可信平台模块中16位微处理器FPGA实现与验证

朱文军
ZHU Wen-jun

北京工业大学 计算机学院,北京 100022
College of Computer Science,Beijing University of Technology,Beijing 100022,China
E-mail:zhuwenjun@bjut.edu.cn

ZHU Wen-jun.FPGA implementation and validation of 16-bit microprocessor of trusted platform module.Computer Engineering and Applications,2008,44(26):80-82.

Abstract: The core of trusted computing framework is a kind of trusted chip named as Trusted Platform Module(TPM).In this paper,a novel design method has been proposed,which tries to design independently microprocessor and instruction set inside TPM based on FPGA,in order to guarantee chip's security from the bottom layer.As a feasibility research,a 16-bit microprocessor with relatively perfect instruction set has been designed and realized.To validate its maneuverability,the output interface modules for the T6963C LCD and 4-bit dynamic common cathode numeral tubes have been also designed separately.As a result,the run-time result of programs can be displayed directly.The higher security and extensibility can be obtained due to the instruction set being designed independently,which will accumulate certain experiences for the development of secure microprocessor in the future.
Key words: Trusted Platform Module(TPM);Field Programmable Gate Array(FPGA);microprocessor;output interface

摘 要:可信计算框架的核心是称为可信平台模块(Trusted Platform Module)的可信芯片。提出一种新型设计理念,尝试在FPGA芯片上自主设计TPM内部的微处理器及指令系统,从最底层保证芯片安全性。作为先期可行性研究,设计实现了具有相对完善的指令系统的16位微处理器,为了验证其对外围设备接口的可操作性,针对内藏T6963C液晶屏和4位动态共阴数码管分别设计出相应输出接口模块,使程序执行结果得到直观的显示。由于指令系统完全自主设计,具有较高的安全性和可扩展性,为将来安全微处理器的研制也积累了一定的经验。
关键词:可信平台模块;现场可编程门阵列;微处理器;输出接口
DOI:10.3778/j.issn.1002-8331.2008.26.024 **文章编号:**1002-8331(2008)26-0080-03 **文献标识码:**A **中图分类号:**TP309

1 引言

目前,可信计算得到了学术界和产业界的高度关注。可信计算框架主要是通过增强现有的终端体系结构的安全性来保证整个系统的安全。其主要思路是在各种终端(包含PC、手机以及其它移动智能终端等)硬件平台上引入可信架构,通过其提供的安全特性来提高终端系统的安全性。在可信计算技术体系中,最核心的就是称为可信平台模块(Trusted Platform Module,TPM)的可信芯片[1]。

以TPM为基础的"可信计算"由几个方面构成:用户的身份认证是对使用者的信任;平台完整性,体现了使用者对平台运行环境的信任;应用程序的完整性,体现了应用程序运行的可信;平台之间的可验证性,体现了网络环境中终端之间的相互信任[2]。

可信平台模块TPM是一个可信硬件芯片,而且是一种SOC(System on Chip)芯片[3-4],可以看作是一个完整的计算机。它由CPU、存储器、I/O、密码运算处理器、随机数产生器和嵌入式操作系统等部件组成。完成可信度量的存储、可信度量的报告、密钥产生、加密与签名,以及数据安全存储等功能。

目前复杂的SOC芯片通常由设计人员利用各现场可编程逻辑器件厂商提供的知识产权(IP)核心库高效准确地设计完成。作为现场可编程逻辑器件的典型代表,现场可编程门阵列(Field Programmable Gate Array,FPGA)是近年来发展迅速的大规模可编程专用集成电路(ASIC)。可编程ASIC器件的使用,使设计的电子产品达到小型化、集成化和高可靠性,而FPGA器件的现场可编程技术使可编程器件在使用上更为方便,并大大缩短了设计周期,减少了设计费用,降低了设计风险。由此导致多数厂商投入相当大的财力、物力专注于FPGA芯片的IP软核研发。虽然这些IP核心库都是预定义的、经过测试和验证的、优化的、可保证正确功能的IP软核,但从TPM芯片应具备高度安全性能的角度进行分析,IP核所提供的指令系统及硬件架构,包括其硬件核心技术仍然由各IP软核设计厂商掌握。为了防范这种潜在的不安全因素,本文提出一种新型设计理念,尝试在FPGA芯片上自主设计TPM内部的微处理器及指令系统,从最底层保证芯片安全性。作为这种设计思想的先期

