计算机工程　2008 34 (8): 1-3　ISSN: 1000-3428　CN: 31-1289/TP

博士论文

基于新复合混沌动力系统的加密算法

佟晓筠1，崔明根2，杨天龙1

(1. 哈尔滨工业大学计算机科学与技术学院，威海 264209；2. 哈尔滨工业大学理学院，威海 264209)

收稿日期　修回日期　网络版发布日期 2008-4-10　接受日期

摘要　提出两个新型混沌映射，并基于Devaney定义给出了严格混沌的理论特性证明。利用复合离散混沌系统的特性，提出基于两个新型混沌映射设计的复合离散混沌系统的序列密码算法，该映射产生的具有均匀分布函数量化后可生成具有平衡性质的0-1序列。 复合离散混沌系统均匀的不变分布还使密文具有很好的随机特性，由于迭代对初始条件的敏感性和迭代函数选择的随机性，密钥、明文与密文之间形成了复杂而敏感的非线性关系，而且密文和明文的相关度也很小，可以有效地防止密文对密钥和明文信息的泄露。分析表明，该系统具有很高的安全性并扩大了密钥空间。

关键词　混沌；复合非线性动力系统；加密算法

分类号　TP391

DOI:

对应的英文版文章：080802

通讯作者:

作者个人主页: 佟晓筠1;崔明根2;杨天龙1