文章编号：1005－8893（2002）02－0039－04

IC 卡终端系统的开发*

符彦惟[1]，蒋益兴[2]，潘　操[2]
（1. 江苏石油化工学院 现代教育技术中心，江苏 常州 213016；2. 江苏石油化工学院 计算机系，，江苏 常州 213016）

摘要：IC 卡应用系统由于其自身的优势正逐步代替磁卡等应用系统，应用领域非常广泛。IC 卡应用系统由 IC 卡、终端系统和上位机 IC 卡管理系统组成。详细介绍了可用于校园各种应用管理系统进行身份认证、数据管理的 IC 卡终端系统各功能模块的软件、硬件设计与实现，以及数据的安全设计与实现。

关键词：IC 卡；单片机；系统设计；数据安全
中图分类号：TP 2034　　文献标识码：A

IC 卡的名称源于集成电路卡，又称“智能卡”。是一种信息存储量大，安全性能好，具有支付、查询、密码查验等多种功能的卡。鉴于 IC 卡优良的读写性能，安全的保密功能，将逐步替代正在使用的各种信用凭证。目前 IC 卡已广泛应用于金融财务、交通、社会保险、零售服务、学生管理等方面。

1　校园 IC 卡的应用系统

1.1　IC 卡应用系统的组成

如图 1 所示，IC 卡的应用系统一般由 4 大部分组成：发行管理系统、终端系统、通讯系统及 IC 卡。

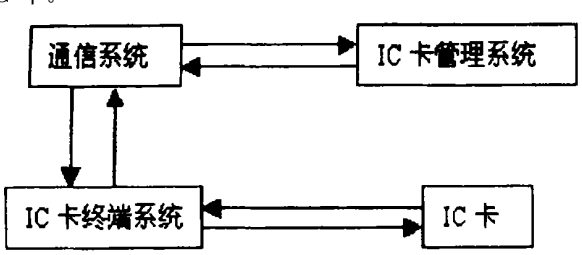

图 1　IC 卡应用系统组成原理框图

发行管理系统：主要管理 IC 卡的发行信息、终端操作信息及系统运作情况。

终端系统：读取 IC 卡中的信息，向 IC 卡中写信息，向有关的信息管理系统输出相关信息和控制信号。

通讯系统：实行发行管理系统与终端系统间的信息传送和反馈，采用的方式可以是有线、无线、磁介质等。

IC 卡：存放数据信息、代码、储值等。

1.2　应用系统的设计原则

IC 卡应用系统的设计是一项综合性技术，并没有统一的模式。它主要取决于应用系统的应用类型、使用范围和使用环境。

1.2.1　选择合适的 IC 卡

IC 卡的选择除了容量和可靠性之外，要着重考虑的是方便性、安全性和成本。从成本来说，射频卡最贵，其它依此是 CPU 卡、加密卡和存储器卡。安全性各种卡排列顺序同前。方便性要从两方面来考虑，即使用的方便性和开发的方便性。非接触式卡使用最方便，但开发比较复杂。存储器卡用于非加密场合时，开发最方便，而有加密要求的场合，则采用加密卡系统设计更为简洁。CPU 卡和

* 收稿日期：2001－12－10
基金项目：江苏石油化工学院科研基金资助
作者简介：符彦惟（1959－），男，江苏江阴人，硕士，主要从事计算机应用及机电一体化方面的教学及科研。

射频卡开发都比较复杂，一般适用于较为重要的场合，表 1 为这几种卡的有关特性对照表。

表 1 各种 IC 卡的有关特性对照表

	存储器卡	加密卡	CPU 卡	射频卡
成本	最低	较低	较高	最高
使用	好	好	好	好
开发	好	好	复杂	复杂
安全性	较差	较高	高	高

考虑到校园应用环境良好，使用人员的单一性以及学生的经济承受能力，本系统采用性能价格比较好的加密卡，但由于应用中涉及费用的计算，要采用一定的加密算法来进一步提高该型卡对数据操作的安全性。

1.2.2 系统设计

一个具体的应用系统的设计要牵涉很多方面，除了与 IC 卡的选型以外，还与系统的应用范围有关。以酒店系统为例，客人消费、开门、房间设施控制都采用 IC 卡，如果全部用一张卡来实现，将大大方便客人，因此各功能的设计既要有独立性，又要有开放性，便于系统的综合，而如果应用系统只是用于身份认证，则系统开发要简单的多。

