云南大学学报（自然科学版），2012，34（1）：33～38　　CN 53－1045/N　ISSN 0258－7971
Journal of Yunnan University　　http://www.yndxxb.ynu.edu.cn

一种片上可配置安全网络适配器的设计与实现*[1]

张伟平，赵　嘎，舒平平，杨　军
（云南大学 信息学院，云南 昆明　650091）

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
中图分类号：TP 309.7　　**文献标识码**：A　　**文章编号**：0258－7971(2012)01－0033－06

随着网络通信技术的飞速发展，人们对数据传输过程中的安全性和实时性的要求也越来越高，从技术角度讲，网络安全除了依赖安全的网络通信协议及应用协议外，更多地取决于网络设备如交换机、路由器、网卡等所提供的加/解密功能，因此开发具备实时处理、安全可靠的加/解密处理器成为网络信息安全的关键. 目前网络处理器缺少可自定义扩展的加/解密功能，大多数网络安全芯片是一种实现固定加密方式的专用芯片，难以满足不同用户多层次的安全性能和硬件资源的需求，从而带来了效率和安全方面的不足. 因此，近些年来许多研究机构都致力于可重构、可配置技术的研究，大大提高了芯片的灵活性、扩展性和高效性. SOPC 就是近几年兴起的一种具有很强的灵活性和可配置性的可编程片上系统技术，由单个芯片完成整个系统的主要逻辑功能，从而提高整体抗干扰能力、降低设计成本.

AES 是密码学中的高级加密标准，算法具有密钥长、抗差分能力强、易于硬件实现、成本低、速度快等优点. 为提高网络数据传输的安全性，同时满足高速网络传输实时性的要求，基于软件方式的加/解密便显得性能不足，需要采用硬件来实现高速加/解密处理[1]. AES 硬件加/解密方式可采用并行流水的优化技术，极大地提高数据的流量并减少密钥的生成时间，使加/解密效率明显提高；另外，用硬件对传输中的数据进行加/解密处理，整个过程封装在芯片内，不易被外部攻击者读取或更改，有较高的物理安全性.

本文以 AES－128/192/256 算法为基础[2]，采用流水可重构技术，设计了一种可时分复用的 AES IP 核，并利用硬件加/解密在网络传输处理方面的优势，结合 SOPC 技术方便快捷和可灵活配置的特点[3]，扩展了本系统在高速网络安全方面的应用，实现一种片上可配置安全网络适配器.

1　核心算法简介

AES（Advanced Encryption Standard）是密码学中的高级加密标准，又称 Rijndael 加密法，是美国联邦政府采用的一种区块加密标准[4]，其基本思想是采用对称分组密码体制. AES－128/192/256 算法相似，唯一的区别是密钥长度及其对应的迭代轮数，当密钥长度为 128，192 或 256Bits 时，迭代轮

* **收稿日期**：2011－04－25
基金项目：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.
作者简介：张伟平（1987－），男，福建人，硕士生，主要从事 FPGA 嵌入式系统及网络安全方面的研究.
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.

数 N_r 分别为 10,12 和 14 轮.

AES 算法包含加/解密算法和密钥扩展算法. 加密过程每轮包括字节替代变换、行移位变换、列混合变换和轮密钥异或变换,算法经过 N_r 轮迭代,其中最后一轮不做列混合变换. 解密过程与加密过程相似,只是各个环节采用了逆变换. 加/解密算法中所用的子密钥相同,每一轮都需要一个扩展密钥的参与,但是使用顺序刚好相反. 由于外部输入的加/解密密钥长度有限,所以 AES 算法中需要一个密钥扩展算法以生成各轮所需的加/解密密钥. AES 加/解密流程如图 1 所示.

1.1 字节替代变换 字节替代变换也称 S 盒变换,是一种可逆的非线性变换,它对每一个字节根据给定的 S 盒/反 S 盒转换表进行置换.

