计算机工程与应用 2010 46 (9): 80-82 ISSN: 1002-8331 CN: 11-2127/TP

网络、通信、安全

对存在特权集的门限群签名方案的安全性分析

王勇兵，王际川

河北师范大学 附属民族学院，石家庄 050091

收稿日期 2009-8-7 修回日期 2009-10-9 网络版发布日期 2010-3-19 接受日期

摘要 针对冯登国提出的“存在特权集的门限群签名”问题，2005年，陈伟东提出了一类存在特权集的门限群签名方案（C-F方案），分析发现它容易受到可信密钥认证中心发起的三种伪造攻击，不具有签名的可区分性和事后身份追踪的特性，也无法抵抗内部成员的合谋攻击。提出了一种改进方案，新方案克服了C-F方案的安全隐患，保护了签名人的合法权益，节省了系统存储空间，是一个安全有效的签名方案。

关键词 门限群签名 特权集 伪造攻击 合谋攻击

分类号 TN918

Cryptanalysis of threshold group signature schemes with privilege subsets

WANG Yong-bing，WANG Ji-chuan

Nationalities College of Hebei Normal University，Shijiazhuang 050091，China

Abstract

Feng Deng-guo suggests a problem called threshold group signature scheme with privilege.In 2005，Chen Wei-dong presented a group of threshold group signature schemes with privilege subsets.Through cryptanalysis of it，KAC or KAC with others can froge signature，and it is not provided with distinguishability and traceability.Furthermore，it can not resist conspiratorial attack.An improved scheme is proposed and the security drawbacks of original scheme are overcome.In the new scheme，the interests of signer are protected and storage space is reduced，so it is more secure and efficient.

Key words threshold group signature privilege subsets frogery attack conspiratorial attack

DOI: 10.3778/j.issn.1002-8331.2010.09.023

通讯作者 王勇兵 wyb723@yahoo.com.cn