另外系统的运作方式也很重要，如将 IC 卡用于收费，是采用代码（通过银行转帐或记帐）还是直接用于储值，两者的系统设计可能截然不同，应对运作的方便性、系统成本及安全性作综合考虑[1]。

对于采用存储器卡（加密或非加密）的应用场合，系统设计最基本的工作是终端系统的设计与开发，如采用标准读卡器（如”终端式”读卡器），则主要工作是软件设计，简单存储器 IC 卡只有读写操作子程序，而加密存储器卡操作子程序较多。如果采用专用终端，则还要进行硬件系统设计。对于采用 CPU 卡和射频卡的应用场合，由于卡本身就是一个单片机系统，因此系统设计最基本的工作可以看作是一个特殊单片机系统的设计（能实现各种加密功能和算法、遵从 ISO7816 标准）。

从校园的具体应用情况来看，虽然使用的人员单一，但应用范围比较广，既有用于身份认证，又要用于计费，因此从开发的成本、使用方便、可靠性和安全等方面综合考虑，本终端系统采用专用设计的读写器，通过自行设计的硬件系统与加密算法相配合，对 IC 卡的数据进行操作，从而达到良好的总体性能。

2 校园 IC 卡终端系统的设计

2.1 终端系统的组成及工作原理

2.1.1 系统组成

本终端系统采用中央处理器为 ATMEL 公司的 AT89C2051 单片机，辅以西门子公司的逻辑加密 SIE4428IC 卡的读写模块、DS1302 时钟显示电路、X25045 信息存储、复位电路、MAX485、MAX232 上下位机通信电路（采用 MAX485 及 MAX485 卡构成网络实时通信）。整套系统绕主控芯片 AT89C2051 设计成五大功能模块：IC 卡读写模块、时钟模块、显示模块、复位模块和通信模块。原理图如图 2 所示。

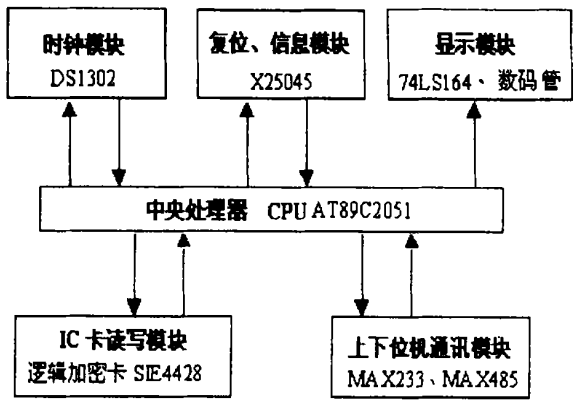

图 2 终端系统原理框图

2.1.2 工作原理

根据应用环节，IC 卡在具体使用时，一般为卡的发行（功能是对卡的系统区信息进行初试化写入）和卡的应用区信息的读写两个步骤，其终端系统加卡工作流程如图 3 所示。IC 卡终端应用于上机管理系统读写卡工作流程如图 4 所示。

2.2 IC 卡终端系统的设计

2.2.1 读写模块

IC 卡读写模块实现对卡进行操作（存储数据和读取数据），其电路连接采用 I2C 总线形式，支持 ISO/7816－3 同步传输协议（本系统通信采用异步传输方式），除去密码区操作外，其它类似于对一般串行 EEPROM 的操作。对 SIE4428 的操作符合 SPI 总线的要求，因此仅需 3 根线，即复位线 RST、串行时钟线 CLK 和双向数据线 I/O。

SLE4428 主存储器可分为保护区和应用区。保护区带位保护功能，一旦实行保护后，被保护的单元不可擦除和改写。在应用系统中，保护区用作存放固定信息，如卡编号、批次号、发行时间、持卡人姓名、身份证号码、学号、班级、所属系部

