中国农业大学学报 2003,8(4):33～35
Journal of China Agricultural University

GIDC-C 密码算法芯片的研制与开发

薛一鸣
(中国农业大学 信息与电气工程学院,北京 100083)

摘 要 GIDC-C 密码算法芯片适用于计算机网络安全领域,该芯片采用超大规模集成电路工艺,是集 CPU、加解密运算部件、存储器等为一体的 SOC 芯片。采用了自顶向下的设计方法,重点讨论了芯片的总体实现方案及 CPU,RSA,DES 等模块的内部结构,分析了功耗、可靠性、仿真等设计难点及解决办法。仿真和物理验证的结果表明,所设计的电路工作正常,运行稳定可靠。1 024 bit 的 RSA 加/解密速率为 5 次·s^{-1},DES 加/解密速率达 2 Mbit·s^{-1},达到了设计的要求。

关键词 CPU; SOC; 加密
中图分类号 TN 492 **文章编号** 1007-4333(2003)04-0033-03 **文献标识码** A

Design of chip based on cryptogrammic arithmetic

Xue Yiming
(College of Information and Electrical Engineering, China Agricultural University, Beijing 100083, China)

Abstract GIDC-C was designed for computer network. Fabricated with very large scale integration technology, the chip is a soc which include CPU,RSA,DES module. The top-down design methodology was adopted. The ASIC scheme and detailed structure of CPU,RSA,DES were presented. Power consumption, reliability and simulation is analyzed. The result of simulation and verification validates that the circuit works stably and reliably. The Encryption rate was reached to 5 times per second for RSA and 2 Mbit per second for DES.

Key words CPU; SOC; encryption

随着信息技术的发展,电子商务、网上银行,网络通讯等的出现,人们的生活与网络越来越密不可分,而利用网络盗窃他人财产,窃取商业机密,以及黑客攻击等网络犯罪也日益增多。现代网络技术需要高性能的信息安全产品,为人们提供一个安全、可靠的信息平台。

正是基于这种需求,笔者研究设计了 GIDC-C 密码算法芯片。该芯片利用 SOC(system on a chip)片上系统技术,采用超大规模集成电路工艺,将拥有自主版权的 CPU 及自主开发的 RSA,DES 加解密算法部件集于一体,可以实现身份认证,数据加解密,数字签名与验证等。它可为我国电子商务、银行在线交易、身份认证和安全电子邮件等网络应用领域提供可靠的安全保证。

1 芯片设计方案

1.1 设计目标

根据市场需求并结合国外同类产品的特点,制定了具体的设计目标:

1) 高度安全的体系结构。

2) 具有较大的存储空间且支持在线编程。

3) 支持非对称加密算法 RSA,实现数字签名、验证、身份识别等。

4) 支持对称加、解密方式,实现 DES 和三重 DES;支持电子密本(ECB)方式和密码分组链接(CBC)方式。

5) 支持 USB1.1 协议规范,实现高速 I/O 接口功能。

收稿日期:2002-12-07
基金项目:国家 863 计划项目(2001AA141030)资助
作者简介:薛一鸣,副教授,主要研究方向为大规模集成电路设计

1.2 设计方法与策略

设计采用 SOC 技术[1],即将 CPU,RSA,DES 及存储器等集成在一块硅片上。与多芯片系统相比,采用 SOC 技术设计的系统级芯片特征尺寸减小,因此大大降低了成本,提高了速度,减小了系统功耗。更重要的是,系统级芯片只有少数引脚外露,系统的可靠性和安全性提高。

采用自顶向下(top-down)的设计方法[2]建立系统的行为模型,用硬件描述语言[3](Verilog HDL)进行电路的寄存器传输级描述,最后利用专门的综合工具将描述的电路转化为实际的门级网表。与传统的设计方法相比,采用自顶向下设计方法使设计者专注于系统级的设计,大大提高了工作效率,降低了专用集成电路的设计风险。

