计算机工程 2012, 38(3) 110-112 DOI: 10.3969/j.issn.1000-3428.2012.03.037 ISSN: 1000-3428 CN: 31-1289/TP



安全技术

# 一种不含双线性对的可截取签名方案

曹素珍[1]，王彩芬[1]，陈小云[2]，吕浩音[3]

(1. 西北师范大学数学与信息科学学院，兰州 730070；2. 平凉市第一中学信息中心，甘肃 平凉 744000； 3. 陇东学院计算机与信息科学学院，甘肃 庆阳 745000)

**摘要：** 现有可截取签名方案需要计算双线性对，计算效率较低。针对该问题，基于无证书思想，提出一个不含双线性对的可截取签名方案。采用绑定技术，通过哈希函数将用户公钥绑定在部分私钥的生成算法及签名算法中，以降低公钥替换攻击的可能性。在随机预言机模型下证明方案效率较高，签名是不可伪造的。

**关键词：** 可截取签名 离散对数问题 双线性对 哈希函数 随机预言机模型

## Content Extraction Signature Scheme Without Bilinear Pairings

CAO Su-zhen [1], WANG Cai-fen [1], CHEN Xiao-yun [2], LV Hao-yin [3]

(1. College of Mathematics and Information Science, Northwest Normal University, Lanzhou 730070, China; 2. Information Center of Pingliang First Middle School, Pingliang 744000, China; 3. College of Computer and Information Science, Longdong University, Qingyang 745000, China)

Abstract: For the existing content extraction signature scheme, because calculated bilinear pairings caused the problem of low efficiency, based on certificateless thinking, this paper proposes an efficient content extraction signature scheme without pairings. Scheme of binding techniques, use hash functions will the public key binding to the partial private key generates and signature algorithms, reduce the possibility of public key substitution attack, and in the random oracle model proved scheme is existentially unforgeable under adaptive chosen-message attacks assuming. Compared with known solutions, the efficiency is higher.

Keywords: content extraction signature Discrete Logarithm Problem(DLP) bilinear pairings Hash function random oracle model

**收稿日期** 2011-07-11 **修回日期** **网络版发布日期** 2012-02-05

DOI: 10.3969/j.issn.1000-3428.2012.03.037

**基金项目**:

国家自然科学基金资助项目(61063041)；教育部科学技术研究基金资助重点项目(208148)；甘肃省教育厅基金资助重点项目(0801-01)

**通讯作者**:

**作者简介**: 曹素珍(1976－)，女，讲师，主研方向：信息安全；王彩芬，教授、博士生导师；陈小云，一级教师；吕浩音，讲师

**通讯作者**E-mail: caosuz@nwnu.edu.cn



**参考文献：**

[3] Bull L, Squire M D, Zheng Yuliang. A Hierarchical Extraction Policy for Content Extraction

Signatures[J].International Journal of Digital Libraries.2004, 4(3):208-222

[6] 张玉磊, 王彩芬. 无证书签名改进方案的安全性证明[J].计算机工程.2010, 36(12):170-172 浏览

[7] Rafael C.[J].Ricardo D. Two Notes on the Security of Certificateless Signature[M]. Berlin, Germany: Springer-Verlag.2007,:-

**本刊中的类似文章**

1. 张韶远, 卢建朱.基于生物特征的鲁棒远程用户认证方案[J]. 计算机工程, 2012,38(3): 137-138
2. 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
3. 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
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. 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
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 | 9720 |
| | | | |