基于MSP430的计算机认证系统设计

■ 装备指挥技术学院　高娟　刘作学　徐冬前

摘　要　提出并设计一种通用计算机IC卡认证系统，综合运用MSP430单片机和逻辑加密IC卡技术，很好地解决了计算机管理中的用户认证问题。用户在启动计算机之前，须插入认证IC卡。若认证通过，正常启动计算机，并在启动后记录用户的操作；否则，计算机系统不上电。

关键词　认证系统　单片机　IC卡　MSP430

引　言

随着计算机技术的日益普及，对于计算机管理，尤其对于涉密计算机的信息保护越来越为人们所重视，单纯地靠计算机开机密码来识别计算机用户也已逐渐满足不了人们的要求。因此，我们提出一种IC卡认证系统，只需在计算机的主板上插入一块PCI板，装上软驱型IC卡读写器，并为每一位计算机的合法用户配发IC卡，这样非法用户就不能随意使用装有本系统的计算机了。

基于MSP430的计算机认证系统包括硬件部分和应用软件部分。硬件部分主要完成如下功能：

◆下载单片机程序；
◆ 读写IC卡；
◆ 控制硬盘、网口及主板工作；
◆ 与计算机串口通信。

应用软件部分主要完成如下功能：

◆ 提供读写IC卡的用户界面；
◆ 安全管理，即应用软件随系统一起启动，启动后实时监测IC卡是否插入卡座，如果发现IC卡被拔除，将自动锁死计算机；
◆ 操作审计，即记录用户在计算机上的操作。

硬件与应用软件的通信主要通过计算机串口进行。应用软件若想让硬件进行某项操作，只需向串口发送命令帧，而硬件的状态也是通过向串口发送信息帧来告知应用软件的。因此，硬件与软件的设计具有相对的独立性。本文只对硬件部分的设计进行论述。

1　硬件系统设计

该系统的硬件部分以MSP430F149单片机为核心，总体框图如图1所示。

晶振电路为整个系统提供时钟源；JTAG接口电路实现单片机程序的下载；IC卡接口电路实现对IC卡的读写；计算机串行接口电路实现与应用软件的通信；硬盘、网卡及主板控制电路控制相应设备的上电。

1.1　IC卡接口电路设计

1.1.1　用户IC卡的分类

出于安全性和成本方面的考虑，在本系统中选用带写保护功能和可编程安全密码的逻辑加密卡SLE4442作为用户IC卡。SLE4442具有以下特点。

◆ 符合ISO7816国际标准。

◆ 256字节EEPROM的主存储器。其中00H～1FH单元为32字节的写保护区，其余字节为数据区。写保护区的每一个字节可单独进行写保护，写保护后，内容不可再更改（即固化）。数据区数据的初始值均为FFH。

◆ 32位保护存储器，对应写保护区的32个字节。每一位的状态决定写保护区的相应字节是否固化。

◆ 4字节的安全存储器。其中3字节存放安全密码，另一个字节存放密码错误计数。安全密码核对正确之前，所有的存储器均可读；但只有安全密码核对正确之后，才能对存储器的内容进行写或修改操作。密码错误次数初始值为07H,密码核对出错1次，将低3位中的1位“1”自动改为“0”，直到计数值为0，卡自动锁死，数据只可读出，不可再进行更改也无法再进行密码核对。若不为0时，有一次密码核对正确，可恢复到初始值。

在本系统中，根据不同IC卡的权限，用户IC卡分

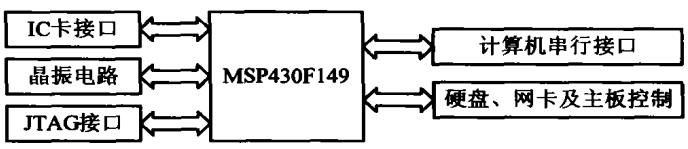

图　1

为三种。

(1) 超级用户 IC 卡

该IC卡在本系统交付使用时为用户提供，不受开机的限制，可以使用任何一个硬盘和网络。当单片机识别出IC卡为超级用户卡时，便根据硬盘转换开关的状态，启动相应的硬盘和网络，同时启动应用软件。拥有该IC卡的用户可以写管理员IC卡和普通用户IC卡。

