

安全技术

基于双线性对的多消息短签名方案

刘 锋, 胡阳洋

(鲁东大学数学与信息学院, 烟台 264025)

收稿日期 修回日期 网络版发布日期 接受日期

摘要 针对现有的多消息签名方案都需要有一个可信的第三者等问题, 提出一个签名中心对特定用户的多消息签名方案。该方案基于双线性运算, 引入t弹性的消息独立技术, 当客户需要同时对多个消息的数字签名时, 该签名中心能够同时签署多个消息, 得到的多个签名的有效性可以被一次性(公开)验证, 并给出方案的安全性证明。

关键词 [多消息签名](#); [短签名](#); [双线性对](#); [可证安全](#); [密钥独立](#)

分类号 [TN918](#)

DOI:

通讯作者:

作者个人主页: [刘 锋](#); [胡阳洋](#)

扩展功能

本文信息

- ▶ [Supporting info](#)
- ▶ [PDF\(88KB\)](#)
- ▶ [\[HTML全文\]\(0KB\)](#)
- ▶ [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“多消息签名; 短签名; 双线性对; 可证安全; 密钥独立”的 相关文章](#)
- ▶ [本文作者相关文章](#)