计算机工程与应用 2009 45 (3): 104-105 ISSN: 1002-8331 CN: 11-2127/TP

网络、通信、安全

对两种基于离散对数代理盲签名的分析

秦宝东

西南科技大学 计算机科学与技术学院，四川 绵阳 621010

收稿日期 2008-1-4 修回日期 2008-4-24 网络版发布日期 2009-1-17 接受日期

摘要 高炜等人和Yu Bao-zheng等人分别提出了两种基于离散对数的代理盲签名方案。对这两种方案进行了安全性分析。研究表明，这两种方案存在以下不足之处：高炜等人的代理盲签名方案是对谭等方案的改进，新的方案仍然具有可连接性，即代理签名者可以从一个合法的代理盲签名中恢复出此签名的中间值从而跟踪消息的拥有者。Yu Bao-zheng等人的代理盲签名方案同样具有可连接性的缺点。除此之外，用户可以通过自己持有的代理盲签名信息恢复出代理签名私钥，从而可以冒充代理签名者伪造消息m的代理盲签名或者直接利用一个合法的代理盲签名伪造出其它消息的合法代理盲签名。为了避免上述不足之处，给出了一个防止代理签名者连接性攻击的改进方案。

关键词 离散对数 代理盲签名 密码分析

分类号

Cryptanalysis of two proxy blind signatures based on DLP

QIN Bao-dong

College of Computer Science & Technology，Southwest University of Science & Technology，Mianyang，Sichuan 621010，China

Abstract

This paper presents a security analysis of two DLP-based proxy blind signature schemes proposed recently by Gao et al and Yu et al respectively and point out that both of the two schemes are insecure against the proxy signer’s linkability attacks as well as the user’s forgery attacks.Gao et al’s scheme is an improved scheme of Tan et al’s.However，it is still vulnerable to the proxy signer’s linkability attacks.Yu et al’s scheme is also insecure against the proxy signer’s linkability attacks.In addition，the user can deduce the proxy signature private key by using a valid proxy signature，and then instead of the proxy signer he can forge a valid proxy signature of a message m.He also can directly forge a valid proxy signature which related to the valid signature received from the proxy signer.This paper presents an improved scheme that can against the proxy signer’s linkability attacks.

Key words discrete logarithm problem proxy blind signature cryptanalysis

DOI: 10.3778/j.issn.1002-8331.2009.03.030

通讯作者 秦宝东 bd_qin@yahoo.com