智能卡表技术与应用

ZHINENG KABIAO JISHU YU YINGYONG

吴叶兰◎著

机械工业出版社
CHINA MACHINE PRESS

智能卡表技术与应用

吴叶兰　著

机 械 工 业 出 版 社

本书以 IC 卡技术和仪表技术为基础，对 IC 卡智能电表、水表和气表的原理、功能和设计进行了研究和探讨。本书内容包括：IC 卡技术，介绍了 IC 卡的分类、传输协议、文件系统和安全机制；智能卡表的安全性分析，针对 IC 卡和卡表的数据攻击手段，分析了 IC 卡表数据存储和数据交换的安全性策略及安全性工具；智能卡电表，给出了智能卡电表的系统设计规范，智能卡电表和电卡设计，提出了电卡的密钥安全体系、智能卡电表及电卡的接口规范及电卡与卡表间的安全认证流程；智能卡水表的功能及原理、水表卡片文件系统的定义、智能卡水表的设计实例；智能卡燃气表的软硬件设计、数据通信协议及系统低功耗测试方法；提出了智能卡表的一卡通方案。

本书是一本介绍 IC 卡表原理、功能、设计的专著。本书可作为电子科学与技术、自动化检测、仪器仪表等相关专业高年级本科生和研究生的参考用书，也可为从事智能仪表、电子技术等相关领域的学者和研究人员提供参考。

图书在版编目（CIP）数据

智能卡表技术与应用/吴叶兰著. —北京：机械工业出版社，2012.10
ISBN 978-7-111-39929-2

Ⅰ.①智… Ⅱ.①吴… Ⅲ.①IC 卡—技术 Ⅳ.①TN43

中国版本图书馆 CIP 数据核字（2012）第 232674 号

机械工业出版社（北京市百万庄大街 22 号 邮政编码 100037）
策划编辑：牛新国 责任编辑：闾洪庆
版式设计：姜 婷 责任校对：赵 蕊
封面设计：赵颖喆 责任印制：李 妍
中国农业出版社印刷厂印刷
2013 年 1 月第 1 版第 1 次印刷
169mm × 239mm · 10.75 印张 · 210 千字
0 001—3000册
标准书号：ISBN 978-7-111-39929-2
定价：29.90元

凡购本书，如有缺页、倒页、脱页，由本社发行部调换

电话服务 网络服务
社 服 务 中 心：（010）88361066 教 材 网：http://www.cmpedu.com
销 售 一 部：（010）68326294 机工官网：http://www.cmpbook.com
销 售 二 部：（010）88379649 机工官博：http://weibo.com/cmp1952
读者购书热线：（010）88379203 **封面无防伪标均为盗版**

前　言

随着IC卡技术的不断发展以及国内相关行业服务意识的提高，在与用户日常生活相关的计量表计中使用IC卡技术得到了迅速的推广，在水、电、气、热力等多个行业得到广泛应用，使得IC卡智能仪表成为当前国内IC卡应用技术发展的一个亮点。但介绍智能卡表技术的相关书籍很少，为弥补这一缺憾，作者结合多年从事IC卡智能仪表的研究工作，编写了本书。

本书从应用角度出发，介绍了智能卡表的原理、功能和设计方法，分析了智能卡表的安全性，给出了各类智能卡表的设计实例。由于IC卡是智能卡仪表的重要组成部分，有关智能卡文件系统、卡片类型设计、卡片和CPU的接口技术以及智能卡表数据项的设计是本书重点研究和讨论的内容，这些内容也是整个系统的核心问题。

本书分为7章，第1章介绍了智能卡表的分类及一般结构；第2章介绍了智能卡技术，包括智能卡分类、传输协议、文件系统和安全机制；第3章介绍了智能卡表的安全机制；第4章介绍了智能卡电表，包括智能卡电表系统的设计规范、智能电卡设计、智能卡电表和电卡的接口文件；第5章介绍了智能卡水表的功能、原理及卡片文件系统的设计；第6章通过一个具体设计实例介绍了智能卡燃气表的软硬件设计及系统测试；第7章给出了一种智能卡表一卡通设计方案。

在本书的编写过程中，得到了北京淳堂科技有限公司陈红军和北京工商大学研究生郑淑芳的大力支持，在此表示衷心感谢！此外，本书的出版得到了北京市教委科技创新平台PXM2011－014213－113551的资助。

由于智能卡表技术还在不断发展和完善之中，限于作者水平，本书难免存在疏漏和错误，恳请读者批评指正。

作　者

目　录

第 1 章　绪　　论

随着 IC 卡技术的不断发展以及国内相关行业服务意识的提高，在与居民用户日常生活相关的计量表计中使用 IC 卡技术得到了迅速的推广和广泛的应用。目前在电表、水表、燃气表中都已经开始采用 IC 卡作为抄表收费、控制以及数据管理的媒介，使得 IC 卡智能仪表成为当前国内应用技术发展的一个亮点。本章主要介绍了 IC 卡智能仪表的分类和 IC 卡表的一般操作流程，并对国内存在的几种抄表收费管理模式进行了分析比较。

1.1　IC 卡智能仪表的分类

目前 IC 卡智能仪表按照行业类型可以划分为 IC 卡智能电表、IC 卡智能水表和 IC 卡智能燃气表（见图1-1）。IC 卡智能电表是在电能计量仪表中加入 IC 卡及负荷开关控制等功能模块，用以完成电量抄收和电量结算的新型电表；IC 卡智能水表是在用水量计量仪表中加入 IC 卡及阀门开关控制等功能模块，用以完成用水量抄收和用水量结算的新型水表；IC 卡智能燃气表是在燃气量计量仪表中加入 IC 卡及阀门开关控制等功能模块，用以完成对燃气量抄收和燃气量结算的新型气表。

图 1-1　IC 卡智能燃气表

IC 卡智能仪表按照基表结构可以划分为机电一体式智能卡表和全电子式智能卡表，目前在 IC 卡智能电表中主要采用全电子式结构，IC 卡智能水表和 IC 卡智能燃气表主要采用机电一体式结构。

按照用户类型可以将 IC 卡智能仪表划分为针对工业用户使用的工业卡表和针对居民用户使用的民用卡表。

按照用户缴费方式可以区别为先缴费后使用的 IC 卡预付费卡表和先使用后缴费的 IC 卡付费卡表。

按照行业分类可分为 IC 卡电表、IC 卡水表、IC 卡气表、IC 卡热力表。

1.2　IC 卡表一般操作流程

IC 卡表的管理模式如图 1-2 所示。

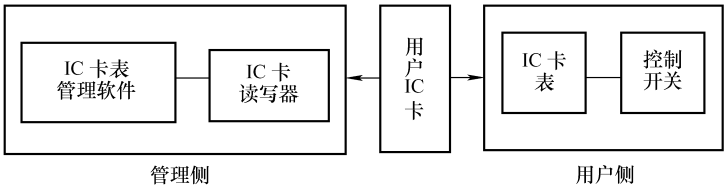


图 1-2　IC 卡表的管理模式

第一步，管理部门为用户安装 IC 卡表；IC 卡表管理系统软件登录用户信息，完成新用户开户；管理部门通过读写器为用户制作用户卡，写入必要的运行参数信息。

第二步，用户将用户卡插入自己的 IC 卡表，将运行参数信息传入 IC 卡表，同时将 IC 卡表内数据返写到用户卡。当满足一定条件时，IC 卡表闭合控制开关，允许用户使用相应的能源（水、电、气、热）。条件不满足时，IC 卡表断开控制开关，不允许用户使用相应的能源。

第三步，用户持用户卡到管理部门缴费充值，IC 卡表管理系统通过 IC 卡读写器将 IC 卡表返写信息读入系统进行结算分析，同时将新的运行参数传递到用户卡。

第四步，用户再次将用户卡插入 IC 卡表，获得相应能源的继续使用权。

1.3　IC 卡表的一般结构

IC 卡表的一般结构如图 1-3 所示。

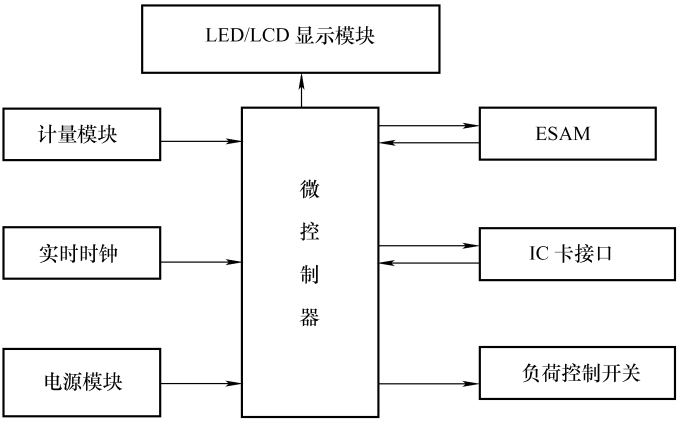


图 1-3　IC 卡表的一般结构

1. 计量模块

计量模块有机电式和电子式两种。

机电式：从机械式仪表的计度器圆盘采样，将计度器圆盘的转动转换为电脉冲信号。

电子式：直接由电子集成电路完成数据的采集、计量并转换为电脉冲信号。

2. LED/LCD 显示模块

用来显示 IC 卡表的计量数据和工作状态。

3. 实时时钟

用来记录时钟和日历，协助微控制器完成多种费率的计量以及按日、周、月的数据统计。

4. IC 卡接口

用于 IC 卡表与 IC 卡片进行数据交换和安全认证工作。

5. ESAM（嵌入式安全控制模块）

用于存放 IC 卡表内的计量和状态数据，并与 IC 卡进行系统的密钥安全认证工作，是 IC 卡表数据安全的核心器件。

6. 负荷控制开关

用于控制用户的水、电、气、热供应的开关，可由 IC 卡表输出控制信号对其进行闭合或断开操作。

7. 电源模块

用于向 IC 卡表提供电源供应。对于单相 IC 卡电表直接由交流转换供电，多费率 IC 卡电表以及水表、气表和热表由电池提供能源。

1.4 IC 卡收费管理模式

1.4.1 抄表收费管理模式

目前存在着三种不同的抄表收费管理模式，分别是人工抄表收费方式、自动抄表收费方式和 IC 卡收费方式。

1. 人工抄表收费方式

人工抄表方式是指为用户安装普通计量仪表，按固定的时间由管理人员上门抄表和收费。需要管理人员多，工作量大；优点是计量仪表成本低，采用付费方式容易被用户接受，基本不存在用户能源被切断问题。

2. 自动抄表收费方式

自动抄表方式是指为用户安装具有通信能力的计量仪表，通过通信网络系统自动完成用户计量仪表的数据抄收，再通过金融网点方式以自动或人工方式完成

缴费。这种方式技术难度高，通信网络建设及维护成本大；优点是自动化程度高，节省人力，并很容易实现系统的实时监控。

3. IC 卡收费方式

IC 卡收费方式是指为用户安装具有 IC 卡接口的计量仪表，将 IC 卡作为传输介质，在用户和管理部门之间传输信息，自动实现计量仪表的抄收以及缴费工作。这种方式成本较高，信息传输不及时，同时让用户充当了信息通道的角色，未体现管理部门服务的宗旨。优点是实现了抄表、收费、控制的三位一体，彻底杜绝了欠费现象的发生，管理人员和管理费用少。

在发达国家主要以人工或自动抄表收费方式为主，原因是金融业高度发达，发生欠费的情况较少，同时管理部门有资金实力建立抄表网络系统，具有较强的自动化管理水平；而在发展中国家目前正从人工抄表收费方式向 IC 卡收费方式过渡，原因是人口众多，人工管理方式已逐渐无法管理，而管理部门还不具备资金和技术实力推行网络化的自动抄表收费管理系统，金融业的发展已经初具规模，IC 卡收费方式恰好成为最佳选择；在欠发达国家，由于没有系统的收费管理模式，只能采用人工抄收方式，但在较为发达的城市或小区，具备推行 IC 卡收费方式或局域自动抄表收费的可能性。

可以确认在未来相当长的一段时间内，在国内和人口较多的发展中国家推广 IC 卡表收费管理方案是可行的，应该具有较为良好的市场前景。

1.4.2 IC 卡收费管理模式

IC 卡收费管理模式是将居民用户家里的普通计量仪表改装为 IC 卡智能仪表，为居民用户提供一张缴费 IC 卡，然后在行业管理部门搭建一个收费管理平台来实现的。按照一定的时间阶段居民用户持缴费 IC 卡到行业管理部门缴费写卡，将购买量等相关信息写入缴费 IC 卡，用户再将缴费 IC 卡插入 IC 卡智能仪表，将相关控制数据传递到表内，从而实现继续使用相关能源。这种收费管理模式结构示意图如图 1-4 所示。

上面的网络结构可以根据实际应用情况进行增减，它反映了整个系统的逻辑构成，主要由 IC 卡智能仪表、IC 卡和 IC 卡收费管理系统三部分组成。

1. IC 卡智能仪表

IC 卡智能仪表是指安装有 IC 卡接口和控制机构的智能仪表。当满足设定的条件时，IC 卡智能仪表会通过控制机构禁止居民用户使用能源；当用户持卡缴费后将缴费 IC 卡插入 IC 卡智能仪表，这时 IC 卡智能仪表就能够自动通过控制机构恢复居民用户使用能源。

2. IC 卡

用户缴费 IC 卡由行业管理部门发行，居民用户持有，用来在 IC 卡智能仪表

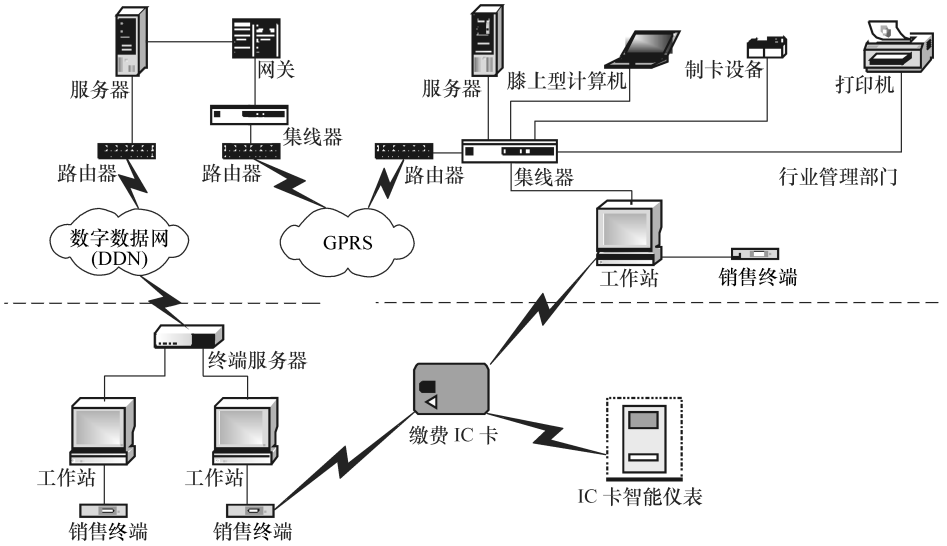


图 1-4　IC 卡收费管理模式结构示意图

和收费管理平台之间传递仪表中的计量和收费管理数据。考虑到卡片传输数据的重要性，根据实际情况，应该尽量选择安全性较高的 IC 卡介质。根据安全性的不同，可以将 IC 卡介质分为三类：

存储卡：能够按物理地址对数据进行读写、存储操作，但没有任何对数据的保护措施。典型的卡片有 24C × × 系列。

逻辑加密卡：能够按物理地址对数据进行读写、存储操作，在对数据进行读写时，首先需要进行密码校验，只有密码校验通过才能够对卡片数据进行正常读写操作，否则卡片拒绝操作并在一定条件下将卡片锁死。

CPU 智能卡：能够按逻辑地址对数据以文件的方式进行读写操作，卡片内部的 CPU 控制器可以进行复杂算法运算，在对数据进行读写操作时，首先需要使用一定的算法进行密钥认证，认证通过后才能够对卡片数据进行正常读写操作，并且还可以根据实际情况对数据进行加密和解密操作。如果认证不通过，则不能对卡片进行正常操作。

将上面三种卡片的安全性进行比较，CPU 智能卡的安全性最高，操作最复杂，存储卡的安全性最低，操作最简单。在实际使用时，如果在城镇或物业小区安装使用 IC 卡智能仪表，由于范围较小，使用存储卡和逻辑加密卡已经可以保证系统的安全性；如果在大中城市使用 IC 卡智能仪表，由于范围较大，数量较多，人为监控较为困难，因此应该使用安全等级较高的 CPU 智能卡作为用户缴费 IC 卡介质。

3. IC 卡表收费管理系统

IC 卡表收费管理系统主要完成用户管理、数据信息管理、交易信息管理和数据查询统计等功能。结合 IC 卡技术和收费管理模式的特点，目前应用成熟的 IC 卡表收费管理模式有两种：采用 IC 卡为抄表介质的收费管理模式和远传卡表收费模式。

