中文摘要

RFID 是射频识别技术和 IC 卡技术相结合的产物，是标签识别领域的一项新兴技术，具有操作快捷、抗干扰性强、操作距离远、安全性高、便于一卡多用等特点，在铁路客票领域具有其他标签识别技术无法比拟的优越性，具有广阔的市场前景。

论文首先对 RFID 技术的特点、关键技术、典型应用和发展现状进行了概述，然后基于 Philips 公司生产的 MIFARE 1 S50 型非接触式射频 IC 卡芯片和相应核心读写模块 MCM200 进行了非接触式 IC 卡读卡器接口电路的研究和制作，以及软件系统的设计和实现。读卡器的硬件主要包括对 MCU、MCM200、RF 单元、EEPROM 存储单元、复位电路及 TC232 电路间的接口电路，软件设计分为对 MCM200 及其他电路的应用程序的设计、对安全认证体系的设计和主程序设计三个部分。论文实现了以下技术指标：

工作频率：13.56MHZ

通信速率：106KBps

读写距离：可达 25mm 以上

模块与卡片通信时，数据加密

接口标准：ISO/IEC 14443 TYPE A 标准

工作温度范围：-20℃～+70℃

读写机具对铁路客票的识别安全、高效、准确，可实现无人职守，系统安装简便、性能稳定、高效快速，大大缩短了售检票时间，且具备很好的可扩展性。

关键词：射频识别，客票系统，Mifare，MCM

分类号：TN409

ABSTRACT

RFID is a kind of new technology in the field of label identification, which is the combination of RF technology and IC card technology, and its high working speed, good anticollsion quality and long working distance give it advantage over common label identification technology, there will be a good prospect for it in rail ticket fields.

At first, RFID technology is generally introduced including its feature, key technology, typical usage and developing tendency. And then, based on the chip model MIFARE 1 S50 and the reader component model MCM200, PHILIPS Semiconductors, the contactless IC card reader is designed and produced, including the interface circuit design and the software design. The contactless IC card reader's circuit is made up of interface circuit between MCU, MCM200, RF, EEPROM and TC232 communication circuit. The software design includes programming of MCM200 and other circuits, and programming of main program. Many targets hereinafter were achieved:

Work frequency: 13.56MHZ

Communication speed: 106KBps

Work distance: 25mm

data encrypted during communication between card and module

Interface standard: ISO/IEC 14443 TYPE A

Work temperature: -20℃～+70℃

The contactless IC card reader has the advantage of safety, efficiency, exactness to identify rail tickets. It can be self-service. The system is easy to install and has a stable, fast and efficient performance which would greatly shortened the time of sell and check tickets. Further more, the contactless IC card reader has good expansibility.

KEYWORDS: RFID, Mifare, MCM, Rail Ticket System

CLASSNO: TN409

学位论文版权使用授权书

本学位论文作者完全了解北京交通大学有关保留、使用学位论文的规定。特授权北京交通大学可以将学位论文的全部或部分内容编入有关数据库进行检索，并采用影印、缩印或扫描等复制手段保存、汇编以供查阅和借阅。同意学校向国家有关部门或机构送交论文的复印件和磁盘。

（保密的学位论文在解密后适用本授权说明）

学位论文作者签名：沈涛　　导师签名：[illegible]

签字日期：2007 年 12 月 26 日　　签字日期：2007 年 12 月 26 日

致谢

本论文的工作是在我的导师娄淑琴教授的悉心指导下完成的，娄淑琴教授严谨的治学态度和科学的工作方法给了我极大的帮助和影响。在此衷心感谢三年来娄淑琴老师对我的关心和指导。

娄淑琴教授悉心指导我们完成了实验室的科研工作，在学习上和生活上都给予了我很大的关心和帮助，对于我的科研工作和论文都提出了许多的宝贵意见，在此向娄淑琴老师表示衷心的谢意。

在实验室工作及撰写论文期间，胡延、鞠伟明等同学对我论文中的研究工作提出了许多宝贵的意见，在此向他们表达我的感激之情。

此外，王成、冯云梅、付晓宇、王海龙、王刚、樊淋、熊欣、王冉等同事在我论文的撰写过程中给予了热情帮助， 在此对他们给予的无私帮助一并表示深深地感谢。

最后要感谢我的父母，他们支持了我近二十年的学校生涯，他们给予我的理解和支持使我能够在学校专心完成我的学业。

第1章 绪论

无线射频识别（Radio Frequency Identification ，RFID）技术作为快速、实时、准确采集与处理信息的高新技术，被公认为21世纪十大重要技术之一，在生产、销售和流通等领域有着广阔的应用前景[1]，已逐渐成为企业提高管理水平、降低成本、实现管理信息化、参与国际经济大循环和增强企业竞争力不可缺少的技术工具和手段。随着科学技术的迅猛发展，特别是随着存储技术的发展，RFID 正逐渐成为 IT 行业新的热点。将 RFID 技术与铁路客票相结合，应用到我国铁路客票系统中去，无论在铁路客票系统客观需求上、RFID 本身的技术特点上、政府对 RFID 技术的扶植上来看，都非常必要。

1.1 课题提出的背景及意义

目前，铁路仍是中国人跨地区出行的首选交通工具，2007 年铁路客运量预计将超过 13.65 亿人次[2]，且呈逐年递增趋势。随着动车组、城际间高速铁路等的修建及逐步运营，可以预见，在未来相当长的一段时期内客运容量仍将继续攀升。

但是，目前我国铁路客票系统的发展却存在着非常大的滞后性，越来越难以满足现代化的要求，主要表现在以下几个方面：

一、由于运力巨大，检票任务繁重，但是人工手工检票的方式效率低下，大中型城市的火车站经常人满为患，空气污浊，人流通行不畅，尤其是春运、黄金周等时间，这一矛顿更显突出，造成了相当大的安全隐患。

二、虽然铁路部门和公安部门不断加大打击制售假票的力度，但是由于人工检票技术上的局限性，使得大量假票得以成功蒙混过关，屡禁不止，严重损害了铁路运输部门和广大旅客的利益。

三、我国铁路部门一直期望将铁路客票向实名制方向发展，但是以目前的纸制条形码形式的客票系统向该方向拓展，在技术上难度极大。

当前使用的纸制条码型客票无论在技术指标还是可持续发展性上，都无法满足要求，迫切需要通过应用一项新技术，开发一套全新的客票形式，使之能够满足高效率、高安全性、可扩展性强等技术要求，并且价格低廉，应用到新的客票系统中去。

RFID 无线射频识别技术，是一种利用射频通信实现的，具有体积小、容量大、寿命长、高效、高安全性、可重复使用等特点的非接触式自动识别技术[3]。随着射频集成电路技术的不断完善，制卡技术的不断提高，卡片功能的不断完善与丰富，

非接触式IC智能射频卡及其相应的读写设备的相关技术也得到了大大发展，设备价格大幅下降，该技术广泛应用于标签识别、公共交通、无线通信、身份识别、门禁系统、金融、物流等领域中，可大幅提高管理与运作效率，降低成本[4]。

将RFID技术与铁路客票相结合，应用到我国铁路客票系统中去，无论在铁路客票系统客观需求上、RFID本身的技术特点上、政府对RFID技术的扶植上来看，都是非常合适的。而且，随着目前全路客运专线、高速铁路建设的相继开始，以及现有的城市轨道交通和即将建设的城际轨道交通等，都为将RFID应用到铁路客票系统中去提供了前所未有的客观潜在机遇和经济市场。

1.2 技术选择论证

对于铁路客票系统中的检票环节来说，铁路客票也是一种标签，对铁路客票的校验也可以看作是进行标签识别操作。在标签识别技术的发展历史上，先后出现了许多种标签形式及识别技术，只有结合我国铁路发展的特点，选择最合适的技术，才能做出适合我国铁路实现全路信息化、自动化、智能化的战略要求，进一步促进我国铁路事业发展的客票系统。

1.2.1 铁路发展状况对客票系统的要求

在党的十六大提出的《国民经济和社会发展第十一个五年规划纲要》中明确提出，要优先加快发展铁路运输业；铁道部在十一五铁路规划中也明确提出要在全路实现信息化、自动化、智能化的目标。

目前，我国铁路客运营业里程已经达到7万公里，年旅客发送量超过13亿人次。按照规划，十一五期间我国铁路将建设新线17000公里，其中客运专线7000公里，既有线路增建二线8000公里，至2010年全国铁路营业里程将达到9万公里以上，旅客年发送量将达到15亿人次，至2020年旅客年发送量将达到30亿人次。在未来几年中，一千公里甚至一千五百公里以内距离的铁路运输公交化的趋势将越来越明显，而且无论从经济角度、还是从快捷便利角度出发，都难以避免地要引入储值或计次形式的优惠客票，以吸引更多的常旅客。

这对新的客票系统提出了更高的要求，要求新的客票系统能够满足购票方便、检票快捷、防伪性高、在一套检票系统中可容纳多种客票形式、低成本且适于重复使用等多方面的要求。此外，随着客运专线的开通和客运铁路的提速，出于国家安全和社会稳定，以及自动化、现代化的要求，新的客票系统还应具备可向实名制及电子钱包方向的可拓展性。

1.2.2 标签识别技术分类及选择论证

经过近一个世纪的发展，标签自动识别技术取得了长足的进步与发展，先后出现了条形码、磁卡、接触式IC卡、非接触式IC卡（RFID）、直至最近涌现出的指纹识别、声音识别、面部识别等多种技术形式，但是应用最为普遍与成熟的，主要还是条形码、磁卡、接触式IC卡、非接触式IC卡等，这些技术有着其各自的特点与优势，在不同领域中获得了广泛地应用。

一、条形码

条形码识别技术是把计算机所需的数据用一维图形或二维图形来表示，通过光电扫描形式的条形码阅读器读取条形码，并将其转换成计算机可以自动阅读的数据来进行识别的[5]。条形码识别的特点在于标签制作成本低廉，识别简单，因此其也是目前采用最为广泛的识别方法，尤其是在超市购物中随处可见，目前我国民航系统中校验登机牌也是采用的该种自动识别技术。

由于纸介质易磨损，条形码票识别率低、不利于检票速度和首读率的提高，且识读设备昂贵且易损坏，可重复利用率也很低。虽然目前我国铁路客票票面上也有条形码，但未真正投入使用，这是因为较之航空旅客，不论是乘坐铁路的旅客总客流量，还是同一班列车的运力都要超过航班的几十倍，人流密度巨大，并且客票在旅客手中持有时间也远远多于登机牌在航空旅客手中持有时间，更易造成客票的磨损。

因此，如果基于条形码开发自动检票系统，对提高效率、杜绝假票等方面帮助不大，且不利于扩展实名制功能，可望升级的空间极为有限，无法适应铁道部提出的十一五期间实现高速铁路信息化、自动化、智能化及铁路跨越式发展的需求。

二、磁卡

磁卡及相应的读写设备，是由一定材料的片基和均匀地涂布在片基上面的微粒磁性材料制成的。在记录和自动识别时，磁卡的磁性面或记录磁头以一定的速度移动。

磁卡的存储容量通常只有几百个字节，一般情况下只记录该卡片的基本信息如卡号，需要通过终端读到卡号后直接和系统进行通信，由系统调用存储在数据库中的卡片信息及卡片持有者的信息，并通过密码等形式进行身份验证及相关操作，因此在使用过程中必须要保证终端与主机之间极强的实时性，一旦主机或网络出现故障就会使整个系统瘫痪。同时，磁卡票对读写设备要求很高，配套的磁票读写设备非常昂贵，且磁头易污损，需要经常清洗，维护成本很高。该系统更适合应用于实时性极强的且全部为专人专用的如银行、金融等领域中。

三、接触式IC卡

接触式IC卡（Integrated Circuit Card，集成电路卡）是继磁卡之后出现的一种新型信息工具，是将一个微电子芯片嵌入符合ISO 7816标准的卡基中，做成卡片形式。在记录和识别时，通过读写器的触点和卡片上IC卡的触脚向卡片提供稳定的电源和时钟，并实现卡片与上位机之间的通信[6]。接触式IC卡也是近年来使用较多的一种技术，广泛应用于如公用电话、汽车加油、缴纳电费等公共事业的支付系统中。

该技术在支付系统中的应用，基本具备了高效及高安全性的特点。但IC卡片上的触脚长期暴露在外，容易造成损坏和形成污垢，造成接触不良，从而影响使用效果，如果将其作为需频繁使用的客票IC卡，会受到其芯片表面易磨损、易腐蚀等弱点的极大制约。

四、非接触式IC射频卡（RFID）

非接触式 IC 射频卡具备了接触式 IC 卡的全部优点，同时其通过射频读写器向 IC 卡发一组固定频率的电磁波，卡片内 IC 串联协振电路频率与读写器发射的频率相同，这样在电磁波激励下，LC 协振电路产生共振，实现为其电路提供工作电压，将卡内数据发射出去或接受读写器的数据，从而实现标签自动识别功能。

该技术可采用加密算法，通过三次认证机制，确保极高的安全性，几乎不可能复制出一张完全一样的卡片；使用非接触式 IC 射频卡，只需要几毫秒至几十毫秒即可完成交易，方便快捷；该技术对实时性要求较低，可通过在读写器中设置单独的存储模块保存数据，有效避免由于主机或网络故障造成的系统瘫痪，适合于脱机使用。由于芯片是以内嵌形式置入卡中，该技术将磨损、腐蚀等不利因素的影响减小到最低，真正实现了高效、高安全性、耐磨损、适于重复使用的要求。此外，多扇区的存储结构，以及该技术在我国第二代身份证上的应用，使之无论在应用范围上还是实名制要求上都具备了功能可扩展性。

1.3 RFID 技术发展进程及应用概状

近一两年来由于受到以沃尔玛为代表的大型零售商的推动，RFID 技术在全球掀起阵阵热潮，吸引了众多厂商参与相关技术及芯片的研究和开发。目前 RFID 技术处于迅速上升的时期，该技术被业界公认为本世纪最有前途的应用技术之一，同时也引起了许多国家的重视，欲将其培育成国家的一项重要产业。

RFID 技术的发展最早可以追溯至第二次世界大战时期，那时它被用来在空中作战行动中进行敌我识别。当时应该空军为了识别返航的飞机是敌军还是我军，在盟军的飞机上装备了一个无线电收发器。当控制塔上的探询器向返航的飞机发