作者简介:朱文军(1974-),男,博士,讲师,主要从事计算机系统结构及组成原理的研究和教学工作。
收稿日期:2007-11-14 **修回日期:**2008-02-05

可行性研究,本文设计实现了具有相对完善的指令系统的 16 位微处理器,其中包括运算器、控制器、寄存器组等模块的开发,同时在此基础上,进行了存储器的设计,并针对内藏 T6963C 液晶屏和 4 位动态共阴数码管分别设计出相应输出接口模块,最终通过 JTAG 接口下载到 Altera 公司的 FPGA 芯片 EP1C6Q240C8 上,使得存储器中的程序执行结果能够直观地显示在液晶屏和数码管上,初步证实了微处理器对外围设备接口的可操作性,为后续研发奠定了坚实的基础。由于指令系统完全自主设计,具有较高的安全性和可扩展性,为相关领域中安全微处理器的研制也积累了一定的经验。

2　16 位微处理器的设计与实现

一般 FPGA 的开发大体有如下几个步骤:设计输入–功能仿真–代码综合–实现–下载。其中最重要的显然是设计部分,产品的功能就是在设计上体现出来的;而仿真主要针对设计,采用 EDA 工具进行波形仿真,只有波形仿真通过才能说明设计的正确性与合理性;综合主要是将用 HDL 语言所作的硬件描述对应到 FPGA 芯片上的单位逻辑电路上;实现是将综合后生成的逻辑网表与具体的 FPGA 相适配;最终生成的位流文件通过特定的下载途径下载到 FPGA 中[5]。

按照上述开发流程,本文在 Altera 公司的 Quartus II 软件平台下,将绘制硬件原理图及编写 Verilog HDL 语言[6]两种方法有机结合在一起,首先设计实现了 16 位微处理器及其指令系统,为了进行指令正确性验证,进行了存储器的设计开发,形成了一台微型计算机主机。以下分别从中央处理器 CPU 的设计、指令系统的设计和主存储器的设计三方面来阐述其设计思想和实现过程。其中各组成模块的隶属关系如图 1 所示。

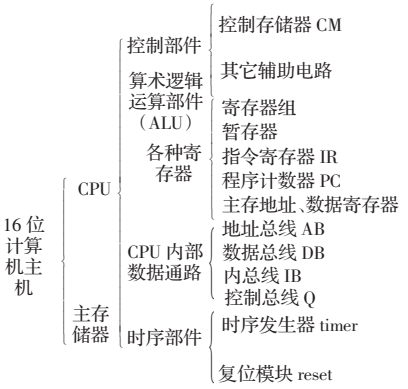

图 1　16 位微型计算机主机的组织结构

2.1　中央处理器 CPU 的设计

中央处理器 CPU 的主要功能是从主存储器中取出指令,解释指令和执行指令,即按指令控制计算机各部件操作,并对数据进行处理。本主机的 CPU 由算术逻辑运算部件、CPU 内部寄存器、CPU 内部数据通路、时序发生器、复位模块和控制部件共 6 部分组成。

(1)算术逻辑运算部件 ALU 的设计,基本仿照 74181 芯片的运算功能,采用 Verilog HDL 语言编写。

(2)CPU 内部寄存器包括通用寄存器组、暂存器、指令寄存器、程序计数器及实现 CPU 与存储器或 I/O 接口之间信息传输的一些专用寄存器。本主机共设有 8 个 16 位通用寄存器以及 3 个暂存器,完成 CPU 内部重要数据的存储,同时利用 16 位的指令寄存器存放正在执行的指令代码的前两个字节。考虑到 CPU 与存储器之间的信息传输,还设计实现了主存地址寄存器 MAR,并运用 Verilog HDL 语言合理实现了具有双向输入输出功能的主存数据寄存器 MDR。

(3)CPU 内部数据通路采用 16 位双向单总线结构,并利用地址总线、数据总线以及控制总线完成与存储器以及 I/O 接口间的通信。

(4)根据本主机的特点,为了在整机系统设计过程中尽量发挥出机器数据通路的并行性,设计了相应的时序发生器。时序发生器提供一个微周期中的 9 个电平及脉冲控制信号,可供整机设计时使用。其中 clk 是外部时钟脉冲输入管脚,在整机中它的值不能小于 13 ns;halt 管脚为低电平时,则使时序发生器停止工作。产生的时序信号分布如图 2 所示。