等。SIE 4428 应用区容量较大，空间安排显得十

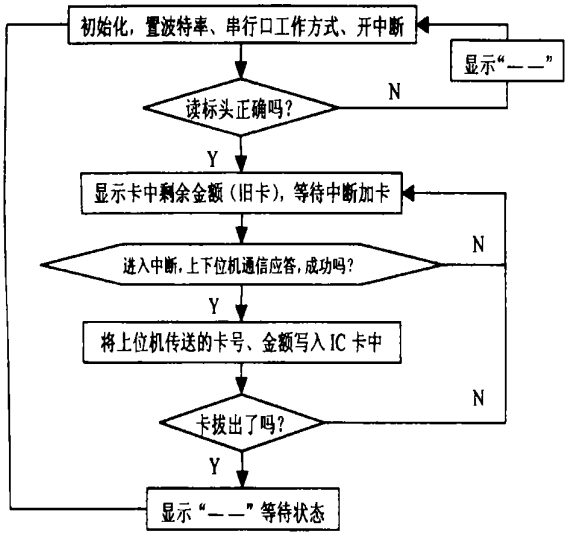

图 3 IC 卡终端系统加卡工作流程图

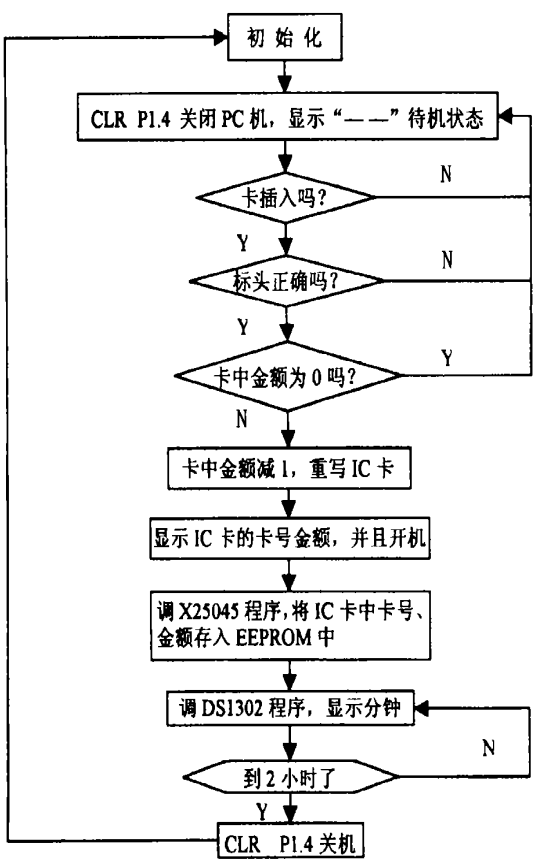

图 4 IC 卡终端系统读写工作流程图

分灵活，在具体应用中，可根据校园不同的管理应用系统需求，将应用区空间分为几个区，如教务信息区、图书馆信息区、后勤生活信息区等实现一卡多用的功能。逻辑加密卡的特性可以保证卡中信息的安全性和可靠性。应用区信息如果不采取措施，安全和可靠性得不到保证。可采通过用将应用区中的信息分别放在几个不同的单元，在读写时用存放在不同单元的信息进行加密比较，若通过验证可进行读写操作，否则终止读写操作。

2.2.2 时钟、显示模块

时钟、显示模块模块实现了 IC 卡上金钱余额、IC 卡卡号和上机计时的显示功能。采用了时钟芯片 DS1302、串入并出芯片 74LS164 和共阳极 LED 数码管。它经过一个简单的串行接口与微处理器通信。使用同步串行通信，简化了 DS1302 与微处理器的通信，但考虑到终端的串行口还要与上位机通信，故采用 AT89C2051 的 P3.3 和 P3.4 来模拟串行口 TXD、RXD 在工作方式 0。实时时钟/日历提供秒、分、时、日、周、月和年等信息。对于小于 31 天的月，月末的日期自动进行调整，还包括了闰年校正的功能。时钟运行可以采用 24 小时或带上午（AM）/下午（PM）的 12 小时格式。

2.2.3 复位模块

复位、信息写入模块实现单片机在开机时进行上电复位，使 AT89C2051 以及其他模块都处于初始状态。当系统因干扰失控，程序跑飞以后，系统将产生错误并且不能恢复正常，这时就需要采取时间监视措施来保证系统失控后能自动恢复正常工作[2]。在本系统中，采用了 Xicro 公司生产的芯片 X25045 设计了“看门狗”（Watchdog）电路，用于保证系统因干扰失控以后能够自动复位。