当采用 IC 卡为抄表介质时，数据传输过程是靠持卡人来完成的，IC 卡具有双向传输数据的能力。当用户或者管理人员将 IC 卡插入到 IC 卡表后，将各种需要的计量数据抄出存储到 IC 卡上，然后将数据由持卡人带回到收费管理系统进行收费以及统计分析工作。

由于 IC 卡传递数据不可避免地出现非实时性，所以建立一套实时的自动抄表系统对现场运行的仪表进行监控以及数据统计分析一直是行业管理部门十分迫切希望实现的事情。但如果仅有自动抄表系统，不能和用户形成良好的信息沟通，当行业管理部门对居民家中的仪表进行操作时，对于居民用户来讲就是突然发生事件，会带来不便甚至误解。而使用 IC 卡表由于用户持 IC 卡进行缴费和数据传递，因此增加了行业管理部门和用户进行信息沟通的渠道，从服务的角度来讲，具有自动抄表系统所不可替代的优势。

因此，在目前国内比较成熟的自动抄表系统的基础上，增加 IC 卡控制收费的功能，这样数据远传用来完成对远传卡表的管理和监控，IC 卡功能提供远传卡表的收费服务。该模式比较适合于在已经推行自动抄表系统的场合下使用，通过增加 IC 卡接口，有效地解决收费控制问题，作为自动抄表系统的有效补充。

第 2 章　智能卡技术

智能卡是智能卡表系统中的重要组成部分，是卡表和收费管理平台的传输介质，用来传递卡表中的计量和收费管理数据。本章介绍了智能卡的概念、智能卡的分类和不同类型卡所遵循的国际标准，重点阐述了智能卡的传输协议、智能卡文件系统和智能卡安全机制。

2.1　智能卡的概念

智能卡（Smart Card）即集成电路卡，又称 IC 卡（Integrated Circuit Card）。它是将一个集成电路芯片镶嵌于塑料基片或其他材质中，封装成卡片式或其他各种形式。

IC 卡的概念是 20 世纪 70 年代初由法国人罗兰·莫雷诺（Roland Moreno）首先提出，并由法国布尔（Bull）公司研制出世界上第一张 IC 卡。IC 卡自问世以来得到飞速发展，已经成为涉及全球众多著名电子巨头的新兴技术产业，被广泛地应用于电信、金融、医疗、交通、身份证、商业购物、数字社区等社会生活的各个领域。

智能卡是半导体技术和计算机技术的结合，其内部的集成电路集成了微处理器和存储器，具有存储、加密、数据处理能力。与磁卡相比，智能卡具有体积小、存储容量大、安全性高、使用方便等特点。随着我国“金卡工程”的大力开展，作为金卡工程的代表，IC 卡技术无疑是最优秀的应用技术之一，为现代信息的处理和传输提供了新的解决方案。

2.2　智能卡分类

智能卡可根据不同方式进行分类。

2.2.1　按内嵌集成电路分类

按内嵌的集成电路类型不同，智能卡可分为存储器卡（Memory Card）、逻辑加密卡（Memory Card with Security Logic）和 CPU 卡（Smart Card）三类。

1. 存储器卡（Memory Card）

存储器卡内嵌的芯片为存储器芯片，通常为电可擦除可编程只读存储器（Elec-

trically Erasable Programmable Read – only Memory，EEPROM）。存储器卡功能简单，价格低廉，使用方便，很多场合可以取代磁卡。但由于其本身没有或很少有安全保护逻辑，对片内信息可以任意存取，因此只能用于保密性要求不高的场合，如医疗上用的急救卡等。常见的存储卡有 Atmel 公司的 AT24C01 ~ AT24C64 等。

2. 逻辑加密卡（Memory Card with Security Logic）

逻辑加密卡除了具有存储卡的 EEPROM 外，还增加了硬件加密逻辑电路，该加密逻辑电路通过密码校验的方式来判断卡内数据能否被外部读写，具有一定的安全性。但这只是低层次的安全保护，不能防范恶意攻击，适用于保密要求较低的场合，如加油卡、电话卡、借书卡、公用事业收费卡等。常见的逻辑加密卡有 Siemens 公司的 SLE4442 卡和 SLE4428 卡等。

3. CPU 卡（Smart Card）

CPU 卡内部集成电路包含微处理器单元（CPU）、存储单元（RAM、ROM 和 EEPROM）和输入/输出（I/O）接口单元，其中，ROM 中固化有卡操作系统（Card Operating System，COS）。由于 CPU 卡内装了 COS，使它不仅具有数据存储处理功能，还具有命令控制和数据安全保护功能，所以 CPU 卡可应用于安全保密性要求高的场合，如金融信用卡、手机 SIM 卡等。

严格地讲，只有 CPU 卡才是真正意义上的“智能卡”。由于工艺技术要求苛刻等因素，目前世界上仅有少数几家著名半导体芯片制造商能设计和生产 CPU 卡芯片，如美国的 Motorola 公司、Atmel 公司，韩国的三星公司，德国的 Siemens 公司，法国的 Bull 公司，荷兰的 Philips 公司等。多数卡制造商均选择这几家芯片制造商的产品，将芯片封装并灌以自行开发的卡操作系统（Card Operating System，COS），而成为拥有各自注册版权的 CPU 卡。

2.2.2 按数据传输接口形式分类

按卡与外界数据传输的接口形式不同可将智能卡分为接触式 IC 卡、非接触式 IC 卡和双界面卡。

1. 接触式 IC 卡

接触式 IC 卡是通过金属电极触点与外部终端直接接触连接，实现数据的读写。接触式 IC 卡的物理特性和通信方式符合 ISO/IEC 7816 标准，其外形尺寸如图 2-1 所示。

ISO/IEC 7816 – 2 对接触式 IC 卡的触点功能作了具体的规定，见表 2-1。

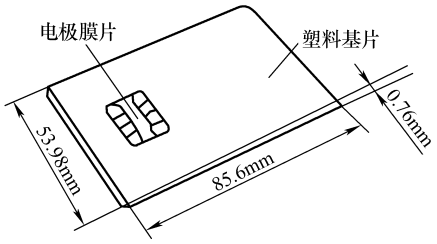


图 2-1　接触式 IC 卡外形尺寸

表 2-1　接触式 IC 卡触点功能定义

触点编号	功　能	触点编号	功　能
C1	VCC（工作电源）	C5	GND（地）
C2	RST（复位信号）	C6	VPP（编程电源）
C3	CLK（时钟）	C7	I/O（数据输入/输出端）
C4	RFU（保留使用）	C8	RFU（保留使用）

2. 非接触式 IC 卡

非接触式 IC 卡又称射频卡（Radio Frequency Card），卡的表面上无触点，是利用射频技术，通过电磁波传输实现数据读写。非接触式 IC 卡由芯片和天线组成，如图 2-2 所示，芯片内设有射频收发电路。根据卡内是否带有电源分为有源和无源两种，目前多使用无源卡。卡所需能量、时钟脉冲和数据是通过天线的电磁耦合作用获得的。

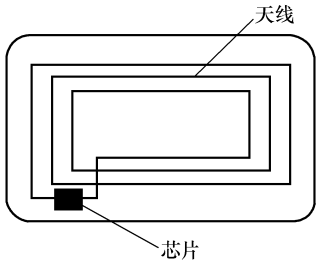


图 2-2　非接触式 IC 卡

非接触 IC 卡分为紧耦合卡、近耦合卡和远耦合卡三种，见表 2-2。目前应用最多的是遵循 ISO/IEC 14443 标准的近耦合卡，该标准主要有 Type A 和 Type B 两种体系，其中 Type A 以 Philips 公司为代表，包括 Siemens、Hitachi、G&D 和 Schlumberger 等公司的各种产品；Type B 以意法半导体（ST）、Motorola、韩国 Samsung 和日本 NEC 等公司为代表。Type A 和 Type B 标准的主要区别在于二进制调制、编码和反碰撞方式的不同。Type A 标准的产品拥有更大的市场份额。

3. 双界面卡

双界面卡是指将接触式接口与非接触式接口集成在一张卡片上的 IC 卡。对芯片的访问，既可以通过触点接触访问，也可以通过射频方式非接触访问。这两

种接口方式分别遵循两个不同的标准，接触接口符合 ISO/IEC 7816，非接触接口符合 ISO/IEC 14443。

表 2-2 非接触 IC 卡类型

非接触 IC 卡类型	通信距离	标准
紧耦合卡	0 ~ 1cm	ISO/IEC 10536
近耦合卡	0 ~ 10cm	ISO/IEC 14443 Type A/Type B
远耦合卡	0 ~ 1m	ISO/IEC 15693

双界面卡可分为以下三种：

1）接触式 IC 卡系统与非接触式 IC 卡系统只是物理地组合到一张卡片中，两套系统互相独立。

2）接触式 IC 卡系统与非接触式 IC 卡系统彼此操作独立，但共享卡内部分存储空间。

3）接触式 IC 卡系统与非接触式 IC 卡系统完全融合，接触式与非接触式运行状态相同，共用一个 CPU 管理。

三种双界面卡中，只有最后一种双界面卡才是真正意义上的非接触式双界面卡。

2.3 智能卡国际标准

ISO/IEC 7816 是 IC 卡遵循的主要国际标准，该标准现有 10 个部分，分别对 IC 卡的物理特性、卡触点的尺寸与位置、电信号与传输协议、行业间交换命令、数据元以及 IC 卡注册管理办法等做出了详细规定。

2.3.1 接触式 IC 卡国际标准

接触式 IC 卡最主要的技术标准为 ISO/IEC 7816 系列，主要涉及 IC 卡的物理特性、电性能、环境适应性、传送协议等，所有的接触式 IC 卡及其应用装置都必须遵循这些技术标准。此系列中应用最多的是前 4 个标准。

1）ISO/IEC 7816 - 1：《识别卡 带触点的集成电路卡 第 1 部分：物理特性》，该标准规定了带触点集成电路卡的物理特性，如触点的电阻、机械强度、热耗、电磁场、静电等。

2）ISO/IEC 7816 - 2：《识别卡 带触点的集成电路卡 第 2 部分：触点尺寸和位置》，该标准规定了 ID - 1 型 IC 卡上触点的尺寸、位置和任务分配。

3）ISO/IEC 7816 - 3：《识别卡 带触点的集成电路卡 第 3 部分：电信号和传输协议》，该标准规定了电源、信号结构以及 IC 卡与终端间的信息交换，包括信

号速率、电压电平、电流数值、奇偶约定、操作规程、传输机制，以及与 IC 卡的通信。

4）ISO/IEC 7816－4：《识别卡 带触点的集成电路卡 第 4 部分：行业间交换用指令》，该标准规定了终端和卡之间所传送的报文、指令和响应的内容；安全体系结构；行业间交换命令和保密报文交换方法等内容。

5）ISO/IEC 7816－5：《识别卡 带触点的集成电路卡 第 5 部分：应用标识符的编号体系和注册程序》，该标准规定了应用提供者的注册内容。

6）ISO/IEC 7816－6：《识别卡 带触点的集成电路卡 第 6 部分：交换用行业间数据元》，该标准规定了用于交换的数据元。

7）ISO/IEC 7816－7：《识别卡 带触点的集成电路卡 第 7 部分：结构化卡查询语言的行业间命令》。该标准规定了基于 SQL 结构化卡查询语言数据库的概念和相关行业命令。

8）ISO/IEC 7816－8：《识别卡 带触点的集成电路卡 第 8 部分：安全操作命令》。该标准规定了与安全相关的行业间命令。

9）ISO/IEC 7816－9：《识别卡 带触点的集成电路卡 第 9 部分：附加的行业间命令和安全属性》。该标准规定了 IC 卡和相关对象生命周期的描述和编码；附加行业间命令的功能和语法规则，以及与这些命令相关的数据元。

10）ISO/IEC 7816－10：《识别卡 带触点的集成电路卡 第 10 部分：同步卡的电信号和复位应答》。该标准规定了功率、信号结构及 IC 卡与终端间同步传输的复位应答。

11）ISO/IEC 7816－11：《识别卡 带触点的集成电路卡 第 11 部分：生物方式的个人身份验证》。

12）ISO/IEC 7816－12：《识别卡 带触点的集成电路卡 第 12 部分：USB 电气接口及操作规程》。

13）ISO/IEC 7816－13：《识别卡 带触点的集成电路卡 第 13 部分：多应用环境下的应用管理命令》。

14）ISO/IEC 7816－15：《识别卡 带触点的集成电路卡 第 15 部分：密码信息应用》。

2.3.2　非接触式 IC 卡国际标准

非接触式 IC 卡表面无触点，因此终端与卡的通信方式及提供电源的方式均与接触式 IC 卡不同。国际标准化组织根据终端与 IC 卡作用距离不同制定了一些国际标准，其中影响最大的主要有 ISO/IEC 14443、ISO/IEC 15693 和 ISO/IEC 18000 三个系列标准。

1. ISO/IEC 14443

ISO/IEC 14443 是识别卡、非接触式集成电路卡、邻近卡标准，采用的载波频率为 13.56MHz，定义了 Type A、Type B 两种类型协议，通信速率为 106 kbit/s。由于调制深度和编码方式不同，Type B 与 Type A 相比，具有速率更高、传输能量不中断、抗干扰能力更强的优点，我国第二代居民身份证中的射频识别技术采用的就是 ISO/IEC 14443 Type B 协议。符合该标准的 RFID 设备及标签的最大识读距离约为 10cm。该标准分四部分：

1）ISO/IEC 14443 -1：物理特性。

2）ISO/IEC 14443 -2：射频功率和信号接口。

3）ISO/IEC 14443 -3：初始化和防冲突。

4）ISO/IEC 14443 -4：传送协议。

2. ISO/IEC 15693

ISO/IEC 15693 是识别卡、非接触式集成电路卡、邻近卡标准，该标准已被广泛应用，符合该标准的 RFID 设备已经非常成熟，最大识读距离可达 1m。该标准分三部分：

1）ISO/IEC 15693 -1：物理特性。

2）ISO/IEC 15693 -2：空中接口和初始化。

3）ISO/IEC 15693 -3：防冲突和传送协议。

3. ISO/IEC 18000

ISO/IEC 18000 是信息技术、项目管理的射频识别技术标准，它涵盖了 125kHz ~ 2.45GHz 的通信频率，识读距离由几厘米到几十米。该系列标准分为六个部分，包括：第 1 部分为标准化的参数定义；第 2 部分为 135kHz 以下的空中接口通信参数；第 3 部分为 13.56MHz 的空中接口通信参数；第 4 部分为 2.45GHz 的空中接口通信参数；第 6 部分为 860 ~ 960MHz 的空中接口通信参数；第 7 部分为 433MHz 的空中接口通信参数。其中第 6 部分应用最广，它包含 Type A、Type B 和 Type C 三种无源标签的接口协议，由于符合 Type C 协议的标签读写速度快，抗干扰性好，抗冲突能力强，该标准已得到世界上众多企业的支持，目前已经开始应用到供应链管理、图书馆管理、资产追踪、后勤管理等众多领域。

2.3.3 测试标准

IC 卡是否符合国际标准，在应用前要进行测试。ISO/IEC 10373 是对各种卡进行测试的国际标准，包括磁卡、接触式 IC 卡、非接触式 IC 卡和光卡。

值得一提的是，国际标准是不断充实和完善的，即使是已经通过的国际标准，仍有修改的可能性，所以应注意国际标准的最新版本。

2.4　智能卡传输协议

IC 卡支持两种传输协议：同步传输协议和异步传输协议。同步传输协议在 ISO/IEC 7816 – 10 中定义，适用于逻辑加密卡；异步传输协议在 ISO/IEC 7816 – 3 中定义，适用于内含微处理器的智能卡。ISO/IEC 7816 – 3 标准提供了多种传输协议，这些协议均以“T = 序列号”来命名，主要采用两种通信协议：T = 0 和 T = 1 通信协议。T = 0 是异步半双工字符传输协议，T = 1 是异步半双工块传输协议。

2.4.1　卡的复位操作

完整的 IC 卡操作过程包括 IC 卡插入接口设备、卡和接口设备的信息交换、IC 卡从接口设备拔出等所有操作。一个正常的操作过程按以下步骤完成：

1）接口设备连接卡并激活电路。

2）卡的冷复位。

3）卡对复位的应答。

4）卡和接口设备间交换信息。

5）接口设备释放电路。

6）从接口设备中取出 IC 卡。

IC 卡利用激活的复位信号，采用异步方式进行复位应答，其复位方式有两种：冷复位和热复位。

1. 冷复位

当接口设备激活电路后，RST 为 L 状态，VCC 加电，接口设备的 I/O 口线处于接收方式，提供稳定的 CLK，此时 IC 卡就处于冷复位状态。在冷复位前 IC 卡内部状态是未定义的。

冷复位的时序如图 2-3 所示。在 T_a 时刻加 CLK 信号；I/O 口线应在时钟信号加于 CLK 的 200 个时钟周期（t_a）内被卡置为 H 状态；时钟信号加于 CLK 后，RST 应至少保持 400 个时钟周期（t_b）的 L 状态，当 RST 为 L 状态时，接口设备会忽略 I/O 口线上的状态。

在时刻 T_b，RST 被置为 H 状态，I/O 口线上的应答应出现在 RST 信号上升沿后的 400 ~ 40000 个时钟周期（t_c）。当 RST 处于 H 状态时，如果应答信号在 40000 个时钟周期内仍未开始，接口设备将释放电路。

