

基于 FPGA 的智能卡控制器的实现

马峰,徐和根,赵曼

(同济大学 电子与信息工程学院,上海 201804)

摘要: 尝试在 FPGA 上实现对 IC 卡的控制,运用 EDK 中的 IP 开发工具生成一个智能卡控制器的 IP 核,用以实现对 IC 卡的硬件控制。

关键词: IC 卡;IP;FPGA

中图分类号: TN409

文献标识码: A

文章编号: 1674-7720(2013)01-0020-03

Realization of smart card controller based on FPGA

Ma Feng, Xu Hegen, Zhao Man

(School of Electronic and Information Engineering, Tongji University, Shanghai 201804, China)

Abstract: This paper try to realize control of IC card on FPGA. It generates an IP core to control the IC card with the IP generator in EDK.

Key words: IC card; IP; FPGA

智能卡 (Smart Card) 又称集成电路卡 (Integrated Circuit Card), 即 IC 卡, 目前大量使用的交通卡、门禁卡、银行支付卡等都是智能卡。智能卡接口控制器是连接智能卡和主控设备的桥梁, 是智能卡处理设备中的重要组成部分之一。面对巨大的市场需求, 越来越多的公司、科研机构都在研究此类控制器。

FPGA 具有可重构性、开发周期短以及开发流程简单等优点, 越来越多的工程师选择将 FPGA 作为工程设计的首选。由于其内嵌微处理器, FPGA 在嵌入式方面也获得了大量的运用。此外, 为缩短产品面市时间, FPGA 厂商还会提供多种知识产权 (IP) 核。这类 IP 核可以作为功能模块运用在不同的设计中, 方便了各种开发的推进。本文尝试在 EDK 中开发一个新的 IP 核, 其功能就是实现对 IC 卡的接口控制。

1 用卡过程

正常的用卡过程可划分为几个阶段: (1) 将 IC 卡插入到接口设备 IFD (Interface Device), 并接通各触点; (2) 对 IC 卡进行复位, 在终端和 IC 卡间建立通信; (3) 执行交易; (4) 释放触点并取出 IC 卡。

2 字符的物理传送

交易过程中, 数据以异步半双工方式经 I/O 线在终端和 IC 卡之间双向传送。由终端向 IC 卡提供时钟信

号, 并以此来控制交易的时序。

数据在 I/O 线上以字符帧传送, 一个字符帧包含着 10 个相连的数位: 1 bit 状态为低 (L) 的起始位、8 bit 组成的数据字节和 1 bit 偶校验位, 如图 1 所示。

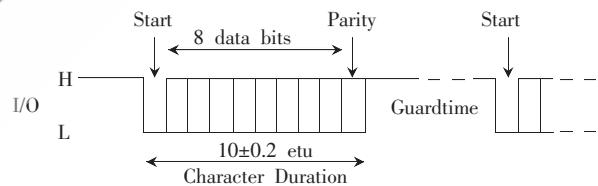


图 1 字符帧格式

3 IP 核的设计

智能卡一般都遵循 ISO7816 通信协议, 因此, 该 IP 核的逻辑设计主要遵循 ISO7816 协议。

3.1 IP 核的整体设计

本 IP 核的整体设计模块如图 2 所示。图 2 中, AFIFO (异步) 的作用主要是接收来自 PLB 总线或 Device Controller 的命令、地址和数据等。由于总线的工作频率与 Device Controller 的工作频率不一致, 故此 AFIFO 不可省略。

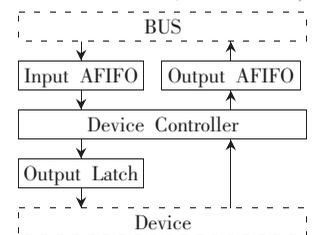


图 2 IP 核设计框图

Input AFIFO 接收来自总线的命令、地址和数据等,依次存储在 FIFO 中(深度为 16 bit),Device Controller 则读取该 FIFO 中数据,并进行相应的操作。

Output AFIFO 用于接收 Device (智能卡)返回的数据,并将其传输给总线。

Output Latch 的作用是进行状态缓存与命令缓存,主要是为了满足相关时序的要求。

Device Controller 是设计的核心环节,它主要有以下功能特征:

- (1) 参数的传递以及协议的设定;
- (2) 时钟频率的转换;
- (3) 功能的激活;
- (4) 时钟的停止;
- (5) 功能的释放;
- (6) 复位;
- (7) 应用协议数据单元 APDU (Application Protocol Data Unit) 传送;
- (8) PPS 交换。

该模块通过 PLB 接收来自 CPU (即 Microblaze) 的数据,并将它们转换成串行信号。智能卡 (Device) 接收这些串行信号,并作出相应的响应。CPU 通过 PLB 总线读取这些响应。其中,协议的选定是通过软件来实现的,而且 Device Controller 的参数传输也是通过软件来实现的。

根据该模块的主要功能特征,将该模块细化成以下几个小的模块。

- (1) 状态机模块:用于对通信状态过程的转换;
- (2) 计数器模块:用于发送或接收数据的位数计算;
- (3) 时钟分频模块:产生合适的时钟频率,用于与智能卡的通信;
- (4) 信号接口模块:接收并解码总线数据(命令、地址和数据);
- (5) 数据接收模块:用于接收 Device 发送的数据,并封装成 32 bit 格式。

