

安全技术

3个秘密共享方案的弱点分析与改进

张建中, 屈娟

(陕西师范大学数学与信息科学学院, 西安 710062)

收稿日期 修回日期 网络版发布日期 接受日期

**摘要** 通过对秘密共享的研究与分析,发现现有的秘密共享方案几乎都有其弱点,导致这些方案不能在实际中得到应用。分析3个秘密共享方案,指出它们各自存在的安全漏洞,并通过系统初始化、秘密份额生成和验证、秘密承诺生成和恢复等对刘锋等人的方案(计算机应用研究,2008年第(1)期)进行改进。结果表明,改进后的方案克服了原有方案的缺点,是一个安全的可验证的秘密共享方案。

**关键词** [秘密共享](#); [主动攻击](#); [欺诈](#); [可验证](#)

**分类号** [TP309](#)

**DOI:**

通讯作者:

作者个人主页: [张建中;屈娟](#)

扩展功能

本文信息

- ▶ [Supporting info](#)
- ▶ [PDF](#)(318KB)
- ▶ [\[HTML全文\]](#)(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“秘密共享; 主动攻击; 欺诈; 可验证”的 相关文章](#)
- ▶ [本文作者相关文章](#)