2. 热复位

当 VCC 和 CLK 保持稳定时，接口设备置 RST 为状态 L 至少 400 时钟周期（时间 t_e）后，接口设备启动热复位，如图 2-4 所示。

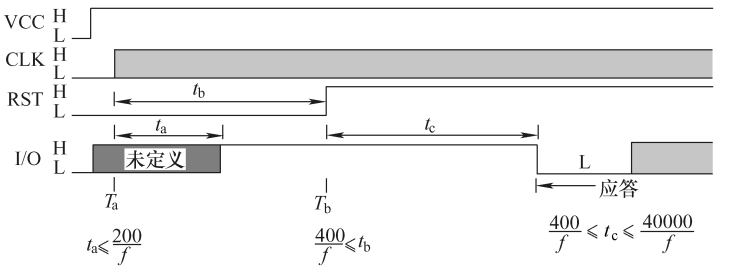


图 2-3 冷复位

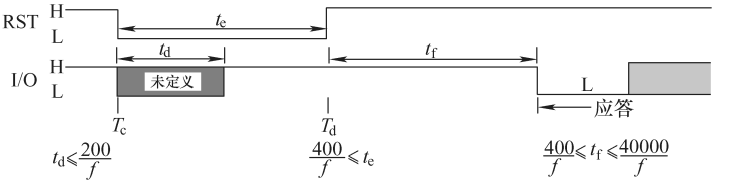


图 2-4 热复位

在时间 T_d，RST 置于 H 状态。I/O 应答应在 RST 信号上升沿之后的 400 ~ 40000 个时钟周期（t_f）之前开始。

在 RST 处于状态 H 时，如果应答信号未在 40000 个周期之后开始，RST 上的信号将返回状态 L，接口设备将释放电路。

3. 时钟停止

对支持时钟停止的卡，当接口设备不希望从卡得到信息，并且 I/O 口线保持在状态 H 至少 1860 个时钟周期（t_g），则按照图 2-5 所示，接口设备可停止 CLK 上的时钟（在时间 T_e）。

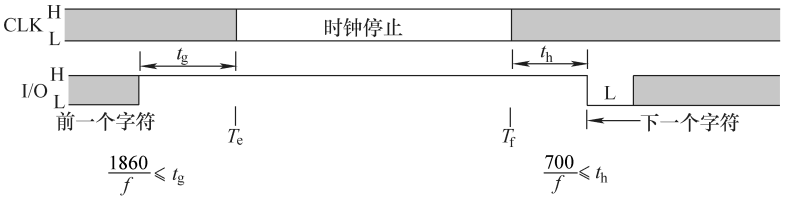


图 2-5 时钟停止

当时钟被停止（$T_e \sim T_f$），CLK 可保持为状态 H 或状态 L。在时间 T_f，接口设备重启时钟，I/O 口线上的信息交换可在至少 700 个时钟周期（在时间 $t_h + T_f$）后继续。

4. 释放

当信息交换结束或失败时，如无卡响应或发现卡被移出时，接口设备应按图 2-6 所示顺序释放电路。

1）RST 为状态 L。

2）CLK 为状态 L（除非时钟已在状态 L 上停止）。

3）I/O 口线置为状态 L。

4）VCC 被释放。

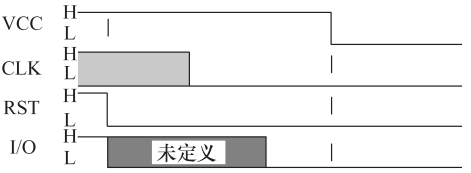


图 2-6　释放

2.4.2　卡的复位应答

当接口设备发出复位信号后，IC 卡将以字符为单位（称为字符帧）发出复位应答信号（Answer to Reset，ATR），复位应答信号是由一串字符组成，它们规定了卡和接口设备间建立的通信特性。下面先介绍字符帧格式，然后描述复位应答信号。

1. 基本时间单元

基本时间单元（Elementary Time Unit，ETU）是指 I/O 口线上传送一位所用的时间。

在复位应答期间，1ETU 应与 372 个时钟周期相等，即 1ETU = 372/f，f 为接口设备提供给 IC 卡 CLK 触点的时钟频率。

复位应答之后，ETU 由公式得到：1ETU = $F/(Df)$。其中 F 为时钟频率转换因子，D 为波特率校正因子。F 和 D 的默认值为 $F = 372$，$D = 1$。

2. 字符帧

数据在 I/O 口线上是按字符帧格式进行传输的，如图 2-7 所示。

字符传输前，I/O 口线应被置为 H 状态。一个字符包括 10 个连续位，由 1 位起始位、8 位数据位、1 位奇偶校验位组成。起始位始终为低电平，表明一个

图 2-7 字符帧格式

字符传输的开始；数据位占 1B；奇偶校验位采用的是偶校验，即一个字符中逻辑 1 的个数必须为偶数，这里是指数据位和奇偶校验位所含逻辑 1 的个数要保证是偶数。

两个连续的字符之间有一个至少保持 12 个 ETU 的延时。在复位应答期间，卡发出的两个连续字符的上升沿间的延迟应不超过 9600ETU，这个最大值被称为“初始等待时间”。

3. 复位应答

复位应答是一系列字节的值，这些字节是卡作为对复位命令的响应发送给接口设备的。复位应答的字节顺序为：初始字符 TS、格式字符 T0、接口字符 TA_i – TB_i – TC_i – TD_i（$i = 1$，2，…）、历史字符 T1 – T2 – … – TK（最多 15 个字符）和校验字符 TCK（Check Character）。其中，TS 和 T0 是必须有的，接口字符和历史字符是可选择的，且 TS 后发送的字符数最大不超过 32 个。

（1）初始字符 TS

初始字符 TS 定义了所有后继字符的编码协议，有反向约定和正向约定两种。

反向约定：IC 卡回送的 TS 为（H）LHHLLLLLLH，值为 3FH。反向约定规定 I/O 口线上的低电平状态等效于逻辑 1，且首先传送的是字节的最高有效位。

正向约定：IC 卡回送的 TS 为（H）LHHLHHHLLH，值为 3BH。正向约定规定 I/O 口线上的低电平状态等效于逻辑 0，且首先传送的是字节的最低有效位。

接口设备一般都支持反向约定和正向约定，能接收 IC 卡回送的 3FH 或 3BH，但实际使用更多的是正向约定。

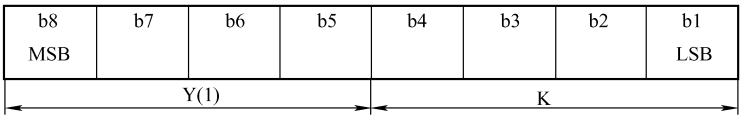
（2）格式字符 T0

格式字符 T0 声明了第一组接口字符和所有历史字符，其编码如图 2-8 所示。可以看出，T0 由两部分组成：高 4 位 b5 ~ b8 用来指明后继接口字节 TA1 ~ TD1 是否存在，为 1 时表明对应的接口字节存在；低 4 位 b1 ~ b4 用来指明历史字符的个数，范围为 0 ~ 15。

（3）接口字符 TA_i – TB_i – TC_i – TD_i（$i = 1$，2，3，…）

接口字符用来指明协议参数。

TD_i 用来指明协议类型 T 和是否存在后续接口字符，其编码如图 2-9 所示。



Y(1): 接口字节存在的标记

b5=1 时 TA_1 存在

b6=1 时 TB_1 存在

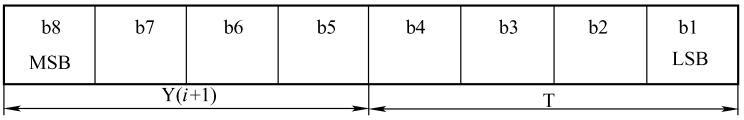
b7=1 时 TC_1 存在

b8=1 时 TD_1 存在

K: 历史字节的数目，为0～15

图 2-8　T0 编码

可以看出，TD_i 由两部分组成：一部分是由高四位 b5 ~ b8 组成的 Y（$i+1$），用来指明后续接口字符 TA_{i+1}、TB_{i+1}、TC_{i+1}和 TD_{i+1}是否存在，若 TD_i 不存在，则 TA_{i+1}、TB_{i+1}、TC_{i+1}和 TD_{i+1}也不存在。另一部分是低 4 位 b1 ~ b4 组成的 T，用来指明后续发送到协议类型。当 T = 0 时，表示为异步半双工字符传输协议，此时 IC 卡不回送 TD_1，且后续传输协议类型为 T = 0。当 T = 1 时，表示为异步半双工块传输协议，此时 IC 卡回送 TD_1 = 0x81，表明 TD_2 存在，且后续传输协议类型为 T = 1。



Y(i+1): 接口字节存在标记

b5=1 时 TA_{i+1} 存在

b6=1 时 TB_{i+1} 存在

b7=1 时 TC_{i+1} 存在

b8=1 时 TD_{i+1} 存在

T: 协议参考和 / 或接口字节限制符

图 2-9　TD_i 编码

TA_1、TB_1、TC_1 和 TA_2、TB_2 是全局性接口字符，TC_2 是 T = 0 协议专用接口字符，TA_i、TB_i 和 TC_i（$i>2$）的解释取决于 TD_{i-1}指定的协议 T 的类型。有关这些接口字符的具体定义请参照 ISO/IEC 7816 – 3。

（4）历史字符 T1 – T2 – … – TK

历史字符由格式字符 T0 的 K 指明历史字符的个数，最多不超过 15 个。有关

历史字符的具体定义请参照 ISO/IEC 7816—4。

（5）校验字符 TCK

校验字符 TCK 的值应使从 T0 到 TCK 的所有字节异或操作结果为 0。当使用协议 T = 0 时，将不发送 TCK，而其他协议将发送 TCK。

4. 基本复位应答（ATR）

通常情况下，协议 T = 0 和协议 T = 1 是 IC 卡和接口设备共同支持的协议。这两种协议的基本复位应答见表 2-3 和表 2-4。

表 2-3　T = 0 协议的基本复位应答

IC 卡回送字符	值	说　　明
TS	0x3B 或 0x3F	正向约定或反向约定
T0	0x6X	TB1 和 TC1 存在，X 表示历史字节个数
TB_1	0x00	不使用 Vpp
TC_1	0x00 ~ 0xFF	所需额外保护时间的长度

T = 0 时，IC 卡回送字符的顺序为 TS、T0、TB_1 和 TC_1。

表 2-4　T = 1 协议的基本复位应答

IC 卡回送字符	值	说　　明
TS	0x3B 或 0x3F	正向约定或反向约定
T0	0xEX	TB_1 ~ TD_1 存在，X 表示历史字节个数
TB_1	0x00	不使用 Vpp
TC_1	0x00 ~ 0xFF	所需额外保护时间的长度
TD_1	0x81	TA_2 ~ TC_2 不存在，TD_2 存在
TD_2	0x31	TA_3 和 TB_3 存在，TC_3 和 TD_3 不存在
TA_3	0x10 ~ 0xFE	返回信息域整数大小 IFSI
TB_3	高半字节 0 ~ 4 低半字节 0 ~ 5	高半字节为块等待时间 低半字节为字节等待时间
TCK		校验字节

T = 0 时，IC 卡回送字符的顺序为 TS、T0、TB_1、TC_1、TD_1、TD_2、TA_3、TB_3 和 TCK。

5. 操作模式

复位应答后，卡处于两种操作模式之一：专用模式（TA_2 存在）和协商模式（TA_2 不存在）。

图 2-10 显示了卡操作模式的选择。

在专用模式下，紧随复位应答之后，由 TA_2 中 b5 位的取值来决定时钟频率转换因子 *F* 和波特率调节因子 *D* 的取值。当 b5 = 1 时，*F* 和 *D* 值取默认值 *F* =

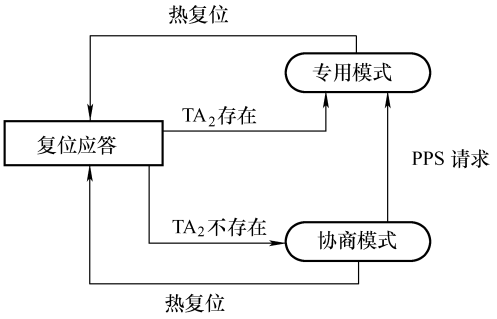


图 2-10　卡的操作模式

372，$D=1$。当 b5 = 0 时，F 和 D 的取值请参考 ISO/IEC 7816 – 3。

在协商模式下，若复位应答后无协议与参数选择（PPS）请求，则 F 和 D 值取默认值；若复位应答有 PPS 请求，则由接口设备发送带有 F 和 D 的 PPS 请求，使卡从协商模式转换为专用模式，并使用该 F 和 D 值。

6. 协议与参数选择（PPS）

卡和接口设备的通信总是由接口设备启动的，这意味着如果没有外部请求，卡不会送出数据。卡只响应从接口设备发来的命令。当卡插入接口设备后，自动执行上电复位，并送出一个复位应答（ATR）信号给接口设备。接口设备对卡 ATR 信号进行解析，然后发出第一条命令，卡对该命令进行处理并产生一应答信号回送给接口设备，这种命令和应答的来往一直持续到卡被激活。

在复位应答之后，卡如果处于协商模式，则允许接口设备向卡发送 PPS（Protocol and Parameters Selection，协议和参数选择）请求。只有接口设备允许发出 PPS 请求，其过程如下：

1）接口设备向卡发送 PPS 请求。

2）若卡收到错误的 PPS 请求，它将不会发出响应信号。

3）若卡收到正确的 PPS 请求，则发出 PPS 响应信号，否则将超出初始等待时间。

4）若成功交换 PPS 请求和 PPS 响应，表明选择好了新的协议类型和（或）传送参数，按规定将数据从接口设备送到卡中。

如果存在下列三种情况之一：初始等待时间超时、错误的 PPS 请求、接口设备收到错误的 PPS 响应信号，接口设备将执行释放操作。

PPS 请求和 PPS 响应信号都是由初始字符 PPSS（代码为 FF）、格式字符 PPS0，三个任选字符 PPS1、PPS2、PPS3 以及最后一个校验字符 PCK 组成。通常情况下，如果 PPS 响应和 PPS 请求相等，则表明 PPS 交换成功，例外情况参见 ISO/IEC 7816 – 3。

2.4.3 数据链路层

本节给出了 T=0 和 T=1 两类协议的数据链路层描述。

2.4.3.1 T=0 协议

T=0 协议是异步半双工字符传输协议，是面向字符的传输协议，卡和终端之间可以传输的最小数据单元是字节。本协议所用的参数都是在复位应答时所指定的，除非被协议和参数选择所修改，此时由 PPS 指定参数。

由终端发出命令，由卡发送过程字节。

1. 命令头

命令头由终端应用层（Terminal Application Layer，TAL）发出，由连续的 5 个字节组成，包含 CLA、INS、P1、P2 和 P3。命令头定义如下：

1）CLA：指令类别，除“FF”外的任何值；值为 FF 时被指定为 PPS。

2）INS：指令码，当最低位是“0”，且高位半字节既不是“6”也不是“9”时，INS 才有效；

3）P1、P2：INS 的附加参数。

4）P3：根据 INS 的功能，P3 指明了发送给 IC 卡的数据长度或者等待从 IC 卡返回的最大数据长度。

对 T=0 协议，这些字节和随命令发送的数据一起构成了命令传输协议数据单元（Command Transport Protocol Data Unit，C－TPDU）。终端传输层（Terminal Transport Layer，TTL）发出这 5B 的命令头后，会等待由卡返回的过程字节。

2. 过程字节

IC 卡收到命令头后，会返回一个过程字节给终端传输层（TTL），以指明 TTL 下一步的动作。过程字节有三种类型，见表 2-5：

1）NULL：值为“60”。表示不对 VPP 状态和数据传输施加任何影响。

2）ACK：除了值“6X”和“9X”以外，在 ACK 字节中的高七个位全都等于 INS 字节中相应位或与之互补。ACK 字节用于控制 VPP 状态和数据传输。

3）SW1－SW2：SW1 的值为“6X”或“9X”，但不包括“60”；SW2 为任意值。SW1－SW2 用于表示命令结束。当 SW1－SW2 =“90”－“00”时表示正常结束。

表 2-5 对过程字节的响应

类型	过程字节值	终端传输层（TTL）执行的操作
ACK	与 INS 字节相同	TTL 传送所有剩余的数据字节
	与 INS 字节补码相同	TTL 传送所有下一个数据字节
NULL	“60”	TTL 延长等待时间
SW1－SW2	SW1 为“6X”或“9X”，除“60”之外；SW2 为任意值	TTL 等待状态码 SW2

对过程字节 ACK 和 NULL，终端传输层（TTL）完成动作后将等待另一个过程字节；对 SW1，在收到第二个状态字节 SW2 后，终端传输层 TTL 将做以下事情：