1.2 行移位变换 该变换是一个字节换位,它将状态中的行按照不同的偏移量进行循环移位如式(1)所示,解密则做反向移位变换.

$$\begin{bmatrix} A0,A1,A2,A3 \\ B0,B1,B2,B3 \\ C0,C1,C2,C3 \\ D0,D1,D2,D3 \end{bmatrix} \xrightarrow{\text{行移位变换为}} \begin{bmatrix} A0,A1,A2,A3 \\ B1,B2,B3,B0 \\ C2,C3,C0,C1 \\ D3,D0,D1,D2 \end{bmatrix}. \tag{1}$$

1.3 列混合变换 列混合变换是对状态中矩阵逐列进行基 2 特征的伽罗瓦域运算,其加/解密变换分别如式(2)、(3)所示.

$$\begin{bmatrix} b0 \\ b1 \\ b2 \\ b3 \end{bmatrix} = \begin{bmatrix} 2,3,1,1 \\ 1,2,3,1 \\ 1,1,2,3 \\ 3,1,1,2 \end{bmatrix} \begin{bmatrix} a0 \\ a1 \\ a2 \\ a3 \end{bmatrix}, \tag{2}$$

$$\begin{bmatrix} b0 \\ b1 \\ b2 \\ b3 \end{bmatrix} = \begin{bmatrix} E,B,D,9 \\ 9,E,B,D \\ D,9,E,B \\ B,D,9,E \end{bmatrix} \begin{bmatrix} a0 \\ a1 \\ a2 \\ a3 \end{bmatrix}. \tag{3}$$

1.4 轮密钥异或变换 在轮密钥异或变换中,状态的变换通过与一个轮密钥进行逐位异或而得到,其逆变换为自身.

2 AES IP 核设计

IP 核设计中介绍了几个重要模块的设计,限于篇幅,比较简单的模块不再赘述.

2.1 S 盒变换模块 S 盒变换是该算法硬件实现时的重要环节,在整个算法中占用了比较大的资源,本设计中,采用近年来对 AES S 盒硬件实现的改进策略,将查找表的内容存储到 FPGA 内部的存储器中,根据输入字节的数值进行快速的查表操作,避免了传统设计使用 CASE 语句描述而占用大量的逻辑资源. 同时该设计让加/解密共用一个 S 盒模块,将 S 盒和逆 S 盒设计成一个可重构处理单元,然后在处理单元内部增加了一个可控节点,使它即能用于加密又能用于解密.

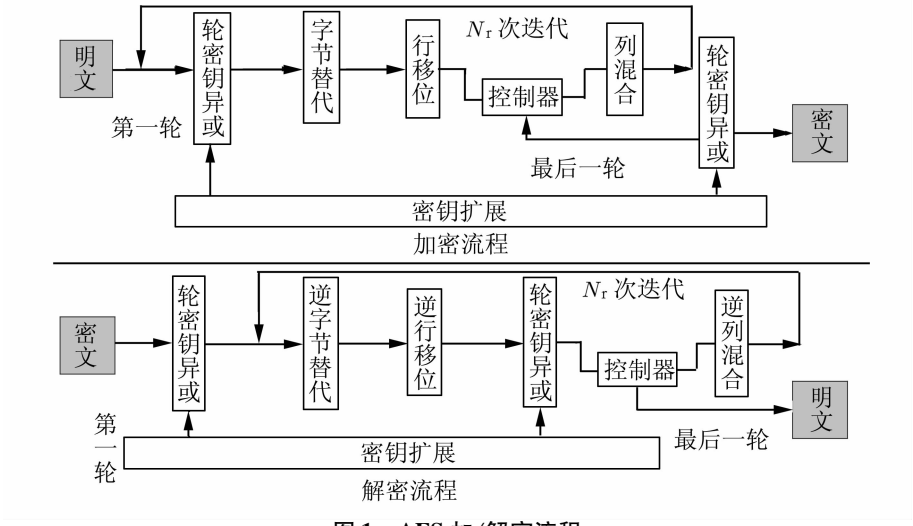

图 1 AES 加/解密流程

Fig. 1 AES encryption/decryption process

2.2　可配置密钥扩展模块　分析 AES 3 种密钥长度的密钥扩展算法可知,128,192Bit 的密钥生成圈函数都可视为 256Bit 密钥生成圈函数的一部分[5],因此可以将 3 种密钥扩展算法设计为一个可配置的共用模块. 本设计以 256Bit 密钥生成算法圈函数为基础,在其内部添加了 1 个控制单元 R,通过控制指令选择路径,即可改变内部结构及和其它模块的连接关系,从而灵活匹配不同类型的密钥算法. 密钥扩展算法的可配置结构设计如图 2 所示.

