计算机工程与应用 2008 44 (16): 83-86 ISSN: 1002-8331 CN: 11-2127/TP

研发、设计、测试

基于FPGA的DES加密芯片的设计

蒋存波, 孙朝华, 杜婷婷, 陈 铭, 程小辉

桂林工学院，广西 桂林 541004

收稿日期 2008-1-17 修回日期 2008-4-21 网络版发布日期 2008-5-25 接受日期

摘要 通过对DES加密原理的分析，推导出了DES的算法公式，通过对算法中核心部分的数学分析和化简，借助Verilog语言与C语言编程以及EDA设计软件的帮助，实现了DES算法的FPGA条件下的重构设计，同时对密钥的动态管理提出了新的设计方案。最后，通过对设计结果的功能仿真和测试分析，论证了整个设计过程的正确性。

关键词 DES FPGA Verilog语言 C语言

分类号

Hardware design of DES algorithm based on FPGA

JIANG Cun-bo,SUN Chao-hua,DU Ting-ting,CHEN Ming,CHENG Xiao-hui

Guilin University of Technology，Guilin，Guangxi 541004，China

Abstract

This paper introduces the basic principles of the DES encryption system，achieves the optimum FPGA reconstructing design on the DES with the help of giving the algorithm of DES encryption under the Verilog language and the C language conditions and the effective dealing with the key issues.Then it gives a new dynamic management design programme of the keys.Finally，the results of the design function simulation and test analysis show that the design of the whole thesis has higher practical significance and value.

Key words Data Encryption Standard（DES） FPGA Verilog language C language

DOI:

通讯作者 蒋存波 sunchaohua1976@163.com

扩展功能

本文信息

Supporting info

PDF(718KB)

[HTML全文](0KB)

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

复制索引

Email Alert

文章反馈

浏览反馈信息

相关信息

本刊中 包含“DES”的 相关文章

本文作者相关文章

- 蒋存波
- 孙朝华
- 杜婷婷
- 陈 铭
- 程小辉