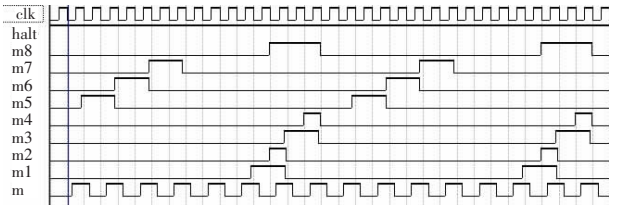

图 2　时序发生器产生的时序

(5)复位模块运用 Verilog HDL 语言编程实现,其功能是根据复位信号 RESET 产生持续 4 个微周期的 halt 低电平信号,来使时序发生器暂停工作,同时完成一些关键寄存器和计数器的初始化任务。

(6)本主机采用微程序控制原理,其控制部件主要由 7 个模块组成:控制存储器 CM、微程序计数器 uPC、微地址形成电路 PLA、微地址返回寄存器 uART、微指令寄存器 uIR、地址/命令区分电路 addrororder、微指令译码电路 decoder。通过这些部件的配合,可以在 CM 内部灵活地实现微子程序转移及返回,有效地利用了 CM 空间。

2.2　指令系统的设计

本主机的指令系统基本参照 Intel8086/8088 较规整的指令代码格式[7]进行设计,采用可变长操作码的形式,指令通常由 2~6 个字节组成,共设计实现了 3 种格式的指令:双操作数指令、单操作数指令以及面向输出接口的指令。其中,双操作数指令包含操作特征、寻址特征、立即数和位移量 4 个字段;单操作数指令仅包含操作特征和相应数据两个字段;面向输出接口的指令主要包括液晶屏初始化指令 INIT 和输出指令 OUT,指令长度分别为 52 Byte 和 30 Byte,用来完成液晶屏的预置、清屏以及输出工作。指令集相对完善,涵盖了常用的数据传送类指令、算术运算类指令、无条件转移指令及条件转移指令,还提供输出接口的控制指令,基本满足小型应用环境的需求。

2.3　存储器的设计

存储器 RAM 中存储将要执行的一系列机器指令以及数据。存储器与 CPU 间进行数据传输主要通过地址总线 AB 和数据总线 DB。存储器的核心部件采用 Quartus II 中的内部元件 lpm_ram_dq 芯片构成,采用读、写双时钟控制方式。其数据宽度为 16 bit,存储单元个数为 2^8=256 个,因此存储空间为 16×256=4 096 bit。同时,通过 Verilog HDL 语言编写了模块,用于实现对 RAM 单元的字或字节访问,并且在三态控制信号 RAM–DB 的控制下将 RAM 的数据输出到数据总线上。

3 输出接口模块的设计与实现

为了验证上述微型计算机主机的可操作性，在 GX-EDA/SOPC 综合实验仪上进行了相应输出接口模块的设计。该实验仪上配备的 T6963C 液晶显示控制器以内藏控制器型图形液晶显示模块的形式出现。T6963C 是点阵式液晶显示控制器，它能直接与 80 系列的 8 位微处理器接口，可以图形方式、文本方式及图形和文本合成方式进行显示，以及文本方式下的特征显示，还可以实现图形拷贝操作等等。T6963C 的内部具有字符发生器 CGROM，共有 128 个字符，可以管理 64 K 显示缓冲区及字符发生器 CGRAM，并允许 MPU 随时访问显示缓冲区，甚至可以进行位操作。除此之外，实验仪上还配备有 6 位动态共阴数码管，用 SS0、SS1、SS2 三个开关来控制某一时刻某一位数码管的显示。

针对 T6963C 液晶控制器的操作规程和动态共阴数码管的特点，设计了两个接口模块：输出接口译码电路 output_decoder 和数码管译码电路 led_decoder。输出接口译码电路主要有以下三个功能：第一，完成液晶屏初始化工作；第二，完成液晶屏显示工作；第三，传送给数码管译码电路待显示的十六进制数据。

数码管显示输出接口包括两部分：数码管译码电路 led_decoder 和数码管动态扫描模块。数码管译码电路主要实现数据译码工作和数码管的位数选择工作；数码管动态扫描模块实现对 4 位动态共阴数码管进行扫描，使数据连续不断地显示在指定数码管上。

INIT 和 OUT 指令是唯一与输出接口有关的指令。INIT 指令的作用是完成液晶屏的初始化工作，并将显示指针移到指定位置；OUT 指令的作用是在液晶屏上显示出：from XX 地址：XX 数据 H；并在第 0~3 位数码管上显示出：XX 数据。数码管上的数据和液晶屏上的数据保持一致。OUT 指令不但能够显示来自任意地址的内容，而且还支持字/字节操作。