射一个询问信号，飞机上的收发器接收到这个信号后，回传一个信号给探测器，探测器根据接收到的回传信号来识别敌我机。这是由雷达的改进和应用所催生的RFID技术第一次应用到实际中去，并奠定了RFID技术的理论基础[7]。

20世纪50年代至60年代末期，RFID技术研究进入到了早期探索阶段，并且在60年代末期终于取得了重大成就，成功地应用到了大型超市和图书馆中，用于物品的电子监视。虽然只是1比特标签系统，只能检测被标识物品是否在场而无法记录更多的数据，甚至不能区分被标识目标之间的区别，但仍然具有重大意义。

进入90年代，随着更多的公司投入到了RFID技术的研发中来，该技术进一步得到了飞跃，从1比特标签逐步发展到智能卡芯片，并且技术标准化问题日趋得到重视，进入到21世纪，许多经济发达国家已经将其应用到了很多领域，并积极推动相关技术与应用标准的国际化[7]。

在美国，TI，Inter等集成电路厂商目前都在RFID领域投入巨资进行芯片开发，Symbol公司已经研发出可以同时阅读条形码和RFID标签的扫描器，IBM、Microsoft和HP等公司也在积极开发相应的软件及系统来支持RFID的应用。目前，美国正在积极进行将RFID技术全面应用到军需物品中去的研究[8]。

日本是一个制造业强国，它在电子标签研究领域起步较早，政府也将RFID作为一项关键的技术来发展。日本邮政与电信通讯部在2004年3月发布了《关于在传感网络时代运用先进的RFID技术的最终研究草案报告》，报告称邮政与电信通讯部将继续支持测试在UHF频段的被动及主动的电子标签技术，并在此基础上进一步讨论管制的问题；2004年7月，日本经济产业省选择了包括消费电子、书籍、服装、音乐CD、建筑机械、制药和物流等七大产业做为RFID的应用试验。通过与行业应用相结合的基于RFID技术的产品和解决方案的集中出现，为RFID在日本的应用和推广，特别是在物流等非制造领域，奠定了坚实的基础。日前，日本NEC公司宣布，生产笔记本电脑的NEC个人产品公司已在米泽工厂中引进了使用RFID标签的生产管理系统[8]。

虽然韩国的RFID技术起步较晚，但是在政府部门的高度重视下，韩国关于RFID技术的开发和应用试验也在加速展开。由于RFID技术的发展是由产业资源部和情报通信部联合企业的力量来推动的，同日本相似，韩国也将RFID技术向开放系统方向发展。2005年3月，韩国政府耗资7.84亿美元在仁川新建了技术研发中心，主要从事包括RFID研发的电子标签技术开发及生产，以帮助韩国企业快速确立在全球RFID市场的主流地位[8]。

在欧洲，许多大型企业也都在纷纷进行RFID技术的应用试验，如诺基亚公司正在尝试开发基于RFID技术的移动电话购物系统[8]。

我国虽然对于RFID技术的研究起步较晚，基础相对薄弱，不具备规模优势，

但随着1993年中央对于IC卡行业的高度重视，建立了“金卡工程”，以发展我国的IC卡事业。RFID在我国的应用发展十分迅速，建立了自己的AUTO-ID实验室及开放的RFID演示平台，并结合应用中出现的问题进行理论分析和基础研究，为建立中国RFID标准提供参考依据，促进EPC和RFID技术在中国的应用并与国际接轨。此举大大加速了我国国民经济信息化的进程，至今已经取得了不小的成就，并将会在不远的将来制定出符合中国国情的技术标准，推动自主公共服务体系的建设，促进具有竞争力的产业链形成，使我国在该领域占有一席之地。

1.4 任务目标

本课题针对市场的需求，采用最新的一套支持卡片上无源、可分为多个独立存储扇区以支持不同功能的、支持高安全性加密算法的、功能强大的非接触式IC智能射频卡及相应的读写模块，开发应用于快速支付系统中的一整套检票系统。安全、高效、准确的识别是基本要求，对读写机具的研制是关键。

自动检票系统主要由三部分组成：卡片、读写卡器和管理系统。卡片分为普通的客票卡和管理卡，根据功能的不同分配给相应的权限。管理卡可以实现对卡片读写设备设置的修改，以及对读写设备中数据的采集；客票卡可再细分为单次卡、储值卡、计次卡等不同形式，卡内根据需要写有所乘车次的各种信息，有效日期，以及持卡人的个人信息等内容。

读写卡器通过相应的加密算法实现与卡片的安全通信，并实现对卡片信息的读取、写入与修改。该系统实现了可根据需要不定时采集数据而不需依赖网络实时传输，可实现25mm内的非接触操作。同时根据需要可将操作记录保存在读写设备中，以供采集。

管理系统的主要功能是卡片的管理与信息的收集。该系统又分为信息管理系统和发卡机。信息系统管理保存各个卡片信息及采集到的记录信息；对于持卡人长期持有的充次、充值卡，由发卡器实现对新发卡片的激活、充值、锁定等功能。

1.5 本文的主要工作

本文针对市场的需求，采用当前先进的非接触式IC智能卡技术，根据我国全面建设小康社会对铁路客运的发展要求，结合铁道部在十一五铁路规划中在全路实现信息化、自动化、智能化的精神，进行应用于铁路客运快速支付系统中的卡片及读写设备的研制，实现以下技术指标：

工作频率：13.56MHZ

通信速率：106KBps

读写距离：可达 25mm 以上

模块与卡片通信时，数据加密

接口标准：ISO/IEC 14443 TYPE A 标准

工作温度范围：-20℃～+70℃

要求读写机具对铁路客票的安全、高效、准确的识别，性能稳定，高效快速，安全性高，系统安装简便，可完全实现无人职守，大大缩短传统方式的售检票时间，且具备很好的可扩展性，以适用不同应用需要，不仅可广泛应用于铁路客票系统中，还可扩展到公路、公共交通、小商品售卖等领域中。

第2章 智能射频卡及读写模块结构

智能射频卡与相应的读写模块之间的通信与数据交换的核心，是卡片及读写设备中相应的读写模块，卡片与读写模块的性能直接影响支付系统的质量。本文采用 Philips 公司的 MIFARE 1 S50 类型的微晶片作为 IC 智能卡的核心模块，Philips 公司的 MCM200 芯片作为读写设备中的核心读写模块，识别卡片信息，并且对卡片进行相应的读写操作。

2.1 Mifare 1 S50

Mifare 1 S50 型 IC 智能射频卡是 PHILIPS 公司生产的一款目前市场上最新的 IC 射频卡微模块。其采用先进的芯片制造工艺，内建高速 CMOS EEPROM，MCU 等，这样可使制成成品的卡片上除了 IC 微晶片和一副高效率天线外，做到无任何其他元件。

2.1.1 主要特征

1. 卡片构造

卡片上内建 8K（bit）的 EEPROM 存储容量，并划分为 16 个扇区，每个扇区划分为 4 个数据存储块，每个扇区可有多种方式的密码管理。此外还内建有增值/减值的专项数学运算电路，非常适合应用于需要检票/收费的相关行业中。

2. 电源及工作频率

卡片上无源，工作时的电源能量由卡片读写器天线发送无线电载波信号耦合到卡片上天线而产生电能，一般可达 2V 以上，供卡片上 IC 工作。工作频率 13.56MHZ。

3. 操作距离与通信速率

依不同的读写器核心模块设备，卡片的操作距离可在 10mm 至 100mm 不等；与读写器间的通信速率可达 106Kbit/s。

4. 卡片识别与防冲突

卡片制造时具有唯一的卡片系列号，没有重复的相同的两张 Mifare 卡片。卡上具有先进的数据通信加密并双向验证密码系统；且具有防重叠功能：可选择在同一时间处理重叠在卡片读写器天线的有效工作距离内的多张重叠的卡片或选择其中某一张来进行操作。

5. 通信方式及相关标准

卡片与读写器通信使用握手式半双工通信协议；Mifare 1 射频卡所具有的独特的 Mifare RF(射频）非接触式接口标准已被制定为国际标准：ISO/IEC 14443 TYPE A 标准。

2.1.2　功能组成

整个 Mifare 卡按照电路功能分可以分为两大部分：RF 射频接口电路和数字电路部分。各功能模块组成如图 2-1 所示。

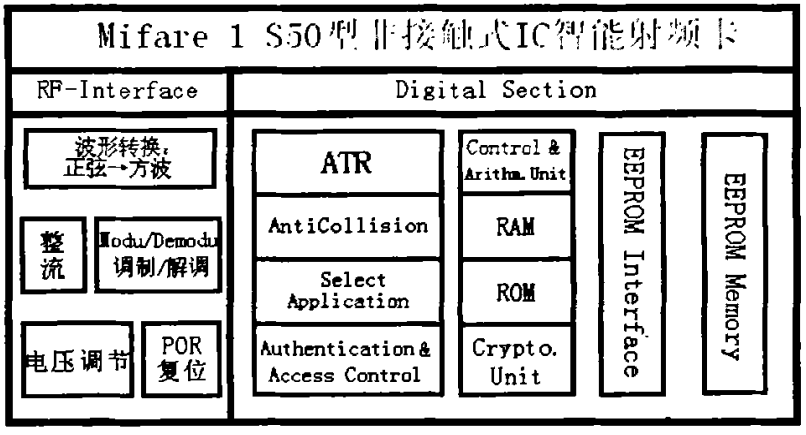


图 2-1 Mifare 1 S50 非接触式 IC 智能射频卡各功能模块组成示意图

Figure 2-1 Mifare 1 S50 contactless IC card function module composing

一、RF 射频接口电路：RF-Interface

在 RF 射频接口电路中，主要包括有波形转换模块。它可将卡片读写器上的 13.56MHz 的无线电调制频率接收，一方面送调制/解调模块，另一方面进行波形转换，将正弦波转换为方波，然后对其整流滤波，由电压调节模块对电压进行进一步的处理，包括稳压等，最终输出供给卡片上的各电路。

POR 复位模块主要是对卡片上的各个电路进行 POWER-ON-RESET（上电复位），使各电路同步启动工作。

二、数字电路部分：Digital Section

1. ATR 模块（请求之应答）：Answer to Request

当一张 Mifare 1 卡片处在卡片读写器的天线工作范围内时，读写器向卡片发出 REQUEST ALL 命令后，卡片的 ATR 模块将启动，将卡片 Block 0 中的卡片类型（TagType）号共 2 个字节传送给读写器，建立卡片与读写器的第一步通信联络。

如果不进行第一步的 ATR 工作，读写器对卡片的其他如读、写等操作将不会进行。

2. AntiCollision 模块：

该模块起防重叠功能。当有多张 Mifare 1 卡片处在卡片读写器的天线工作范围内时，AntiCollision 模块的防重叠功能将被启动。在程序员控制下的卡片读写器将会首先与每一张卡片进行通信，取得每一张卡片的系列号。由于每一张 Mifare 1 卡片都具有唯一系列号，因此卡片读写器将根据卡片的序列号来识别、区分已选择的卡片。卡片读写器内 MCM 中的 AntiCollision 防重叠功能配合卡片上的防重叠功能模块，由程序员来控制读写器，根据卡片的序列号来选定一张卡片。被选中的卡片将直接与读写器进行数据交换，未被选择的卡片则被给予一定的时延而处于等待状态，在时延到达后尝试与卡片读写器再次通信。

3. Select Application 模块：

该模块主要用于卡片的选择。当卡片与读写器完成上述两个步骤，程序员控制的读写器要想对卡片进行读写操作，必须对卡片进行选择（select）操作，以使卡片真正地被选中。被选中的卡片将卡片上存储在 Block 0 中的卡片容量“Size”2 个字节传送给读写器。当读写器收到该字节后，将明确可以对卡片进行进一步操作，如进行密码验证等。

4. Authentication & Access Control 模块：

该模块为认证及存取控制模块。在确认了上述三个步骤，成功选择了一张卡片后，在程序员对卡片进行读写操作之前，必须对卡片上已经设置的密码进行认证，如果匹配，则允许进一步的读、写操作。Mifare 1 卡片上共有 16 个扇区，每个扇区都可分别设置各自的密码，互不干涉，每个扇区可独立地应用于一个应用场合，因此使整个卡片成为真正可一卡多用的“一卡通”成为可能。

在卡片认证时，采用三次认证过程，如图 2-2 所示。

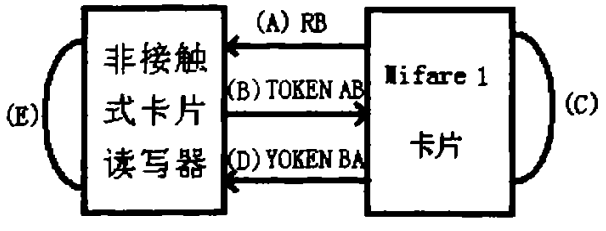


图 2-2 三遍认证过程示意图

Figure 2-2 Three times authentication process

认证过程如下：

A：由 Mifare 1 卡片向读写器发送一个随机数据 RB；

B：由读写器收到 RB 后向 Mifare 1 卡片发送一个令牌数据 TOKEN AB，其中包含了读写器发出的一个随机数据 RA；

C：Mifare 1 卡片收到 TOKEN AB 后，对 TOKEN AB 的加密的部分进行解密，并校验第一次由（A）环中 Mifare 1 卡片发出去的随机数 RB 是否与（B）环中接收到的 TOKEN AB 中的 RB 相一致；

D：如果（C）环校验是正确的，则 Mifare 1 卡片向读写器发送令牌 TOKEN BA 给读写器；

E：读写器收到令牌 TOKEN BA 后，将对令牌 TOKEN BA 中的 RB 进行解密，并校验第一次由（B）环中读写器发出去的随机数 RA 是否与（D）环中接收到的 TOKEN BA 中的 RA 相一致；

如果上述的每一个环都能正确通过验证，即都为“真”，则整个认证过程将为成功，读写器将能对刚刚认证通过的卡片上的相应扇区进入下一步的操作。反之，若认证过程中的任何一环出现差错，则整个认证将告失败，必须重新开始。

