

安全技术

基于PDA的高效真随机密钥生成系统

肖攸安, 周祖德

(武汉理工大学信息工程学院, 武汉 430070)

收稿日期 修回日期 网络版发布日期 2007-6-15 接受日期

摘要 为满足基于PDA的移动电子商务等应用的需求, 针对现有高质量密钥生成方法的速度慢、效率低的问题, 提出了一种高效随机密钥生成方法, 设计了一个基于PDA的高效密钥生成系统。按照FIPS 140-2标准中的规定对由该系统产生的随机密钥的质量进行了测试和分析。说明该系统能快速产生具有高质量的、满足信息安全系统标准的高强度安全密钥, 特别适用于基于PDA的移动电子商务、电子政务等环境, 具有很好的实用价值。

关键词 [定点设备](#) [密钥](#) [信号源](#) [真随机密钥](#)

分类号 [TP393.08](#)

DOI:

对应的英文版文章: [45](#)

通讯作者:

作者个人主页: 肖攸安;周祖德

扩展功能

本文信息

- ▶ [Supporting info](#)
- ▶ [PDF\(194KB\)](#)
- ▶ [\[HTML全文\]\(0KB\)](#)
- ▶ [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“定点设备”的 相关文章](#)
- ▶ 本文作者相关文章
 - [肖攸安](#)
 - [周祖德](#)