

安全技术

基于ElGamal公钥密码体制的电子拍卖协议

周 然, 黄根勋, 魏福山

(解放军信息工程大学理学院数理系, 郑州 450001)

收稿日期 修回日期 网络版发布日期 2007-2-13 接受日期

摘要 提出一种基于分布式ElGamal公钥密码体制的多拍卖物电子拍卖协议。该协议采用无拍卖行的方式对多个物品进行拍卖, 使得整个计算过程仅有投标者参与, 并且根据分布式ElGamal公钥密码体制的特点, 只有当全部合法投标者共同提交自己的子密时, 才能计算出该次拍卖活动的中标价以及中标者, 因而提高了安全性。与以往协议不同, 它不仅适用于一个投标者买一件物品的情况, 也适用于一个投标者买多件物品的情况, 计算量较少, 更适合于实际情况。

关键词 [电子拍卖](#) [分布式ElGamal公钥密码体制](#) [同态性](#) [数字签字](#)

分类号

DOI:

对应的英文版文章: [2007-4-051](#)

通讯作者:

作者个人主页: 周 然; 黄根勋; 魏福山

扩展功能

本文信息

- ▶ [Supporting info](#)
- ▶ [PDF \(327KB\)](#)
- ▶ [\[HTML全文\]\(0KB\)](#)
- ▶ [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“电子拍卖”的 相关文章](#)
- ▶ 本文作者相关文章
 - [周 然](#)
 - [黄根勋](#)
 - [魏福山](#)