同样，卡片中的其他扇区由于各自有其密码，因此若想对其他扇区进行操作，也必须完成上述的认证过程。

5. Control & Arithmetic Unit：

该模块为控制及算术运算单元，这一单元是整个卡片的控制中心，是卡片的“头脑”。它主要进行对整个卡片的各个单位进行微操作控制，协调卡片的各个步骤；同时它还对各种收/发的数据进行算术运算处理，递增/递减处理，CRC 运算处理，等等。是卡片中内建的中央微处理机 MCU。

6. RAM/ROM 单元：

RAM 主要配合控制及算术运算单元，将运算的结果进行暂时存储，如果某些数据需要存储到 EEPROM，则由控制及算术运算单元取出送到 EEPROM 存储器中；如果某些数据需要传送给读写器，则由控制及算术运算单元取出，经过 RF 射频接口电路的处理，通过卡片上的天线传送给卡片读写器。RAM 中的数据在卡片失掉电源后（卡片离开读写器天线的有效工作范围内）将被清除。

同时，ROM 中还固化了卡片运行所必需的程序指令，由控制及算术运算单元取出去对每个单元进行微指令控制，使卡片能有条不紊地与卡片的读写器进行数据通信。

7. Crypto Unit 数据加密单元：

该单元完成对数据的加密处理及密码保护，加密的算法可以为 DES 标准算法或 SSF33 算法等。

8. EEPROM INTERFACE/EEPROM MEMORY：

该单元为 EEPROM 存储器及其接口电路，主要用于数据的存储。EEPROM 中的数据在卡片掉电（卡片离开读写器天线的有效工作范围内）后仍将被保持，用户所要存储的数据被存放在该单元中。Mifare 1 卡片中的这一单元容量为 8196bit，分为 16 个扇区。

2.1.3　存储结构

Mifare 1 卡片的存储容量为 8192 bit×1 位字长（即 1K×8 位字长），采用 EEPROM 作为存储介质，整个结构划分为 16 个扇区，编为扇区 0~15。每个扇区有 4 个块（Block），分别为块 0、块 1、块 2 和块 3，每个块为 16 个字节。一个扇区共有 16Byte×4=64Byte。如下图所示：

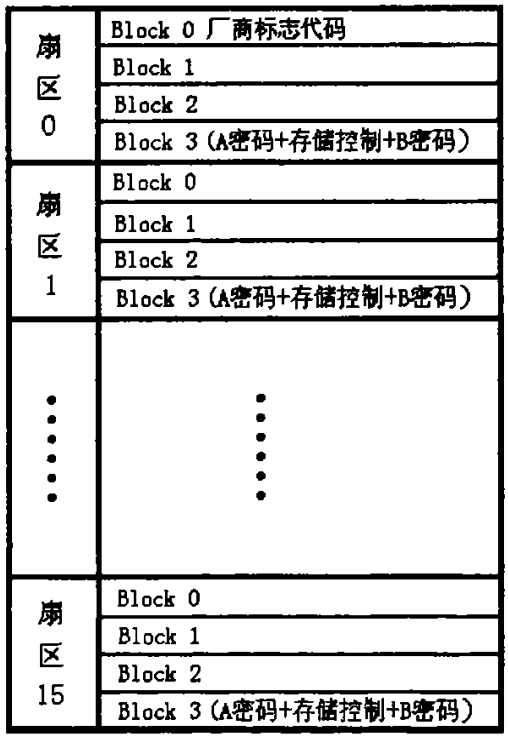


图 2-3 Mifare 1 卡片存储结构

Figure 2-3 The memory structure of Mifare 1

扇区 0 的块 0 是特殊的，是厂商代码，已经固化，不可改写。其中第 0~4 个字节为卡片的序列号，第 5 个字节为序列号的校验码，第 6 个字节为卡片的容量“SIZE”字节，第 7，8 个字节为卡片的类型号字节，即 Tagtype 字节，其他字节可另加定义。基于保密性和系统的安全性，这一块在 IC 卡厂商编程之后被置为写

保护，因此该块不能再复用为应用数据块。

例如，读取的数据是 420A7E00368804004481740630373937H，则序列号 SN 为 420A7E00H 和校验码 36H，容量字节是 88H，卡类型号为 0400H。

此外，每个扇区的块 3 包含了该扇区的密码 A（6 个字节）、存取控制（4 个字节）、密码 B（6 个字节），是一个特殊的块，其余三个块是一般的数据块（0 号扇区的块 0 除外）。

例如，如果块 3 中的值为 $A_0A_1A_2A_3A_4A_5FF078069B_0B_1B_2B_3B_4B_5$，则 $A_0A_1A_2A_3A_4A_5$ 是密钥 A，$B_0B_1B_2B_3B_4B_5$ 是密钥 B，FF078069 为读写控制位，卡初始化后的存取控制条件为：密码 A 永不可读，校验密码 A 或密码 B 正确后可以修改；密码 B 在校验密码 A 或密码 B 正确后可读，可修改；数据块在校验密码 A 或密码 B 正确后可读，可修改。

2.2 MCM200

MCM 的全称是 Mifare Core Module，即 Mifare 核心模块。MCM 智能模块被用于读写 Mifare 1 非接触式 IC 智能射频卡的读写器中，负责读写器中对非接触式 IC 智能射频卡片的读写等功能，一般在读写器中还必须有 MCU 来对 MCM 进行控制，及对读写器的其他方面如键盘、显示、存储、通信等部分进行控制等。

2.2.1 主要特征

1. 芯片构造

MCM200 型核心读写模块为标准的双列直插 32 引脚的芯片，内有 16 个字节的 FIFO（先进先出）队列接收/发送缓冲寄存器。

2. 电源及工作频率

标准的＋5V 供电，供电范围 4.75V~5.25V。典型工作状态下电流消耗 40mA，最大不超过 80mA，最小不低于 10mA。工作频率 13.56MHZ。

3. 操作距离与通信速率

读写卡片距离可达 25mm 以上；与卡片间的通信速率可达 106Kbit/s。

4. 卡片识别与防冲突

模块与卡片通信时，数据加密，在对卡片进行认证时，采取 3 次认证过程，对卡片上通过认证的相应扇区进行下一步操作；且具有防重叠功能：可选择在同一时间处理重叠在卡片读写器天线的有效工作距离内的多张重叠的卡片或选择其中某一张来进行操作。

5. RF特性及相关标准

模块可对RF射频通道自动监控，支持多种方式的活动天线，并且不需天线调节系统对天线进行补偿调节；符合ISO/IEC 14443 TYPE A标准。

2.2.2 引脚说明

MCM200模块为标准的双列直插32引脚的芯片，其引脚图如图2-4所示：

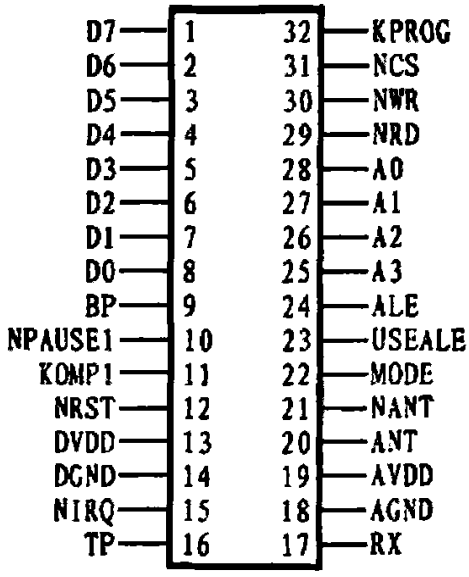


图2-4 MCM200型核心模块引脚图

Figure 2-4 Pins of MCM200

D0~D7：8位双向数据总线；

A0~A3：4位地址线；

BP：后备电池输入端，用于保护MCM内部密码RAM；

NPAUSE1：串行数据输出，用于驱动RF单元，该引脚必须连到RF单元的TP端；

NWR：写信号使能端；

NRD：读信号使能端；

NCS：该脚为低电平时选中MCM；

KOMP1：RF的比较输入端，使用时必须连到RF单元的RX端；

NIRQ：MCU数据处理控制端。当该端为低时，MCU将用MCM状态寄存器中的内容来对MCM中的数据进行处理；

ALE：地址锁存使能端；

USEALE：选择从内部地址锁存器或 A0~A3 引脚取地址；

DGND：数字电路接地端；

DVDD：＋5V 电源端；

MODE：并行协议模式选择引脚，可用高电平驱动；

AVDD：＋5V 模拟电源输入引脚，用于 RF 射频单元；

AGND：RF 射频单元(模拟电路)接地端；

NANT、ANT：天线连接端；

2.2.3　内部寄存器描述

MCU 是通过对 MCM 内核特殊的内存寄存器的读写来控制 MCM 的。这些寄存器位于 MCM 中的 ASIC（特殊应用 IC）内部，共有 16 个寄存器可存取。在对 MCM 进行读/写操作时，各寄存器担负着不同的功能和作用，并且不是所有的寄存器都是可写或可读的，即有些寄存器只能读而不能写,有些则反之。

MCM 实际上是 MCU 与非接触式 IC 智能射频卡之间信息（数据）交换的“中间人”。任何读取卡片上的数据，或写进卡片上的数据均必须通过 MCM 来传递。写 MCM 意味着去控制 MCM，例如，送一些类型的指令给它。

以下是 MCM 中 ASIC 内核特殊寄存器一览表。

表 2-1 MCM - ASIC 寄存器

Table 2-1 Registers of MCM-ASIC

寄存器名	地址	读	写
DATA	00H	READ-BYTE	WRITE-BYTE
STACON	01H	DV TE PE CE BE AE - -	SOR RFS - - 1 1 NRF AC
ENABLE	02H	N/A	1 PR CE CR - - - - - -
BCNTS	03H	N/A	BIT-COUNT-SEND
BCNTR	04H	N/A	BIT-COUNT-RECEIVE
BAUDRATE	05H	N/A	- - - - - 1 1 1 BR
TOC	06H	N/A	TIMEOUT-COUNTER
MODE	07H	N/A	1 1 0 0 0 P2 P1 P0
CRCDATA	08H	CRC-BYTE-READ	CRC-BYTE-WRITE
CRCSTACON	09H	CV - - - - - - - - CZ	C8 - - - - - - - - CR
KEYDATA	0AH	N/A	KEY-BYTE-WRITE
KEYSTACON	0BH	- - - - - - - - - -	AL 0 - - - - - - KS1 KS0
KEYADDR	0CH, 0DH	N/A	AL AB A5 A4 A3 A2 A1 A0
RCODE	0EH, 0FH	N/A	- - - - - - 0 0 RC1 RC0

各个寄存器的说明如下：

1. DATA 寄存器：

寄存器名	地址	读	写
DATA	00H	READ-BYTE	WRITE-BYTE

任何传递到 Mifare 1 卡的数据或来自 Mifare 1 卡的数据都必须分别地被写入 DATA 寄存器或从 DATA 寄存器中读出。例如，MCU 向卡片写数据 Xi，则 Xi 必须首先被写入到 DATA 寄存器中，然后再 MCM 与 Mifare 1 卡片进行通信，由卡片上的 ASIC 将 DATA 寄存器中的数据读取并存放在卡片上指定的存储器中，从而完成 MCU 向 Mifare 1 卡片写数据的过程。

DATA 寄存器中有一个 16Byte 的 FIFO（先进先出）队列寄存器。 数据写到 DATA 寄存器后，被存放在这个 16Byte 的 FIFO（先进先出）队列寄存器中，等待向卡片或 MCU 传送。

2. STACON 寄存器

寄存器名	地址	读	写
STACON	01H	DV TE PE CE BE AE -- --	SOR RFS -- -- 1 1 NRF AC

SATCON 是 STATUS CONTROL（状态控制）的缩写，是一个状态控制寄存器。

将数据写到 STACON 寄存器中将对 MCM 进行状态控制，具体如下表：

表 2-2 STACON 寄存器的写控制

Table 2-2 Writing control of STACON register

Bit name	Name	Function
SOR	Soft Reset (软复位)	"0"—表示无作用 "1"—自动清除一切
RFS	RF-Select (RF 选择)	"0"—RF 单元 0 被选中激活 "1"—RF 单元 1 被选中激活
NRF	No RF (无 RF)	"0"—将活动 RF 单元接上 "1"—将活动 RF 单元关闭
AC	Anti Collision (防重叠)	"0"—不启动防重叠状态机制 "1"—启动防重叠状态机制

当写数据到 STACON 寄存器时（即对 STACON 寄存器进行设置），在写数据到 STACON 寄存器的这一写周期中，RFS 位的设置必须与 RF 单元相互一致。另外，设置了 AC 位，即"AC=1"，将使防重叠状态机启动工作，执行内部存取。为了保证防重叠状态机处理软件的正确运行，让其能识别叠放在一起的多张 Mifare 1 卡片，为下一步进行选择一张指定 SN（Serial Number）的 Mifare 1 卡片进行数据读/写而作准备，这一存取在设置 AC 位后的 12μs 开始，至 35μs 结束，在这一时间间隔内，不允许 MCU 向 MCM 进行写（WRITE）数据操作，必须延迟 35μs。

读取 STACON 寄存器，将告诉我们一系列 MCM 及卡片的当前状况信息。以下是读取 STACON 寄存器后的一系列标志位表。

表 2-3 STACON 寄存器的读信息

Table 2-3 Read information of STACON register

Bit name	Name	Function
DV	Data Valid（数据有效）	卡上的数据传输到 FIFO 寄存器中。DV 位也可以在正确的认证操作完成后而被设置。
TE	Timeout Error （溢出出错）	定时计数器溢出
PE	Parity Error （奇/偶校验错）	通讯时发生奇/偶校验错
CE	CRC Error （CRC 错）	通讯时有 CRC 错
BE	Bitcount Error（位记数器出错）	在 BCNTR 寄存器中有大量的指定 bits（位）没有收到。
AE	Authentication（认证出错）	卡的认证应答码不正确或当执行一个取密码操作时指定的 ROM KEY（只读存储器中密码）不正确。

当卡片上的数据流接收结束或没有被接收时，STACON 寄存器中的 DV 标志被置位“1”，并且 MCM 上的引脚 NIRQ 也将由“HIGH”变为“LOW”。仅当 DV 位被设置有效（即 DV=1）时，TE、PE、CE、BE 及 AE 标志才有效。但有一例外，即当认证正确完成后，AE 标志也直接有效。当执行 SOR 后，所有的这些标志将被清除，且当对 MCM 的任何一个寄存器执行写周期时，所有的这些标志也将被清除。

