计算机工程 2012, 38(3) 139-140,144 DOI: 10.3969/j.issn.1000-3428.2012.03.047 ISSN: 1000-3428 CN: 31-1289/TP

安全技术

基于椭圆曲线的盲代理盲签名方案

李方伟，万 丽，闫少军

(重庆邮电大学移动通信安全技术重点实验室，重庆 400065)

摘要： 针对现有签名方案不能同时保护代理签名者和消息拥有者安全的问题，提出一种基于椭圆曲线的盲代理盲签名方案。该方案不需要可信方，在隐藏代理签名者身份信息的同时，盲化需要签名的消息。分析结果表明，该方案满足盲代理签名和代理盲签名的安全特性，能有效保护代理签名者和用户的身份隐私。

关键词： 椭圆曲线 盲代理 盲签名 匿名性 不可伪造性

Blind Proxy Blind Signature Scheme Based on Elliptic Curve

LI Fang-wei, WAN Li, YAN Shao-jun

(Key Lab of Mobile Communication Security Technology, Chongqing University of Posts and Telecommunications, Chongqing 400065, China)

Abstract: To solve the contradiction that current signature schemes can not protect the benefits of proxy signer and message owner at the same time, a blind proxy blind signature scheme without trusted party base on elliptic curve is presented. It hides both the identity of the proxy signer and the message to be signed. The property analysis shows that the proposed scheme satisfies the security properties of proxy blind signature and blind proxy signature scheme. It can effectively protect the proxy signer and user's identity privacy and prevents abusing signature. It also has a higher safety and efficiency compared with other schemes.

Keywords: elliptic curve blind proxy blind signature anonymity unforgeability

收稿日期 2011-07-08 **修回日期** **网络版发布日期** 2012-02-05

DOI: 10.3969/j.issn.1000-3428.2012.03.047

基金项目:

国家自然科学基金资助项目(61071116)；重庆市发改委高技术产业技术开发基金资助项目(20091537)

通讯作者:

作者简介: 李方伟(1960－)，男，教授、博士，主研方向：信息安全，第三代移动通信技术，组网技术；万丽、闫少军，硕士研究生

通讯作者E-mail: wan85103@126.com

参考文献：

[3] Lee B.[J].Kim H, Kim K. Strong Proxy Signature and Its App- lications[C]//Proceedings of ICS'00. Tainan, China: [s. n..2000,:-

[9] 张建中, 马伟芳. 椭圆曲线上的盲代理盲签名方案[J].计算机工程.2010, 36(11):126-127 浏览

本刊中的类似文章

1. 周才学, 周顽, 胡日新, 江永和.基于身份的签密方案分析与改进[J]. 计算机工程, 2012,38(2): 132-134
2. 李忠, 彭代渊.低存储需求的快速标量乘法算法[J]. 计算机工程, 2012,38(04): 137-139
3. 胡吉旦, 卢建朱.无线网络中一种基于智能卡的匿名认证方案[J]. 计算机工程, 2012,38(01): 122-124
4. 张建中, 马冬兰.一种高效的门限部分盲签名方案[J]. 计算机工程, 2012,38(01): 130-131,134
5. 周莹莹, 张建中.一种有代理门限签名方案的密码分析与改进[J]. 计算机工程, 2012,38(01): 120-121,124
6. 姜东焕, 徐光宝.可追踪签名者身份的匿名代理签名方案[J]. 计算机工程, 2011,37(9): 153-154
7. 强小强, 何小卫, 韩建民, 李静.基于谱约束的随机化社会网络多点扰动方法[J]. 计算机工程, 2011,37(9): 98-100,103
8. 宋明明, 张彰, 谢文坚.一种无证书签密方案的安全性分析[J]. 计算机工程, 2011,37(9): 163-164
9. 陈逢林, 胡万宝, 孙广人.基于超椭圆曲线的顺序多重盲签名[J]. 计算机工程, 2011,37(9): 160-162
10. 孙静, 廖凯宁, 王伟 .一个可证明安全的短环签密方案[J]. 计算机工程, 2011,37(8): 140-142

文章评论

反馈人		邮箱地址	
反馈标题		验证码	7361