

软件技术与数据库

随机数发生器探讨及一种真随机数发生器实现

宋 勇, 陈贤富, 姚海东

(中国科学技术大学电子科学与技术系, 合肥 230027)

收稿日期 修回日期 网络版发布日期 2007-1-9 接受日期

摘要 高质量随机数在信息安全中具有重要的应用。该文利用双重随机思想, 基于真随机源对一个高质量伪随机数发生器进行参数重置, 同时对该伪随机数发生器产生的随机数的特定二进制位进行采样从而获得0-1序列, 将之填充到一个整数单元, 归一化后作为输出。分析表明, 该真随机数发生器具有良好的性能。

关键词 [真随机数发生器](#) [信息安全](#) [双重随机](#)

分类号

DOI:

通讯作者:

作者个人主页: [宋 勇](#); [陈贤富](#); [姚海东](#)

扩展功能

本文信息

- ▶ [Supporting info](#)
- ▶ [PDF \(127KB\)](#)
- ▶ [\[HTML全文\]\(0KB\)](#)
- ▶ [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“真随机数发生器”的相关文章](#)
- ▶ [本文作者相关文章](#)
- ▶ [宋 勇, 陈贤富, 姚海东](#)