2.2.4 通信模块

在校园实际的应用中，如图书馆借阅系统、教务管理系统、食堂饭票系统等等都存在着多站间通信的问题，通常要求用最少的信号线完成通信，使设备简单，成本降低。RS－485 总线用于多站互连十分方便，用一对双绞线便可实现多站分时通信。RS－485 是采用平衡发送和差分接收方式来实现通信的。RS－485 采用平衡差分电路，因此抗共模干扰能力强，同时接收灵敏度也很高，能够长距离、高速度地传输数据，而且通过 RS－485 接口电路可以很方便地构成总线型通行网络。在本系统的下位机中，采用单片机和 MAX485 接口的方式，来实现通信的功能。AT89C2051 单片机采用的是 TTL 电平而上位机采用的 EIA 电平，因此与 PC 机串口通信涉及到 RS－485 与 RS－232 之间的电平转换问题，与一般的三线制通信有很大的区别。在本系统中采用 MAX233 芯片来实现 TTL 与 RS－232 电平之间的转换，用 MAX485 芯片来实现 TTL 与 MAX485 电平的转换。

2.3 IC 卡的安全设计

在本系统中，为保证卡上数据的安全、可靠性以及校园使用惯例，卡上的卡号和学号在一次设置后不可变，在卡被发给学生后，学生持卡使用时卡上的卡号和学号信息仅可读，不可改写；而卡上其它的数据如金额信息、借阅书籍的情况等可读、可写。具体过程如下：

IC 卡卡号和学号存放在 SIE4428 逻辑加密卡指定的保护区，由逻辑加密卡的特性可以保证卡中信息的安全性和可靠性。其它存放在应用区的信息需采取不同的操作策略，对于一般性的数据可采用常规的读写操作，而有些涉及学生切身利益的信息如金额等信息，如果不采取措施，安全和可靠性就得不到保证。所以可以采用如下的方法：假设一张卡上最多存放金额 99 元，因此在 IC 卡上存放金额的信息占用 IC 卡应用区 1 个字节。本系统设计的时候在 IC 卡的应用区开辟 3 个字节，地址不同的单元存放金额信息。在设置 IC 卡时分别在此 3 个单元存放金额信息，然后读出这 3 个单元的内容加以比较，如果相同则成功，不同则重设置；如果 3 次设置不成功则提示此卡无效。由此可保证金额信息读/写的可靠性，工作流程如图 5 所示[3]。为提高金额信息的安全性，还可以采用 EDS 对信息进行软件加密。

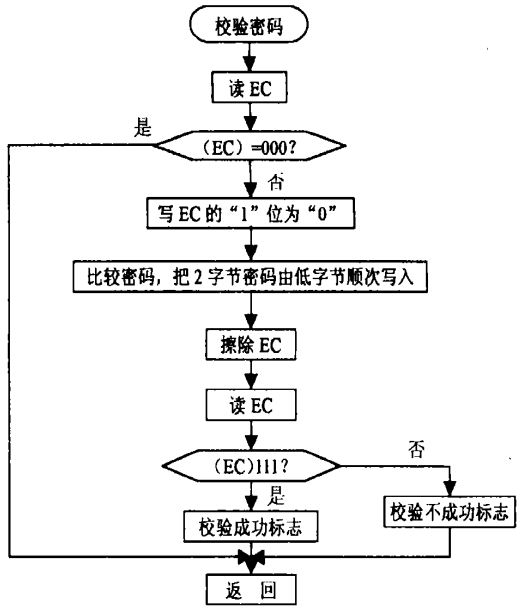

图 5 校验密码程序框图

参考文献：

[1] 王卓人，邓晋钧，刘宗祥. IC 卡的技术与应用 [M]. 北京：电子工业出版社，1999. 334－338.

[2] 吕能元. MCS－51 单片微型计算机原理、接口技术、应用实例 [M]. 北京：科学出版社，1993. 290.

[3] 何立民. 单片机应用技术选编〈6〉[M]. 北京：北京航天航空大学出版社，1998. 74.

The Development of IC Card Terminal System

FU Yan－wei[1]，JIANG Yi－xing[2]，PAN Cao[2]

(1. The Center of Modern Education Technology，Jiangsu Institute of Petrochemical Technology，Changzhou 213016，China；2. Department of Computer Science and Engineering，Jiangsu Institute of Petrochemical Technology，Changzhou 213016，China)

Abstract：IC card application system is replacing magnetic bar code card. It is an advanced system because of its advantages and the application field is very extensive. IC card uses its build－in system，terminal system and IC card′s administrative system of of the last location machine. The general design principle is that IC card application system and the particulars should be noticed when the card is applied in the campus management system. Terminal system is the major component of that application system.

Key words：IC card；one－chip computer；systematic design；data safety