计算机工程 2010 36 (8): 163-164 ISSN: 1000-3428 CN: 31-1289/TP

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