(2) 管理员 IC 卡

在使用时，由超级用户IC卡为每一个分系统配备，管理员IC卡受开机的限制，可以使用任何一个硬盘和网络。启动计算机前，先核对IC卡上的用户信息。通过，则根据硬盘转换开关的状态，启动相应的硬盘和网络，同时启动应用软件；否则，计算机系统不加电，无法启动。拥有该IC卡的用户只能写普通用户IC卡。

(3) 普通用户 IC 卡

由超级用户或管理员为合法用户配备。根据标志位的设置，有的普通用户只能使用1号硬盘和网络，有的用户只能使用2号硬盘和网络，有的用户可以使用任何一个硬盘和网络。启动计算机前，先核对IC卡上的用户信息。通过，则根据相关标志位的设置，启动相应的硬盘和网络，同时启动应用软件；否则，计算机系统不加电，无法启动。普通用户IC卡只能用来启动计算机，不能写别的卡。

超级用户IC卡的识别信息和各个分系统的识别信息存储在写保护区，写保护后不可更改。分系统的识别信息用来标识不同分系统的IC卡，以确保不同分系统的IC卡不能互相通用。假如我们把不同计算机作为不同的分系统，计算机1的IC卡不能用来启动计算机2。IC卡上的用户信息格式如表1所列。

表 1

用户ID	硬盘号	用户名	用户口令	用户级别	用户创建时间
1字节	1字节	8字节			

用户ID为用户在一个分系统中的唯一标识；硬盘号为该IC卡用户被允许使用的硬盘和网络号；用户名和口令可以通过应用软件修改；用户级别表示该IC卡用户是管理员，还是普通用户。

1.1.2 接口电路设计

SLE4442型IC卡的外部引脚有6根，实际用到5根，即VCC、RST、CLK、GND和I/O。卡座上还有2个引脚ICKEY1和ICKEY2，用来判断IC卡是否插入卡座。MSP430F149有48个I/O引脚。这里我们采用端口P1的几个引脚与IC卡通信。

从安全性来考虑，IC卡的电源和时钟是受单片机控制的，在卡未插入时，应不给卡供电。在这个电路中，用2个三极管来实现这一点，电路如图2所示。

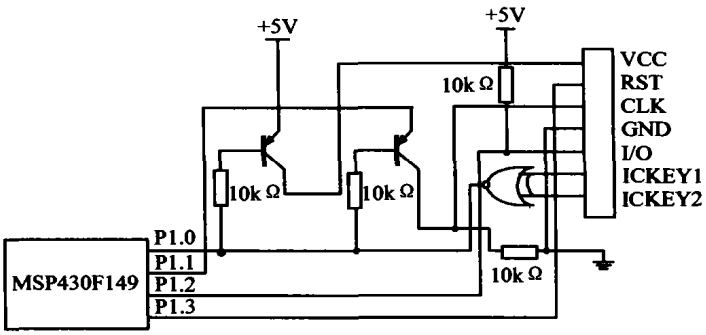

图 2

IC卡未插入时，卡座上的ICKEY1和ICKEY2电平状态相同，异或门输出为高电平，即P1.0为高电平，此时卡未上电；当IC卡插入时，P1.0为低电平，IC卡上电。单片机的P1.1口用来输出IC卡工作的时钟，时钟频率由单片机程序控制。单片机的P1.2用来实现单片机和IC卡的双向数据通信，在时钟的控制下，SLE4442与单片机采用同步半双工方式进行数据传输。由于IC卡的I/O口采用的是集电极开路方式，使用时要在口线上外接上拉电阻。单片机的P1.3口用来控制IC卡的复位，SLE4442采用高电平复位方式，复位时P1.3为高电平，IC卡工作时为低电平。

