吉林大学学报(工学版)　2006 36 (增刊2): 134-138　ISSN: 1671-5497　CN: 22-1341/T

扩展功能

本文信息

- Supporting info
- PDF(390KB)
- [HTML全文](0KB)
- 参考文献

服务与反馈

- 把本文推荐给朋友
- 复制索引
- 文章反馈
- 浏览反馈信息

相关信息

- 本刊中 包含“计算机工程”的相关文章
- 本文作者相关文章
  - 裴士辉
  - 赵宏伟

基于RSA的三次传递不可否认签名方案

裴士辉，赵宏伟

吉林大学 计算机科学与技术学院， 长春 130022

收稿日期 2005-4-13　修回日期 2005-9-22　网络版发布日期 2006-9-20　接受日期

摘要　提出了一个新的基于RSA的不可否认签名方案，该方案的确认协议和否认协议是三次传递的，因而提高了效率。该方案同时实现了可转换性，可以把不可否认签名方案转换成通常的RSA数字签名方案。方案在随机问答器模型下证明是安全的，其不可伪造性等同于CDH(Computational Diffie　Hellman)问题；不可分辨性等同于DDH(Decisional Diffie　Hellman)问题；不可扮演性等同于离散对数问题。

关键词　计算机工程　信息安全　不可否认签名　证据不可分辨性　不可伪造性　不可扮演性

分类号　TP309

RSA based 3 move undeniable signatures scheme

Pei Shi-hui，Zhao Hong-wei

College of Computer Science and Technology, Jilin University, Changchun 130022,China

Abstract A new RSA based undeniable signature scheme was proposed which is more efficient because of its 3 move confirmation and disavowal protocols. The scheme is convertable and can be converted into the conventional RSA digital signature scheme. The scheme was proved secure against the active and concurrent attacks in the random oracle model. The existential unforgeability of the proposed scheme is equivalent to the computational Diffie Hellman problem and its witness indistinguishableness is equivalent to the decisional Diffie Hellman problem. Its anti impersonation ability is equivalent to the discrete logarithm problem.

Key words computer engineering　information security；undeniable signature；　witness indistinguishableness；unforgeability　anti　impersonation ability

DOI:

通讯作者 赵宏伟 zhaohw@jlu.edu.cn