Technology Institute，Beijing 100070，China
2.College of Communication Engineering，Xidian University，Xi’an 710071，China

Abstract

In order to solve the problem that KGC can not be trusted in ID-based group signature，a new ID-based dynamic group signature scheme is proposed.The new verify and open algorithms make sure the scheme can against forgery attack.Additional，this scheme can delete members simply and efficiently without changing the group public key and the other group members’ key.At the same time，the sizes of signature and key are independent on the numbers of the group members.

Key words group signature ID-based dynamic

DOI: 10.3778/j.issn.1002-8331.2010.06.027

通讯作者 欧海文 breashjiali@163.com