计算机工程 2012, 38(04) 4-6 DOI: 10.3969/j.issn.1000-3428.2012.04.002 ISSN: 1000-3428 CN: 31-1289/TP



博士论文

# 一种应用于双重数字签名的电子拍卖方案

**王秀利，王 萌**

(中央财经大学信息学院，北京 100081)

**摘要：** 针对电子拍卖中存在的身份匿名性等安全问题，基于秘密分享思想，提出一种安全高效的电子拍卖方案。应用双重数字签名，保证投标过程中参与者之间的信息传输安全。投标者采用临时身份投标，标价不直接发送给其他参与者。拍卖服务器根据单调递增函数所计算出的投标值判断中标者，若与注册中心计算结果相符，则投标结果有效。安全性分析结果表明，该方案满足电子拍卖的各项安全性要求，且计算简便、运算效率高。

**关键词：** 电子拍卖 双重数字签名 秘密分享 可信第三方 单调递增函数 投标值

## Electronic Auction Scheme Applied for Double Digital Signature

WANG Xiu-li, WANG Meng

(School of Information, Central University of Finance and Economics, Beijing 100081, China)

Abstract: Aiming at the safety problems of identity anonymity in electronic auction, a safe and efficient scheme is designed based on secret sharing idea, which uses double digital signature to guarantee the safe information transfer among the parties. The bidder is covered by a temporary identity and the bid is send to others indirectly. The auction server can speculate the winner by arranging the figures calculated by a monotone increasing function. If the results from the auction server and the register manager are the same, the winner can be declared. Safety analysis result shows that the proposed scheme is not only secure but also simple and efficient.

Keywords: electronic auction double digital signature secret sharing trusted third party monotone increasing function bid value

**收稿日期** 2011-08-03 **修回日期** **网络版发布日期** 2012-02-20

DOI: 10.3969/j.issn.1000-3428.2012.04.002

**基金项目**:

国家自然科学基金资助项目(60970143,70872120)；教育部科学技术研究基金资助重点项目(109016)；北京市自然科学基金 资助项目(4112053, 9092014)；北京市教育委员会共建专项基金资助项目；中央财经大学“211工程”三期重点学科建设基金资助项目；中央财经大学科研创新团队支持计划基金资助项目

**通讯作者**:

**作者简介**: 王秀利(1977－)，男，博士、CCF会员，主研方向：网络与信息安全，电子商务；王 萌，本科生

**通讯作者**E-mail: xlwang.cufe@gmail.com

**参考文献：**

[3] 韩宝明, 杜 鹏, 刘 华. 电子商务安全与支付[M]. 北京: 人民邮电出版社, 2001.

[4] 王继林, 陈晓峰, 王育民. 一个安全的封闭式电子拍卖协议[J].电子学报.2003, 31(10):1578-1579

扩展功能

本文信息

Supporting info

PDF(244KB)

[HTML] 下载

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

本文关键词相关文章

电子拍卖

双重数字签名

秘密分享

可信第三方

单调递增函数

投标值

本文作者相关文章

王秀利

王萌

PubMed

Article by Wang, X. L.

Article by Wang, M.

[5] 曹 刚. 基于不可信第三方的电子拍卖方案[J].计算机工程.2010, 36(20):140-141 浏览

## 本刊中的类似文章

1. 张韶远, 卢建朱.基于生物特征的鲁棒远程用户认证方案[J]. 计算机工程, 2012,38(3): 137-138
2. 唐俊, 彭敏.一种私钥容侵的数字签名方案[J]. 计算机工程, 2011,37(10): 123-124
3. 李向东;陈 莉;王清贤.离线公平交换协议的子协议分析[J]. 计算机工程, 2010,36(3): 7-9,12
4. 曹刚.基于不可信第三方的电子拍卖方案[J]. 计算机工程, 2010,36(20): 140-141
5. 胡江红, 朱晓宁, 张建中.基于自认证公钥的多重代理签名方案[J]. 计算机工程, 2010,36(19): 159-161,164
6. 刘文远;张 爽.基于签名者隐私保护的公平合同签署协议[J]. 计算机工程, 2009,35(9): 153-154,
7. 刘 晶;伏 飞;肖军模;陆 阳.一种不可否认协议形式化设计方法[J]. 计算机工程, 2008,34(4): 164-166
8. 耿 波;仲 红;彭 俊;王大刚.隐私保护的时序规则分布挖掘[J]. 计算机工程, 2008,34(24): 69-70
9. 王 翠;房礼国;郁 滨.基于恒权码的(2,n)视觉密码方案[J]. 计算机工程, 2008,34(2): 114-116
10. 周菊香;赵一鸣.基于环签名理论的电子拍卖方案[J]. 计算机工程, 2008,34(19): 32-34

## 文章评论

| | | | |
|---|---|---|---|
| 反馈人 | | 邮箱地址 | |
| 反馈标题 | | 验证码 | 4866 |
| | | | |

Copyright by 计算机工程