当 MCM 接收少于 8bits 时，MCM 将不影响 PE、CE、及 AE 标志。

3. ENABLE 寄存器

ENABLE 寄存器的设置将影响卡片在通信时对 parity 和 CRC 的校验。在 ENABLE 寄存器中有针对 parity 和 CRC 校验的复位允许位（reset ENABLE bits）。

寄存器名	地址	读	写
ENABLE	02H	N/A	1 PR CE CR -- -- -- --

对 ENABLE 寄存器进行写操作，将执行对 parity 和 CRC 块的控制。

表 2-4 ENABLE 寄存器的写控制

Table 2-4 Writing control of ENABLE register

Bit name	Name	Function
PR	Parity Reset（Parity 复位）	"0"—无效 "1"—复位 parity 块，自动清除
CE	CRC ENABLE（CRC 使能）	"0"—关闭 CRC 发生器及校验 "1"—打开 CRC 发生器及校验
CR	CRC Reset（CRC 复位）	"0"—无效 "1"—复位 CRC 块，自动清除

在对 MCM 进行编程时，必须对 ENABLE 寄存器进行写操作，即必须将 CE 位关闭，仅当执行"Select"命令操作时才打开 CE 位；由于 MCM 在电源接通或在任何数据通信开始时都会复位 Parity 和 CRC 块，因此无须额外地去执行这一操作。

4. BCNTS 寄存器

BCNTS（Bit-Counter-for-Sending）即传送时的位计数器。

寄存器名	地址	读	写
BCNTS	03H	N/A	BIT-COUNT-SEND

这里的传送指的是 CPU 向 MCM 的 DATA 寄存器写数据。因此 BCNTS 寄存器实际上是一个字节发送控制器，它控制了 MCU 向 DATA 寄存器中写进的数据字节数目。如要传送 DATA 寄存器中的数据，必须首先设定要传输多少位（bit）或多少字节（Byte），即必须对 BCNTS 寄存器进行有效的正确设置，以确定有多少字节将要被传送。

由于 BCNTS 寄存器是控制向 DATA 寄存器写数据的字节数目，因此这一操作必须在数据写入 DATA 寄存器之前完成，使用 2 进制代码来操作。在大量的字节数据被写入 DATA 寄存器之后，MCM 自动地与卡片进行通信。

5. BCNTR 寄存器

BCNTR（Bit-Counter-for- Receiving）即接收时的位计数器。

寄存器名	地址	读	写
BCNTR	04H	N/A	BIT-COUNT-RECEIVE

与 BCNTS 寄存器相反，BCNTR 寄存器控制了 MCU 读取 DATA 寄存器的数据字节数目。由于 BCNTR 寄存器是控制向 DATA 寄存器读取数据的字节数目，因此这一操作必须在读 DATA 寄存器之前完成，使用 2 进制代码来操作。BCNTR 寄

存器中的值将与实际接收到的数据字节相比较，如果有差别，则 STACON 寄存器中的 BE 标志被设置。

6. BAUDRATE 寄存器

BAUDRATE 为位速率寄存器，即卡片与 MCM 之间传输数据时通信的位速率。虽然 BAUDRATE 寄存器的后四位相关于指定的位速率，但实际有用于 MIFARE 1 卡的只是最后一位。

寄存器名	地址	读	写
BAUDRATE	05H	N/A	-----111BR

BAUDRATE 寄存器的设置将直接影响着 MCM 与 Mifare 1 卡片之间的数据通信速率。MCM 中有一个时钟发生器（Clock Generator），写数据至 BAUDRATE 寄存器，可以控制时钟发生器。位速率的计算公式为

$$t_{bit} = \frac{(BRX + 2) \times 8}{13.56} \mu s \tag{2-1}$$

若 BRX=0x0Eh，则有 t_{bit}=9.44μs，即 105.94kHz。上述 BRX=0x0Eh 为对 BAUDRATE 寄存器进行设置的推荐值，即初始化时 BAUDRATE 寄存器应设置为：00001110b=0Eh。

7. TOC 寄存器

TOC(Time Out Counter)即时间溢出记数器。

寄存器名	地址	读	写
TOC	06H	N/A	TIMEOUT-COUNTER

对 TOC 寄存器的设置即对定时时间的控制，写数据至 TOC 寄存器，可以控制定时溢出记数器。定时溢出公式为：

$$t_{TO} = 100 \times TOC \mu s \tag{2-2}$$

该寄存器中的值必须在 MCM 与 MIFARE 1 卡片通信时被设置，TOC 寄存器常用的设置值为 0Ah，相应的 t_{TO}=100×10μs=1ms。

TOC 寄存器中的值将在没有通信时被永久地递减，因此在没有通信或通信刚结束时，TOC 寄存器中的值必须被设置，即设置 TOC=0x00H，否则将影响 STACON 寄存器中的 TE 出错标志。如果有溢出出现，则 TE 标志被设置，DV 标志将被激活。

一般在读取和保存了 STACON 寄存器中的数据之后，定时溢出记数器必须被关闭。

8. MODE 寄存器

MODE（MODE of DATA coding），即与卡片数据相互往来时的数据编码模式，其设置控制了 MCM 与卡片数据通信时的数据编码模式。该寄存器的每一位都与数据通信模式有关，但在使用 MIFARE 1 卡时，只与最后 3 位相关联。

寄存器名	地址	读	写
MODE	07H	N/A	1 1 0 0 0 P2 P1 P0

写数据至 MODE 寄存器，可以控制接收器和发生器。

9. CRCDATA 寄存器

计算 CRC 的数据必须被写入 CRCDATA 寄存器中，计算后的 CRC 也必须从 CRCDATA 寄存器中读出。

寄存器名	地址	读	写
CRCDATA	08H	CRC-BYTE-READ	CRC-BYTE-WRITE

在写入一个 Byte 到 CRCDATA 寄存器后，计算开始；计算完成后，STACON 寄存器的 CV 标志将被设置。当要写下一个字节到 CRCDATA 寄存器或在读取 CRCDATA 寄存器以得到 CRC 之前，或在检查 CZ 标志之前，都必须先读取、检查 CV 标志。

10. CRCSTACON 寄存器

CRCSTACON 是 CRC 处理器状态和控制寄存器。

寄存器名	地址	读	写
CRCSTACON	09H	CV - - - - - - - - CZ	C8 - - - - - - - - CR

写数据到 CRCSTACON 寄存器中，即执行对 CRC 处理器的控制。

表 2-5 CRCSTACON 寄存器的写控制

Table 2-5 Writing control of CRCSTACON register

Bit name	Name	Function
C8	8 bit CRC	“0”—选择 16 位 CRC 处理器 “1”—选择 8 位 CRC 处理器
CRE	CRE (CRC 复位)	“0”—无效 “1”—复位 CRC 处理器

读取 CRCSTACON 寄存器后用户将知道 CRC 处理器数据传输的状态。当标志被设置为“1”时，标志被激活。

表 2-6 CRCSTACON 寄存器的读信息

Table 2-6 Read information of CRCSTACON register

Bit name	Name	Function
CR	CRC-Ready	最后一个字节被处理完成
CZ	CRE-Zero	CRC 寄存器内容为 00H，即 CRC-校验完成

11. KEYDATA 寄存器

被存储在 MCM 中 RAM 的密码数据必须先被写入 KEYDATA 寄存器中。

寄存器名	地址	读	写
KEYDATA	0AH	N/A	KEY-BYTE-WRITE

为了能够存取 MCM 内部 RAM 中的密码，密码的存放地址必须首先在 KEYSTACON 寄存器和 KEYADDR 寄存器两者中指定。在做密码存放或密码验证前，必须首先对 KEYSTACON 寄存器进行设置，在密码存入 RAM 之前，相关的传输密码 Tkey（Transport key）必须被写入 KEYDATA 寄存器中。传输密码和写入 RAM 中的密码都是 6Byte 长，连续被写入 KEYDATA 寄存器中。但在 AUTHENCATION 操作时这一寄存器不必使用。

12. KEYSTACON 寄存器

KEYSTACON 寄存器是指密码 Key 状态和控制寄存器。

寄存器名	地址	读	写
KEYSTACON	0BH	----------	AL 0 ------ KS1 KS0

写入数据到 KEYSTACON 寄存器进行设置，将确定存取 RAM 中的密码(Key)或传输密码（Key）的密码地址的一部分。

表 2-7 KEYSTACON 寄存器的写控制

Table 2-7 Writing control of KEYSTACON register

Bit name	Name	Function
AL	Authenticate//Load Keys	“0”—准备提取密码 “1”—准备认证
KS1,KS0	Key-Set (密码集)	“00”—选择 RAM，Key-set0 “01”—选择 RAM，Key-set1 “10”—选择 RAM，Key-set2 “11”—选择传输密码

AL=0，表明将要进行提取密码；AL=1，表明将要进行认证操作。

13. KEYADDR 寄存器

KEYADDR 寄存器将存放 RAM 密码 Key 和传输密码 Key 各自的密码地址的一部分。

寄存器名	地址	读	写
KEYADDR	0CH, 0DH	N/A	AL AB A5 A4 A3 A2 A1 A0

写入数据到 KEYADDR 寄存器将确定存取 MCM 的 RAM 中的密码或传输密码的密码地址的一部分。

表 2-8 KEYADDR 寄存器的写控制

Table 2-8 Writing control of KEYADDR register

Bit name	Name	Function
AL	Authenticate//Load Keys	“0”—准备提取密码 “1”—准备认证
AB	KeyA or KeyB	“0”—使用密码 A “1”—使用密码 B
A5…A0	Key address	指定密码的地址 A5 至 A0

14. RCODE 寄存器

该寄存器用于代码接收。

寄存器名	地址	读	写
RCODE	0EH, 0FH	N/A	-- -- -- -- 0 0 RC1 RC0

写入数据到 RCODE 寄存器对其进行设置，将使接收器的译码器参数化。

2.3 本章小结

本章先是从主要特征、功能组成及存储结构的角度，对所选用的 Philips 公司生产的 Mifare 1 S50 型号的智能射频卡芯片做了详细的介绍，之后对与之相应的核心读写模块 MCM200 型芯片做了细致的说明，阐述了其主要特征、引脚说明，并详细描述了其芯片内部的各个寄存器。

第3章 快速支付系统的软、硬件设计与实现

读写器作为读写卡片的有效工具，其关键部分是 MCU 和非接触 IC 射频卡核心读写模块的选择。在开发过程中，本文主要围绕这两部分及其相应的外围电路进行软、硬件的设计工作。

3.1 系统结构

快速支付系统的系统框图如图 3-1 所示：

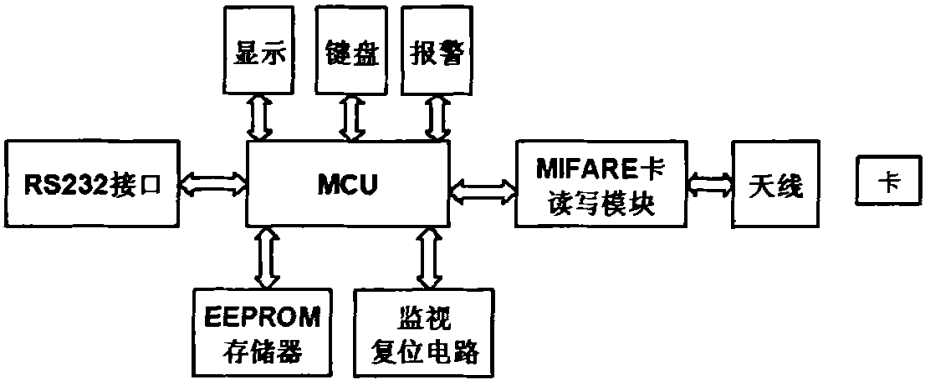


图 3-1 系统结构原理框图

Figure 3-1 Principle frame of system structure

本方案中 IC 卡结构较为简单，只需采用 Mifare 1 S50 型智能 IC 射频芯片和一副天线即可，智能卡片的读写设备将作为本系统的重点介绍。本方案选用 Philips 公司与 Mifare 卡片相配套的 MCM200 型读写模块作为读写设备系统的核心模块，完成对 Mifare 1 智能射频卡的控制与读写操作；EEPROM 存储功能模块采用 Atmel 公司 24C64 芯片，监控电路采用 Dallas 公司生产的 DS1232LP 型芯片，显示电路中采用 Motorola 公司的 MC14499 显示模块，TS232 接口电路部分采用 TelCom 公司生产的 RS-232 芯片。单片机选用 Atmel 公司 AT89C52 芯片，其内建有 8K 的 EEPROM，256bytes 的 RAM，内设 P0、P1、P2、P3 等四个端口，主要完成对 MCM200 核心模块的初始化与配置工作，并控制该模块与射频卡的通信，以及 LED 显示、键盘输入、串口通信程序等。

3.2 系统的硬件设计

本系统中最典型的操作是 MCU 控制 MCM 核心读写模块，通过 RF 单元和卡片建立通信，进行对卡片的识别与读写操作，并将记录操作结果的数据保存在 EEPROM 中，以备上位机的采集。因此，MCM 核心读写模块与 RF 单元的接口电路，MCU 对 MCM 核心读写模块、EEPROM 存储模块和 TC232 接口电路的控制以及监控复位模块将在本节被重点介绍。