1.3 总体结构

GIDC-C 芯片采用模块化设计方法,主要由 CPU 模块、RSA 模块、DES 模块,存储器和 USB 模块组成,其中存储器由 SPRAM,DPRAM 和 FLASH 组成。系统设计了 2 套总线:RSA 模块、DES 模块和 USB 联接于 I/O 总线,SPRAM,DPRAM 和 FLASH 共享存储器总线。系统通过 USB 和 DPRAM 与外电路连接。由于 FLASH 具有面积小、数据非易失性并可重复擦写的特点,所以选择 128 K×16 bit 的 FLASH 作为程序存储器。数据存储器包括 4 K×16 bit SRAM 和 4 K×16 bit DPRAM。USB 采用 IP 复用技术,利用成熟的 USB IP 核,以缩短研发周期。

1.4 CPU模块结构

CPU 模块是系统的核心,其结构见图 1。

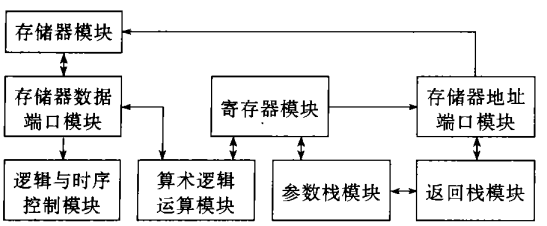

图 1 CPU 结构框图

Fig. 1 Structure of CPU core

1)算术逻辑运算模块。CPU 的主要部件,其中包括自主开发的单拍乘、单拍乘累加、开方等高速运算硬部件,可完成各种复杂运算,实现各种算法。

2)参数栈模块。包括栈顶寄存器和物理栈,运用映象技术将栈顶寄存器和物理栈融为一体,数据处理方便快捷。

3)返回栈模块。实现各种寻址方式,并支持中断现场的自动保护。

4)寄存器模块。包括数据寄存器和控制寄存器:数据寄存器用于运算结果的存取,设有单拍乘寄存器、开方根寄存器和乘除寄存器等;控制寄存器包括程序指针寄存器 PC、中断允许寄存器和中断屏蔽寄存器。

5)存储器数据模块和存储器地址模块。生成存储器地址和控制信号,实现存储器与 CPU 内核的数据交换,并可完成字符比较和断点设置等功能。

6)逻辑与时序控制模块。CPU 的控制中枢,经指令译码后产生控制时序,并实现中断响应和中断嵌套控制。

设计了独特的指令系统。指令中设置了数据选择、运算选择、参数栈和返回栈动作、移位判断等多控制域,在逻辑与时序控制模块的协调下,实现了多域并行执行的功能,指令执行效率高。

1.5 RSA 模块结构

RSA 模块为 1 024 bit 的非对称加解密运算部件,采用全硬件结构,所有的加/解密运算,包括中间数据的保存和传送,均由专门的硬部件完成,从而实现了高效高速。RSA 模块主要包括:

1)除法单元、模值单元、段积累加器单元。这是 RSA 的核心部分,采用自适应流水结构,对数据进行分割并逐段处理。

2)控制逻辑单元。采用自适应的控制逻辑,根据实际数据(包括运算过程产生的中间数据)的长度,自动控制各个子循环的长度和流水线的级数。

3)输入输出寄存器单元。这是 RSA 模块和 CPU 模块的输入输出接口部件。

1.6 DES 模块结构

DES 模块包括:

1)基本 DES 模块。完成单重 DES 加/解密算法,包括密钥生成,IP 转置,IP^{-1}转置,16 轮加密与解密电路。

2)输入输出接口模块。输入输出模块分别实现 DES 模块与 CPU 之间的接口,包括明文和密钥的输入,密文数据的输出。

3)逻辑控制模块,将基本 DES 运算的结果反馈至输入模块,重复调用,从而实现三重 DES 加解密。

4)反馈模块。实现密码分组链接(CBC)方式和电子密本(ECB)方式。

2　电路验证

2.1　设计与仿真

系统设计与仿真流程见图 2,共分为 4 个阶段:

1)行为级建模及仿真,采用行为级描述语言建立各模块及系统的行为级模型,确保系统设计的可靠性。尤其是 RSA 和 DES 算法部件尚没有电路可以参考,所以必须建立起可靠的行为级模型,才能保证设计的可行性。

2)寄存器传输级建模及仿真。用硬件描述语言建立各模块的寄存器传输级模型并进行仿真验证。

3)电路综合及前仿真。按照对芯片功耗、频率、面积的约束,进行电路的综合和优化,将电路由抽象的描述转换为门级网表。前仿真考虑了电路的门延迟,因此比行为级仿真和寄存器传输级仿真更加严格。

4)后仿真。后仿真是在布局布线完成后,提取了布局布线的阻容特征参数进行的仿真,因此后仿真的模型即为实际芯片的模型。必须保证后仿真的正确才可以投片。

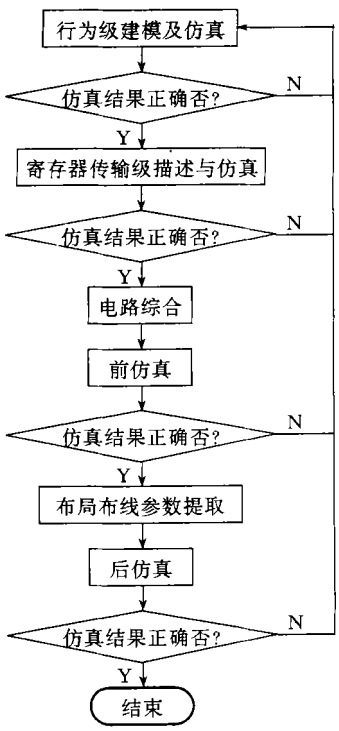

图 2　系统设计流程

Fig. 2　Design flow chart of the system

2.2　物理验证

采用 FPGA 芯片对设计电路进行功能验证是芯片设计不可缺少的环节,利用 FPGA 芯片可在实际工作环境中进行大数据量检测。该器件具有高密度、高速度硬件单元及连续布线结构,另外还设有嵌入式阵列(EAB),能满足本系统在规模和寄存器方面的特殊要求。

物理验证实测 1 024 bit 的 RSA 加/解密速率为 5 次·s^{-1},DES 加/解密速率达 2 Mbit·s^{-1},达到了系统设计的要求。

3　电路设计难点

在 GIDC-C 密码算法芯片的设计过程中存在几个技术难点。

1)功耗问题。巨大的功耗给芯片正常工作及封装带来不利影响,必须解决此问题。主要的解决方法是:采用空闲(Idle)模式,使主要部件的触发器时钟在没有任务的情况下不翻转,有效降低了时序逻辑的功耗;主要运算部件的输入端设置多路选通器,使加解密运算模块的乘除部件在无加解密运算的情况下保持其输入不变,从而降低组合逻辑的功耗;优化逻辑结构,缩小电路规模。

2)可靠性问题。由于芯片包括数字电路、模拟接口(USB 接口)和存储器等,它们的制造工艺不同,且工作频率较高,可靠性问题越来越突出。主要的解决办法是:在布局布线后进行串扰分析;设计看门狗电路监视芯片状态,故障情况下实现自动复位;关键信号,如存储器的读、写信号,设计去毛刺电路等。

3)仿真问题。研发过程中,芯片需经过行为级仿真、寄存器传输级仿真、前仿真和后仿真等严格的仿真验证。由于仿真数据量极大,采用人工波形比较的方式势必影响研究的进展。为此,建立了专门的验证平台,将仿真预期结果事先存入文件,然后将系统程序和运算数据自动加载至存储器,同时通知 CPU 启动加/解密部件执行加/解密过程。运算结束后,自动读出运算结果,并与预期结果比较,输出正确或错误标志。整个验证过程无需人工干预。

