计算机工程 2011, 37(24) 114-116 DOI: 10.3969/j.issn.1000-3428.2011.24.038 ISSN: 1000-3428 CN: 31-1289/TP

安全技术

一种基于身份的代理盲签名方案

丁圣龙，赵一鸣

(复旦大学软件学院，上海 200433)

摘要： 分析一种代理盲签名方案，指出其在生成代理盲签名过程中存在的安全问题，由于不恰当地使用预计算，使攻击者可以轻易计算出代理密钥。为克服该缺陷，提出一种新的基于身份的代理盲签名方案，该方案能够满足不可伪造性、盲性等安全特性，相比于同类方案，其计算复杂度更低。

关键词： 基于身份 代理盲签名 双线性对 盲性 代理密钥安全

ID-based Proxy Blind Signature Scheme

DING Sheng-long, ZHAO Yi-ming

(Software School, Fudan University, Shanghai 200433, China)

Abstract: A proxy blind signature scheme is analyzed. It is found that proxy blind signature generation phase in this scheme is not secure, adversaries can easily find out the proxy key due to improper use of pre-computation. To resolve the problem, this paper proposes a new ID-based proxy blind signature scheme which satisfies the required security properties of unforgeability and blindness. It has lower computing complex compared with other schemes.

Keywords: ID-based proxy blind signature bilinear pairings blindness proxy key security

收稿日期 2011-06-22 **修回日期** **网络版发布日期** 2011-12-20

DOI: 10.3969/j.issn.1000-3428.2011.24.038

基金项目:

“十一五”国家密码发展基金资助项目

通讯作者:

作者简介: 丁圣龙(1988－)，男，硕士研究生，主研方向：密码学，信息安全；赵一鸣，副教授

通讯作者E-mail: 10212010009@fudan.edu.cn

参考文献：

[2] 张学军, 王育民. 高效的基于身份的代理盲签名[J].计算机应用.2006, 26(11):2586-2588

[3] 李素娟, 张福泰. 基于ID的代理盲签名[J].计算机工程.2006, 32(17):203-204 浏览

[4] 张 妮, 奚雪峰, 陆卫忠, 等. 基于身份的代理盲签名方案分析与改进[J].计算机工程.2010, 36(16):110-112 浏览

本刊中的类似文章

1. 曹素珍, 王彩芬, 陈小云, 吕浩音.一种不含双线性对的可截取签名方案[J]. 计算机工程, 2012,38(3): 110-112
2. 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
3. 牛淑芬, 王彩芬.多源线性网络编码的同态签名算法[J]. 计算机工程, 2012,38(2): 126-128
4. 杨路.无对运算的无证书隐式认证及密钥协商协议[J]. 计算机工程, 2012,38(2): 138-140
5. 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
6. 高欢欢, 张建中.一种基于身份的门限代理签名方案[J]. 计算机工程, 2012,38(01): 132-134
7. 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
8. 魏靓, 张串绒, 郑连清.一种基于身份的广义签密方案[J]. 计算机工程, 2011,37(8): 4-6
9. 张玉磊.高效的无证书紧致有序多重签名方案[J]. 计算机工程, 2011,37(8): 108-111
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	5615