3.2.1 核心读写模块与单片机间接口电路

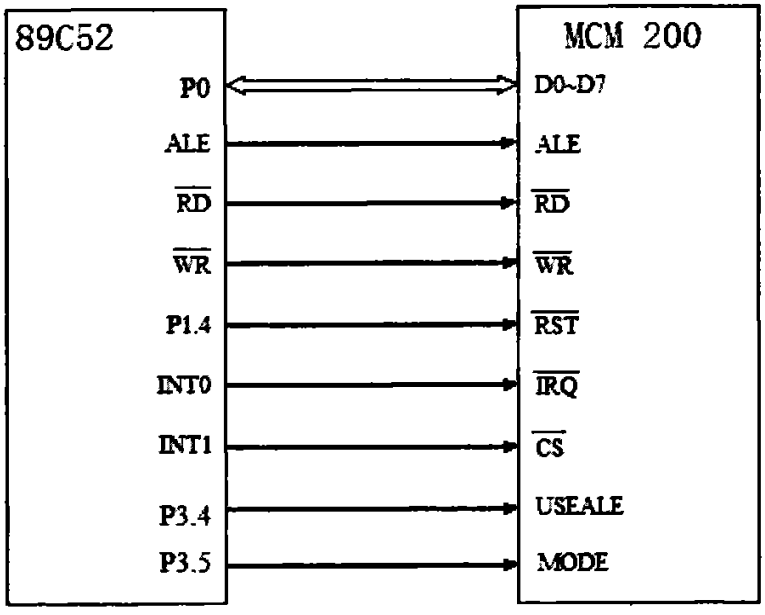


图 3-2 读写核心模块与单片机间接口电路

Figure 3-2 Interface circuit between MCM and MCU

本方案中 MCM200 核心读写模块对卡片的读写工作是由 89C52 单片机驱动及控制的。MCU 的 INT1 口驱动 MCM 的 NCS 端，当其为低电平时，激活该 MCM 模块；MCU 的 INT0 口通过 MCM 的 NIRQ 端控制其对数据进行处理，当为低电平时，MCU 将用 MCM 状态寄存器中的内容来对 MCM 中的数据进行处理，并可用查询或中断方式接收 MCM 发送的数据 ；MCU 和 MCM 间直接用数据总线传送地址和数据，ALE 相互对接，读写模块的 MODE、USEALE 接高电平，A0~A3 悬空；MCU 的 P1.4 口控制 MCM 的复位端 NRST。

3.2.2　核心读写模块与 RF 单元接口电路

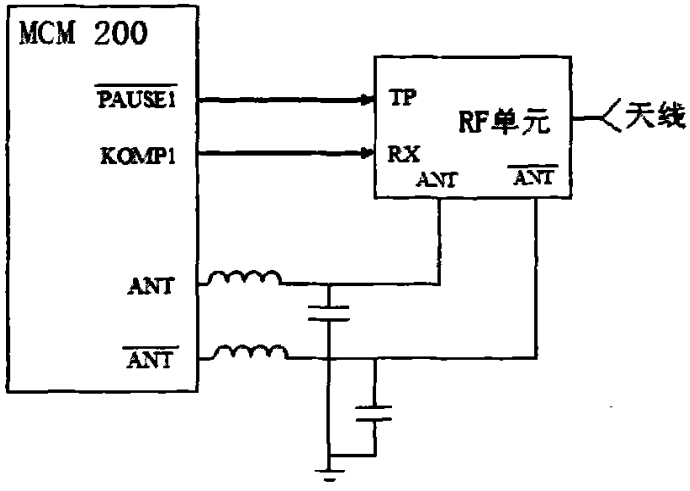


图 3-3 读写核心模块与 RF 单元间接口电路

Figure 3-3 Interface circuit between MCM and RF

MCM 模块的 NPAUSE1 端为串行数据输出端，与 RF 单元的 TP 端相连，驱动 RF 单元；KOMP1 端为 RF 的比较输入端，与 RF 单元的 RX 端相连；ANT、NANT 是天线端点，分别接天线的两端，同时必须对地接高频滤波电容，并串接高频电感，以组成 MCM200 输出信号的滤波电路。为了达到良好的电磁兼容，这些元件在布局时有严格的要求，必须紧靠 MCM 的 ANT 和 NANT 引脚。

3.2.3　存储模块接口及电路

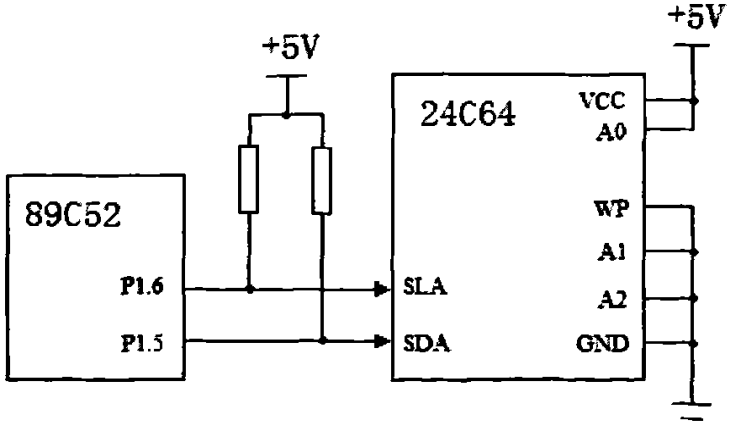


图 3-4 EEPROM 存储单元电路

Figure 3-4 Interface circuit of EEPROM

在存储模块中，本文采用 Atmel 公司的 24C64 型号的 EEPROM 作为读写设备的存储单元。WP 为写保护功能，接低电平，若需对存储区进行编程，则需事先将此端接至高电平。MCU 的 P1.5 口与 EEPROM 的串行数据端 SDA 相连，实现数据收发功能，1.6 口控制 EEPROM 的串行时钟端 SCL，当其为低电平时，数据由 MCU 的 P1.5 口送往存储模块的 SDA 数据总线，高电平时，SDA 总线上数据稳定，可供读写器读写。

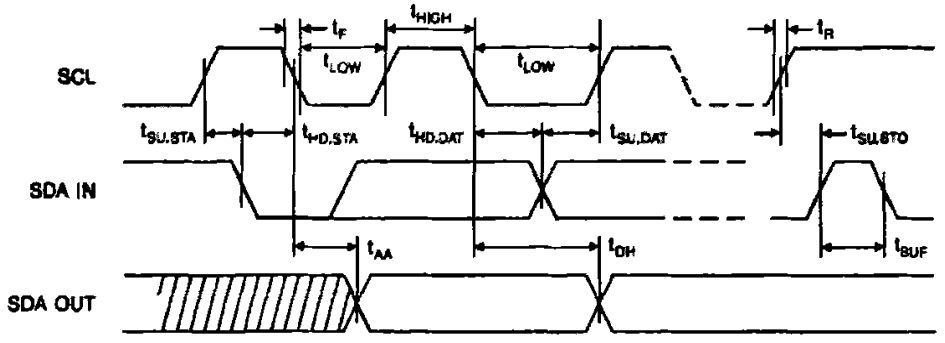


图 3-5 存储模块读写操作时序

Figure 3-5 Read-write scheduling of memory module

3.2.4 监视复位电路

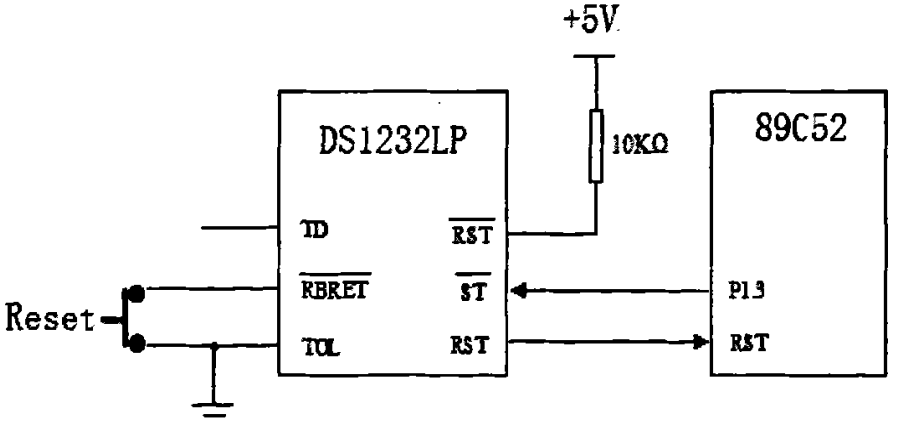


图 3-6 监视复位电路

Figure 3-6 Reset circuit

本文采用 Dallas 公司生产的 DS1232LP 作为本系统的监视复位单元。在电路设计中，TD 端为延迟时间设定端，接其高电平时间将被设定延迟为 1.2 秒，将其

悬空延迟时间将被设定为 0.6 秒，将其接地延迟时间将被设定为 0.15 秒。综合考虑本系统的实际情况，本文将其延迟时间设置为 0.6 秒，即以 600ms 为一个周期，在每个 600ms 周期内，NST 端必须至少收到一次高电平向低电平转换的下降沿，否则 RST 端会向 MCU 的复位端 RST 发出复位信号，强制其复位。

3.2.5　TC232 接口电路

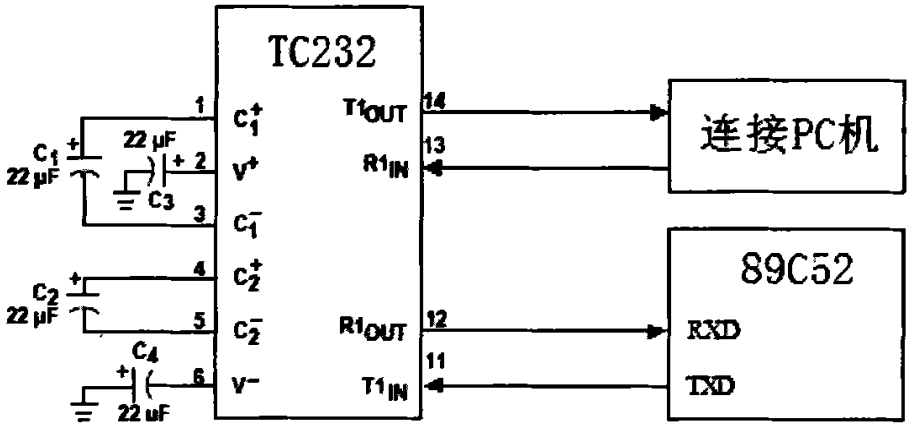


图 3-7 TC232 接口电路

Figure 3-7 Interface circuit of TC232

本系统与上位机间的通信采用 TC232 串口通信方式，TC232 芯片的 R1OUT 和 T1IN 管脚分别与 MCU 的 RXD 端和 TXD 相连，在信息采集时执行对 MCU 的数据存取，T1OUT 和 R1IN 分别与上位机串口的 2、3 号相连，在信息采集时执行对 PC 机的数据存取。

3.2.6　电源供应电路设计

本读卡器内所有芯片的工作电压均为 5V，读卡器采用外接电源供电，220V 市电经变压器降压，再经稳压电路稳压成 5V 后供应读卡器内芯片。本读卡器选用东芝公司的 TA78L05S 稳压芯片，该稳压芯片具有以下特点：

—内部短路电流保护

—内部过热保护

—最大输出电流为 100mA

—输出 5V 电压

稳压电路的电路连接如图 3-8 所示：

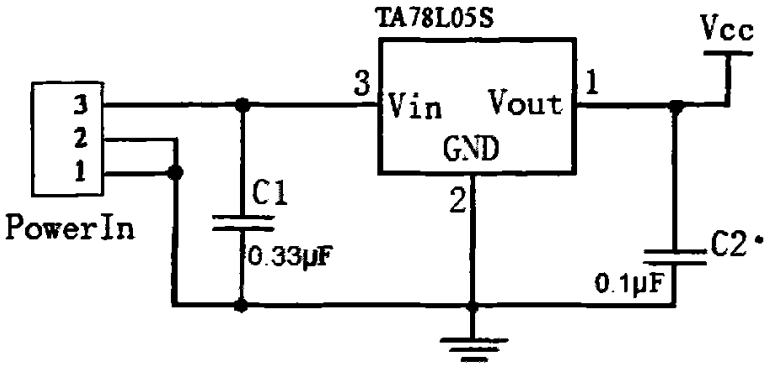


图 3-8 电源供应电路图

Figure 3-8 Circuit of power supply

该芯片 3 号脚为输入端，接 220V 交流电，2 号脚为地，1 号脚为输出端，稳定输出 5V 直流电，供读写器内各芯片使用。

3.2.7 蜂鸣器驱动电路设计

本读卡器中的蜂鸣器在每次操作不成功的时候发出报警指示音，如密码验证没有通过、卡内余额不足、车次日期不符等情况。读卡器对卡进行的任何一次读或写的操作都是由几个步骤完成的，任何一个步骤没有成功蜂鸣器都将发出报警信号。本课题选用蜂鸣器的工作电流为 12mA，蜂鸣器驱动电路如图 3-9 所示：

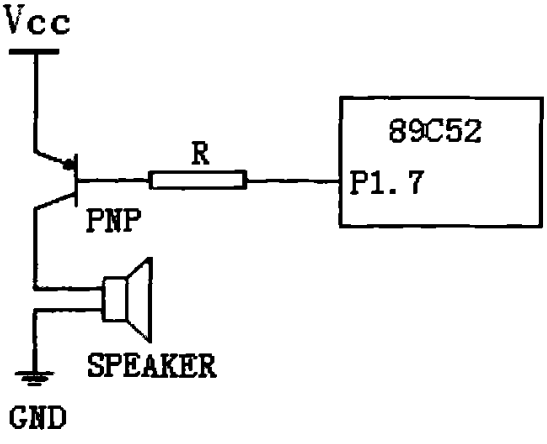


图 3-9 蜂鸣器驱动电路

Figure 3-9 Drive circuit of buzzer

由于单片机的 I/O 口驱动能力有限，一般不能直接驱动压电式蜂鸣器，因此选用一 PNP 型晶体管组成晶体管驱动电路，单片机 I/O 口(P1.7)输出经驱动电路放大后即可驱动蜂鸣器。

3.2.8　显示电路设计

在本文中，显示电路采用 Motorola 公司的 MC14499 显示模块，接口电路如图 3-10 所示：

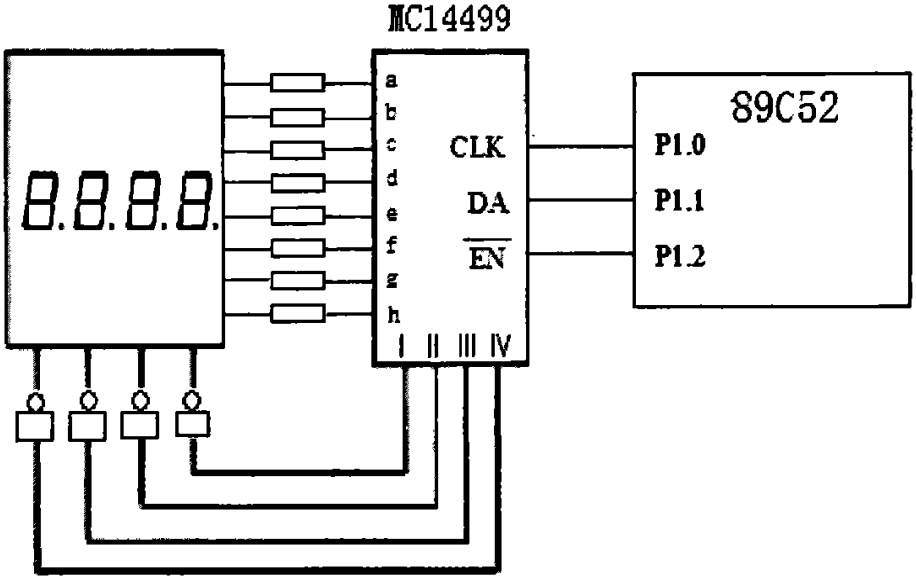


图 3-10 显示模块接口电路

Figure 3-10 Interface circuit of display module

4 位共阴极数码管由 MC14499 芯片驱动，MCU 的 P1.2 口接显示模块 MC14499 芯片的始能端，低电平有效；MCU 的 P1.0 和 P1.1 分别为 MC14499 芯片提供时钟脉冲和数据。