1）如果过程字节为“61”，TTL 将发送一个 P3 = “XX” 的命令（GET RESPONSE）给卡，“XX” 为 SW2 的值。

2）如果过程字节为“6C”，TTL 将立即重发前一个命令的命令头给 IC 卡，此时的 P3 = “XX”，“XX” 为 SW2 的值。

3）如果状态码是“6X”（除“60”、“61” 及“6C” 之外）或“9X”，TTL 将通过命令响应 APDU（Response Application Protocol Data Unit，R – APDU）返回状态码 SW1 和 SW2 给终端应用层（TAL），并等待下一个命令应用协议数据单元（Command Application Protocol Data Unit，C – APDU）。

当返回的状态码 SW1 – SW2 = “90” – “00” 时，表示正常结束；若 SW1 的高半字节为 6，则表示发生了与应用无关的错误，见表 2-6。

表 2-6　SW1 的错误代码

SW1	含　义
“6E”	卡不支持这类指令
“6D”	指令代码没有被编程或者无效
“6B”	参数错误
“67”	长度错误
“6F”	没有给出准确的诊断
其他值	保留

2.4.3.2　T = 1 协议

T = 1 协议是异步半双工块传输协议，卡和终端之间可以传输的最小数据单元是块组（Block）。本协议定义了异步半双工块传输协议使用的命令结构和处理，这些命令由接口设备（Interface Device，IFD）和集成电路卡（Integrated Circuit Card，ICC）启动，包括卡专用的控制，以及流控制、块链和错误校正等的数据传输控制。

1. 块帧（Block Frame）

一个块帧由一串字节组成，每个字节以异步字符的形式传输。块帧包括三部分：起始域（Prologue Field）、信息域（Information Field）和终止域（Epilogue Field），其中起始域和终止域是必须要发送的，信息域是可选的。块帧格式见表 2-7。

表 2-7 块帧格式

起始域			信息域	终止域
节点地址（NAD）	协议控制字节（PCB）	长度（LEN）	控制信息（INF）	错误校验码（EDC）
1B	1B	1B	0～254B	1B LRC 或 2B CRC

（1）起始域

起始域含有三个子段：节点地址（NAD）、协议控制字节（PCB）和长度（LEN），每个子段占 1B。

1）节点地址（Nod Address，NAD）。

起始域的第 1 个字节称为节点地址（NAD），用于标识块的目的节点地址和源节点地址。其中，b1～b3 是源节点地址（Source node Address，SAD），b5～b7 是目的节点地址（Destination node Address，DAD），b4 和 b8 用于表示 VPP 状态控制。当不使用节点地址时，将 SAD 和 DAD 置 0。当使用节点地址时，由 IFD 发送给 IC 卡的第一个数据块的 SAD 与 DAD 应设为不同的值。当 SAD 与 DAD 值相等且不为 0 时，NAD 的其他值保留将来使用。

由 IFD 发送的第一个块的 NAD 确定了 SAD 与 DAD 的逻辑关系，在随后块中的 NAD 域包含了相同的 SAD 与 DAD 地址对，并具有相同的逻辑关系。例如，由 IFD 发送的块，其 SAD 的值为 X，DAD 的值为 Y；由 ICC 发送的块，其 SAD 的值为 Y，DAD 的值为 X，这属于一个逻辑连接（X，Y）。如果 IFD 发送块的 SAD 值为 V，DAD 值为 W，ICC 发送块的 SAD 值为 W，DAD 值为 V，则属于另一个逻辑连接（V，W）。

2）协议控制字节（Protocol Field，PCB）。

起始字段的第 2 个字节称为协议控制字节（PCB），用来传送控制传输所需要的信息，表明了传输块类型。本协议定义了三种基本类型块：

信息块（I－block，I 块）：传送应用层信息及确认信息。

接收准备块（R－block，R 块）：发送确认信息，没有信息域。

管理块（S－block，S 块）：在 IFD 和 ICC 之间交换控制信息，其信息域的存在与否取决于 S 块控制功能的需要。

不同基本类型块的 PCB 编码不同，见表 2-8～表 2-10。

表 2-8 I 块的 PCB 编码

字节位（b8～b1）	取值及含义
b8	0，I－block 的标识符
b7	N（S），序列号
b6	M 位，M＝1 表示后面还有块数据
b5～b1	保留

表 2-9　R 块的 PCB 编码

字节位（b8 ~ b1）	取值及含义
b8 ~ b7	10，R - block 的标识符
b6	0
b5	N（R），序列号
b4 ~ b1	0000：无差错 0001：EDC 或奇偶错 0010：其他错 其他值：保留

表 2-10　S 块的 PCB 编码

字节位（b8 ~ b1）	取值及含义
b8 ~ b7	11，S 块的标识符
b6	0：请求 1：应答
b5 ~ b1	00000：再同步请求或应答（由 IFD 发出） 00001：请求或应答改变信息域大小（由卡发出） 00010：请求或应答异常终止 00011：请求或应答改变等待时间 00100：VPP 状态错误（b6 = 1） 其他值：保留

3）长度（Length，LEN）。

LEN 表示被传送的信息域字节数，其值为“00”~“FE”（0 ~ 254B），0 值表示没有信息域 INF。

（2）信息域（Information Field）

信息域（INF）是可选的，当它存在时，可以是应用数据（I 块）或控制和状态信息（S 块），被传送的字节数由 LEN 指出。R 块中没有信息域。

（3）终止域（Epilogue Field）

终止域用来传送差错校验码（Error Detection Code，EDC），可以采用纵向冗余校验（Longitudinal Redundancy Check，LRC），也可以采用循环冗余校验（Cyclic Redundancy Check，CRC）。其中 LCR 占 1B，CRC 占 2B。LCR 的值与块中所有字节进行异或运算时结果都为 0。CRC 的值参照 ISO/IEC 13239。

2. 协议参数

（1）特殊接口字符

当特殊接口字符 TA_i、TB_i、TC_i 出现在复位应答中，且在 TD_{i-1}（$i > 2$）中的 T = 1 第一次出现之后时，这些特殊接口字符用来将协议参数设为非默认值，将此时的这三个字节命名为第一 TA_i、第一 TB_i、第一 TC_i。

（2）卡的信息域尺寸（IFSC）

卡的信息域尺寸是卡能接受的各个块中信息域的最大长度，由第一 TA_i 设置其初值，默认值为 32。

（3）接口设备的信息域尺寸（IFSD）

接口设备的信息域尺寸是指接口设备能接受的各个块中信息域的最大长度，默认值为 32。

（4）IFSC 和 IFSD 的编码

IFSC 和 IFSD 在协议启动时被初始化。其编码规则为“01” ~ “FE”，为数字 1 ~ 254，“00”和“FF”保留。需要注意的是：块的尺寸是起始域、信息域和终止域所传输字节的总和，所以块的最大尺寸为 IFSC 加上 4B 或 5B（取决于终止域的长度）。

3. 等待时间

在数据传输时，定义了不同的等待时间以使收发双方能在规定的最小和最大时间区间内作不同的处理，同时也提供了规定的方法来结束通信，以防止在出差错的情况下死锁。

（1）字符等待时间

字符等待时间定义为同一块中两个连续字符起始沿之间的最长时间，如图 2-11 所示。由第一 TB_i 的 b4 ~ b1 给出字符等待时间整数值（CWI），其范围为 0 ~ 15，CWT 的计算公式为

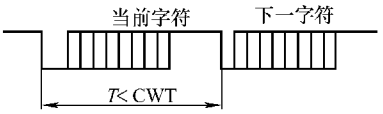


图 2-11 字符等待时间

$$CWT = (2^{CWI} + 11)ETU \tag{2-1}$$

CWT 的最小值等于 12ETU，默认值为 13。

（2）块等待时间（BWT）

块等待时间定义为送达到卡的最后一个字符的起始沿与由卡发送出的第一个字符的起始沿之间的最长时间，如图 2-12 所示。

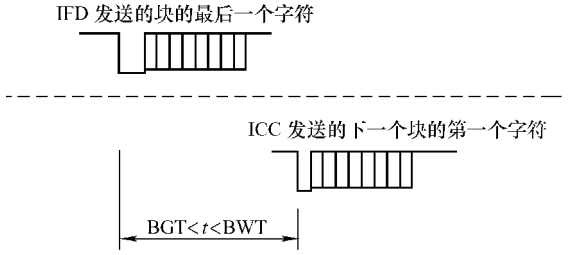


图 2-12 块等待时间和块保护时间

第一 TB_i 的 b8 ~ b5 给出块等待时间整数值（BWI），其范围为 0 ~ 9，10 ~ 15

留待将来使用。BWI 的默认值为 4。BWT 的计算公式为

$$BWT = (2^{BWI} \times 960 \times 372D/f + 11)\,ETU \tag{2-2}$$

BWT 用来检测无响应的卡。

（3）块保护时间（BGT）

块保护时间为两个相对方向发送的连续字符起始沿之间的最短时间，所以一个已接收块的最后一个字符与一个被传输块的第一个字符之间的延时至少应大于 BGT 且小于 BWT。

4. 数据链路层——字符部分

VPP 状态由 NAD 的 b8 和 b4 控制：

1）b8 = 0，b4 = 0：VPP 置为 0 或保持空闲状态。

2）b8 = 1，b4 = 0：VPP 置为编程状态，在接收 PCB 后回到空闲状态。

3）b8 = 0，b4 = 1：VPP 置为编程状态，直到终端收到另一个 PAD 字节。

4）b8 = 1，b4 = 1：禁用。

如果 NAD 上发生奇偶错，VPP 应返回或保持空闲状态。如果发生超时，即在 CWT 或 BWT 期间卡发送一个预期字符失败，则 VPP 应返回或保持空闲状态。一个字符触发的所有 VPP 传输应发生在该字符上升沿起的 12ETU 期间。

5. 数据链路层——块部分

在复位应答或协议类型选择之后的第一个块是由终端传送到 IC 卡的，可以是信息块或管理块。

发送一个块（I 块、R 块或 S 块）后，在下一个块传送之前，发送方应该接收到确认，描述如下：

信息块 I – block 的序列号位 N(S) 是一个二进制位（bit），它的起始值为 0，在传送一个信息块 I – block 之后加 1（模 2）；

接收准备块 R – block 的序列号位 N(S)，它的值等于下一个要传送的 I – block 中的 N(S)，R – block 用于链接 I – block；

管理块 S – block 有请求块 S（... request） – block 和响应块 S（... response） – block 两种，接收到请求块后发出一个响应块。

块的链接情况受 I – block 中的协议控制字节（PCB）的 M 位控制，M 位指出 I – block的两种状态，当 M = 1 时，表示链组后面还有块，为 0 时表示是链组的最后一个块。

6. 链接

数据链接允许接口设备（IFD）和 IC 卡传输比 IFSC 或 IFSD 长的信息。如果接口设备（IFD）和 IC 卡传输的信息必须比相应的 IFSC 或 IFSD 长，则该信息应分为几个信息块，每个块的 LEN 应小于或等于 IFSC 或 IFSD，并且采用链接功能发送多个块。

应用数据（Application Data）由接口设备（IFD）传送到 IC 卡，假设分成三个信息块，分别为 Applic、action 和 Data，每次传送信息时还传送 PCB，以 I(N(S)，M）表示，其中 N（S）是发送序列号，M 表示后面是否还有块需要传送。当发送第一个块时，PCB 给出 I(0，1)，表示发送序列号为 0，且具有后续块的 I 块；IC 卡接收后，给出 R－block，其中包括 R(N(R))，N(R）为下一个要接收的块序列号，所以 N(R）＝1，…当发送完第三个块时，IC 卡发回信息长度为 0 的 I－block，I(0，0）表示传送结束。其操作过程如图 2-13 所示。

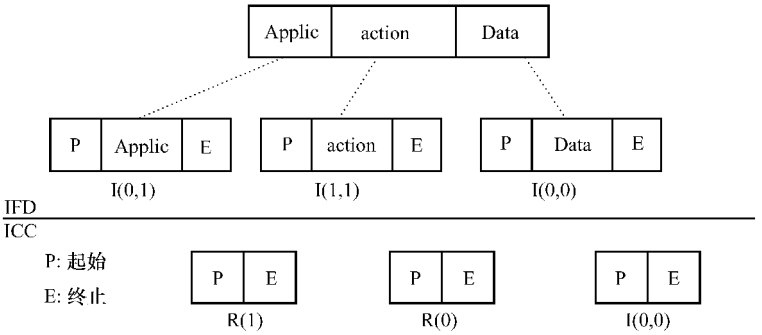


图 2-13　链接功能

I 块的链接由 PCB 中的 M 位（多数据位）控制，M＝1 表示链接了下一个块，且其为 I 块。当接收方正确接收到多数据 I 块时，它应发送 R(N(R))，其中N(R)等于下一个 I 块的 N(S)。另外，可在一个链中使用长度为 0 的 I 块。

2.4.4　终端传输层

终端传输层（TTL）定义了在 TTL 与卡片之间的命令和响应 APDU（Application Protocol Data Unit，应用协议数据单元）机制，APDU 是命令 APDU（C－APDU，Command APDU）或响应 APDU（R－APDU，Response APDU），可以包含数据。根据命令和响应 APDU 包含的数据情况，共有四种不同的 APDU（见 2.4.5 节），TTL 应能够对四种情况进行处理，完成终端和卡之间的数据交换。

传输应用层（TAL）传输 C－APDU 给 TTL，在 IC 卡接收到之前，应将 C－APDU 转换为传输协议认可的格式，IC 卡处理完命令后，将以 R－APDU 的格式将状态字和数据回送给 TTL。

1. T＝0 协议的 APDU 传送

C－APDU 到 T＝0 协议命令头的映射取决于命令的类型，卡片返回的数据和状态到 R－APDU 的映射取决于返回数据的长度。这里根据 APDU 四种不同的情况（见 2.4.5 节），分析 C－APDU 和 R－APDU 的映射方法，并对使用 GET RE-

SPONSE 命令取回 IC 卡中的数据进行说明。

1）C – APDU 和 R – APDU 均不含有数据。这种情况下，C – APDU 的 CLA、INS、P1、P2 被映射为 T = 0 协议命令头的 CLA、INS、P1、P2，T = 0 协议命令头的 P3 置为 0x00，该命令头由 TTL 发送给 IC 卡，IC 卡执行命令后，返回状态码给 TTL，该状态码原样映射到 R – APDU 的强制性尾标上。

2）C – APDU 不含有数据而 R – APDU 含有数据。这种情况下，C – APDU 的 CLA、INS、P1、P2、Le 被映射为 T = 0 协议命令头的 CLA、INS、P1、P2、P3，其中 P3 可以置为“00”，也可以置为需要返回的数据字节数。当卡片接收到该命令头后进行命令处理，在过程字节控制下，IC 卡回送数据和状态给 TTL。当 IC 卡回送给 TTL 的状态码为“6Cxx”或“61xx”时，TTL 将重新发送命令头；当状态码为“6Cxx”时，TTL 根据 xx 重发命令取回数据；当过程字节为“61xx”时，TTL 发 GET RESPONSE 命令取回数据。TTL 数据和状态到 R – APDU 的转换为：当状态码 SW1 – SW2 =“90” –“00”时，IC 卡回送给 TTL 的数据和状态会不做改变地变换到 R – APDU 的条件体和强制性尾标上；当状态码 SW1 – SW2 ≠“90” –“00”时，将被直接变换到 R – APDU 的强制性尾标上，并扔掉可能的数据。

3）C – APDU 含有数据而 R – APDU 不含数据。这种情况下，C – APDU 的 CLA、INS、P1、P2、Lc 被映射为 T = 0 协议命令头的 CLA、INS、P1、P2、P3。当卡片接收到该命令头后，如果卡片返回的是过程字节而不是状态码，则 TTL 将继续向卡片发送 C – APDU 的数据部分；如果卡片回送的是状态码 SW1 – SW2，则 TTL 会终止对命令的处理。TTL 数据和状态到 R – APDU 的转换为：任何由 IC 卡回送给 TTL 的状态码会直接变换到 R – APDU。

4）C – APDU 和 R – APDU 均含有数据。这种情况下，C – APDU 的 CLA、INS、P1、P2、Lc 映射为 T = 0 协议命令头的 CLA、INS，P1、P2、P3。当卡片接收到该命令头后，如果卡片返回的是过程字节而不是状态码，则 TTL 将继续向卡片发送 C – APDU的数据部分；当卡片返回给 TTL 过程字节“6Cxx”或“61xx”时，为“6Cxx”时 TTL 根据 xx 重发命令取回数据；为“61xx”时，TTL 发 GET RESPONSE 命令取回数据。TTL 数据和状态到 R – APDU 的转换为：当状态码 SW1 – SW2 =“90” –“00”时，IC 卡回送给 TTL 的数据和状态会不做改变地变换到 R – APDU的条件体和强制性尾标上；当状态码 SW1 – SW2 ≠“90” –“00”时，它将被直接变换到 R – APDU 的强制性尾标上，并扔掉可能的数据。

2. T = 1 协议的 APDU 传送

C – APDU 从传输应用层（TAL）传递到 TTL，TTL 将其原样映射到 I 块的 INF 字段上，并把该 I 块发送给 IC 卡。IC 卡通过 I 块的 INF 域向 TTL 回送响应数据和状态码，该 INF 域会原样映射到 R – APDU 上并回送给 TAL。如果需要，C – APDU 和响应数据状态码可以在多个 I 块的 INF 域链接起来。