3.2 IP 核的顶层模块

控制器的顶层模块的结构图如图 3 所示。

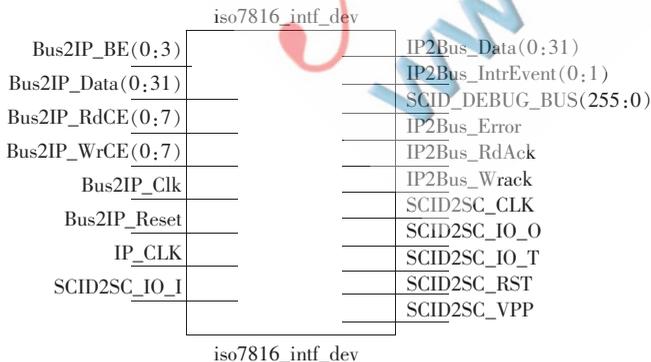


图 3 控制器顶层模块结构图

在这个控制模块中,有 6 个输入信号是本控制器接收来自主控制器 (Microblaze) 的信号,分别为总线时钟信号 Bus2IP_Clk、总线复位信号 Bus2IP_Reset、数据信号

Bus2IP_Data、总线选择信号 Bus2IP_BE、总线读使能信号 Bus2IP_RdCE 以及总线写使能信号 Bus2IP_WrCE。5 个信号用于本控制器发送响应给主控制器 (Microblaze),分别为 IP 发送数据信号 IP2Bus_Data、IP 读响应信号 IP2Bus_RdAck、IP 写响应信号 IP2Bus_WrAck、IP 报错信号 IP2Bus_Error 以及 IP 中断信号 IP2Bus_IntrEvent。还有 6 个信号用于本控制器与智能卡之间的通信,分别为输出给智能卡的时钟信号 SCID2SC_CLK、复位信号 SCID2SC_RST、电压信号 SCID2SC_VPP、接收智能卡返回值 SCID2SC_IO_I、输出信号给智能卡 SCID2SC_IO_O、输入输出选择信号 SCID2SC_IO_T。在时钟频率的选择上,由于 Spartan-3A 的工作频率是 62.5 MHz,因此 Bus2IP_Clk 采用的是 62.5 MHz,而智能卡在这样的高频下则无法有效工作,因此通过 DCM 来实现分频,最终选取 IP_CLK 的频率为 33.25 MHz。

3.3 控制器的工作流程

当此控制器 IP 核接收到来自总线的命令后,就开始工作,实现对智能卡的接口控制,其工作的状态转换如图 4 所示。

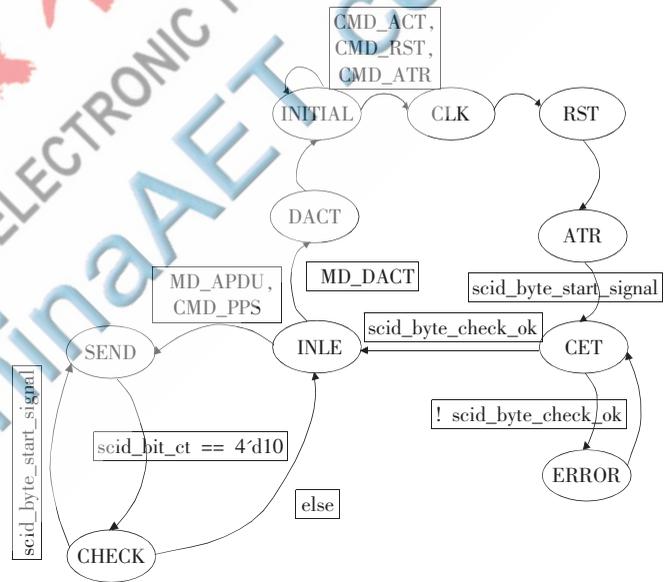


图 4 状态转换图

上电后,该控制器开始处于起始状态 (INITIAL),当接收到来自总线的信号后,信号接收模块便会识别信号中的命令。当命令为 CMD_ACT、CMD_RST、CMD_ATR 时,则开始工作;否则,继续处于起始状态。

开始工作后,首先进入到 SIGNAL_ST_CLK 状态,在这个状态里,时钟生成模块开始工作,它将产生一个需要的时钟频率,作为控制器与智能卡进行通信的工作频率。接着就要对智能卡进行第一次复位(冷复位),即进入到 SIGNAL_ST_RST 状态,复位后进入 SIGNAL_ST_ATR 状态(ATR 为复位应答),等待来自智能卡的返回信息。当智能卡发送信号有效时,进入到 SIGNAL_ST_GET 状态,接收来自智能卡的响应。如果返回值正确,则将进入空闲状态 (IDLE),等待下一命令。如果返回值不正确,