3.3　系统的软件设计

本系统主要由读写模块和相关外围设备如存储单元、复位单元、显示单元、TC232 串口等组成。下面对各个部分的软件设计思想进行介绍。

3.3.1 读写器的软件设计

MCU 对 MIFARE 非接触式 IC 卡的控制是通过核心读写模块 MCM 来实现的，MCM 是 MCU 和 MIFARE 非接触式 IC 卡之间的通信载体。MCU 对 MCM 读写模块的控制是以 MCU 发出 MCM 的指令来达到的，MCM 收到这些指令之后将执行这些指令。

MCM200 的指令主要有：Request std、Request all、Anticollision、Select、Loades key、Authentication(Auth-la、Auth-lb)、Read、Write、Increment、Decrement、Restore、Transfer、Halt 等。

表 3-1 MCM200 指令集

Table 3-1 Instruction set of MCM200

指 令		指令代码	出错标志	接收卡片上的数据
Answer to Request (Request 的应答)	Request std	26	TE、BE	Tagtype
	Request all	52		
AntiCollision(防冲突)		93	TE、BE	Serial Number
Select Tag(选卡片)		93	TE、BE、PE、CE	Size
Authentication (认证)	Auth_1a	60	TE、BE、PE、CE	/
	Auth_1b	61		
Load KEY(存取密码)		/	AE	/
Read		30	TE、BE、PE、CE	Data
Write		A0	TE、BE	/
Increment(增值)		C1	TE、BE	/
Decrement(减值)		C0	TE、BE	/
Restore(重储)		C2	TE、BE	/
Transfer(传送)		B0	TE、BE	/
Halt(停机)		50	TE、BE	/

其中比较重要的是前 8 条指令及 Halt 停机指令等，因为它们可以完成 MCU 对 MIFARE 非接触式 IC 卡的很多应用场合的控制。

在读写器对卡片进行操作前，需事先进行请求应答、防冲突、卡片选择、认

证、检测等操作。

一、请求应答

Request 指令将通知 MCM 在天线有效工作范围内寻找卡片。如果有 MIFARE 1 卡片存在，这一指令将分别与有效区域内的卡片进行通信，读取卡片类型号 TAGTYPE，并由 MCM 传递给 MCU，进行识别处理。

从一个指定的卡片开始，后续的卡片可根据 TAGTYPE 而被选择。当使用“Request std”指令来寻卡时，只有那些卡片上未被设置成“HALT_MODE”的卡片将响应这一指令。

Request all 指令是非连续性的读卡指令，可以防止 MCM 多次选择同一卡片。该指令在成功读取一张卡片后，将一直等待该卡片被拿走，直到再有卡片进入 MCM 天线有效工作范围内。但当某一次 Request all 指令读卡失败，如卡片没能通过密码认证时，Request all 指令将连续读卡，直到读卡成功后才进入非连续性的读卡模式。

Request std 指令和 Request all 相反，该指令是连续性的读卡指令，在成功对某张卡片执行某种操作后，Request std 指令将连续性地再次进行读卡操作，而不管这张卡片是否被拿走。

二、防冲突

如果有多于一张的 Mifare 1 卡片在 MCM 天线的有效工作范围内，则须使用 AntiCollision 指令，使 MCM 能够在若干卡片中选择其中之一。AntiCollision 指令有序地读取所有处在有效工作范围内的卡片，读完第 Xi 张卡片后，待 MCM 及 MCU 对这 Xi 张卡片进行处理完毕后，再读第 Xi+1 张卡片，直至所有的卡片处理完毕。

AntiCollision 指令的启动必须是在程序员完成了对 STACON 寄存器中的 AC 位的成功的设置之后。该指令事实上仅仅是读取 Mifare1 卡片上的序列号 SN，MCM 对卡片的选择和通信，是由 MCU 向 MCM 发送“SELECT”命令来完成的。

三、卡片选择

在一个成功的 AntiCollision 指令之后，须使用 Select 指令，以建立与所选卡的通信。

被选择的卡片将给出其存储器容量，Select 指令成功完成后，MCU 将得到 MCM 的 DATA 寄存器传送来的一个字节长的卡片容量信息。

四、认证操作

在读写器对卡片实施读写操作之前，必须证明该读写操作请求是允许的。该操作可以通过选择存储在 RAM 中的密码集(KEYSET)中的一组密码来进行认证而实现，如果该组密码与卡片上的密码相匹配，将允许读写器对卡片进行读写操作。

卡片上存储器中每一个块(block)都分别指定了该块的存取条件，这些存取条件将根据密码 A(Key A)或密码 B(Key B)而定，密码在 MCM 的 KEYSTACON 寄存器中指定。

五、有效期限检测

在通常使用的交通 IC 卡中，通常是不记名不挂失的，这是因为：读卡器通常脱机运行，挂失的卡片数据存放在读卡机具的黑名单中，当由卡片需要读写时先检测该卡是否在黑名单中，如果在，则锁定该卡；如果不在，则继续进行相关操作。但如果挂失的卡片长时间没有使用，黑名单就会不断增加，随着黑名单的增加，读卡机具每次对卡片的所需的操作时间就会不断增加，会造成交易速度明显下降；若将黑名单设置为一定的容量，在黑名单存满后会自动冲掉之前的纪录，造成经济损失。

通常人们使用的公交卡因单次交易金额不大，因此卡内金额通常不多，无法挂失是可以接受的。但是随着城际高速铁路及客运专线的运行，如果发行储值卡、计次卡或年卡等形式的客票，可以预计将会涉及到较高的金额，没有挂失功能将变得非常不合理，势必将影响该种客票的发行。

为了解决这一矛盾，在本课题设计的系统中，将引入年检机制。根据统计、论证，我们认为在一定时间内，正常情况下所挂失的卡片会控制在一定数量之内，因此可以考虑在读写器读取卡片时，先查询该卡片上一次的交易(充值、使用等)时间，如果在所设定的时间范围内，则对卡片进行正常操作处理，如果该时间在所设定的时间范围内，则对该卡进行锁定，需由卡片使用者持有效证件到发卡机构进行解确认即可继续使用，这样可以最大限度地保护卡片使用者的利益。通过对卡片丢失频率的调查，考虑到通常购买储值卡形式铁路客票旅客的出行频率，以及为提高交易效率而尽量减少黑名单所需的设定容量，本系统拟将卡片检测周期设为 1 年，注意该 1 年的不是从发卡日算起的卡片有效期，而是两次临近交易的时间间隔。

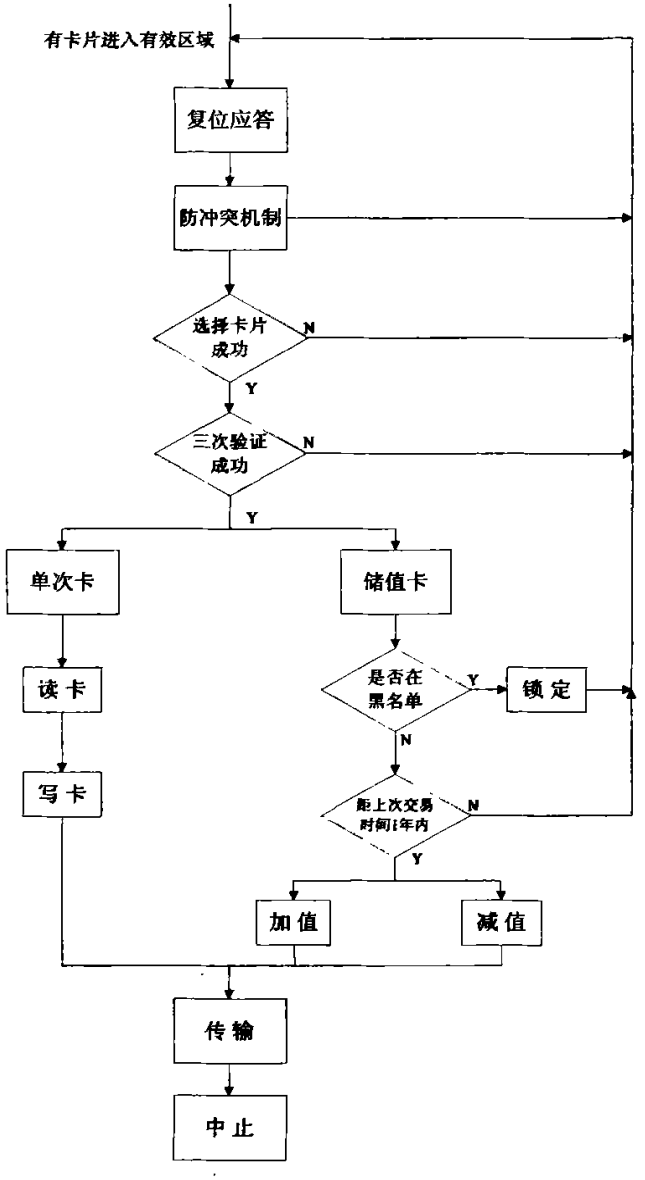


图 3-11 卡片应答、认证流程图

Figure 3-11 Card response and authentication flow chart

3.3.2 存储器的软件设计

由于读写设备并不是实时联机、而是脱机工作，读卡器的检票操作无法实时传送到数据中心，因此需要在读写机具内设一 EEPROM 存储单元。读卡器对卡片

进行操作后，将所做的操作存储在该 EEPROM 中，以供采集。

数据按字节（8 位）逐位串行传输，每个时钟脉冲传输一位，所有地址和数据字以 8 位码串行输入/输出 EEPROM，EEPROM 在收到每个地址或数据码之后，置 SDA 于低电平作为确认应答，该确认应答发生于第九个时钟周期。当读写器向卡发送完 8 位数据后，程序将产生第 9 个时钟脉冲并将 SDA 线读入 Cy 位，此时 Cy 位的状态即为卡应答 ACK。Cy=1 表示卡尚未接收到数据，不能进行下一步的操作，而 Cy=0 则说明卡已接收到数据，可以进行下一步的操作。

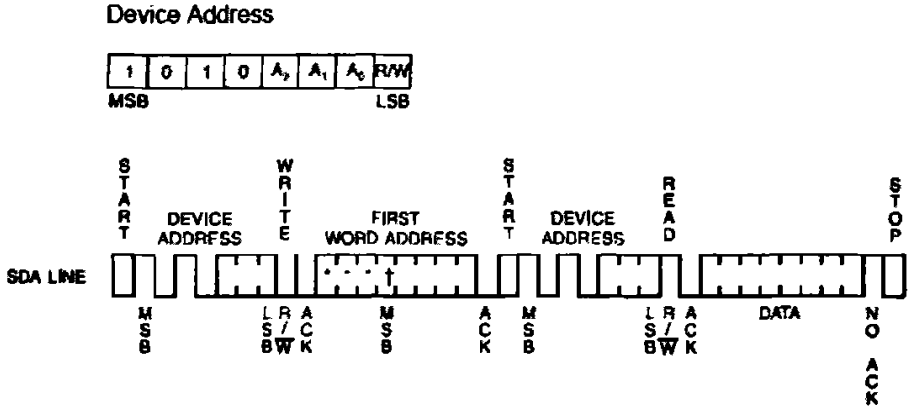


图 3-12 读写操作图示

Figure 3-12 Read-write operation

顺序读取由立即寻址读取或随机寻址读取开始，读写器每收到一个字节数据之后，通过“ACK”应答，EEPROM 收到 ACK 之后，会继续将数据码地址+1（动指向下一存储单元）串行输出数据码。当终止顺序读操作时，读写器不产生确认信号，而是使 SDA 总线处于高电平应答（NAK），使之进入停止状态中。

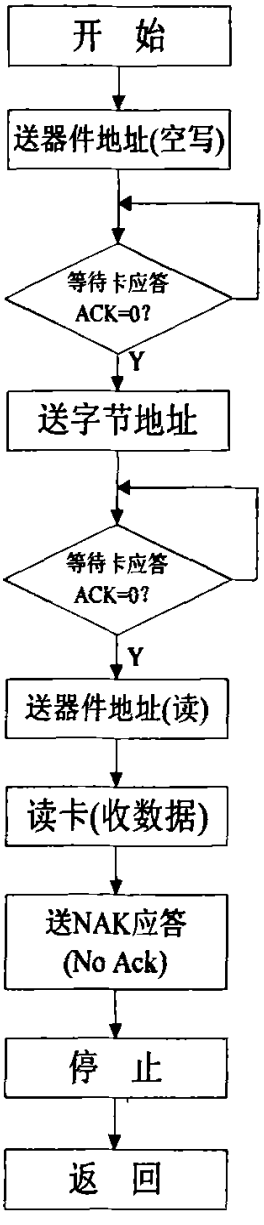


图 3-13 存储器读操作

Figure 3-13 Read operation of memory

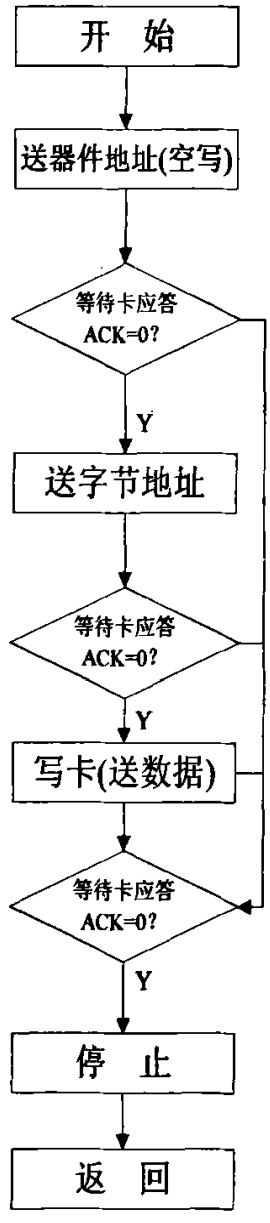


图 3-14 存储器写操作

Figure 3-14 Writing operation of memory

3.3.3 安全体系的设计

智能卡的安全体系是一个极为重要的部分，它涉及到卡的鉴别与核实方式的选择，包括对卡中文件进行访问时的权限控制机制，以及卡中信息的保密机制。安全体系在概念上包括三大部分：安全状态(Security Status)，安全属性(Security

