

## 安全技术

### 多重代理盲签名分析

王国瞻, 亢保元, 成林

(中南大学数学科学与计算技术学院, 长沙 410075)

收稿日期 修回日期 网络版发布日期 接受日期

**摘要** 多重代理盲签名是代理盲签名的延伸, 被授权的代理签名者代替多个原始签名者进行签名。采用构造方法, 分析一个不需要安全渠道的多重代理盲签名方案的安全性, 结果证明其不安全, 不满足不可伪造性和不可链接性, 不能用于电子商务、电子货币、电子投票等系统。

**关键词** [代理签名](#); [盲签名](#); [多重代理](#)

**分类号** [TN918](#)

**DOI:**

通讯作者:

作者个人主页: 王国瞻; 亢保元; 成林

## 扩展功能

### 本文信息

▶ [Supporting info](#)

▶ [PDF \(74KB\)](#)

▶ [\[HTML全文\]\(0KB\)](#)

▶ [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“代理签名; 盲签名; 多重代理” 的相关文章](#)

▶ [本文作者相关文章](#)