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) » 2012, Vol. » Issue (1): 33-38 DOI:

一种片上可配置安全网络适配器的设计与实现

张伟平, 赵嘎, 舒平平, 杨军

云南大学 信息学院, 云南 昆明 650091

The design and implementation of a configurable security network adapter on chip

ZHANG Wei-ping, ZHAO Ga, SHU Ping-ping, YANG Jun

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

- 摘要
- 参考文献
- 相关文章

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

摘要 为了满足当前高速网络传输处理中安全性与实时性的要求,以AES-128/192/256算法为基础,设计了一种采用流水可重构技术的AES加/解密IP核,并通过SOPC技术将该IP核、Nios II处理器、网络控制器等功能模块与外围设备进行集成,实现了一个可根据具体应用资源多少与安全系数要求而灵活配置的片上网络适配器.本设计采用硬件描述语言VHDL设计,利用Quartus Ⅱ8.0进行了综合与布线,最后在DE2实验平台上进行下载测试验证.整个设计硬件结构简单、安全性高、运行速度快、灵活性强,可被广泛应用于网络信息安全领域.

关键词： 网络适配器 AES SOPC Nios Ⅱ IP核

Abstract： To meet the requirements for real-time and security of high-speed network transmission in the current,we designed a kind of AES encryption/decryption IP core based on AES-128/192/256 algorithm and using pipeline reconfigurable structure in this paper.Meanwhile,this IP core,the Nios Ⅱ processor,the network controller,including other function modules and the corresponding peripherals are integrated by SOPC technology,implementing a network adapter on chip can according to specific application resources and safety demand to configuration flexible.The design uses hardware description language VHDL,and layout and wire on Quartus Ⅱ8.0.Finally the system is downloaded to DE2 for testing.The design hardware structure is simple,security,high-speed,flexibility,which can be widely used in the field of network information security.

Key words： network adapter AES SOPC Nios Ⅱ IP Core

收稿日期: 2011-04-25;

基金资助:云南大学2010年度研究生优秀教材建设基金项目经费的资助.

通讯作者: 杨 军(1963-),男,云南人,教授,硕士生导师,主要从事EDA及计算机系统结构的研究.

引用本文:

张伟平,赵嘎,舒平平等. 一种片上可配置安全网络适配器的设计与实现[J]. 云南大学学报(自然科学版), 2012, (1): 33-38.

ZHANG Wei-ping,ZHAO Ga,SHU Ping-ping et al. The design and implementation of a configurable security network adapter on chip[J]. , 2012, (1): 33-38.

[1] 秋小强,蔡觉平.网络处理器高速AES协处理器设计[J].计算机应用,2007,27(12):2 957-2 959.

[2] 丁俊,李娜,杨军.面向Avalon总线的AES-128/192/256 IP核的设计与实现[J].电子测量技术,2010(8):70-73.

[3] 董演,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):379-401.

[4] 贾旭,李兴.AES算法的可配置硬件结构的设计与实现[J].电子技术应用,2009(11):132-134.

[5] 付勇,智刘琳.可重构平台下AES算法的流水线性能优化[J].单片机与嵌入式系统应用,2009(6):23-24.

[6] 王简瑜,张鲁国.基于FPGA的AES加/解密算法可重构设计[J].计算机工程,2008,34(7):163-164.

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
- 张伟平
- 赵嘎
- 舒平平
- 杨军

[7] 刘泽文,唐柳春.基于SOPC的安全网络适配器设计与实现[J].计算机工程,2008,34(14):246-247.

[8] 陈小毛,陈尚松.32位软核处理器NIOS Ⅱ的以太网接口设计[J].电子测量技术,2007,30(1):150-151.

[9] 时建雷,肖铁军.面向LwIP的Nios Ⅱ网络驱动程序开发[J].微计算机信息,2008,24(2):36-38.

[10] 刘航,戴冠中,李晖晖,等.一种用于IPSec协议的AES算法可配置硬件实现[J].小型微型计算机组成,2005,26(12):2 082-2 086.

[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, .

[2] 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 .

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