计算机工程　2008 34 (8): 132-134　ISSN: 1000-3428　CN: 31-1289/TP

安全技术

基于双密钥的对称加密方案

徐江峰，赵 峰

(郑州大学信息工程学院，郑州 450001)

收稿日期　修回日期　网络版发布日期 2008-4-11　接受日期

摘要　在对混沌加密和传统加密特性进行分析的基础上，该文提出一个基于双密钥的对称加密方案，该方案通过一个对密钥极其敏感的函数及一个公开的动态密钥，可以实现类似于“一次一密”的加密目标。给出一个基于Lorenz混沌系统的实现方案，理论分析和实验结果表明，该方案可以提高传统加密方案的安全性能，并且实现简单。

关键词　双密钥；混沌；对称加密；敏感函数

分类号　TP309

DOI:

对应的英文版文章：080853

通讯作者:

作者个人主页: 徐江峰;赵 峰