云南大学学报(自然科学版)
JOURNAL OF YUNNAN UNIVERSITY(NATURAL SCIENCES)
中文核心期刊
中国科技核心期刊

云南大学学报(自然科学版) » 2009, Vol. 31 » Issue (6): 576-579 DOI:

SHA-224/256复用IP核的设计与实现

郭跃东, 杨军, 黄道林

云南大学信息学院, 云南昆明 650091

The design and implementation of the multiplexing SHA-224/256 IP cores

GUO Yue-dong, YANG Jun, HUANG Dao-lin

School of Information Science and Engineering, Yunnan University, Kumming 650091, China

- 摘要
- 参考文献
- 相关文章

全文: PDF (954 KB) HTML (1 KB) 输出: BibTeX | EndNote (RIS) 背景资料

摘要 以SHA-224与SHA-256算法的相似性为基础,设计了一个可时分复用的SHA-224/256IP核.该设计采用并行结构与流水线技术,在简化硬件设计的同时,提高了该IP核的运行速度(速度提高26%).最终以Altera的EP2C20F484C6芯片为下载目标,其时序仿真可正常运行在100MHz的时钟频率下,该IP核可广泛应用于信息安全领域.

关键词： FPGA SHA-224/256 IP核

Abstract： In this paper,we designed a time-division multiplexing SHA-224/256 IPcore based on the algorithm's similarity.The IPcore used parallel structure and pipeline technology to simplify the hardware designing and improved the speed of the IPcore.Finally we implemented the IPcore in Altera's EP2C20F484C6 FPGA.We also gave the result of timing simulation which demonstrates the IPcore can run under the 100MHz frequency.This IPcore could be widely used for digital signature system and double-key system of 3DES.

Key words:

收稿日期: 2008-12-26;

通讯作者: 杨军(1963-)男,云南人,副教授,主要从事计算机体系结构、EDA技术方面的研究.

服务
- 把本文推荐给朋友
- 加入我的书架
- 加入引用管理器
- E-mail Alert
- RSS

作者相关文章
- 郭跃东
- 杨军
- 黄道林

引用本文:

郭跃东,杨军,黄道林. SHA-224/256复用IP核的设计与实现[J]. 云南大学学报(自然科学版), 2009, 31(6): 576-579 .

$author.xingMing_EN,$author.xingMing_EN,$author.xingMing_EN. The design and implementation of the multiplexing SHA-224/256 IP cores[J]. , 2009, 31(6): 576-579 .

没有本文参考文献

[1] 董寅 杨军 唐佐侠. 基于SOPC的Twofish加/解密单元的设计与实现[J]. 云南大学学报(自然科学版), 2011, 33(4): 397-401, .

编辑出版：云南大学学报编辑部 (昆明市翠湖北路2号, 650091)
电话：0871-5033829(传真) 5031498 5031662 E-mail: yndxxb@ynu.edu.cn yndxxb@163.com