Attributes)以及安全机制(Security Mechanisms)。安全状态是指智能卡在当前所处的一种状态，这种状态是在智能卡进行完复位应答或者是在它处理完某命令之后得到的。安全属性实际上是定义了执行某个命令所需要的一些条件，只有智能卡满足了这些条件，该命令才是可以执行的。因此，如果将智能卡当前所处的安全状态与某个操作的安全属性相比较，那么根据比较的结果就可以很容易地判断出一个命令在当前状态下是否是允许执行的，从而达到了安全控制的目的。和安全状态与安全属性相联系的是安全机制，安全机制可以认为是安全状态实现转移所采用的转移方法和手段，通常包括：通行字鉴别，密码鉴别，数据鉴别及数据加密。一种安全状态经过上述的这些手段就可以转移到另一种状态，把这种状态与某个安全属性相比较，如果一致的话，就表明能够执行该属性对应的命令，这就是安全体系的基本工作原理。由此可以看出，安全体系是建立在密码技术的基础之上的，而在这一体系中，安全算法是核心内容。

安全算法，即安全计算方法。随着系统结构、对安全级别的要求等的不同，可采取多种安全算法，本系统采用的算法是通过软件实现的标准 DES 算法。

在安全计算中，卡片应用将随机数作为过程密钥产生因子或作为 MAC 的初始值。

1. 密钥分散计算方法

对单倍长密钥，用指定的分散因子作为输入数据，做 DEA 加密计算，产生的 8 个字节的结果作为子密钥。

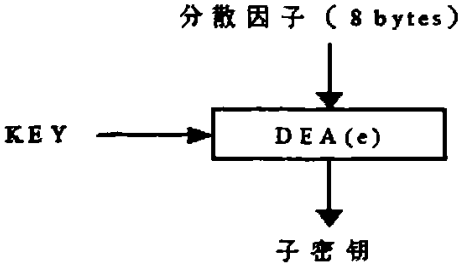


图 3-15 单倍长密钥分散出单倍长子密钥

Figure 3-15 Single sub-key separated by single key

对双倍长密钥，需要分别推导子密钥的左右两部分。左半部分的推导方法是：

第一步：将系统提供的分散因子（8 个字节）作为输入数据；

第二步：用主密钥作为加密密钥，对输入数据进行 Triple-DEA 运算。

右半部分的推导方法是：

第一步：将系统提供的分散因子（8 个字节）求反作为输入数据；

第二步：用主密钥作为加密密钥，对求反后的输入数据进行 Triple-DEA 运算。

将左右两部分连接在一起，产生双倍长子密钥。

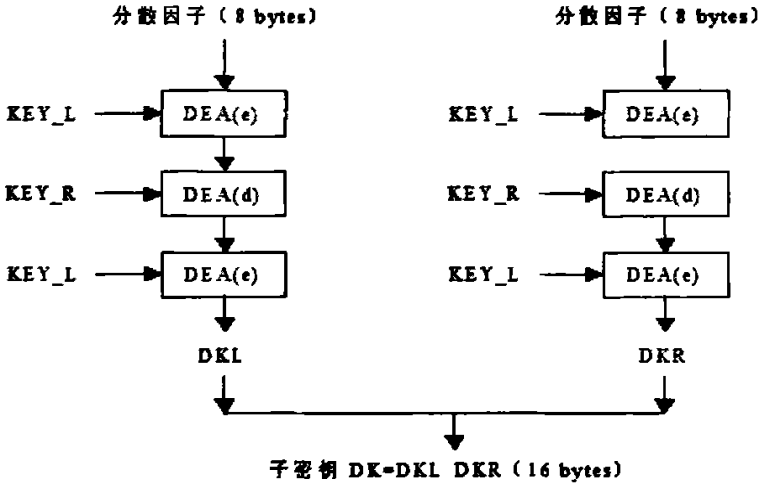


图 3-16 双倍长密钥分散出双倍长子密钥

Figure 3-16 Even sub-key separated by even key

2. 数据加密的计算方法

第一步：用 LD（1 个字节）表示明文数据的长度，在明文数据前加上 LD 产生新的数据块。

第二步：将该数据块分成以 8 个字节为单位的数据块，分别表示为 BLOCK1、BLOCK2、BLOCK3、BLOCK4 等，最后的数据块有可能是 1~8 个字节。

第三步：如果最后（或唯一）的数据块的长度是 8 个字节，则转到第四步；如果最后（或唯一）的数据块的长度不足 8 个字节，则在其后加入 16 进制数‘80’，如果长度达到 8 个字节，则转到第四步，否则在其后加入 16 进制数‘00’直到长度达到 8 个字节。

第四步：按照图 3-16 所述的算法使用指定密钥对每一个数据块进行加密。

第五步：计算结束后，所有加密后的数据块依照原顺序连接在一起。

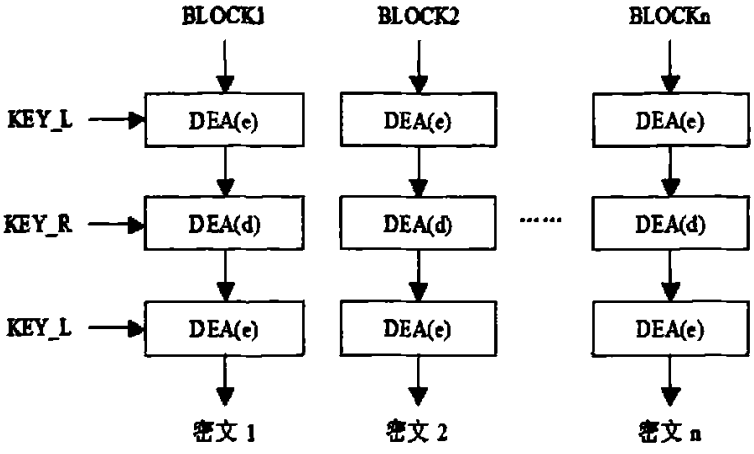


图 3-17 双倍长密钥 DEA 数据加密算法

Figure 3-17 DDA of DEA by even key

3. 安全报文 MAC 的计算方法

第一步：终端向 IC 卡发 GET CHALLENGE 命令获得随机数。

第二步：将 5 个字节命令头（CLA，INS，P1，P2，Lc）和命令数据域中的明文或密文数据连接在一起形成数据块。其中，Lc 的长度应是数据长度加上将计算出的 MAC 的长度（4 个字节）后得到的实际长度。

第三步：将该数据块分成 8 字节为单位的数据块，分别表示为 BLOCK1、BLOCK2、BLOCK3 等。最后的数据块有可能是 1~8 个字节。

第四步：如果最后的数据块的长度是 8 个字节的话，则在该数据块之后再加一个完整的 8 个字节数据块‘80 00 00 00 00 00 00 00’，转到第五步；如果最后的数据块的长度不足 8 个字节，则在其后加入 16 进制数‘80’，如果长度达到 8 个字节，则转到第五步，否则补 16 进制数‘00’直至长度达到 8 个字节。

第五步：按照图 3-18 所述的算法，使用指定密钥完成运算。

第六步：取最终结果（高 4 个字节）作为 MAC。

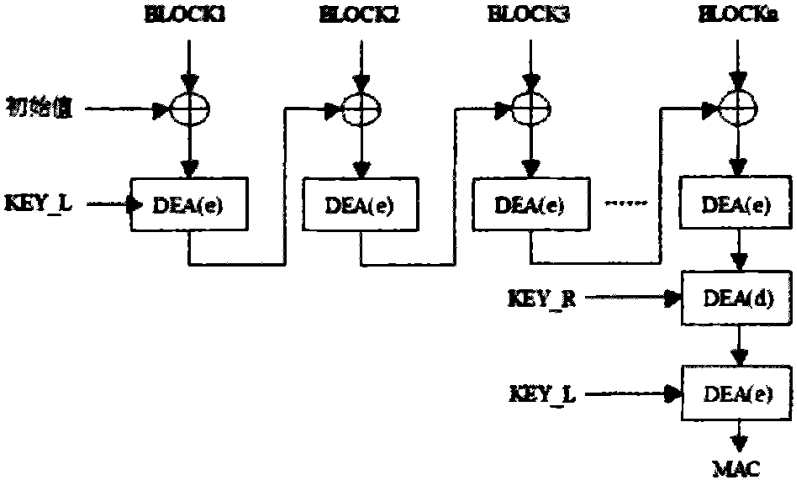


图 3-18 安全报文中双倍长密钥 MAC 算法

Figure 3-18 MAC arithmetic by even key in security message

3.4 本章小结

本章作为本文重要的组成部分，首先阐述了总的系统结构，之后按照硬件设计与软件实现两大部分给出了完成本课题的具体设计方案。在硬件设计中，主要介绍了对单片机与核心读写模块、存储模块、监视复位模块、接口模块、显示模块、蜂鸣器等不同功能模块间的接口电路；在软件设计中，主要介绍了整个系统的软件实现思想与步骤，以及对本系统安全体系的设计思想。

第4章 制作及调试与结果

选择好元器件并设计好解决方案后，进行电路图设计、绘制、制板、调试等工作。

4.1 SCH与PCB设计

在整个系统方案经确认以后，设计SCH原理图与印刷电路板PCB图。

一、SCH设计

根据各模块结构图中各芯片以及模块间芯片的连接方式，通过Protel99软件进行SCH原理图设计，最后输出网络表。

1、根据设计需要设置图纸尺寸和设计环境

2、根据系统功能实现选择器件并放置选定的元件

3、原理图布线

4、输出报表

二、PCB设计

在进行PCB设计时，进行尺寸定义、层定义以及定义布线规则等后开始芯片布局，布局之后就可以布线了，布线全部布通后进行DRC检查，DRC检查无误后即可投板。

1、调入网络表，设置线路板尺寸、层数及布线规则

2、根据功能模块和相关规则摆放元件进行布局

3、布局结束开始布线

4、布线完毕，DRC检查，无误后制光绘文件输出

线路板制版后焊上芯片即可进行设备调试。

4.2 电路板上电硬件调试

在线路板制版后焊上芯片及各种器件后首先进行一些上电的调试，主要测试电源、晶振、时钟及射频部分。本方案中使用的电压为5V，时钟需要重点测试的是单片机晶振时钟11.059MHz，RF模块需要对电容及电感值进行调试，以确定最好的RF性能及读写距离。在各个方面确认无误，各芯片上电后状态正常，无异常现象，如过分发热，即可进行以下的软件调试。

硬件电路板如图4-1所示：

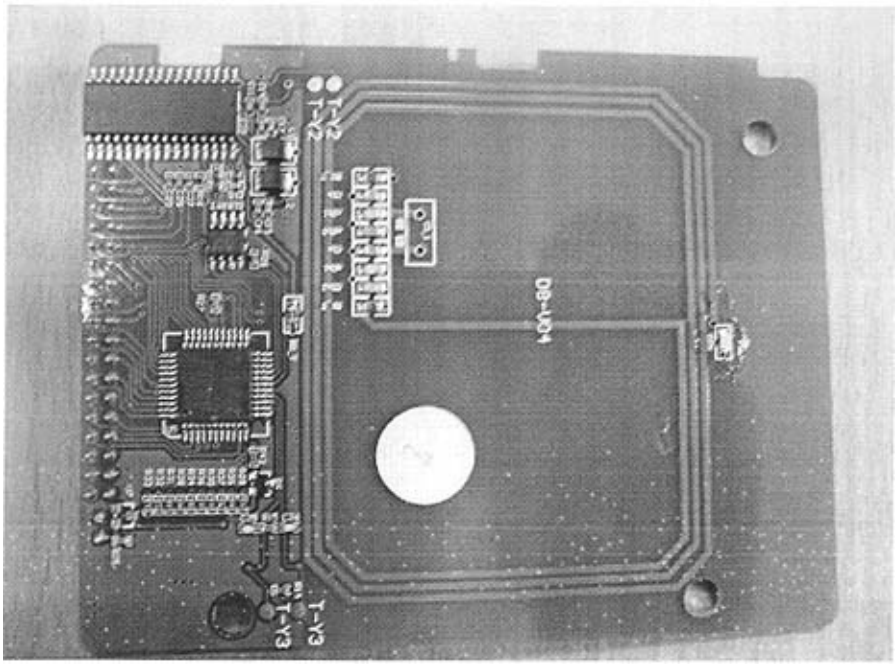


图 4-1 读写器电路板

Figure 4-1 Hardware circuit board

4.3 系统软件调试

电路板上电之后，先下载程序，然后再调试单片机程序。单片机程序完成后，经编译，用 51 仿真器仿真调试程序，将仿真头插入 51 单片机的芯片位置，打开仿真软件，调入编译完成的文件，单步运行调试程序。