4　结　论

成功开发了具有自主版权的 16 bit CPU,1 024 bit RSA 及 DES 加/解密部件,实现了集 CPU,RSA,DES,USB 及 SRAM,DPRAM 和 FLASH 为一体的 SOC 系统,其主要特点为:

(下转第 62 页)

```
glBegin();
  glVertex3f(x,y,z);
glEnd();
```

可以生成如图 4 的网格面,同时由:

```
glColor4f(r,g,b,a);
glNormal3f(x,y,z);
glTexCoord2f(u,v);
```

可定义仿真水面的颜色、真实感纹理和表面矢量来生成具有真实感的动态仿真水面(图 5)。

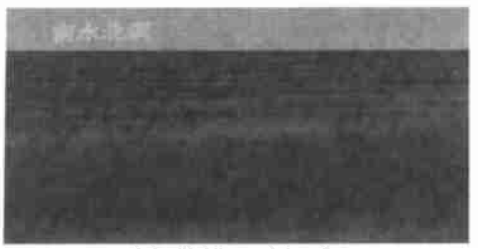

图 5 真实感水面

Fig. 5 Reality water surface

3 结束语

利用基于水波动理论建立的动态网格模型,能够对模拟水面进行较好的控制,并减少计算量,最终形成的虚拟场景中仿真水面较为逼真,效果较好,并能满足水力学仿真的需要。但因为波浪的形成比较复杂,又有各种随机因素的影响,本文中所论述的模型及其实现条件都是在理想情况下进行的。随着计算机图形处理技术的不断提高,以及有关水动力现象和参数研究的不断完善,用计算机模拟出更加逼真的三维动态虚拟水环境是完全可能的。

参 考 文 献

[1] Peachy D. Modeling waves and surf[A]. Proceedings of SIGGRAPH86[C],Louisana:ACMSIGGRAPH,1986. 65～74

[2] Foumier A, Reeves W. A simple model ocean waves[A]. Proceedings of SIGGRAPH86[C], Louisana: ACMSIGGRAPH,1986. 75～84

[3] Ts'o. p, Barsky B. Modeling and rederi waves[J]. ACMT Ransactions on Graphics, 1987,6(3):191～214

[4] Michael E, Goss A. Real time particle system for display of ship waakes[J]. IEEE Computer Graphics & Applications,1990,272(7):30～35

[5] Michl K, Gavin M. Rapid, stable fluid dynamics for computer graphics[J]. Computer Graphics, 1990, 24(4):49～54

[6] 曾芬芳,黄建国. 虚拟海洋场景中波浪的模拟[J]. 计算机应用,2000,21(4):33～36

[7] 孙家广. 计算机图形学[M]. 北京:清华大学出版社, 1994. 262～331

(上接第 35 页)

1) 采用面向安全的体系结构,通过 USB 和 DPRAM 与外电路接口,内部总线不外露。

2) 自主开发了 16 bit 的栈式结构 CPU 及其指令系统。

3) 支持对称和非对称加/解密,实测 1 024 bit 的 RSA 加/解密速率为 5 次·s^{-1},DES 加/解密速率达 2 Mbit·s^{-1}。

严格的软件仿真和物理验证结果表明,系统工作稳定,性能可靠,速度快;达到了设计要求。目前,GIDC-C 密码算法芯片已通过验收,并已开始投片生产。

参 考 文 献

[1] JozWiak L. Quality-driven system on a chip design[J]. IEEE 2000 First International Symposium on Quality Electronic Design, 2000,6(3):93～102

[2] 王志华,邓仰东. 数字集成系统的结构化设计与高层次综合[M]. 北京:清华大学出版社,2000:80～101

[3] 夏宇闻. 复杂数字电路与系统的 Verilog HDL 设计技术[M]. 北京:北京航空航天大学出版社,1998:18～30