计算机应用 2007 (12): 2960-2961 ISSN: 1001-9081 CN: 51-1307/TP

网络与信息安全

一种不使用Hash和Redundancy函数的代理盲签名

邱成刚[1];李方伟[1]

重庆邮电大学 移动通信重点实验室[1]

收稿日期 2007-6-11 修回日期 网络版发布日期 2007-12-1 接受日期

摘要 在密码学中，使用Hash函数和Redundancy函数必然使签名方案因这些函数的不安全性而遭受相关攻击，从而导致签名方案的安全性降低。提出了一种不使用Hash和Redundancy函数的代理盲签名，其安全性等价于解离散对数问题，而且避免了使用相关函数带来的威胁。分析表明，新方案实现了电子交易中的不可伪造性和不可链接性，有效防止了双方事后抵赖；而且减少了求幂运算的次数，避免了求Hash函数运算，使签名速度有了较大提高。

Abstract In Cryptography, the scheme of signature using Hash and Redundancy functions will be faced with related attacks. Therefore it will result in lower security. So a proxy blind signature scheme without using Hash and Redundancy Functions was proposed, whose security equaled to the difficulty of the discrete logarithm problem. And it avoided the insecurity of the related function. Analysis shows that this scheme has really completed unforgeability and unlinkability in the electronic tractions of business, and prevents the repudiation efficiently. Meantime, the new scheme reduces the computational load for exponentiation, avoids the computation for Hash function and improves the signing speed.

关键词 不可链接性 代理盲签名 不可伪造性

Key words unlinkability;proxy blind signature;unforgeablity

分类号 TP309.7

DOI:

通讯作者:
邱成刚 qiu0301110@126.com

作者个人主页: 邱成刚 李方伟

扩展功能

本文信息

Supporting info

PDF(1133KB)

[HTML全文](0KB)

参考文献[PDF]

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

相关信息

本刊中 包含“不可链接性”的 相关文章

本文作者相关文章

· 邱成刚
· 李方伟