

安全技术

基于Logistic映射的混沌流密码设计

王化丰¹, 张桂香², 邵 勇³

(1. 大连理工大学电信学院, 大连 116023; 2. 齐齐哈尔大学计算中心, 齐齐哈尔 161005; 3. 北京工业大学软件工程学院, 北京 100022)

收稿日期 修回日期 网络版发布日期 2007-5-17 接受日期

摘要 混沌系统特有的一些优良属性较适合流密码的设计, 比如混沌迭代序列对初始条件和控制参数的敏感性、伪随机性、混和性和确定性等。该文以Logistic映射为例说明了其主要特性和初值敏感性, 并重点图示了在字节输出方式和比特输出方式下, 其离散分布和均匀分布的差异和改善。

关键词 [流密码](#) [伪随机性](#) [混沌](#) [Logistic](#)

分类号 [TP309](#)

DOI:

对应的英文版文章: [071055](#)

通讯作者:

作者个人主页: 王化丰¹;张桂香²;邵 勇³

扩展功能

本文信息

▶ [Supporting info](#)

▶ [PDF\(145KB\)](#)

▶ [\[HTML全文\]\(0KB\)](#)

▶ [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“流密码”的 相关文章](#)

▶ 本文作者相关文章

· [王化丰](#)

· [张桂香](#)

· [邵 勇](#)