4 下载及调试

下载采用的芯片是嵌在 GX-EDA/SOPC 综合实验仪上的 Cyclone 系列 EP1C6Q240C8 芯片，通过连接计算机并行接口 LPT 的数据线实现 JTAG 下载。下载之前，先要进行管脚分配和连线工作，然后进行下载设置。

首先利用 Quartus II 软件的布局布线工具 Assignment Editor 对相关的输入输出管脚进行分配。进行完管脚分配并编译通过后，利用 Quartus II 软件的编程工具 Programmer 进行下载，下载时要确保 GX-EDA/SOPC 综合实验仪打开。最终，16 位微型计算机主机及输出接口模块整体封装及管脚分配效果如图 3 所示。

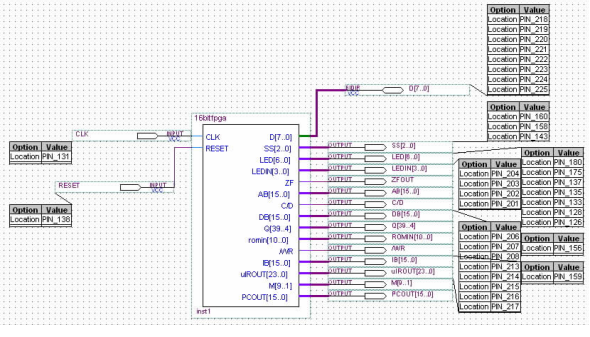

图 3 16 位微型计算机主机整体封装及管脚分配连线图

16 位计算机主机下载到 EP1C6Q240C8 芯片上后，还要进行繁杂的调试工作。这里的调试不再基于 EDA 仿真平台，而是在真正的人机接口电路中。在 GX-EDA/SOPC 综合实验仪上将 RESET 信号连接到多功能复用按键 F12 上，通过与自主设计的复位模块相连，实现了正常的主机复位工作。通过波形仿真验证以及实际硬件操控后，从存储器 0002H 地址单元取出相应内容 87edH，送到输出接口显示的最终执行效果如图 4 所示。图中 LCD 显示内容为：from 0002H：87edH。

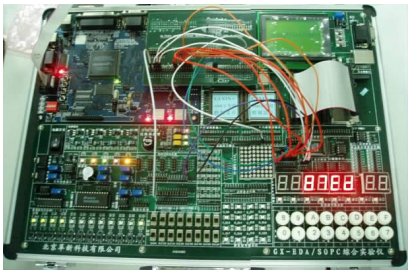

图 4 16 位微型计算机主机的实际执行结果

5 结论

基于可信平台模块需要具备高度安全性的特点，本文提出一种新型设计理念，尝试在 FPGA 芯片上自主设计 TPM 内部的微处理器及指令系统，从最底层保证芯片安全性。作为这种设计思想的先期可行性研究，本文在 EDA 平台上设计实现了具有相对完善的指令系统的 16 位微处理器，其中包括运算器、控制器、寄存器组等模块的开发，同时在此基础上，进行了存储器的设计，并针对内藏 T6963C 液晶屏和 4 位动态共阴数码管分别设计出相应输出接口模块，最终通过 JTAG 接口下载到 Altera 公司的 FPGA 芯片 EP1C6Q240C8 上，使得存储器中的程序执行结果能够直观地显示在液晶屏和数码管上，初步证实了该微处理器对外围设备接口的可操作性，为后续研发奠定了坚实的基础。由于指令系统完全自主设计，具有较高的安全性和可扩展性，为相关领域中安全微处理器的研制提供了相关借鉴。针对目前实现的微处理器具有的工作主频较低等弱点，后期还需进一步改进，并进行密码运算处理器等方面的研发。

参考文献：

[1] 张旻晋.从终端到网络的可信计算技术[J].信息技术快报，2006，4(2)：20-31.

[2] The Trusted Computing Group.TCG PC Specific Implementation Specification，2003.

[3] 张焕国.一种新型嵌入式安全模块[J].武汉大学学报：理学版，2004，50(S1).

[4] 张焕国.一种新型安全计算机[J].武汉大学学报：理学版，2004，50(S1).

[5] 孙富明，李笑盈.基于多种 EDA 工具的 FPGA 设计[J].电子技术应用，2002，28(1)：70-73.

[6] 王金明.Verilog HDL 程序设计教程[M].北京：人民邮电出版社，2004.

[7] 俸远祯.计算机组成原理与汇编语言程序设计[M].北京：电子工业出版社，2004.