2.4.5 应用层

应用层协议定义了 C – APDU 和 R – APDU 的具体结构。传输应用层（Transmission Application Layer，TAL）之间的数据交换都是由一个命令 – 响应对完成的，传输应用层（TAL）通过终端传输层（TTL）给 IC 卡发送命令 C – APDU，IC 卡处理完后将处理结果组成 R – APDU 通过 TTL 送给 TAL。每个命令都有一个特定的响应相匹配，一个 APDU 就是一个命令报文或响应报文。

根据 C – APDU 和 R – APDU 是否包含数据域，APDU 有四种情况，见表 2-11。

表 2-11 APDU 的类型

种类	命令 APDU 数据域	响应 APDU 数据域
1	无	无
2	无	有
3	有	无
4	有	有

1. C – APDU

C – APDU 由四字节命令头 CLA、INS、P1、P2 和一个可变长度的条件体组成，其中 4B 命令头是必需的，条件体随命令的不同而变化。C – APDU 的结构如图2-14 所示。

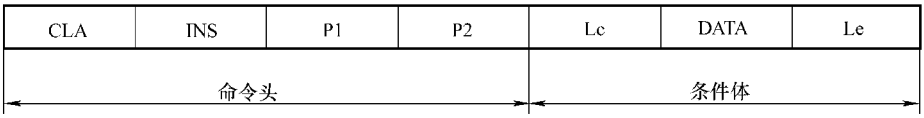


图 2-14 C – APDU 结构

1）CLA：命令类型，占 1B，不能为 0xFF。

2）INS：指令码，当最低位是“0”，低半字节为 0 且高半字节既不是“6”也不是“9”时，INS 才有效。

3）P1、P2：INS 的附加参数，分别占 1B。

4）Lc：发送数据长度，占 1B，在命令中定义为发送数据的字节数，取值范围是 1 ~ 255。

5）Data：为将要发送的命令数据域，字节数由 Lc 定义。

6）Le：接收数据长度，占 1B，指出命令响应中预期的数据最大字节数。Le 的取值范围是 0 ~ 255。如果 Le = 0，预期数据字节的最大长度是 256。

根据不同的命令，条件体的组成也不相同，C – APDU 有四种情况，

见表 2-12。

表 2-12　C – APDU 类型

命令类型	命令格式
1	CLA INS P1 P2
2	CLA INS P1 P2 Le
3	CLA INS P1 P2 Lc Data
4	CLA INS P1 P2 Lc Data Le

2. R – APDU

R – APDU 由一个最大长度为 Le 的数据域和一个强制性尾码组成，强制性尾码为 2B 状态代码，状态代码给出了 IC 卡对当前命令的处理结果，如图 2-15 所示。

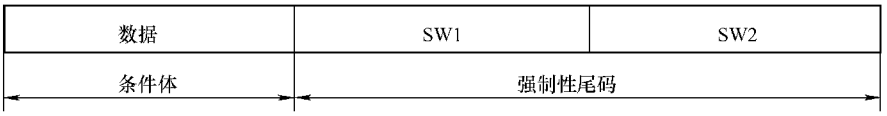


图 2-15　R – APDU 结构

2.5　智能卡文件系统

文件系统是智能卡（CPU 卡）的重要组成部分，负责智能卡内部数据的组织、管理和维护，文件系统的设计与实现随着应用的不同而变化。

2.5.1　文件组织结构

按 ISO/IEC 7816 标准的规定，智能卡中的数据在存储器中以树形文件结构的形式组织存放。文件分成三种层次级别：一是主文件（Master File，MF），形成文件系统的根，类似于 DOS 中的根目录；二是专用文件（Dedicated File，DF），在主文件下，类似于 DOS 中的目录，DF 文件之下的 DF 文件，类似 DOS 的子目录；三是基本文件（Elementary File，EF），用来存储实际应用数据和相应的系统管理信息。智能卡文件的树形结构如图 2-16 所示。

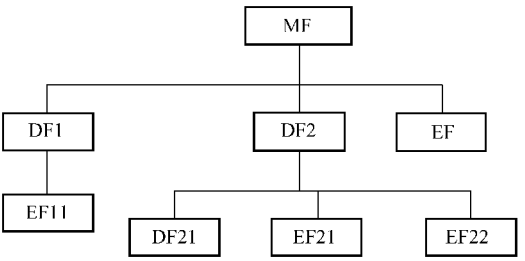


图 2-16　智能卡文件的树形结构

智能卡的文件系统结构中，MF 有且只能有一个；DF 是可选的，这两种文件主要起管理和形成树形文件系统结构的作用，真正存放数据的是 EF。

2.5.2 文件格式

智能卡中的所有文件都是由文件头和文件体组成。文件头包含有文件的格式和结构方面的信息，以及存取的条件；文件体用来存储可变的数据。文件头和文件体总是放在分离的存储器页面。文件格式是在建立文件时唯一确定的。文件格式见表 2-13。

表 2-13 文件格式

文件头 （文件类型，文件标识符，文件大小，权限，校验等）
文件主体

1. 文件类型

文件类型指明了文件的不同种类，见表 2-14。

表 2-14 文件类型

类型字（HEX）	文件描述	文件类型
38	MF 或 DF	
28	二进制文件	透明文件
2A	定长记录文件	定长记录文件
2E	循环文件	循环文件
2F	钱包文件	循环文件
2C	变长记录文件	变长记录文件
3D	私钥文件	透明文件
3E	公钥文件	透明文件
3F	密钥文件（存放密钥和 PIN，不允许外部访问）	变长记录文件

2. 文件标识符

文件标识符（File Identifier，FID）是文件的标识代码，用来唯一标识文件，占 2B。文件类型不同，FID 的编码也不相同，同一目录下的 FID 必须是唯一的，相嵌套的 DF 不能有相同的 FID，EF 不能有与其更高一级或更低一级目录相同的 FID。对 MF，其 FID 为 3F00H。FID 的值 FFFFH 被保留。

3. 短文件标识符

短文件标识符（Short File Identifier，SFI）由 5 个二进制位组成，取值范围为 0 ~ 31。短 FID 仅针对 EF，用于文件的隐含选择。若文件需要用短文件标识符进行选择，则在建立文件时就需将文件标识符取在 1 ~ 31（00000001 ~ 00011111）之间。

2.5.3　文件层次级别

智能卡的文件系统有三种层次级别，分别为主文件（MF）、专用文件（DF）和基本文件（EF）。每一层次级别的文件分不同的种类，具有不同的用途。

1. 主文件（MF）

主文件（MF）是文件系统的根，在智能卡中是唯一的，并且是必须存在的。智能卡复位后将自动选择主文件（MF）为当前文件。主文件（MF）中含有系统文件控制信息及可分配的存储空间，其下可以建立各种文件。主文件（MF）的建立在卡片初始化阶段完成。主文件（MF）的标识符定义为 3F00H。主文件（MF）的文件头定义见表 2-15。

表 2-15　主文件（MF）的文件头定义

文件头	字节/B	描　　述
文件类型	1	“38”
文件标识（FID）	2	“3F 00”
文件大小	2	“FFFF”指自动将 MF 空间建立为最大值
访问权限 1	1	建立权限：在 MF 下建立文件的权限
访问权限 2	1	擦除权限：擦除 MF 下所有文件的权限
保留	1	“FF”
保留	1	“FF”

2. 专用文件（DF）

专用文件（DF）相当于目录文件，其下可以建立各种 DF 和 EF。一般来说，一个 DF 被用来存储某一应用的所有数据，任何一个 DF 在物理上和逻辑上都保持独立，都有自己的安全机制和应用数据。

DF 在用户存储器中占有一块静态存储器，一旦 DF 建立，其存储器的大小就不能变动，但在该 DF 下的 EF 可以重新分配存储器的大小，也可以被删除。DF 下还可以再建立 DF，此时，较高层的专有文件称为父专用文件（Parent – DF），较低层的称为子专用文件（Child – DF）。当 DF 被删除后，其下的子 DF 和 EF 被一并删除。

根据 DF 是否包含子 DF，可以将 DF 分为目录专用文件（Directory Definition

File，DDF）和应用专用文件（Application Definition File，ADF）两种。其中 DDF 包含多个 ADF，而一个 ADF 只代表一个应用；DDF 下可以有多个 EF 和子 DF，而 ADF 下则只能有 EF。

为了标识不同的 DF，每个 DF 具有一个同级 DF 下唯一的文件标识符（File Identity，FID）和一个卡内全局唯一的应用标识符（Application Identity，AID），专用文件（DF）的文件头定义见表 2-16。

表 2-16　专用文件（DF）的文件头定义

文件头	字节/B	描　　述
文件类型	1	“38”
文件标识符（FID）	2	
文件大小	2	表示 DF 文件体大小
访问权限 1	1	建立权限：在 DF 下建立文件的权限
访问权限 2	1	擦除权限：擦除 DF 下所有文件的权限
保留	1	“FF”
保留	1	“FF”

3. 基本文件（EF）

基本文件（EF）是树形文件系统中的叶节点，其下没有任何子节点。EF 是卡内数据的基本载体，用来存放用户数据或密钥。

存放用户数据的 EF 称为工作基本文件（Working Elementary File，WEF），在满足一定条件时可以被读、写、删除等。WEF 按数据结构可分为四类：透明二进制文件、线性定长文件、线性变长文件和循环文件。

存放密钥的文件称为内部保密文件（Internal Secret Files，ISF），密钥包括内部认证密钥、外部认证密钥、口令密码等，可被输入、修改、覆盖，但在任何情况下都不可读出，不能部分删除。每个 MF 或 DF 下有且仅有一个密钥（KEY）文件，在 KEY 文件中可以存放多个密钥，每个密钥为一定长记录，规定了其标识、版本、算法、属性及密钥本身等相关内容。

EF 大小在创建时指定，且仅受存储空间的限制。

（1）透明二进制文件

透明二进制文件是将数据作为一个字节流来进行处理，其文件结构如图 2-17 所示。

图 2-17　透明二进制文件结构

（2）线性定长文件

线性定长文件也称为定长记录文件，由一系列具有相同固定长度的记录序列组成。文件体划分为 n 个等长的区段，每一个区段对应一条数据记录，不同的记录通过记录号来区分。记录只能整条访问，不允许访问记录的部分数据。其文件结构如图 2-18 所示。

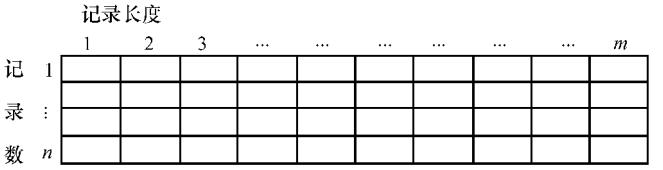


图 2-18　线性定长文件结构

（3）线性变长记录文件

线性变长记录文件以记录为单位进行存储，每个记录的长度都不相同，通过记录号或记录标识符来选择每条记录。变长记录通常以 TLV（Tag – Length – Value）格式存在。其文件结构如图 2-19 所示。

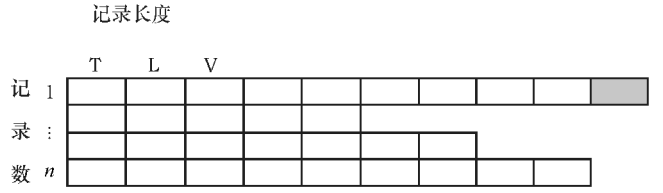


图 2-19　线性变长文件结构

（4）循环定长记录文件

循环文件是由长度相同的记录组成，相当于环形记录队列，遵循先进先出的存储原则。它和线性定长文件的区别是在第一条记录和最后一条记录间有一个链接指针，指针总是指向最后一条写入的记录，该记录总是编号为 1。最后被写入的记录为 1 号，之前刚写入的记录为 2 号，以此类推。记录写满后自动覆盖最早的记录。其文件结构如图 2-20 所示。

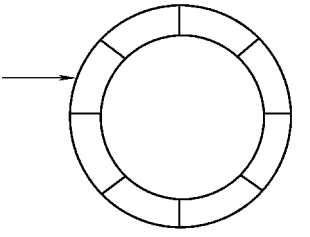


图 2-20　循环定长记录文件结构

此外，EF 还可以按照文件用途来分类，可以分为 DIR 文件、PIN 文件、KEY 文件及应用自定义解释文件等。

2.6 智能卡安全机制

智能卡的安全级别在概念上包括安全状态、安全属性和安全机制。安全状态是指卡在当前所处的一种安全级别；安全属性是对某个文件进行某种操作时必须达到的安全状态，即进行操作所需满足的条件，也称访问权限；安全机制是指从某种安全状态转移到另一种安全状态所采用的方法和手段，这些方法和手段包括数据的加密和解密、鉴别和核实、文件访问的安全控制。数据的加/解密存在于安全体系的整个过程中；鉴别和核实的本质是身份认证；文件访问的安全控制则与文件管理器联系密切。

2.6.1 加密技术

1. 加密算法

智能卡中的加密算法是整个智能卡安全体系的基础，包括对称密钥加密算法和非对称密钥加密算法两种。

对称密钥加密算法也称为私钥加密算法，其加密和解密采用相同的密钥，且该密钥必须保持秘密。对称加密算法的优点是对称加密算法效率高，速度快；缺点是由于加/解密双方都要使用相同的密钥，密钥的分发便成了该加密体系中最薄弱的环节，一旦密钥被破解，整个体系就会崩溃。

常用的对称加密算法有 DES、3DES 及 AES 算法。

DES（Data Encryption Standard，数据加密标准）算法是美国 IBM 公司研制的一种分组密码算法，目前已广泛使用。该算法输入的是 64bit 明文，在 64bit 密钥的控制下产生 64bit 的密文；反之输入 64bit 的密文，输出 64bit 的明文。由于 64bit 的密钥中含有 8bit 的奇偶校验位，所以实际有效密钥长度为 56bit。

3DES 是 DES 算法扩展其密钥长度的一种方法，可使加密密钥长度扩展到 128bit（112bit 有效）或 192bit（168bit 有效）。明文长度依然是 64bit，其基本原理是将 128bit 的密钥分为两组 64bit，对明文多次进行普通的 DES 加/解密操作，从而增强加密强度。

AES（Advanced Encryption Standard，高级加密标准）是 2001 年 NIST（美国国家标准与技术研究院）宣布的 DES 后继算法，明文长度为 128bit，可以用长为 128bit、192bit 或 256bit 的密钥加密。

非对称密钥加密算法也称为公钥加密算法，要求每个参与方拥有一对密钥、一个公钥（Public Key）和一个私钥（Private Key）。用公钥加密的密文只能用私钥解密，用私钥加密的密文只能用公钥解密。在操作过程中，公钥是公开的，私钥是秘密的。如果 A 要发一份秘密信息给 B，则 A 只需要得到 B 的公钥，用 B 的公钥加

密秘密信息，此加密的信息只能用 B 保密的私钥进行解密。反之，B 也可以用 A 的公钥加密保密信息给 A。信息在传送过程中，即使被第三方截取，也不可能解密其内容。非对称加密算法的加/解密速度比对称加密算法要慢，但它适合于保密通信、密钥分配和鉴别，成功解决了网络环境下的身份鉴别、数字签名等问题。典型的非对称密钥加密算法有 RSA 算法、ECC（Elliptic Curve Cryptosystem，椭圆曲线密码系统）等。

2. 密钥管理

加密算法的核心是对密钥的管理。对密钥的管理可采用分级管理。通常采用主控密钥、子密钥和会话密钥三级管理，如图 2-21 所示。

图 2-21　密钥三级管理

在智能卡和终端设备中存放着相同的主控密钥（假设为对称密钥体系），主控密钥可以是一个或多个。通常在专用文件（DF）下都包含一个主控密钥，主控密钥是整个 DF 下密钥体系的基础，只有通过主控密钥的验证，才能对该 DF 下的子文件做进一步的操作。主控密钥可由几个相互信任的人独立给出数据组合成一个密钥，然后用该密钥对随机数做加密运算而获得，这样获得的主控密钥很难预先估计。

子密钥是通过主密钥对某些指定的数据加密后生成的。一般每张卡片内置了制造商标识码、卡的序列号或应用序列号等，其中卡的序列号或应用序列号是各不相同的，因此可利用序列号进行加密生成子密钥，这样即使主控密钥相同，各卡的子密钥也是互不相同的。

会话密钥是利用子密钥对可变数据进行加密，加密的结果即为会话密钥（或过程密钥）。如 IC 卡和终端设备间传送的数据就是用会话密钥加密的。一个会话密钥仅使用一次。为保证会话密钥的不同，通常采用子密钥对交易时间或命令计数器进行加密生成会话密钥，这样即使是同一张卡，每次使用时其会话密钥都不同。

2.6.2　认证

认证是指对智能卡或读写设备的合法性进行验证，即是如何判定一张智能卡或读写设备不是伪造的卡或读写设备的问题。认证包括内部认证和外部认证。内部认证是指读写设备验证智能卡的合法性，判断智能卡是否为伪造的卡；外部认证是智能卡验证读写设备的合法性，判断读写设备是否为伪造的。

