计算机应用 2009, 29(05) 1330-1333 DOI: ISSN: 1001-9081 CN: 51-1307/TP

本期目录 | 下期目录 | 过刊浏览 | 高级检索　　[打印本页]　[关闭]

论文

基于双线性对的高效无证书签名方案

张玉磊[1],王彩芬[2],张永洁[3],程文华[1],韩亚宁[4]

1. 西北师范大学数学与信息科学学院
2. 西北师范大学 数学与信息科学学院
3. 甘肃省卫生学校
4. 西北师范大学

摘要：

为了避免身份密码系统中密钥托管问题，出现了无证书密码系统。基于双线性对提出了一个高效的无证书签名方案。在方案中，签名算法需要一个指数运算，验证算法仅需要一个对运算和一个指数运算。与许多已有方案相比，具有较高的效率。方案的安全性依赖于q-SDH困难问题和Inv-CDH困难问题，并在随机预言机模型下，证明能够抵抗适应性选择消息攻击下的存在性伪造。

关键词： 双线性对 q-SDH问题 Inv-CDH问题 无证书签名 bilinear pairings q-SDHP Inv-CDHP certificateless signature

Efficient certificateless signature scheme based on bilinear parings

Abstract:

Due to eliminating the inherent key escrow in identity-based cryptosystem, the certificateless public key cryptosystem came into being. A new efficient certificateless signature scheme based on bilinear pairing was put forward. The signing algorithm did not need any pairing computation but need one exponentiation computation, and the verification algorithm only needed one pairing and one exponentiation computation. The new scheme is more efficient than other exsiting schemes in terms of computation overhead. Furthermore, the security relies on the hardness of the q-Strong Diffie-Hellman （q-SDH） problem and Inverse-Compute Diffie-Hellman （Inv-CDH） problem. Under the random oracle model, the new scheme is proved to be secure against existential forgery on adaptively chosen message attack.

Keywords:

收稿日期 2008-11-28 修回日期 2009-01-14 网络版发布日期 2009-06-09

DOI:

基金项目:

国家级基金;省部级基金;校级基金

通讯作者: 张玉磊

作者简介:

参考文献：

本刊中的类似文章

扩展功能

本文信息

- Supporting info
- PDF(614KB)
- [HTML全文]
- 参考文献

服务与反馈

- 把本文推荐给朋友
- 加入我的书架
- 加入引用管理器
- 引用本文
- Email Alert
- 文章反馈
- 浏览反馈信息

本文关键词相关文章

- 双线性对
- q-SDH问题
- Inv-CDH问题
- 无证书签名
- bilinear pairings
- q-SDHP
- Inv-CDHP
- certificateless signature

本文作者相关文章

- 张玉磊
- 王彩芬
- 张永洁
- 程文华
- 韩亚宁

PubMed

- Article by Zhang,Y.L
- Article by Yu,C.F
- Article by Zhang,Y.J
- Article by Cheng,W.H
- Article by Han,Y.N

文章评论 (请注意:本站实行文责自负, 请不要发表与学术无关的内容!评论内容不代表本站观点.)

反馈人		邮箱地址	
反馈标题		验证码	1054