计算机工程与应用 2010 46 (12): 82-84 ISSN: 1002-8331 CN: 11-2127/TP

网络、通信、安全

一个新的多代理盲签名方案

毛卫霞，李志慧，柳 烨

陕西师范大学 数学与信息科学学院，西安 710062

收稿日期 2008-10-17 修回日期 2008-12-25 网络版发布日期 2010-4-21 接受日期

摘要 多代理盲签名综合了多代理签名和盲签名的优点，是一种特殊的数字签名。它由一个原始签名人授权给一组代理签名人，并且这组代理签名人并不知道消息的具体内容。基于离散对数问题提出了一种新的多代理盲签名方案。该方案不需要安全信道传送代理密钥，且具有不可伪造性、不可链接性。

关键词 离散对数 多代理签名 盲签名 安全信道 不可伪造性 不可链接性

分类号 TP309

New multi-proxy blind signature scheme

MAO Wei-xia，LI Zhi-hui，LIU Ye

College of Mathematics and Information Science，Shaanxi Normal University，Xi’an 710062，China

Abstract

Multi-proxy blind signature is a special digital signature which satisfies the security properties of both the proxy signature and blind signature.It permits that an original signer authorizes a group of proxy signers who don’t know the concrete content of the message.A new multi-proxy blind signature is proposed based on DLP.This scheme doesn’t need security channel to transmit proxy cipher key，and has properities of unforgeability and unlinkability.

Key words discrete logarithm problem multi-proxy signature blind signature security channel unforgeability unlinkability

DOI: 10.3778/j.issn.1002-8331.2010.12.022

通讯作者 毛卫霞 ccde456@163.com