1. 内部认证

内部认证的流程如下（见图 2 – 22）：

1）读写器将生成的随机数 N 送给智能卡，同时向卡发内部认证（Internal Authentication）指令。

2）卡对随机数 N 加密成密文 M 送读写器（密钥已存在卡和读写器中）。

3）读写器将 M 解密成明文 N_1。

4）比较 N_1 和原随机数 N，相同则读写器判断卡是真的。

2. 外部认证

外部认证的流程如下（见图 2-23）：

1）读写器发送“生成随机数”指令给智能卡。

2）卡产生的随机数 N 回送给读写器。

3）读写器对随机数进行加密生成密文 M（密钥已存在卡和读写器中）。

4）读写器向卡发外部认证（External Authentication）指令，并将密文 M 送卡。

5）卡将密文 M 解密成明文 N_1，并将明文 N_1 和原随机数 N 比较，相同则卡判断读写器是真的。

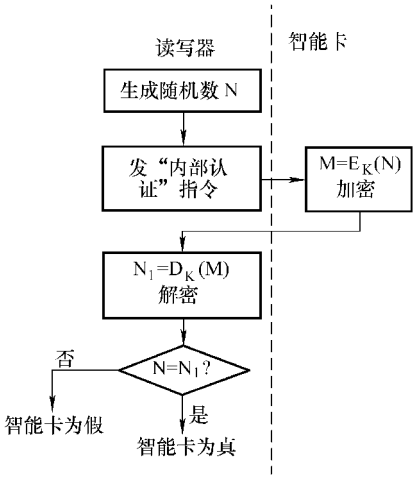


图 2-22　内部认证

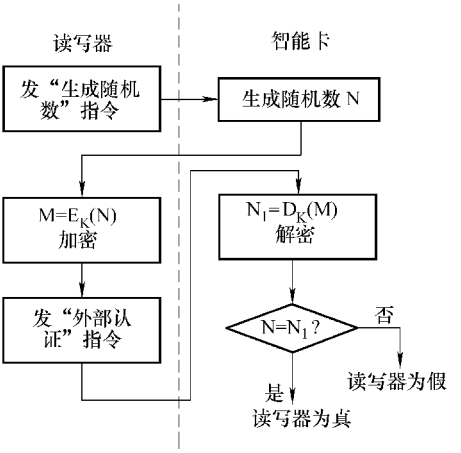


图 2-23　外部认证

认证还可以根据密钥的类型不同分为对称算法认证和非对称算法认证，认证所需要的数据一般由双方共同随机产生并共享。

第 3 章　智能卡表的安全性分析

由于用户的结算信息和公用仪表的计量信息都是通过用户手中的 IC 卡进行传输的，用户的分布又是一个十分复杂、分散的群体，因此如何保证用户卡中传递信息的安全性已经变成一个十分重要的问题。这个问题解决得好坏，将直接影响 IC 卡表以及预付费管理系统的推广使用。本章主要分析了针对 IC 卡和卡表的数据攻击手段，给出了 IC 卡表数据存储和数据交换的安全性策略及安全性工具。

3.1　智能卡表的安全性内容

在智能卡表和预付费管理系统之间，信息的传递是通过 IC 卡作为传输介质进行的，安全性的主要内容是如何保证 IC 卡中信息的安全性，与此相关，还要保证不能用非法的手段获得或者修改智能卡表中的数据信息。

对 IC 卡和智能卡表中的信息安全性保护主要体现在对数据信息进行非法攻击的防护上，常用的攻击行为有以下几种。

1. 截取信道中的信息

通过非法设备以及相关技术手段读取 IC 卡中存储的数据信息以及在 IC 卡与智能卡表进行操作时截取数据交换信息，如图 3-1 所示。

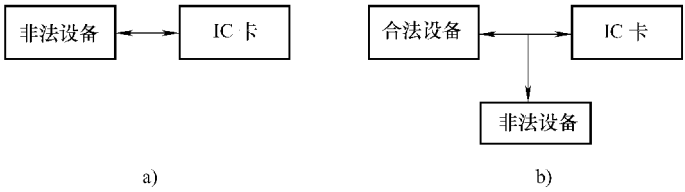


图 3-1　非法获取数据

图 3-1a 所示为非法设备直接从 IC 卡读取数据信息，图 3-1b 所示为非法设备在 IC 卡与合法设备进行数据交换时对数据信息进行截获。这两种攻击方式是不可控制的，并且也是最常用的攻击方式。

2. 破译 IC 卡中的信息

攻击者在采用上述两种方式截获数据信息后，根据 IC 卡中数据信息的变化情况以及数据交换过程中数据流的变化，对数据进行分析，从而确认 IC 卡中所有数

据的含义以及数据流的变化规则，完成对 IC 卡以及智能卡表中数据信息的破译，进而达到非法改变数据信息的目的。

3. 复现 IC 卡中的数据信息

攻击者在截获数据信息后，并不对数据进行分析破译，而是记录在特定操作中数据流的变化情况，在需要时，将记录的数据流直接复制发送到 IC 卡或智能卡表，从而达到非法改变数据信息的目的。这种情况经常发生在当 IC 卡与智能卡表之间进行数据交换采用加密处理的时候。

在上述所描述的攻击方法中，第一种方式是手段，由于 IC 卡和智能卡表全部由用户掌握和使用，管理方无法实现实时跟踪，因此在现实中是无法阻止攻击者进行这种尝试的。第二、三种方式是数据分析处理，是攻击的目的所在。如果对 IC 卡与智能卡表之间的数据未进行安全保护处理或者采用较为简单的安全保护，攻击是非常容易达到效果的。为此在设计智能卡表及其相关管理系统时，必须对数据的安全性给予高度的重视，从某种角度来说，一个智能卡表及系统设计是否成功，关键在于其对数据安全性的处理。

3.2 智能卡表及数据存储的安全性分析

由于在智能卡表及系统中，IC 卡是数据存储和传递的载体，因此 IC 卡的数据存储安全性是需要着重予以考虑的。

在智能卡表及系统中所使用的都是集成电路卡（IC 卡）（从数据容量和安全性的角度以及读写设备的成本考虑，没有使用磁条卡作为信息载体的，因此磁卡表的名称是不准确的）。集成电路卡的核心是采用集成电路芯片来进行数据的存储。目前广泛使用的 IC 卡采用电可擦除数据存储器（EEPROM），这种芯片读写速度快，掉电后数据可以长期保存，并且数据可以反复进行擦写。应该说，正是由于 EEPROM 芯片的出现才带来了 IC 卡技术的广泛应用。

IC 卡根据对 EEPROM 读写处理方式的不同，可以分为存储卡、逻辑加密卡以及智能卡（CPU 卡）三大类，它们具有不同的数据保护安全级别。

1. 存储卡数据保护

存储卡是直接将 EEPROM 芯片封装在卡片上，外部设备可以直接访问到 EEPROM 中的任何一个单元，如图 3-2 所示。

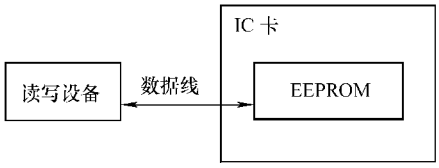


图 3-2 存储卡数据保护

由于存储卡中只有 EEPROM 一个芯片，因此 IC 卡的对外接口实际上就是 EEPROM 的对外接口，这样外部读写设备就可以十分方便地对 EEPROM 进行数据

读写操作，对 IC 卡而言，无法对合法或非法的读写设备进行判断和识别，非常容易进行攻击。存储卡只是用来对数据进行存储，而无法对数据进行安全性保护，因此存储卡不具备数据安全性保护措施，数据安全级别很低。

2. 逻辑加密卡数据保护

逻辑加密卡是在将 EEPROM 芯片封装在卡片上的同时，将一组硬件逻辑电路也封装在卡片上，外部读写设备必须通过硬件逻辑电路的判断后才能访问到 EEPROM 中的任何一个单元，如图 3-3 所示。

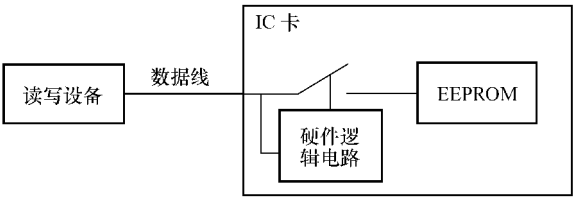


图 3-3　逻辑加密卡数据保护

由于在 IC 卡中存在一组硬件逻辑电路，EEPROM 芯片的接口并不直接对外，在初始状态 IC 卡芯片中的数据开关处于断开状态。外部读写设备在访问 IC 卡芯片中的 EEPROM 单元之前，必须首先发一组数据给硬件逻辑电路，硬件逻辑电路在判断数据的合法性后（即密码校验），才决定是否将 IC 卡内的开关闭合。只有密码校验正确后，硬件逻辑电路才能将开关闭合，这时外部读写设备才能对 EEPROM 中的数据进行读写操作，这样逻辑加密卡就可以对外部合法和非法的读写设备进行识别判断。通过这种方式，逻辑加密卡对内部 EEPROM 中的数据进行了安全性保护，因此逻辑加密卡具备数据安全性保护措施。

但逻辑加密卡的安全性级别并不是很高，有两种攻击方式可以对其进行攻击测试，一种是当合法读写设备在发送数据进行密码校验时，非法设备可以跟踪到校验密码，这样今后非法设备通过重放也可以通过密码校验，从而对逻辑加密卡进行数据攻击；另一种方法是非法设备在跟踪到合法设备已经通过逻辑加密卡的密码校验，IC 卡内部开关闭合后，再通过数据线对逻辑加密卡中 EEPROM 的数据进行攻击破坏。因此逻辑加密卡虽然具备一定的数据安全性保护，但它的安全级别依然较低，具备一定的手段仍然是可以攻破的。

造成这种情况出现的原因是因为逻辑加密卡中的安全性是依赖一组硬件逻辑电路，这种电路只有判断能力，但不具备分析处理能力，因此不能及时发现和处理变化的环境。

3. 智能卡（CPU 卡）数据保护

智能卡是在将 EEPROM 芯片封装在卡片上的同时，将微处理器（CPU）芯片也封装在卡片上，外部读写设备只能通过 CPU 与 IC 卡内的 EEPROM 进行数据交换，在任何情况下都不能再访问到 EEPROM 中的任何一个单元，如图 3-4 所示。

由于在智能卡中封装了微处理器（CPU）芯片，这样 EEPROM 的数据接口在任何情况下都不会与 IC 卡的对外数据线相连接。外部读写设备在与智能卡进行数

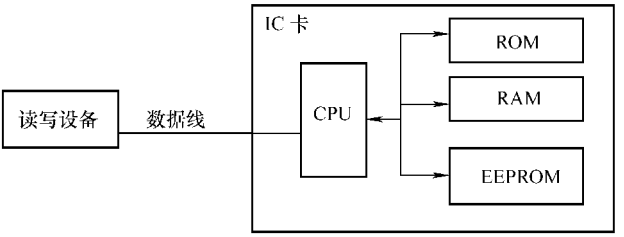


图 3-4　智能卡数据保护

据交换时，首先必须发指令给 CPU，由 CPU 根据其内部 ROM 中存储的卡片操作系统（COS）对指令进行解释，并进行分析判断，在确认读写设备的合法性后，允许外部读写设备与智能卡建立连接。之后的数据操作仍然要由外部读写设备发出相应的指令，并且 CPU 对指令进行正确解释后，允许外部读写设备和智能卡中的数据存储区 RAM 进行数据交换，数据交换成功后，在 CPU 的控制下，利用智能卡中的内部数据总线，再将内部 RAM 中的数据与 EEPROM 中的数据进行交换。可以看到，在数据处理过程中，外部读写设备只是与 CPU “打交道”，同时数据交换也只能与数据存储区 RAM 进行，根本无法实现对智能卡中 EEPROM 数据的直接访问。这就实现了对智能卡 EEPROM 中数据的安全保护，因此智能卡也具备数据安全性保护措施。

与逻辑加密卡相比，由于智能卡内部具有 CPU 芯片，在具有数据判断能力的同时，也具备了数据分析处理能力，因此智能卡可以随时区别合法和非法读写设备，并且由于有了 CPU 芯片，具备数据运算能力，还可以对数据进行加密解密处理，因此具备非常高的安全性，其安全级别很高。

从对攻击方式的分析可以看到，保证 IC 卡内数据的安全性是最基本的要求，如果非法设备可以容易地与 IC 卡进行数据信息交换，进而进行分析处理，智能卡表及系统就不再具备任何安全性。因此提高 IC 卡的安全性是设计好的智能卡表及系统的关键。

根据上面的分析，如果智能卡表及系统对数据的安全性非常重视，应该选用安全级别高的 IC 卡，从发展趋势看，应尽量选用智能卡作为智能卡表信息传递的介质。

在设计实际的智能卡表系统时，安全性的指标也是相对而言的。如果设计的是单机版的物业小区管理系统，对安全性的要求不高，为简化设计和降低成本，可以选用逻辑加密卡或存储卡；但如果是行业管理部门或在大中城市推广智能卡管理系统，数据的安全性将是一个非常重要的指标，这时应该首先选择智能卡作为管理系统的数据信息载体。

3.3　智能卡表及数据交换的安全性分析

根据上面的分析，在智能卡表及系统中选择使用智能卡可以有效保证数据存储的安全性，但即使这样也只是阻止非法读写设备直接对 IC 卡中数据的操作，并不能保证在 IC 卡与智能卡表或合法读写器之间进行数据交换时不被非法设备跟踪破译，要解决这种类型的非法攻击，还需要采用安全认证以及对数据在传输时进行线路保护处理。

3.3.1　安全认证

安全认证用来在读写设备（包括智能卡表）与 IC 卡进行数据交换之前，首先进行必要的安全认证，用来确认双方身份的合法性。只有双方身份确认后，才能建立相互之间联系的通道进行必要的数据交换。如果双方不能确认身份的合法性，则不能建立进行数据交换的通道。

安全认证有两种方式可以实现，一是通过密码进行安全认证；二是通过密钥进行安全认证。

1. 密码认证

密码认证的过程如图 3-5 所示。IC 卡在进行密码比较时，如果读写设备发来的密码与 IC 卡中存储的密码相同，IC 卡向读写设备返回密码认证通过的结果，并打开 IC 卡数据与外部进行交换的权限。如果密码不同，则返回错误结果，IC 卡数据与外部进行交换的权限被关闭。

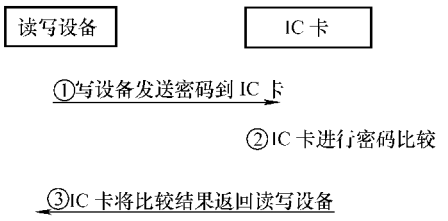


图 3-5　密码认证过程

在逻辑加密卡中使用的就是这种认证方式，同时智能卡中的口令密钥认证也是采用这种方式进行的。密码认证的方式比较简单实用，是一种常用的安全认证手段。其最大的缺陷在于进行认证的密码在线路上进行了传输，如果非法设备跟踪到密码认证的第一步，就比较容易破译整个密码认证过程，这样非法设备也能够正确地与 IC 卡进行密码认证，从而能够非法与 IC 卡进行数据交换，而这个过程是无法阻止的。

2. 密钥认证

密钥认证的过程如图 3-6 所示。与密码认证过程相比，密钥认证增加了两个内容，一是引入了密钥的概念，增加了加密运算过程；二是增加了产生随机数的过程，有了这两个过程，就可以有效地保证密钥认证过程被非法跟踪后，仍然能够保证认证过程的安全性。

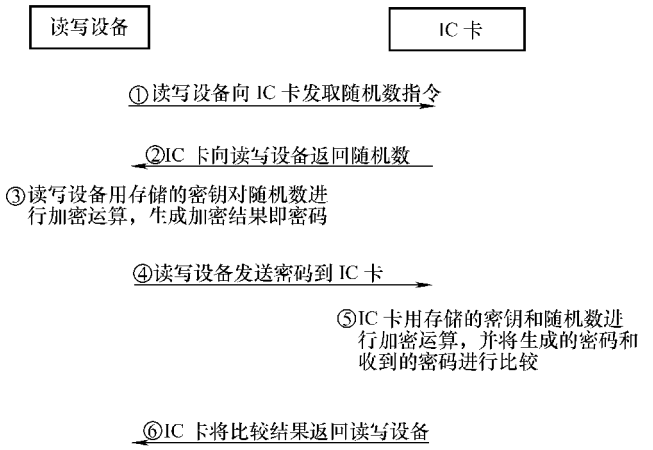


图 3-6　密钥认证过程

密钥是事先设置到读写设备和 IC 卡中的，它在认证过程中只参与运算，但不在线路中进行传输，这样非法跟踪是不可能截获到密钥的；由于有随机数的概念，这样每次进行密钥认证虽然使用的是相同的密钥，但经过加密运算产生的密码也是随机的，无规律可循的，这样非法跟踪截获到的密码无法在下次进行认证时使用，只要不知道密钥，非法设备就无法再向密码认证那样模拟安全认证的过程，也就不能非法与 IC 卡进行数据交换。