4.3.1 系统初始化

1、系统复位，各芯片的复位端均接到 P1.0 口，命令执行后，观察各芯片是否正常复位。

2、单片机的初始化，主要包括设置中断方式，串口工作方式，波特率，定时器等。

3、读写模块的初始化，以及各种读写参数的设定

4.3.2 密钥管理系统调试

1、输入三组 32 位长度的分散因子，如图 4-2 所示。

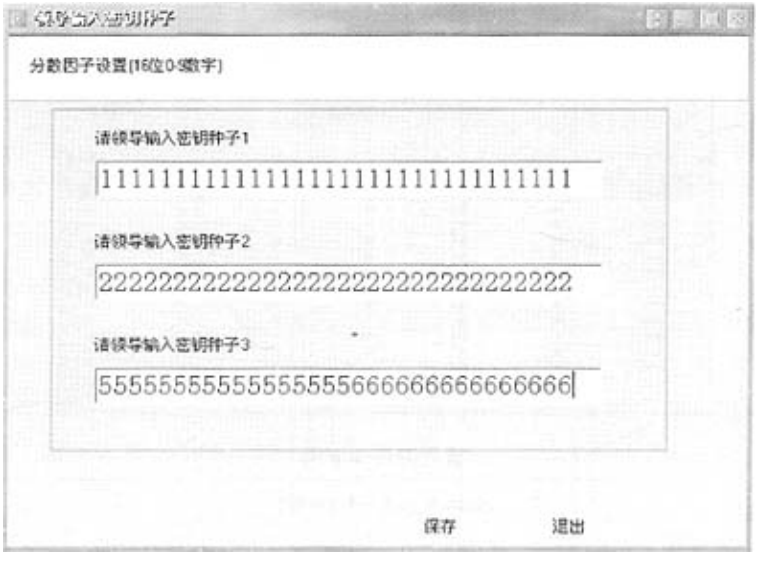


图 4-2 分散因子设置

Figure 4-2 Separation gene setting

2、点击保存按钮，系统提示保存成功或失败，如图 4-3 所示。

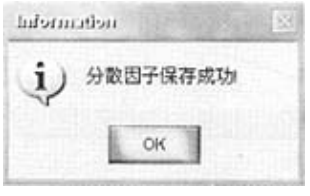


图 4-3 分散因子保存成功

Figure 4-3 Separation gene saved success

3、输入密钥标识、密钥索引、密钥名称和加密机地址，选择是否分散、密钥长度标识、密钥用途、密钥认证标识。点击新建、修改、删除按钮，系统提示保存成功或失败，如图 4-4 所示。

图 4-4 密钥设置

Figure 4-4 Key setting

4.3.3 卡片初始化

1、插入卡片至读卡器用户卡槽，读卡器上方红灯变绿。

2、选择卡片类型，输入卡号、初始化机构代码、初始化机构、卡初始密码和操作员，执行初始化，如图 4-5 所示。

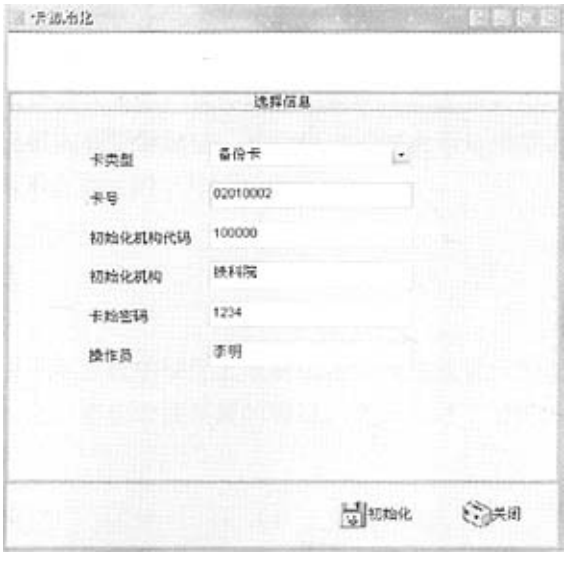


图 4-5 卡片初始化

Figure 4-5 Card initialization

4.4 测试结果

本系统需在正常的室内工作环境下进行测试，考虑到我国幅员辽阔，测试环境的温度应该包括-20℃和+50℃两极限值。首先对系统上电，观察各个模块单元是否能够正常启动，以及没有不正常的发热现象。将多张卡片同时放入有效读写区域，观察读卡器是否能成功选中其中一张卡片进行操作；将一张非正常使用状态下的卡片放入有效读写区域，读写器应报警并不能进行相关交易。在读卡器中设置好减值（金额），将一张处于正常使用状态下的卡片放入有效读写区域，检查交易是否正确；将一张处于非正常使用状态（如未经初始化、处于读写器黑名单中、余额不足、距离上次交易时间超过一年等）下的卡片放入有效读写区域，检验读写器是否正确发出警报，及卡片是否被成功锁定；通过复位键对读写器进行复位操作，读写器应进行正常的复位，并且存储在 EEPROM 中的数据不丢失；检验读写器能否和上位机正常通信，且数据传输过程中数据不丢失。

经过在正常室内工作环境、在-20℃和+50℃下的温度下对本系统进行反复测试，系统复位正常，能准确、快速地对卡片进行读写操作，经测试对数据的读写、加减等操作均准确无误正确，对余额不足或未经初始化的卡片能正确报警；对某张卡片进行读写操作后，对读写器中的日期进行重置，使两者间隔超过 1 年，或将该卡信息存入读写器黑名单中，再将该卡片放入读写有效区域，读写器能正确报警，并将卡片锁定，黑名单中该项信息自动删除；将该锁定的卡片经管理系统解锁后，功能恢复正常。经过对 100 张卡片的反复测试，识别距离均在 25mm 以上，达到了预期的效果；系统与上位机通信正常，可以进行正常的数据采集，且在传输过程中无数据丢失现象；读写器存储模块工作正常，掉电后没有丢失数据现象，并能和上位机实现正常通信。显示模块能够对卡片类型、余额进行正确显示，并经蜂鸣器对不合要求的卡片进行报警。

4.5 本章小结

本章主要介绍了本系统的硬件上电调试，以及系统软件的调试过程，包括对系统及卡片的初始化、密钥管理系统的调试。之后阐述了最终的系统测试过程及测试结果。

第5章 总结与展望

本课题经过近1年的摸索，针对市场的需求，采用当前先进的非接触式IC智能射频卡技术，根据我国全面建设小康社会对铁路客运的发展要求，结合铁道部在十一五铁路规划中在全路实现信息化、自动化、智能化的精神，进行了应用于铁路客运快速支付系统中的卡片及读写设备的研制，下面有必要对本文所做的工作做一总结并对其还需进一步完善的地方和应用前景进行展望。

一、总结

该系统实现了高效、快速、高安全性地对卡片进行识别、认证及读写操作，卡片识别距离在25mm以上，可以脱机工作并大容量地存储数据，能够正常与上位机通信并进行采集和参数的修改，完成了既定目标。

在开发过程中，经过无数次的调试和试验，克服了许多困难，为今后对系统的进一步完善积累了宝贵财富。

二、前景展望

铁路客票系统是一个极其复杂的系统，对其改革需要进行多方面的技术、可行性、安全性、可靠性、经济成本、接受程度等多方面的研究及论证，不是一朝一夕的。本文也是就铁路客票与RFID技术相结合，开发全新的、适合于我国国情的铁路客票系统做一前瞻性的研究。虽然本文解决了很多问题，但是还有很多方面有待完善，其中既有技术方面的，也有社会方面的。例如，如果在铁路客票系统实行实名制，与二代身份证相结合的具体方案还有待研究，如何在保证检票效率的情况下进行身份验证，以及人们对将身份信息写入客票卡中的接受程度；再如，是否可以将该系统与银行系统联网，使使用者可以通过银行转账形式进行充值，为旅客提供方便，甚至将该系统与城市公共交通系统进行联网，真正实现“一卡通”的目标，这些也都需要在技术上进行进一步的探索，以及社会各方面的协调。

参考文献

[1] [美]Robert Kleist. RFID Labeling: Smart Labeling Concepts & Applications for Consumer Packaged Goods Supply Chain. Second Edition. 机械工业出版社. 2007.P8-P9

[2] 全国铁路工作会议报告. 北京. 中华人民共和国铁道部. 2007

[3] 中国 RFID 技术政策白皮书. 北京. 中华人民共和国科技部. 2006

[4] 熊立雇. 非接触式 IC 卡技术. 深圳大学学报(理工版). 2006.第 15 卷. P18-P19

[5] 郎为民. 射频识别（RFID）技术原理与应用. 北京. 机械工业出版社. 2006

[6] 杨振野. IC 卡技术及其应用. 北京. 科学出版社. 2006

[7] 陆永宁. 非接触 IC 卡原理与应用. 北京. 电子工业出版社. 2006

[8] [德] Klaus Finkenzeller 著. 陈大才译. 射频识别(RFID)技术. 北京. 电子工业出版社. 2004

[9] Pobanz.C. "A microwave noncontact identification transpondent using subharmonic interrogation". IEEE Transactions on Microwave Theory and Techniques Vol:43 Iss:7. P1673-1679. 1995

[10] Yamada Junichi, Miwa. A 128-kb FeRAM macro for contact/contactless smart-card microcontrollers IEEE Journal of Solid-State Circuits. Vol:37. P1073-1079. Aug 2002

[11] Sanchez-Reillo R. Smart card information and operations using biometrics IEEE Aerospace and Electronic Systems Magazine .Vol:16. P3-6. Apr 2001

[12] P.Hemandez, J.D.Sandoval. Mathematical Model for a Multiread Anticollision Protocol, Communications,Computers and signal Processing.2001.

[13] Philips Semiconductors. Mifare Standard Card IC MFI IC S50 Functional Specification

[14] Philips Semiconductors. MIFARE Micro Module MFCM200 Specification

[15] Philips Semiconductors. MIFARE Core Module MFCM200 Specification

[16] Philips Semiconductors. Mifare MF RC500 Highly Integrated IS014443A Reader IC Data Sheet

[17] Atmel Corporation. 8-bit Microcontroller with 8K Bytes Flash-AT89C52

[18] Toshiba Semiconductors,Toshiba Bipolar Linear Integrated Circuit:Three Terminal Positive Voltage Regulators

[19] Dallas Semiconductors. DS1232 MicroMonitor Chip

[20] Atmel Corporation. 2-Wire Serial EEPROM AT24C64

[21] 刘长征. 基于智能标签的射频识别系统的研究和实现. 计算机工程. 2003.第 29 卷.P20

[22] 李科让. 一种实用的非接触式 IC 卡读写器的设计. 微型机与应用. 2001. 第 9 期

[23] [美] Joseph J. Carr. 射频电路设计（第 3 版）. 北京. 电子工业出版社. 2002

[24] 余永权. ATMEL89 系列 Flash 单片机原理及应用. 北京. 电子工业出版社. 1997

[25] 李群芳. 单片机原理、接口及应用. 北京. 清华大学出版社. 2005

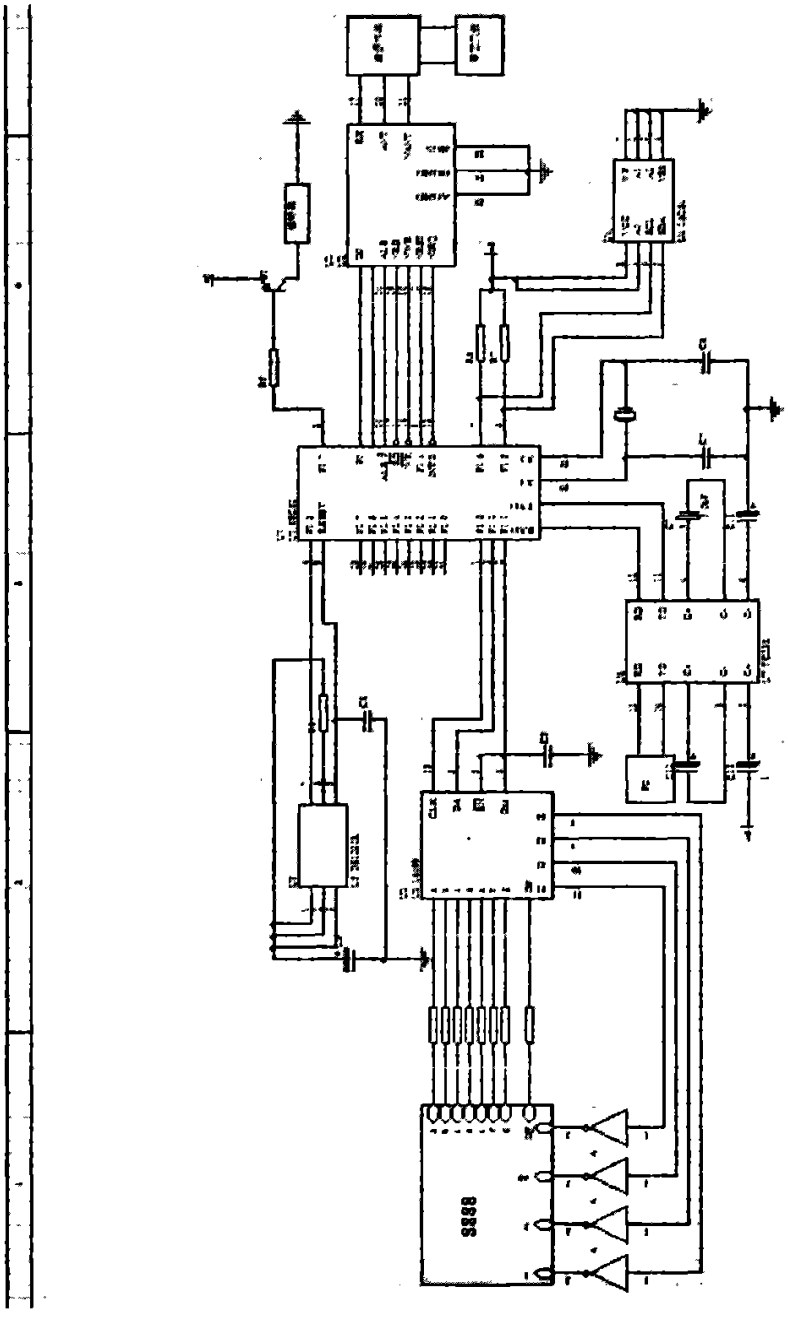
[26] 李刚. 51 系列单片机系统设计与应用技巧. 北京. 北京航空航天大学出版社. 2004

[27] 张俊谟. 单片机中级教程. 北京. 北京航空航天大学出版社. 2003

[28] 李共，毛健丰. 基于 DES 加密算法的射频智能 IC 门禁系统. 微电子与基础产品. 2002. 第 28 期

附录 A

读写器的硬件电路图



作者简历

沈骞，男，1982年11月26日生，2005年9月至2008年3月于北京交通大学攻读硕士研究生学位，攻读学位期间，主要完成了对电路与系统以及嵌入式系统方向的学习，并对第三代通信技术TD-SCDMA有所研究，期间发表论文“基于VW2010芯片的网络视频压缩编解码器设计与实现”一篇于《计算机测量与控制》。