1.2 硬盘、网卡及主板控制电路设计

对于硬盘及主板的控制主要是通过继电器控制其电源来实现的，而对于网卡的控制则是通过模拟开关控制其数据线来实现的。根据设计要求，IC卡接口电路应先于计算机硬盘及主板加电，只有当IC卡接口电路判断出某一用户为合法用户时，才为主板加电，并根据相应的设置启动相应的硬盘及网络（本系统计算机默认为2个硬盘、2个网卡，并且硬盘与网卡为一一对应关系）。该部分电路如图3所示。

P1.5接硬盘转换开关，当IC卡用户可以使用任何一

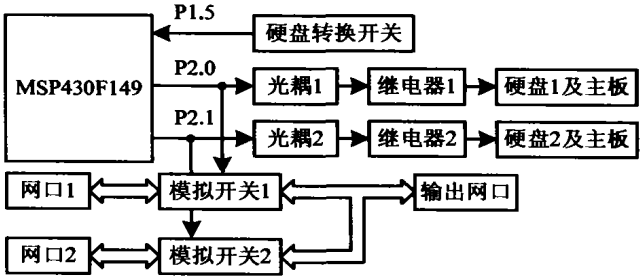

图 3

个硬盘和网络时，则根据硬盘转换开关的状态选择相应的硬盘和网络。P2.0 和 P2.1 为硬盘和网卡控制端，平时为低电平。当 P2.0 为高电平时，光耦 1 导通，计算机电源通过继电器加到硬盘 1 和主板上，启动计算机；同时模拟开关 1 接通，网口 1 通过模拟开关与输出网口接通。P2.1 的工作过程与 P2.0 相同。

1.3 计算机串行接口电路设计

MSP430F149 片内集成了 2 个通用串行同步/异步（USART）通信接口，允许 7 位或 8 位串行位流以预设的速率或外部时钟确定的速率移入、移出 MSP430。USART 接口支持两种不同的串行协议：通用异步协议（UART）和同步协议（SPI）[1]。本系统中利用 USART0 的 UART 模式，以 9600 的波特率与计算机串口进行通信，其信息的帧格式为 1 位起始位、8 位信息位、1 位停止位，无奇偶校验位。

为使硬件部分与应用软件协调工作，必须有一定的通信协议来确定串口数据的开始和结束。串口数据流帧格式如表 2 所列。

表 2

帧头	帧长度	信息/命令类型	信息	校验字节
2 字节	1 字节	1 字节	待定	1 字节

帧头（2 字节）：整帧开始的标志。

帧长度（1 字节）：整帧的字节长度，最大为 256 字节，包括校验字节。

信息/命令类型（1 字节）：由单片机发送到串口的帧均为信息帧，对应信息类型；由串口发送到单片机的帧均为命令帧，对应命令类型。

信息：根据信息/命令类型确定。

校验（1 字节）：检测信息在传输过程中是否正确。

2 单片机软件设计

单片机软件部分的主要功能如下：

- ◆ 读写 IC 卡；
- ◆ 产生硬盘、网卡及主板的控制电平；
- ◆ 写单片机的 Flash。

2.1 IC 卡时钟、复位及复位响应

SLE4442 正常工作的时钟频率为 7~50kHz。在本系统中，由 P1.1 口产生频率为 10kHz 的时钟作为 IC 卡工作的时钟。SLE4442 的复位和复位响应符合 ISO7816-3 标准。在程序设计中，作为 RST、CLK 的 P1.3 和 P1.1 应严格按照 ISO7816-3 规定的时序关系设计。