2.3　流水线优化设计　根据以上对 AES 算法的分析可知,该算法前 N_r-1 轮迭代包括 4 种完全相同的变换,因此为提高数据吞吐率,本设计采用轮间流水线技术对该 IP 核进行了优化,如图 3 所示. 该设计将整个加密过程按各加密轮划分为前后相连的多级实体,并在各级流水间插入寄存器存储上一级执行结果,这样每一级在一个时钟周期内完成一级数据处理,然后在下一个时钟到来时将处理后的数据传递给下一级,使得一个时钟周期内能同时处理多个数据块的加密,从而提高并发程度,该结构理论的加密速率是迭代结构的 12 倍[6].

在该 IP 核设计中,AES 加/解密可被归结为同一个计算流程,因此在实现过程中可共用相同的控制资源,如状态机资源、中间结果寄存器以及密钥生成模块等[7],同时 S 盒的重用设计和 3 种密钥生成算法模块的集成,使得该 IP 核所消耗的硬件资源大大减少;另外,本设计中利用了 S 盒的改进策略和流水优化技术,使得加/解密速率也大大提升.

3　片上安全网络适配器的设计

随着半导体技术飞速发展,电路规模越来越大,可编程片上系统(SOPC)已经成为 IC 设计的发展趋势. SOPC 支持灵活的定制功能和系统升级,可根据用户功能需求快速地进行扩充或裁减相应的 IP Core,不但开发周期短且无需改变硬件版图设计. 因此,采用 SOPC 技术,使得片上网络适配器的设计方便快捷、功能灵活、可重构性强[8].

3.1　系统硬件框架　本系统定制了一个 32 位的 Nios Ⅱ软核 CPU,将上述自定义的 AES IP 核和网络控制芯片 DM9000A 挂到 Avalon 总线上,同时将必要的外围电路和处理器集成在一块芯片上,构成完整的片上系统. 整个系统的硬件结构框架如图 4 所示.

通过 SOPC Builder 工具,运用组件化的方式进行硬件设计,可以很快在 FPGA 上构建一个嵌入式系统[9-10]. 系统主要包括以下功能模块:

