计算机工程 2011, 37(24) 18-21 DOI: 10.3969/j.issn.1000-3428.2011.24.007 ISSN: 1000-3428 CN: 31-1289/TP

博士论文

基于双线性对的无证书签名与群签名方案

李凤银 [1,2]，刘培玉 [1]，朱振方 [1]

(1. 山东师范大学信息科学与工程学院，济南 250014；2. 曲阜师范大学计算机科学学院，山东 日照 276826)

摘要： 传统数字签名方案的证书存储和管理开销较大，基于身份的数字签名方案无法解决其固有的密钥托管问题，而无证书签名方案无需使用公钥证书，且没有密钥托管问题。为此，提出一个基于双线性映射的无证书签名方案，并在随机预言机模型下证明其安全性。在此基础上设计一个无证书群签名方案，其安全性建立在计算Diffie-Hellman问题的困难性假设上。性能分析表明，2种签名方案在保证安全性的前提下，具有较高的执行效率。

关键词： 无证书密码体制 群签名 双线性映射 Diffie-Hellman问题 随机预言机

Certificateless Signature and Group Signature Schemes Based on Bilinear Pairings

LI Feng-yin [1,2], LIU Pei-yu [1], ZHU Zhen-fang [1]

(1. School of Information Science and Engineering, Shandong Normal University, Jinan 250014, China; 2. College of Computer Science, Qufu Normal University, Rizhao 276826, China)

Abstract: Traditional digital signature schemes need much more storage and management overhead for the use of certificates, while the identity-based digital signature schemes fail to solve the inherent key-escrow problem. Certificateless signature schemes need no certificates and can solve the key-escrow problem. This paper presents a certificateless signature scheme from bilinear pairings, and verifies its security under the random oracle machine. It designs a certificateless group signature scheme from the certificateless signature scheme, and its security is founded under the assumption of the computational Diffie-Hellman problem. Performance analysis shows that both signature schemes are secure and have high performing efficiency.

Keywords: certificateless cryptography group signature bilinear mapping Diffie-Hellman problem random oracle machine

收稿日期 2011-03-18 **修回日期** **网络版发布日期** 2011-12-20

DOI: 10.3969/j.issn.1000-3428.2011.24.007

基金项目:

国家自然科学基金资助项目(60873247)；山东省自然科学基金资助重点项目(ZR2009GZ007)；山东省高新技术自主创新工程基金资助项目(2008ZZ28)

通讯作者:

作者简介: 李凤银(1974－)，女，副教授、博士研究生，主研方向：信息安全，数字签名；刘培玉，教授、博士生导师；朱振方，博士研究生

通讯作者E-mail: lfyin318@126.com

参考文献：

[4] Park S, Kim S, Won D. ID-based Group Signature[J].Electronics Letters.1997, 33 (19):1616-1617

[6] 陈 虎, 宋如顺. 高效的无证书环签名方案[J].计算机工程.2009, 35(21):125-127 浏览

[9] 陈 虎, 宋如顺. 无证书群签名方案[J].计算机工程.2009, 35(9):130-132 浏览

[10] Chen Xiaofeng, Zhang Fangguo, Kim K. A New Id-based Group Signature Scheme from Bilinear Pairings[EB/OL]. (2003-11-06). http://PPeprint.iacr.org/P2003P116.

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. 张玉磊, 戴小武, 韩亚宁, 王彩芬.广义指定多个验证者有序多重签名方案[J]. 计算机工程, 2011,37(5): 149-151
3. 蔡志伟, 王立斌, 马昌社.一种基于身份的高效短群签名方案[J]. 计算机工程, 2011,37(18): 145-147
4. 曾亮, 杜伟章.自选子密钥的可验证广义秘密共享方案[J]. 计算机工程, 2011,37(16): 138-139
5. 张建中, 彭丽慧, 薛荣红.一个无证书代理盲签名方案[J]. 计算机工程, 2011,37(14): 112-113
6. 张建中, 李瑞, 乔晓林.一般访问结构上无可信中心的群签名方案[J]. 计算机工程, 2011,37(13): 113-114,118
7. 王永峰, 张建中.一种改进的群签名方案[J]. 计算机工程, 2010,36(24): 110-112
8. 顾永军, 齐敬敬, 王雅坤.基于身份加密的匿名漫游无线认证协议[J]. 计算机工程, 2010,36(17): 176-178,181
9. 贺军, 李丽娟, 李喜梅, 唐春明.前向安全的代理多重数字签名方案[J]. 计算机工程, 2010,36(14): 122-123
10. 张玉磊, 王彩芬, 张永洁, 韩亚宁, 程文华.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

文章评论

反馈人		邮箱地址	
反馈标题		验证码	1803