

## 安全技术

### 一种部分盲签名方案

成 林, 亢保元, 王国瞻

(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** 提出一个基于离散对数的部分盲签名方案, 分析其安全性和效率。该方案满足部分盲性、不可追踪性和不可伪造性, 可以防止消息提供者滥用签名, 保证签名者不能侵犯消息提供者的身份隐私。与基于Schnorr签名算法和基于DSA变形签名算法的部分盲签名方案相比, 该方案效率较高。

**关键词** [盲签名](#); [部分盲签名](#); [离散对数](#)

**分类号** [TP309](#)

**DOI:**

通讯作者:

作者个人主页: [成 林](#); [亢保元](#); [王国瞻](#)

## 扩展功能

### 本文信息

▶ [Supporting info](#)

▶ [PDF \(75KB\)](#)

▶ [\[HTML全文\]\(0KB\)](#)

▶ [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“盲签名; 部分盲签名; 离散对数”的 相关文章](#)

▶ [本文作者相关文章](#)