电子与信息学报 2007 29 (6): 1511-1513 ISSN: 1009-5896 CN: 11-4494/TN

学述讨论

一种高效群签名方案的密码学分析

谢 琪

杭州师范学院信息工程学院 杭州 310036

收稿日期 2005-8-23 修回日期 2006-6-20 网络版发布日期 2008-2-18 接受日期

摘要
2005年，张键红等提出了一种基于RSA的高效群签名方案，签名与验证的计算量只需要9次模幂乘运算。该文提出了一种伪造攻击方案指出张等的方案是不安全的，任一群成员在撤消中心的帮助下可以不利用自己的秘密参数对任何消息生成有效的群签名。同时，指出了群成员的识别算法是错误的，身份追踪式是与具体签名无关的常量，即身份追踪算法无法追踪到真实的签名者。最后，指出了他们的方案具有关联性。

关键词 群签名 RSA 密码学

分类号 TN918.2

Cryptanalysis of an Efficient Group Signature Scheme

Xie Qi

School of Information and Engineering, Hangzhou Teachers College, Hangzhou 310036, China

Abstract
In 2005, Zhang et al. proposed an efficient group signature scheme based on RSA, the total computation cost of signature and verification requires only 9 modular exponentiations. This paper will show that Zhang et al.'s scheme is insecure, any group member colludes with repeal center can generate a valid group signature without using his secret parameters. Additional, it will show that the signer identity verification algorithm is error, identity verification expression is independent of the group signature. That is, the signer identity verification algorithm cannot find who the signer is. Finally, it will show that their scheme is not unlinkable.

Key words Group signature RSA Cryptography

DOI:

通讯作者

作者个人主页 谢 琪