西安电子科技大学学报 2008 35 (2): 351-355 ISSN: 1001-2400 CN: 61-1076/TN

一种新的基于离散对数的签名方案

贾晓芸1, 3, 罗守山2, 3, 袁超伟1

(1. 北京邮电大学 通信网络综合技术研究所，北京 100876;
2. 北京邮电大学 软件学院，北京 100876;
3. 西安电子科技大学 综合业务网理论及关键技术国家重点实验室，陕西 西安 710071)

收稿日期 修回日期 网络版发布日期 2008-3-28 接受日期

摘要 针对传统签名方案中验证者的验证权限是相同的缺点，提出了一种新的基于离散对数的链式验证签名方案. 利用有序秘密分享方法将验证参与者分为签名验证者和链式验证授权者，签名验证者只有在经过链式验证授权组中每一个成员的依次授权时，才可以验证签名的有效性，而且链式验证授权组中的任何成员(即使所有成员合谋)都不能验证签名的有效性. 此外，该方案可以方便地增删链式验证授权组中的成员和维护链式验证授权者和签名验证者的私钥.

关键词 离散对数 数字签名 链式验证签名
分类号 TN918.1

New digital signature scheme based on the discrete logarithm

JIA Xiao-yun1,3,LUO Shou-shan2,3,YUAN Chao-wei1

(1. Inst. of Communication Networks Integrated Technique, Beijing Univ. of Posts and Telecommunications, Beijing 100876， China;
2. School of Software Eng., Beijing Univ. of Posts and Telecommunications, Bejing 100876， China;
3. State Key Lab. of Integrated Service Networks, Xidian Univ., Xi′an 710071， China)

Abstract

A new chain verification digital signature scheme based on the discrete logarithm is proposed, which can avoid the equal verifying right of the verifiers which normally accompany the conventional schemes. In this scheme, by means of the sequence secret sharing scheme, the verification participators can divide the signature verifier from the chain grantors, the signature verifier cannot verify the validity of the signature until he is authorized by all chain grantors in turn, and any chain grantor (even all chain grantors are collusive)cannot verify the validity of the signature. What's more, the signature scheme can conveniently add or delete the chain grantor and defend the secret key of the chain grantors and signature verifier.

Key words discrete logarithm digital signature chain verification digital signature

DOI:

通讯作者 贾晓芸 purping@gmail.com

扩展功能
本文信息
Supporting info
PDF(510KB)
[HTML全文](0KB)
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
复制索引
Email Alert
文章反馈
浏览反馈信息
相关信息
本刊中 包含“离散对数”的相关文章
本文作者相关文章
· 贾晓芸
· 罗守山
· 袁超伟