在这里值得特别指出的是加密运算过程也是保证密钥认证安全性的一个非常重要的环节，加密运算的算法必须满足下面的条件：

1）已知加密因子和密钥可以计算出加密结果，即数据加密运算。

2）已知加密结果和密钥可以推出加密因子，即数据解密运算。

3）已知加密因子和加密结果不可以推出密钥。

4）加密算法应该是公开的算法。

这样的加密算法就可以有效地保证密钥的安全性。同时需要特别指出的是在智能卡表及系统中采用的算法一定应该是国际上公认的具备上述特征的算法，只有采用这样的算法，才能够有效保证安全性，同时也能使智能卡表及系统具有兼容性和互换性。目前有些厂家采用自己编制的算法进行密钥安全认证存在两大隐患：一是算法未经过权威部门认证，算法的安全级别实际上很低，其安全性完全取决于算法不公开，但即使不公开的算法也很容易被非法攻击攻破，因为厂家的技术人员往往只是表计设计专家，而不是密码安全算法专家，而进行非法攻击的人员却往往是密码算法专家；二是由于安全原因算法不公开，系统的安全性就永远与厂家的人员有关，而真正关心系统运行安全的行业管理部门却不能掌握核心安全，同时也无法实现在系统中使用多家的智能卡表，从而对产品招标选型带来不方便，在某种程度

上，不安全的算法可能反而保护了产品性能并不高的厂家，因为即使发现智能卡表产品有性能缺陷，使用者却由于安全算法的原因不能更换更好厂家的产品。

目前国际上公认的加密算法主要分为两大类型：一种是对称加密算法，这种算法的加密密钥和解密密钥是相同的，代表性的算法有 DES 算法和 3DES 算法；另一种算法是非对称算法，这种算法的加密密钥和解密密钥是不相同的，代表性的算法有 RSA 算法。从安全性的角度来讲，不对称算法的安全性更高，但计算过程也更复杂，一般都应用在需要对身份进行合法性认证、防伪认证等场合；对称性算法也具有很高的安全性，算法相对比较简单使用，目前金融应用、公用事业应用基本上都采用对称算法。

在智能卡表应用中，如果是非金融的单机系统，采用 DES 算法比较适宜；如果考虑和金融系统联网收费，则应满足银行规范使用 3DES 算法。

3.3.2　数据的线路保护

线路保护是指读写设备和 IC 卡通过安全认证后进行数据交换传输时，要保证数据在线路上被非法设备截获后不能被破译、篡改和重放复现。数据的线路保护分为两个层面：一是数据的机密性保护；二是数据的完整性保护。

数据的机密性保护是指对要传输的数据用密钥进行加密处理后再进行传输。这样在线路中传输的数据为密文数据，非法设备截获后无法进行数据破译和分析，接收方收到密文数据后再用解密密钥进行解密重新得到明文数据。

数据的完整性保护是指在要传输的数据后面附加校验码字节，发送方将发送数据与线路保护密钥以及随机数进行运算，生成校验码后进行数据传输，接收方接收到数据后用相同的密钥对接收到的数据重新计算校验码并与接收到的校验码进行比较，相同则接收数据有效，否则数据无效。由于密钥不在线路上传输，这样非法设备截获数据后如果对数据进行篡改，必然会导致校验码不正确，接收方就能够拒绝接收错误数据。

由于校验码在运算过程中也有随机数参与运算，因此即使采用相同的密钥，将相同的数据进行多次传输，每次形成的校验码也是各不相同的，这样非法设备即使截获了某一次的合理数据，也不能再进行二次传输，这就有效避免了非法设备对数据进行重放复现。

综合运用上述两种方法，就可以有效地保证数据在传输过程中的安全性，也就最终实现了在公开的传输介质或信道上，采用公开的加密算法进行数据传输，保证数据是有效的、正确的、安全的。也就是说，数据传输的安全性不是依靠传输信道的封闭性、加密算法的不公开性来保证的。因此，在智能卡表及系统中要具备高的数据安全性，一是要采用安全级别高的 IC 卡即智能卡（CPU 卡）作为传输介质，二是利用密钥和相应的加密算法进行数据的安全认证和有效传输。

3.4 智能卡表中的安全性工具

根据上面的论述，智能卡表在广义上也是一种 IC 卡读写设备，要保证智能卡表以及所使用 IC 卡中数据的安全性，除了使用智能卡外，必须实现智能卡表和智能卡之间能够进行数据的安全认证和线路保护处理，也就是要求智能卡表必须具有存储密钥以及进行加密运算的能力。

1. 普通卡表的逻辑组成

普通卡表的逻辑组成如图 3-7 所示。

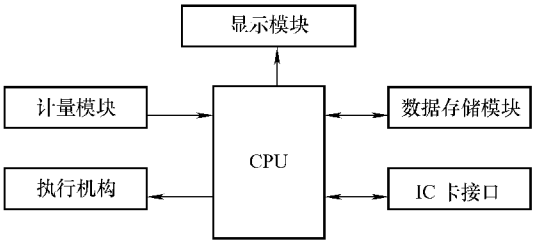


图 3-7 普通卡表的逻辑组成

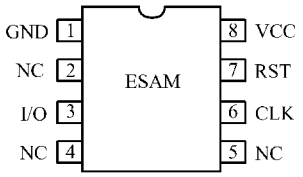
卡表中的核心器件是微处理器（CPU），通过编制合理的程序，CPU 可以对计量数据进行计算、存储、显示、与 IC 卡进行数据交换以及对相关数据进行分析判断控制执行机构。因此 CPU 的主要作用是完成卡表的数据处理流程以及实现设计好的功能。

从安全性的角度来讲，智能卡表除了要完成上述内容以外，还要完成密钥存储和加密运算功能，这样就产生了一个不可调和的矛盾。

由于 CPU 中的程序是需要生产厂家（或第三方）的设计人员进行设计的，这部分程序的功能和处理流程可以是由智能卡表使用方提出需求而委托设计的，需求本身也是公开的。但如果要在 CPU 的控制下存储密钥和进行加密运算，出于安全性的考虑，密钥值应该是不公开的，因此这部分程序编制是不能委托开发设计的，必须掌握在智能卡表使用方手里。换言之，智能卡表的功能、数据操作流程和数据的安全性是两个不同的概念，应该由不同的功能模块去完成。解决这个问题最好的方案就是在智能卡表中增加嵌入式安全控制模块（Embedded SAM，ESAM）。

2. ESAM

ESAM 为 8 脚 DIP 封装，如图 3-8 所示。具体引脚定义为 1—地；3—数据端；6—时钟端；7—复位端；8—电源端；2、4、5—空闲。ESAM 的时钟频率可在 1 ~ 5MHz 之间选择。



GND	地	VCC	电压
NC	空	RST	复位
I/O	输入 / 输出	CLK	时钟
NC	空	NC	空

图 3-8　ESAM 引脚及定义

3. 增加了 ESAM 的智能卡表逻辑组成

增加了 ESAM 的智能卡表逻辑组成如图 3-9 所示。

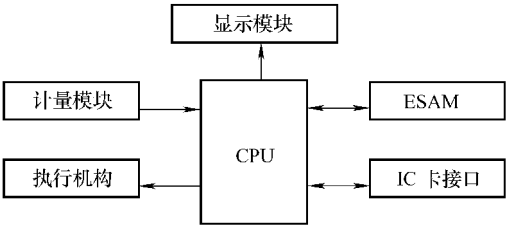


图 3-9　增加了 ESAM 的智能卡表逻辑组成

与普通卡表相比，增加了 ESAM 的智能卡表只是将数据存储模块换成 ESAM，这样智能卡表中的 CPU 还是完成原来普通卡表的功能，程序也完全可以由生产厂家（或第三方）根据用户需求进行灵活编制，当需要进行数据交换时，由 CPU 启动 ESAM 与智能卡完成安全认证以及数据保护工作，密钥和智能卡表数据都保存在 ESAM 中。ESAM 可以由智能卡表的使用方发行，安装在智能卡表中即可，这样密钥和算法的安全性和 CPU 程序就可以完全分开，整个智能卡表及系统的安全性就全部由使用方掌握。同时使用方没有由于安全的原因限制生产方灵活设计不同功能的智能卡表，厂家可以随时对智能卡表中的程序进行修改和升级而不影响使用方的数据安全性。

从技术发展的角度来看，由于半导体芯片技术的发展，CPU 芯片升级速度很快，新的 CPU 芯片不断出现，芯片的价格也在不断调整，生产厂家必然要使用性能价格比最高的芯片，如果将数据安全性的实现和 CPU 芯片联系在一起，一旦一个系统使用后，即使有更好的芯片出现，出于安全性的考虑，也无法再对 CPU 以及程序进行调整，也不利于新技术的推广使用。如果使用 ESAM，这个问题也可以得到解决。

综合上面的因素，在智能卡表中使用 ESAM 技术可以实现智能卡表数据流程和数据安全的分离，便于实现产品的兼容和升级，可以不断推动技术进步，是规范智能卡表技术发展的有效技术手段。

3.5　卡表终端 ESAM 检测方法

3.5.1　卡表终端与用户卡数据交换流程

可以把卡表终端与用户卡的数据交换过程划分为三个阶段，即安全认证阶段、消费交易阶段和数据返写阶段，如图 3-10 所示。

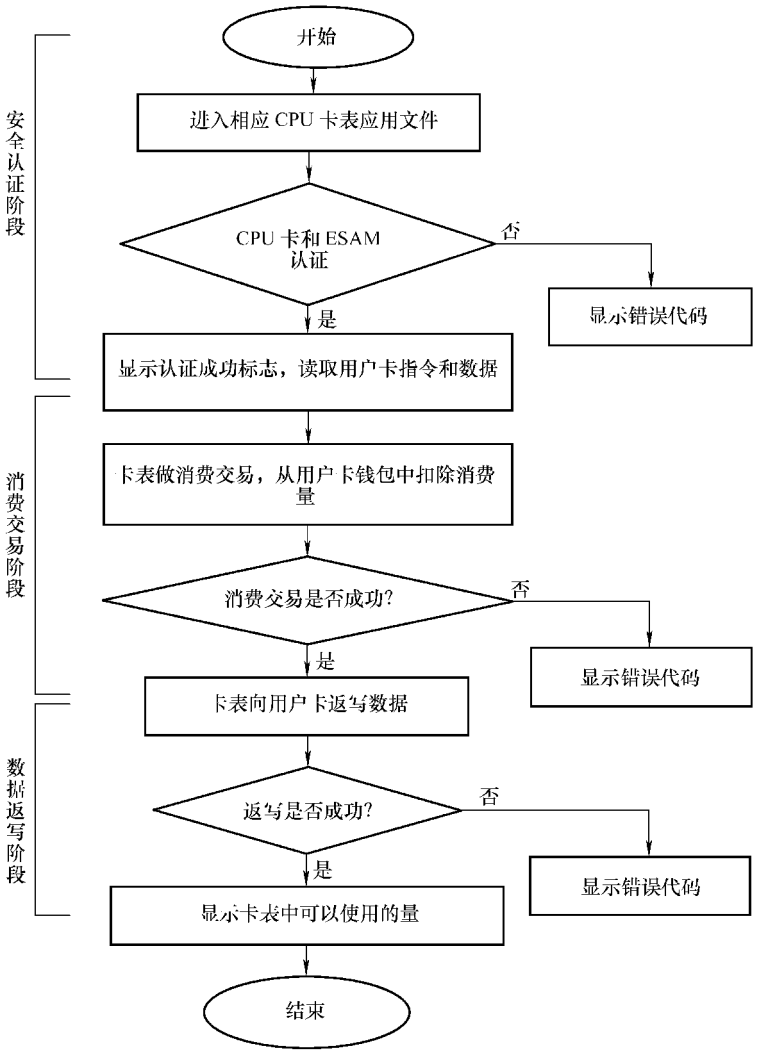


图 3-10　卡表终端与用户卡数据交换过程

从这三个阶段来看，对数据安全性要求最高的是安全认证阶段和消费交易阶段。安全认证阶段主要是卡表终端来判断用户卡和 ESAM 是否具有合法性，与数据交换过程无关，只与安装在用户卡和 ESAM 中的密钥值和安全认证流程有关，并且认证过程对所有的卡表终端来讲是完全相同的。消费交易阶段主要是用来将用户卡中的消费量追加到卡表终端中，是数据交换的核心，该阶段涉及交换的数据以及进行数据交换所需要的密钥，交易内容和流程随着卡表终端的不同会发生变化，不容易硬性规定相同的交易流程，但可以建议尽量参考中国人民银行金融规范中的电子钱包消费交易进行。数据返写阶段主要是将卡表终端中的相关数据返写到用户卡上，通过用户卡将这些数据返回到收费管理系统，以便进行结算和监控，这部分数据的格式定义与操作流程不同的卡表终端完全不同，无法形成统一的规定。

3.5.2　卡表终端检测方法

基于以上分析，为了保证使用卡表终端数据交换的安全性，有必要对卡表终端的数据交换过程进行规范，但不能将卡表终端所有的数据交换流程都列入规范内容，这样存在以下问题：

如果对所有的数据交换流程进行规范，虽然可以保证数据的安全性，但卡表终端的所有数据交换流程全部被统一定义，由于卡表终端的种类和使用场合有很大的变化，这样对数据规范的包容性要求会很高，对规范的技术要求难度很大；并且即使定义出一个目前比较满意的规范，但卡表终端的应用需求和技术是在不断进步的，在不长的时间内就需要对规范进行修订，使得规范在一定的时间内不具备稳定性。在对数据流程进行规范的同时，也需要考虑对与数据交换有关的安全认证过程进行规范，这就不可避免地涉及有关认证密钥的管理和发行，如果对所有与数据交换有关的密钥都进行统一管理和发行，会使密钥系统的发行环节非常复杂，导致卡表终端生产厂家和运行商都不对系统安全性承担责任，造成混乱。

因此，在制订卡表终端检测办法时，必须在考虑规范卡表终端设备安全性的同时，兼顾考虑实施过程的可操作性以及卡表终端应用需求的灵活性。确定卡表终端检测方法的原则是，为保证卡表终端数据交换的安全性，要求卡表终端生产厂家尽量使用 CPU 智能卡，并在卡表终端内安装 ESAM。

在对卡表终端进行检测时，只对用户卡与卡表终端进行数据交换的第一个过程即安全认证过程进行测试，安全认证过程能够通过，证明卡表终端使用了 CPU 智能卡和 ESAM，具备了进行数据交换安全性的基础，但不意味着受检测的卡表终端已经具备了较高的数据安全性。也就是说，卡表终端的检测是规范和引导行业以及卡表终端生产厂家使用具有较高安全性的硬件平台，在这个平台下如何设计安全的系统和卡表终端设备则由行业管理部门和卡表终端生产厂家自行设计，并对所设计的系统及设备的安全性负责。为保证下传安全认证密钥的安全性，需要在 ESAM 中

预先安装默认的传输密钥，该密钥由建设事业 IC 卡密钥管理系统生成并进行控制，所以卡表终端生产厂家所使用的 CPU 智能卡和 ESAM 必须由建设部主管部门指定认可的卡片商或 ESAM 供应商提供，而不能由卡表终端生产厂家随意采购。

3.5.3 卡表终端检测安全认证流程

用检测卡对卡表终端检测流程如图 3-11 所示。

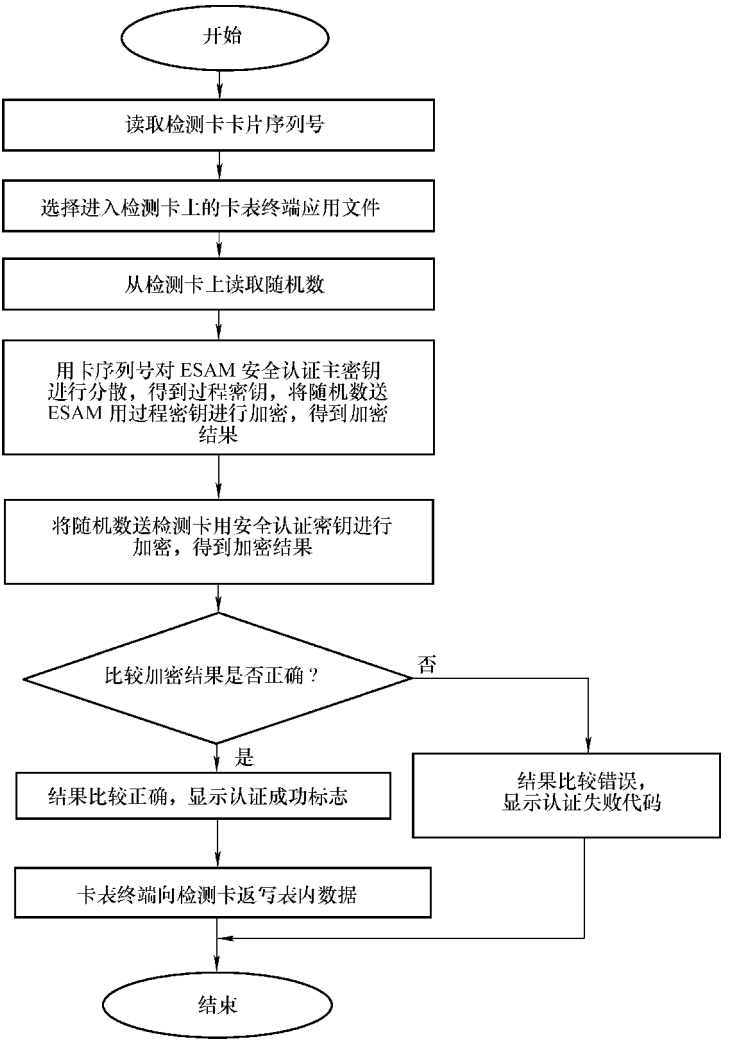


图 3-11 卡表终端检测流程

安全认证成功与失败必须在卡表终端上有明确的提示，卡表终端生产厂家可以

根据实际情况用能够表达两种不同状态的文字或图形在卡表终端的显示部分给予指示，不允许只指示其中一种状态。

采用上面所论述的方法，在卡表终端中使用 ESAM 安全模块和 CPU 智能卡技术，可以使卡表终端的数据安全性得到充分的保证；使用主密钥卡发行传输安全认证的方式可以有效地对卡表终端生产厂家进行有效的管理。综合使用上面的技术方法和技术管理手段，可以使得在行业内将卡表终端的使用和管理达到一个更加安全和规范的层次。

