

- >> 首页
- >> 被收录信息
- >> 投稿须知
- >> 模板下载
- >> 信息发布
- >> 常见问题及解答
- >> 合作单位
- >> 产品介绍
- >> 编委会/董事会
- >> 关于我们
- >> 网上订阅
- >> 友情链接

友情链接

- >> 中国期刊网
- >> 万方数据资源库
- >> 台湾中文电子期刊
- >> 四川省计算应用研究中心
- >> 维普资讯网

基于双混沌映射的文本hash函数构造*

Novel hash function construction based on double chaotic maps

摘要点击: 20 全文下载: 10

[查看全文](#) [查看/发表评论](#) [下载PDF阅读器](#)

中文关键词: [混沌](#) [hash函数](#) [Logistic映射](#) [斜帐篷映射](#)

英文关键词: [chaos](#) [hash function](#) [Logistic map](#) [skew tent map](#)

基金项目: 国家自然科学基金资助项目(60873201, 60703035); 重庆市自然科学基金资助项目(2009BB2211); 重庆大学研究生科技创新基金资助项目(200903A1B0010303)

作者

单位

[康小培¹](#), [李艳涛¹](#), [邓绍江¹](#), [冯艳茹²](#) (1. 重庆大学 计算机学院, 重庆 400044; 2. 济源职业技术学院 计算机系, 河南 济源 454650)

中文摘要:

提出了一种基于混沌Logistic映射和斜帐篷映射的文本hash函数算法。该算法将明文信息分组并转换为相应的ASCII码值, 然后把该值作为Logistic映射的迭代次数, 迭代生成的值作为斜帐篷映射的初始值进行迭代, 然后依据一定的规则从生成值中提取长度为128 bit的hash值。通过仿真对该算法的单向性、混乱与扩散、碰撞等性能进行分析, 理论分析和仿真实验证明该算法可以满足hash函数的各项性能要求。

英文摘要:

This paper proposed a novel hash function construction based on chaotic Logistic map and skew tent map. Set the proposed algorithm divided the message into groups and then changed groups into their corresponding ASCII codes which were used for the iteration times of Logistic map. Set the generated values of Logistic map as the initial values of the skew tent map, and finally generated hash value with length of 128 bit according to the rules. Studied the one-way hash function, diffusion, confusion and collision of the algorithm by simulation. Theoretical analysis and computer simulation indicate that the proposed algorithm can satisfy the performance requirements of hash function.

您是第2828125位访问者

主办单位: 四川省计算机研究院 单位地址: 成都市武侯区成科西路3号

服务热线: 028-85249567 传真: 028-85210177 邮编: 610041 Email: arocmag@163.com

蜀ICP备05005319号 本系统由北京勤云科技发展有限公司设计