2.2 读写 IC 卡

复位响应之后，IC 卡进入命令模式，每条命令包括 3 个字节，以一个“启动状态”开始，“停止状态”结束。命令模式的时序如图 4 所示[2]，命令格式如表 3 所列[2]。然后，IC 卡便根据命令类型进入输出数据模式或处理模式进行数据处理。输出数据模式将 IC 卡中的数据传送给外部接口设备(IFD)，输出的顺序是从每个字节的最低位(LSB)开始，输出结束时，需要再附加一个时钟脉冲把 I/O 线置高。处理模式是 IC 卡作内部处理的模式。IC 卡在第 1 个时钟脉冲的下降沿将 I/O 线从高拉到低并开始处理。此后 IC 卡在内部连续计数，直到第 n 个时钟脉冲之后再附加一个时钟脉冲的下沿，I/O 线被再次置高，完成 IC 卡的内部处理过程。

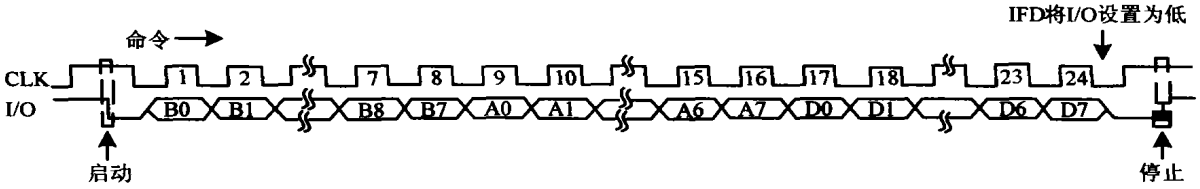

图 4

表 3

控制字节	地址字节	数据字节	功 能	命令模式
30H	A7~A0	无效	读主存储器	输出数据模式
38H	A7~A0	D7~D0	修改主存储器	处理模式
34H	无效	无效	读保护存储器	输出数据模式
3CH	A7~A0	D7~D0	写保护存储器	处理模式
31H	无效	无效	读加密存储器	输出数据模式
39H	A7~A0	D7~D0	修改加密存储器	处理模式
33H	A7~A0	D7~D0	比较校验数据	处理模式

读写 IC 卡的流程如图 5 所示，其中在发送命令或接收数据过程中要用到发送或接收 1 个字节子程序。由于 SLE4442 的 I/O 端是在 CLK 下降沿时对数据进行判决，所以向 SLE4442 发送数据时，数据要在下降沿之前准备好。根据这一原则，发送一个字节子程序流程如图 6 所示，其中寄存器 R12 中存放待发送的数据。又由于 SLE4442 输出数据时是在 CLK 下降沿时将数据发送到 I/O 端口，所以 MSP430F149 接收数据时，应在上升沿将数据读入。根据这一原则，接收一个字节子程序如图 7 所示，其中 R12 中存放接收到的数据。