(1) 定制 Nios Ⅱ软核 CPU　Nios Ⅱ具有 32 位

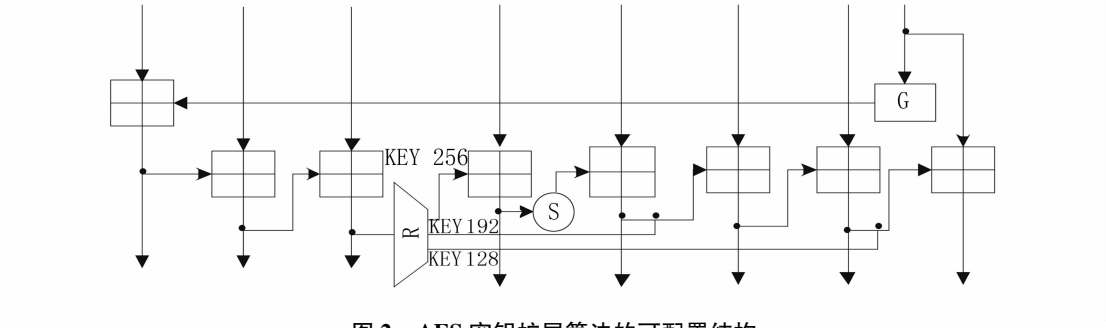

图 2　AES 密钥扩展算法的可配置结构

Fig. 2 The design of AES key expansion configurable structure

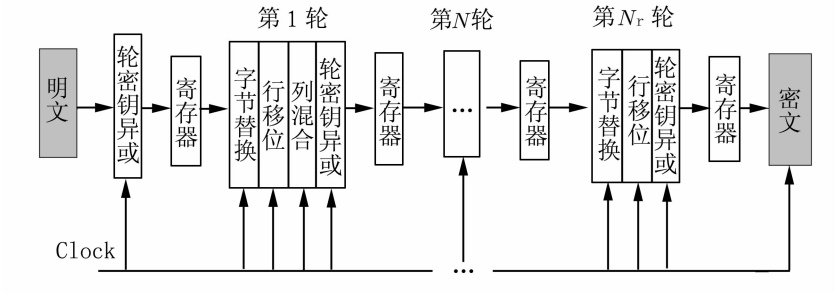

图 3　AES 算法流水线结构

Fig. 3 AES pipeline line structure

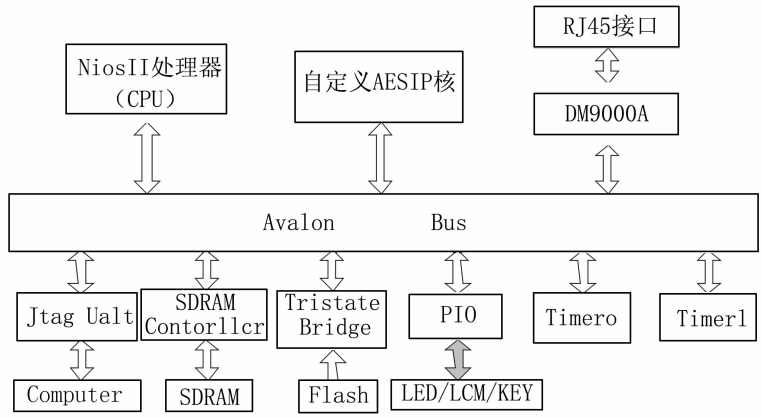

图4 系统硬件结构

Fig. 4 System hardware structure

数据线宽度,2GB 寻址空间,丰富的调试工具,并支持硬件断点、数据触发以及片外和片内的调试跟踪. 本系统选择 Nios Ⅱ/f 全功能 CPU 核,4KB 指令缓冲器,并将指令数据宽度配置为 32 Bits,主要完成链路的连接和控制以太网接口与 AES IP 核接口之间的数据传输,负责对整个系统进行管理和控制;

(2) 自定义 AES 加/解密 IP 核 处理从输入端和接收端进来的数据,经加/解密模块后正确的存放到存储器中以供后续的处理,加密模块负责对向网络发送的数据帧加密,解密模块负责对从网络接收到的数据帧解密;

(3) 网络控制模块 设计用户接口电路与 DM9000A 连接,并设定 DM9000A 为 Avalon 总线的从器件,通过 Avalon 总线与 Nios Ⅱ系统相连,实现高速以太网通信;

(4) 其它功能子模块 JTAG UART 核实现基于 FPGA 的嵌入式系统与主机之间的串行符号流通信;SDRAM 用来在系统运行时的程序和数据存储;Flash 主要用来存放软件代码以及一些需要保存的参数;LED、LCM 和按键 KEY 用来指示工作状态、显示数据和系统复位;Timer 0 操作系统使用的定时器和 Timer 1 网络协议栈使用的定时器.

3.2 系统软件设计 运行 SOPC Builder 定制的硬件系统,然后利用 Nios Ⅱ IDE 针对系统的硬件平台开发相应的应用软件,实现网络通信模块的软件设计. 本系统的软件平台采用 MicroC/OS Ⅱ嵌入式操作系统,使用 LwIP 网络协议栈,利用 C 语言和系统所带的 API 函数,针对所使用的 DM9000A 芯片,设计其在 LwIP 下的驱动程序,在此基础上开发特定功能的网络通信程序. 最后在完成底层函数构建和应用程序设计后,即可通过在网络接口与以太网上的 PC 机连接,实现该网络适配器中传输数据的加/解密. 系统模型如图 5 所示.

图5 系统模型图

Fig. 5 System model figure

4 系统测试

本设计在 Quartus Ⅱ 8.0 平台上进行综合,并利用 ModelSim 做了功能仿真,最后以 DE2 开发板作为测试平台进行下载验证.

4.1 综合 表 1 给出了 AES IP 核 3 种密钥长度分别所消耗逻辑单元数、占用的存储资源以及最大的工作频率,综合表明当密钥加长的同时虽然提高了加密的安全性但也消耗了更多的资源. 在实际当中应该根据具体情况选择合适安全系数等级,以发挥 IP Core 的最佳性能.

