吉林大学学报(工学版)  2008 38 (04): 886-889  ISSN: 1671-5497  CN: 22-1341/T

# 一种公平的可公开验证的电子拍卖协议

杨加喜1，李磊1,2，朱辉1，王育民1

1.西安电子科技大学 综合业务网国家重点实验室, 西安 710071； 2.郑州大学 信息工程学院，郑州 450052

收稿日期 2007-2-27 修回日期 2007-7-29 网络版发布日期 2008-6-29 接受日期 2007-8-12

摘要 提出了一种公平安全、简单高效的可公开验证电子拍卖协议。该方案采用较多的对称加解密代替公钥体制加解密，克服了第三方和恶意投标者勾结，使恶意投标者以一个最优价赢得投标的缺陷，体现了拍卖的公平性，可以保护投标者的匿名身份，任何投标者不能否认所投的标书, 所有投标价可以公开验证。对比分析表明，该方案满足效率高、易于实施的要求。

关键词 计算机系统结构 电子拍卖 公平性 秘密分享 Hash函数

分类号 TP309. 7

# Publicity verifiable fair electronic auction protocol

YANG Jia-xi1, LI Lei1,2，ZHU Hui1, WANG Yu-min1

1.State Key Lab of Integrated Service Networks, Xidian University, Xi'an, 710071, China;
2.School of Information Engineering, Zhengzhou University, Zhengzhou, 450052, China

**Abstract** A fair and efficient secure electronic auction scheme is presented, which is simple and can be publicly verified. The scheme adopts more symmetric encryption/decryption instead of public key cryptosystem, overcomes the drawback that the third party conspires with a malicious bidder so that he can win the auction with an optimal bidding price, and then provides fairness. The scheme preserves losing bids and bidders's anonymous identities. No bidder can repudiate his or her bid and all the bidding prices can be publicly verified. Compared with the recently proposed schemes, the proposed scheme is more efficient and easily to be implemented.

**Key words** computer systems organization electronic auction fairness secret sharing Hash function

DOI:

通讯作者 王育民 ymwang@xidian.edu.cn

扩展功能

本文信息

- Supporting info
- PDF(487KB)
- [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“计算机系统结构”的 相关文章
- 本文作者相关文章
  - 杨加喜
  - 李磊
  - 朱辉
  - 王育民