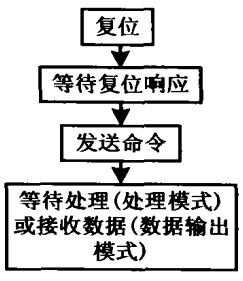

图 5

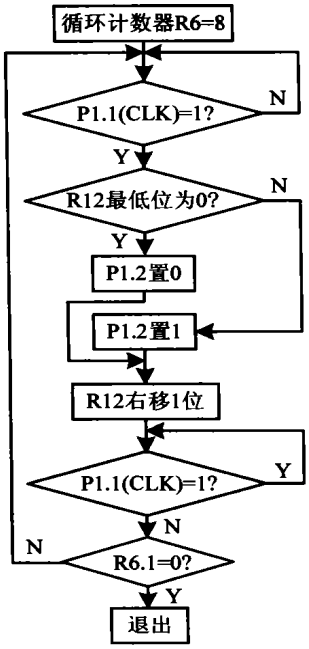

图 6

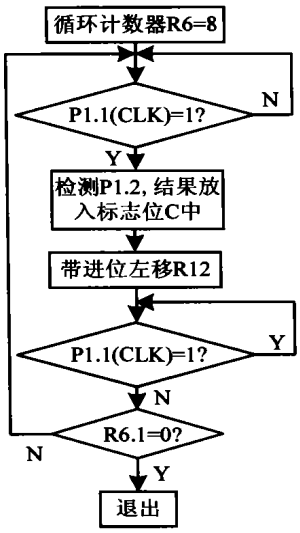

图 7

2.3 写单片机Flash

MSP430F149的存储器空间采用“冯·诺伊曼”结构，寻址空间可达64KB，其中Flash存储器为60KB（主存储器）+256B（信息存储器）。Flash存储器可以按字或字节读写，经过擦除各位为“1”，可以写“0”。60KB的主存储器又被分为若干段，段是擦除或编程操作的最小单位。

每台计算机所有合法用户的信息均存储在MSP430F149的Flash存储器中。增加新用户时，不仅要将用户信息写入IC卡，同时还要写入Flash存储器；修改用户信息时，不仅要修改IC卡信息，同时还要修改Flash存储器的有关内容。对于用户信息的操作有三种：删除旧用户、增加新用户和修改用户信息。删除旧用户是将原有的用户信息都修改为“1”，增加新用户也是将原有的“1”修改为新用户的信息。这些操作都可以归结为修改Flash，修改Flash中用户信息的子程序流程如图8所示。

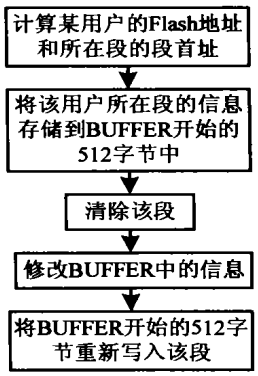

图 8

结 语

该系统可为多达2×10^{31}个分系统提供唯一的分系统标识，每个分系统的用户最多可达256个，用户信息可根据需要扩展为128字节，可以充分满足实际需要。该系统已应用于工程实践，并取得了良好的效果。

参考文献

1 胡大可编著. MSP430系列Flash型超低功耗16位单片机[M]. 北京：北京航空航天大学出版社，2001

2 ICS for Chip Cards, Intelligent 256-byte EEPROM SLE 4432/SLE 4442 Data Sheet. Siemens Corporation[C], 1995

3 MSP430x13x, MSP430x14x Mixed Signal Microcontroller. TI Corporation[C], 2001

4 魏小龙编著. MSP430系列单片机接口技术及系统设计实例[M]. 北京：北京航空航天大学出版社，2002

5 MAX4751 Technical Manual. MAXIM Corporation[C], 2002

6 MSP430 C Compiler Programming Guide. IAR Corporation [C], 1996

（收稿日期：2003-04-28）

首届“中国嵌入式技术应用论坛”在京召开

由嵌入式厂商研祥智能科技股份有限公司、赛迪顾问有限公司和英特尔（中国）有限公司联合主办的首届“中国嵌入式技术应用论坛”于9月16日在北京新世纪饭店隆重拉开帷幕。

本次“中国嵌入式技术应用论坛”是研祥公司携手著名芯片厂商Intel公司举行的首届面向全国嵌入式领域技术人员及工程商、系统集成商的行业技术交流会，旨在推动产业、拓展视野、促进交流。会议除对嵌入式应用行业的政策动态及中国嵌入式行业发展趋势进行介绍和分析外，一些业界知名厂商如Intel公司、研祥智能、长城计算机、红旗LINUX、风河、方舟、鼎钛克公司等也进行了主题演讲。

继深圳之后，此次论坛将在广州、武汉、南京、上海、北京、西安、成都、重庆等另外八个城市巡回举办，这是2003年度在国内召开的大规模、影响面广的嵌入式领域行业盛会，对促进中国嵌入式市场更快速的走向成熟起到推动作用，并有着极其深远的意义！