4.2 仿真 图 6 是对该网络适配器在实时传输中的数据加/解密进行的功能仿真,仿真时钟频率为 97.6 MHz,在此只给出密钥长度为 256 位的仿真结果(其它情况相似). 在仿真波形中,输入 256 位的密钥:49C12E59_5B727361_24472915_43162051_40162224_14816C51_292315D3_4A317423,测试数

表 1　综合结果

Tab. 1 The results of synthesis

密钥长度/位	逻辑单元数	存储资源/Bits	实际运行频率/MHz
256	3 568	39 027	108.64
192	3 394	39 027	129.82
128	3 187	39 027	151.32

据 128 位: 9A852465 _ 5359C257 _ 23B13338 _ 2811A356, 运行的加密结果为: CDD32741 _ 8370D117_279C0876_83A1F975. 从仿真波形中可知测试结果与理论的加/解密结果安全一致,该片上系统在功能与时序上都达到了预期的目的.

本设计对系统核心功能模块 AES IP 核进行了优化,从系统测试的结果可以看到,该系统可正常运行在 97.6 MHz 的时钟频率下,数据吞吐量达到 592.3 Mb/s,实现的处理速度接近单一算法的专用芯片[11],同时相比于同类设计在运行速度和资源消耗方面也有较大的提升. 测试结果比较如表 2 所示.

表 2　测试结果比较

Tab. 2 Compared with the test results

设计方案	逻辑单元数	存储资源/Bits	吞吐量/(Mb · s^{-1})
本设计	3 568	3 9027	592.3
同类设计[4]	3 235	40 960	396.7
专用芯片[10]	2 085	77 824	610.0

5　结　语

本文将流水线和可重构技术有效地结合起来,设计了一个可灵活配置的 AES IP 核,并结合 SOPC 技术成功定制了一个片上安全网络适配器,能够满足当前高速网络中不同用户多层次的安全性能和硬件资源的需求. 该片上系统较好地兼顾了资源和速度两方面的性能,充分体现了硬件加/解密的安全性和实时性,以及 SOPC 技术的灵活性和可配置性,整个设计具有硬件结构简单、资源消耗低、可靠性高、灵活性强、速度快、性价比突出的显著特征,具有良好的应用前景.

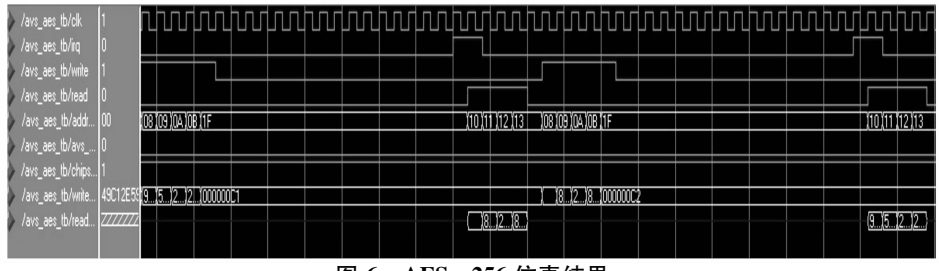

图 6　AES – 256 仿真结果

Fig. 6 The results of AES – 256 simulation

参考文献:

[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] Fips – 197, advanced encryption standard[S]. National Institute of Standards and Technology (NIST),2001.

[5] 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.

[6] 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.

[7] 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.

[8] 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.

[9] 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.

[10] 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.

[11] 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.

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)

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 Ⅱ 8.0. 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

* *

(上接第32页)

An approach of basing-on fuzzy-grey noncooperative Nash games to multi-team dynamic weapon-target assignment

ZHANG Yi[1], JIANG Qing-shan[2], CHEN Guo-sheng[1]
(1. Brigade of Graduate Student's, Naval Aeronautical and Astronautical University, Yantai 264001, China;
2. Department of Command, Naval Aeronautical and Astronautical University, Yantai 264001, China)

Abstract: Aiming at the uncertainties in weapon-target assignment (WTA), a kind of oppositive multi-team dynamic WTA (MT-DWTA) problem is studied. Firstly, the oppositive MT-DWTA model is built. Secondly, with distance discount factor (DDF) and fuzzy-grey target relative value and team Nash pair of strategies, a model of MT-DWTA is formed basing on fuzzy-grey noncooperative Nash games. And then the MT-DWTA model is transformed into quadratic programming problem. Finally, a kind of genetic algorithm (GA) and ant colony optimization (ACO) with cyclic multiexchange (CME) heuristic algorithm is designed to solve a more large-scale MT-DWTA problem, and the simulation result shows that new algorithm can solve it in a short time.

Key words: weapon-target assignment; Nash games; algorithm; distance discount factor; target relative value; team Nash pair of strategies