计算机工程　2007 33 (10): 164-165,168　ISSN: 1000-3428　CN: 31-1289/TP

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下和比特输出方式下，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