计算机应用 2008 28 (05): 1144-1145 ISSN: 1001-9081 CN: 51-1307/TP

信息安全(Information security)

对一种代理盲签名方案的密码学分析

雷治军[1];刘文化[2];禹勇[3]

洛阳师范学院[1]

济源职业技术学院[2]

西安电子科技大学[3]

收稿日期 2007-11-21 修回日期 2008-1-14 网络版发布日期 2008-5-7 接受日期

摘要 Zhao等提出了一个新的代理盲签名方案，并在此基础上，考虑了签名方程中所有可能的参数选取方法，由此给出了构造代理盲签名方案的一般方法，给出了生成代理密钥的8个方程式。对他们提出的代理盲签名进行了分析，给出了一种伪造攻击，利用这种攻击，不诚实的原始签名人可以成功伪造代理签名密钥，从而假冒诚实的代理签名人生成验证有效的签名，威胁到代理签名人的权益。在Zhao等给出的8种代理密钥方程式中，有一半都无法抵抗这种攻击。

Abstract A new proxy blind signature scheme was proposed by Zhao et al. recently. Based on this scheme, all possible parameters to be chosen in signature equations were considered and a general method to construct proxy blind signature was obtained. They also proposed eight equations to generate secure proxy signing key. However, their scheme was insecure. A forgery attack on their proxy blind signature scheme was proposed in this paper. Using the forgery attack, a dishonest original signer can forge the proxy signing key and produce valid proxy blind signatures. Among the eight equations of producing proxy signing key, half of them can not resist this kind of attack.

关键词 数字签名 代理签名 代理盲签名

Key words digital signature;proxy signature;proxy blind signature

分类号

DOI:

通讯作者:
禹勇 yuyong@mail.xidian.edu.cn

作者个人主页: 雷治军 刘文化 禹勇

扩展功能

本文信息

- Supporting info
- PDF(353KB)
- [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“数字签名”的 相关文章

本文作者相关文章

· 雷治军
· 刘文化
· 禹勇