则需要智能卡重新发送,并重新进入到 SIGNAL_ST_GET 状态。

在 IDLE 状态下,控制器会根据总线后续的命令来进行操作,在本设计中主要是发送 CMD_ATR、CMD_APDU 和 CMD_PPS 命令,其过程是对智能卡进行数据的发送。首先进入到 SIGNAL_ST_SEND 状态,每发完一组数据(10 bit)后,都会对这组数据进行检查,即进入 SIGNAL_ST_CHECK 状态。

当所有操作命令都完成,就需要对此状态机进行释放,进入 SIGNAL_ST_DACT 状态。释放过程分为 3 步:首先对智能卡进行复位操作,然后要停止向智能卡输出时钟信号,最后将控制器对智能卡的输出信号拉低。至此,本次状态转换就结束了,对智能卡的一次控制也就完成了。

4 FPGA 的实现

在 ISE 12.4 开发环境中新建一个 SmartCard 控制器的工程,并添加 EDK 开发模块,运用其 IP 生成功能来生成一个智能卡的控制 IP 核 iso7816_intf_dev,输入相应的 Verilog HDL 代码,并将生成的 IP 添加到 EDK 系统中。整个 EDK 系统的工作平台如图 5 所示。



图 5 EDK 工作平台

只需在将此工程生成相应的比特流,并下载到 FPGA 开发板上,就可以对智能卡进行控制操作了。

为了在硬件上实现该控制器的功能,选用 Xilinx 公司的 Spartan-3A 系列 XC3S700A-4FG484 开发板来实现该控制器。其内部消耗资源概况如图 6 所示。

最后,借助于 Xilinx 的 SDK 对该控制器进行测试。在 SDK 中,可以运用函数 Xil_Out32 或者 Xil_In32 来进行数据的发送与接收。Xil_Out32(Base_Address+Offset, command/data), Xil_In32(Base_Address+Offset)。

验证此 IP 核能否正常工作,主要需要验证 ATR、APDU 和 PPS 这 3 个命令是否能够正确地发送并接收正确的响应。由于这 3 个命令的发送与接收都是运用同样的函数,只是命令符与地址不同,因此只列出 ATR 的测试情况。

运用下面的函数向对应的地址发送命令:

```
Xil_Out32(0xcce00004, 0x03000003);
```

```
Xil_Out32(0xcce00000, 0x00000101)。
```

运用下面的函数接收来自智能卡的响应:

Device Utilization Summary				
Logic Utilization	Used	Available	Utilization	Note(s)
Total Number Slice Registers	4,684	11,776	39%	
Number used as Flip Flops	4,683			
Number used as Latches	1			
Number of 4 input LUTs	5,356	11,776	45%	
Number of occupied Slices	4,587	5,888	77%	
Number of Slices containing only related logic	4,587	4,587	100%	
Number of Slices containing unrelated logic	0	4,587	0%	
Total Number of 4 input LUTs	5,645	11,776	47%	
Number used as logic	4,638			
Number used as a route-thru	289			
Number used for Dual Port RAMs	320			
Number used as Shift registers	398			
Number of bonded IOBs	56	372	15%	
IOB Flip Flops	21			
IOB Master Pads	3			
IOB Slave Pads	3			
Number of ODDR2s used	24			
Number of BUFMUXs	10	24	41%	
Number of DCMs	3	8	37%	
Number of BSCANs	1	1	100%	
Number of BSCAN_SPAREs	1	1	100%	
Number of MULT18K10s	20	20	100%	
Number of MULT18K10Bs	14	20	70%	
Number of 18K10s used	21			
Average Fanout of Non-Clock Nets	3.04			

图 6 FPGA 资源消耗

```
fpireg0=Xil_In32(0xcce0001c);
```

```
xil_printf("data0:%x\r\n",fpireg0)。
```

智能卡对此命令的响应如下,它返回 12 个字符:

```
3B,19,96,00,21,02,00,00,00,FF,90,00。
```

这些响应是符合此类智能卡的响应规定,因此,该 IP 核对于 ATR 功能是正确的。

利用同样的验证方法可以看出,该 IP 核对于 APDU 以及 PPS 等命令的响应都是完全正确的。

经验证,本方案所设计的智能卡控制器是可行的。在进行嵌入式设计时,可以将该 IP 核直接添加到相关的 EDK 工程中去,从而减少了设计的复杂度。但是本设计还只是局限于将 IP 核运用在 FPGA 上,以后需要继续研究,能够将该 IP 核通用化,这样就可以添加到任何目标系统中去,方便 SoC 的设计,这将是今后研究的重点所在。

参考文献

- [1] International Standard ISO/IEC 7816-3[S].
- [2] Xilinx 公司. Spartan-3 FPGA Family Data Sheet[Z].
- [3] Xilinx 公司. Spartan-3 Starter Kit Board User Guide[Z].
- [4] 夏宇闻,甘伟.Verilog HDL 入门[M].北京:北京航空航天大学出版社,2008.

(收稿日期:2012-0-0)

作者简介:

马峰,男,1988 年生,硕士研究生,主要研究方向:网络通信技术。

徐和根,男,1972 年生,博士,副教授,主要研究方向:数模混合电路等。

赵曼,女,1986 年生,硕士研究生,主要研究方向:通信加密技术。