

安全技术

基于多个Logistic映射的分组加密算法

王 永<sup>1,2</sup>, 李盛竹<sup>1</sup>, 杜茂康<sup>1</sup>, 罗龙艳<sup>1</sup>, 杨德刚<sup>2,3</sup>

(1. 重庆邮电大学经济管理学院, 重庆 400065; 2. 重庆大学计算机科学与工程学院, 重庆 400044; 3. 重庆师范大学数学与计算机科学学院, 重庆 400047)

收稿日期 修回日期 网络版发布日期 2007-10-11 接受日期

**摘要** 分析了设计加密算法时应该注意的问题, 并在此基础上, 提出了一种基于多个logistic映射的分组加密算法。该算法中使用了多个混沌映射, 有效地扩展了其密钥空间。加密过程中, 子密钥序列以密文反馈和从混沌映射中抽取数据相结合的方式产生, 这使子密钥序列在保持良好的均匀分布和随机统计特性的同时, 还与明文相关, 有效地增强了算法的安全性。理论分析和模拟试验表明, 该加密算法具有加密速度快, 保密性好等优点。

**关键词** [混沌; 分组加密; 密码系统; 安全](#)

**分类号** [TP309](#)

**DOI:**

对应的英文版文章: [072051](#)

通讯作者:

作者个人主页: 王 永<sup>1,2</sup>; 李盛竹<sup>1</sup>; 杜茂康<sup>1</sup>; 罗龙艳<sup>1</sup>; 杨德刚<sup>2,3</sup>

扩展功能

本文信息

- ▶ [Supporting info](#)
- ▶ [PDF \(229KB\)](#)
- ▶ [\[HTML全文\]\(0KB\)](#)
- ▶ [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“混沌; 分组加密; 密码系统; 安全 ”的 相关文章](#)
- ▶ 本文作者相关文章
  - [王 永](#)
  - [李盛竹](#)
  - [杜茂康](#)
  - [罗龙艳](#)
  - [杨德刚](#)