第 4 章　智能卡电表

智能卡（IC 卡）电表是在电能计量仪表中加入 IC 卡及负荷开关控制等功能模块，用以完成电量抄收和电量结算的新型电表。由于使用 IC 卡电表能省去人工抄表过程，提高了工作效率，得到了广泛使用。本章给出了智能卡电表的系统设计规范，阐述了 IC 卡电表收费管理系统的构成和设计要求，介绍了智能卡电表和电卡设计，提出了电卡的密钥安全体系、智能卡电表及电卡的接口规范及电卡与卡表间的安全认证流程。

4.1　智能卡电表系统规范要求

4.1.1　制定统一的智能卡电表技术规范

在 IC 卡电表的设计过程中，需要有一个设计规范用来描述 IC 卡电表的功能，IC 卡电表中的数据项定义、IC 卡电表和 CPU 卡进行数据交换的流程以及 CPU 卡和收费管理系统进行数据交换的流程。不同的生产厂家由于掌握的需求不一样，所制定的设计规范也是不同的，这样就导致电力公司安装的不同生产厂家的 IC 卡电表功能以及数据交换协议是互不相同的。

同时，由于市场需求的不断变化以及新的设计技术不断应用，即使是同一个生产厂家在不同时期制定的设计规范也有可能是不相同的，从而导致电力公司在不同时期安装的同一家 IC 卡电表生产厂家的电表功能和数据交换协议也有可能互不相同。

上述问题如果是在独立的物业小区安装和使用 IC 卡电表，同时物业小区有单机运行的购电管理软件的情况下是不存在，但如果是数量群体较大的用户使用并要求统一由电力公司进行收费管理时就会出现较大的障碍，主要表现在以下几个方面：

1）从电力公司的角度考虑，一旦为居民用户安装了 IC 卡电表，在其使用周期内，应该尽量不再对用户使用的 IC 卡电表进行更换和升级，否则将导致电力公司的生产运营成本增加，这就要求电力公司使用的 IC 卡电表功能和数据交换协议必须在较长时间内保持稳定，而 IC 卡电表生产厂家是不能保证这一点的，需要电力公司有一个统一的技术规范。

2）由于电力公司对 IC 卡电表的需求量较大，一家 IC 卡电表生产厂家所提供

的 IC 卡电表数量不能够完全满足电力公司的需要，因此会出现多家 IC 卡电表生产厂家向电力公司供表的情况，如果各家的设计规范不一致，电力公司就需要根据各个厂家的情况为居民用户发行设计规范不同的 CPU 用户卡，同时要求收费管理系统能够和各家的 CPU 卡设计规范都能够实现兼容，这样就会使得收费管理系统设计非常复杂庞大，并且对使用人员的要求较高，容易出现混乱。同时在 IC 卡电表的安装运行过程中，可能会出现有的 IC 卡电表生产厂家由于各种原因退出，以及新的 IC 卡电表生产厂家继续为电力公司提供 IC 卡电表的情况，这时会要求收费管理系统不仅要保留已退出的生产厂家设计规范，还要再添加新的生产厂家设计规范的情况，这就很难保证收费管理系统运行的稳定性，同时电力公司还必须专门安排人力、财力不断对变化的收费管理系统进行修改维护。

3）现场运行的 IC 卡电表由于各种原因总会出现更换、维修等情况，由于 IC 卡电表的种类多，维修人员在修理时必须首先确定是哪一个生产厂家的电表，再准备好该生产厂家的备件以及操作规范才能进行处理，这样一方面增加了维修人员的工作难度，同时容易造成维修服务效率低而引起用户投诉。

综合上面各种因素，制定统一的 IC 卡电表技术规范，并要求参与该项目的各方提供的产品和系统都必须满足规范要求，通过技术测试验收后才能够提供产品和系统是十分必要的。

4.1.2　统一设计收费管理系统

单机运行收费管理系统是由 IC 卡电表生产厂家根据自己的设计规范独立进行编程设计维护。但城市级的网络收费管理系统还采用这种方式运行是存在问题的：

1）IC 卡生产厂家设计人员的重点主要集中在相关表计产品设计上，对大型数据库系统、网络编程等技术的掌握上能力相对不足，这样设计的收费管理系统可能会存在技术缺陷，从而对系统的稳定运行带来障碍。

2）如果委托开发的 IC 卡生产厂家由于各种原因退出 IC 卡电表产品的供应，收费管理系统就会出现无人维护的情况，使得今后电力公司系统运行的风险性大为增加；即使没有发生这种情况，由于 IC 卡生产厂家表计产品的提供范围非常广，其软件人员精力分散，当系统需要维护时，也不能保证及时提供服务。

3）收费管理系统的设计会涉及整个系统数据安全的部分功能，这部分功能设计如果由生产厂家掌握，会导致对运行的 IC 卡电表维护以及购电安全存在安全隐患，生产厂家可能会不通过电力公司就能够对现场的 IC 卡电表进行处理，并能够对收费管理系统的数据进行人为修改保持一致，从而造成数据不安全，也会导致生产厂家之间的不公平竞争。

4）银行和专业的系统集成商一方面具有专业收费管理系统设计所需的各项技术和经验，同时他们不会参与 IC 卡电表生产厂家之间的商业利益，所以能够独立

地保持技术的中立性，最大程度地为电力公司提供优质的服务，使电力公司运行的收费管理系统能够长时间地保证安全和稳定。

基于以上考虑，委托银行和系统集成商进行收费管理系统的设计，IC 卡电表生产厂家将只提供满足统一设计规范要求的 IC 卡电表产品。

4.1.3 安全性

安全性的考虑可以分为三个方面：卡片介质的安全性、表计生产过程的安全性、运行管理的安全性。

1. 卡片介质的安全性

由于用户群体庞大，并且表计安装后 IC 卡向表计传递的数据管理系统无法监控，因此必须要求用户卡片具有较高的安全性。较好的方式是选用带有密钥控制的 CPU 卡。并且在 CPU 卡的设计过程中，尽量靠近 PBOC 规范（中国人民银行金融卡规范），在卡片的发行过程中，对用户卡中的密钥进行分散处理，最大限度地减少被黑客攻击破译系统密钥的可能性。同时在用户卡中传递的关键数据最好进行线路加密保护处理，以防止非法篡改数据的可能性。

2. 表计生产过程的安全性

严格区分表计的生产过程和运行管理过程，保证 IC 卡电表一旦安装运行，对 IC 卡电表中任何数据的修改都应该在运行管理系统的控制下进行，坚决杜绝生产厂家或管理部门工作人员持有特殊工具卡可以不经管理系统对 IC 卡电表数据进行改写的行为。要保证这一点，就应该在 IC 卡电表中安装 ESAM，该模块用来存储表中的数据和安全密钥，在运行过程中由用户卡和 ESAM 进行安全认证和数据传输，ESAM 由运行管理系统发行并提供给表计生产厂家安装。在 IC 卡电表生产完毕测试合格后再用管理系统提供的修改密钥卡将 ESAM 中的密钥修改为运行密钥，这样未经授权，任何人都不可以对表里的数据进行修改。

3. 运行管理的安全性

在 IC 卡电表系统中，系统的安全主要取决于密钥的发行和管理，因此必须有一套合适的卡片以及 ESAM 密钥发行和传递方式。由于系统的组成环节中有银行、电力公司、表厂、卡片供应商和系统集成商，这几个环节都可能涉及密钥管理，如果密钥在传递过程中被窃取，系统的安全性将受到极大影响。建议成立卡片发行和密钥管理机构，密钥发行传递采用总控卡、母卡、应用卡的三级方式，每一级在向下传递时采用密文线路保护方式或密钥密文导出方式。

4.1.4 网络售电管理系统的建立

在网络版的管理中，应实现以下目标：

1. 异地实时缴费购电

每一个安装 IC 卡电表的用户都分配了一个具有唯一卡号的购电卡，用户不论在任何一个售电网点插入购电卡，都可以通过网络实时连接到电力公司售电管理中心数据库，查询用户信息并为用户计算电费，并将购电数据下传到售电网点终端为用户写卡购电，这样极大地方便了用户。

2. 购电交易和购电业务的分离

在以往的售电管理系统中，售电终端既能够为用户购电写卡，同时也能够处理开户、查询统计等管理业务，这样就造成操作人员权限过大，可以人为地进行某些数据操作，发生“人情电”等状况。因此，应对此做严格划分，即能够进行购电交易操作的终端不能够处理购电业务，同时能够进行购电业务操作的终端不能够进行购电写卡交易操作，各供电分局只能进行购电业务操作，形成的数据由售电管理中心进行维护，每天的交易记录由售电管理中心下传给各供电分局进行业务处理。而银行和各个供电分局的售电交易网点只能够写卡售电，但写卡售电的数据全部来自于售电管理中心，终端不能自行产生数据。售电管理中心也只能对所有的数据进行维护，但不能对任何数据进行修改，这样通过三个方面就有效保证了数据的安全性，不会出现人为的虚假售电。

4.2　智能卡电表收费管理系统

4.2.1　智能卡电表收费管理系统的构成

一般的 IC 卡电表收费管理系统由 IC 卡电表、购电 IC 卡、IC 卡读写器、收费管理软件四个部分组成，如图 4-1 所示。

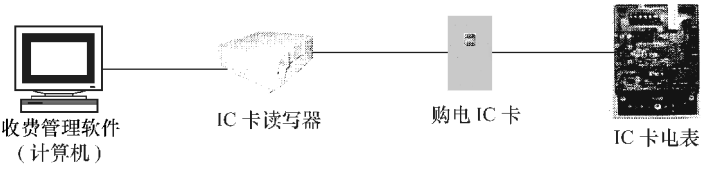


图 4-1　IC 卡电表收费管理系统

1. IC 卡电表

IC 卡电表主要完成对用户用电量的计量和控制功能，同时能够接受购电 IC 卡中传来的购电量，并把购电量准确地追加到 IC 卡电表中。目前 IC 卡电表的种类较多，使用数量最大的是居民单相单费率 IC 卡电表，还有三相三线、三相四线单费率 IC 卡电表，同时也有少部分单相和三相复费率 IC 卡电表。

2. 购电 IC 卡

购电 IC 卡是一种卡片介质，它能够进行数据读写并长时间保存数据不丢失，主要用来完成用户购电量数据的传递，将用户在收费管理系统所购买的购电量写入到购电 IC 卡并传递到 IC 卡电表中。按照 IC 卡的安全型不同，可以分为普通存储卡、逻辑加密卡、CPU 智能卡。普通存储卡只能存储读写数据，没有对数据进行安全性保护；逻辑加密卡具有密码保护功能，只有通过密码校验才能够对 IC 卡的数据进行读写，具有一定的安全性；CPU 智能卡是含有微处理器的 IC 卡，只有通过密钥认证以及相关的加密解密算法才能够对卡片中的数据进行操作，具有极高的安全性。

3. IC 卡读写器

IC 卡读写器是购电 IC 卡和计算机进行数据交换的接口设备，可以根据需要选择串口或 USB 口与计算机进行连接。目前有很多专业的读写设备公司生产 IC 卡读写器，而原来大部分使用的是由 IC 卡电表生产厂家自制的 IC 卡读写器，通用性较差。

4. 收费管理软件

收费管理软件安装在电力公司营销网点，主要来完成对用户的缴费购电写卡工作，并进行相关的业务统计查询工作。根据实际使用的状况，可以选择使用单机版的收费管理软件和网络版的收费管理软件。单机版的收费管理软件主要在 IC 卡电表数量不多，物业小区代收费的情况下使用，网络版的收费管理软件主要在 IC 卡电表数量较多，用户覆盖范围较广，由电力公司直接进行收费的情况下使用，可以实现与电力公司营销系统以及银行代收费系统的联网。

4.2.2 智能卡电表收费管理系统设计要求

1. IC 卡电表收费管理系统方案的确立

在 IC 卡电表收费管理系统的初期设计中，存在着一个认识上的误区，即把 IC 卡电表等同于整个 IC 卡电表收费管理系统，这样一旦选择了某个电表生产厂家的 IC 卡电表，也就意味着选择了这个厂家的收费管理软件、IC 卡读写器以及购电 IC 卡，而由于各个生产厂家的收费管理系统设计方案各不相同，这样就导致了在同一个电力公司如果安装了多个电表生产厂家的 IC 卡电表，就必须安装多套收费管理系统，造成使用管理上的混乱和不方便。所以必须统一制订整个收费管理系统的整体方案，该方案应该覆盖前面所讲的 IC 卡电表、购电 IC 卡、IC 卡读写器以及收费管理软件各个部分的内容，而不仅仅只是 IC 卡电表的内容，这样就可以实现整个系统的规范和统一。

2. 购电 IC 卡的选择

购电 IC 卡是由用户持有，用来传递用户的购电量数据，由于购电量数据的重

要性，必须保证用户无法通过技术手段对购电 IC 卡中的数据进行改写，也就是必须要考虑购电 IC 卡的数据安全性。

从目前成熟的应用来看，选择使用具有高安全等级的 CPU 智能卡可以保证购电 IC 卡的数据安全性，主要体现在：

CPU 智能卡内含微处理器芯片，能够进行算法运算和逻辑分析处理，不是简单地进行密码或口令的校验，而是利用密钥进行认证处理。

CPU 智能卡的密钥只能使用，不能读出，在认证或数据传输过程中不能被跟踪，私密性好。

CPU 智能卡中可以对要存储的数据进行加密或解密处理，并能够对数据的完整性进行判断，数据如果被跟踪或修改能够及时被发现。

CPU 智能卡满足中国人民银行金融卡规范，可以方便地开展电费代收业务。

随着电子技术的不断发展，CPU 智能卡的容量越来越大，价格逐渐降低，已经可以充分满足电力部门的数据要求，非常适合作为购电 IC 卡传输介质。

3. IC 卡电表类型的选择

IC 卡电表类型主要涉及以下几种类型：单相单费率 IC 卡电表；三相单费率 IC 卡电表（包括三相三线、三相四线）；单相复费率 IC 卡电表；三相复费率 IC 卡电表（包括三相三线、三相四线）；多功能复费率 IC 卡电表。

在上面所列的 IC 卡电表类型中，使用数量较多、性能比较稳定的是单相、三相单费率 IC 卡电表，主要原因是其功能比较单一，设计的成熟度高，产品稳定可靠，多数电表厂家都可以设计制造；单相、三相复费率 IC 卡电表相对数量较少。

4. 建立统一的检测管理规范

对 IC 卡电表的检测不能等同于对普通智能电表的检测，除了需进行电表的计量精度以及电磁兼容等常规性能指标的检测外，还需要对 IC 卡电表的数据传输流程、预付费功能进行统一的检测。如果这部分不统一检测，即使是在统一的收费管理技术方案规范下，各个电表厂家生产的 IC 卡电表在功能上也会存在差异，一旦 IC 卡电表安装出去，发现功能、数据接口存在差异，对整个收费管理系统的运行就会产生很大的影响，所以必须保证各个电表厂家（包括卡片供应商提供的卡片）的电表经过统一的测试，数据流程完全相同，这样才能做到产品互相兼容并能够互换，保证电力公司收费管理平台总体的安全性。

5. IC 卡电表收费管理系统

在 IC 卡电表收费管理系统投入运行后，如何方便地为用户提供良好的电费收缴、购电写卡服务对各供电分公司来讲都是一项非常重要的内容，以往都是在各供电分公司由电表厂家建立一套单机版收费管理软件。这种方式对物业小区进行收费服务非常到位，但作为一个城市的电力公司只有一个购电收费网点对用户缴费购电写卡是非常不方便的。必须能够使电力公司的所有营业网点都能够为用户提供

服务。

如果在所有的营业网点都建立安装单机版 IC 卡电表收费管理软件，也不能很好地解决用户购电服务问题，由于单机版收费管理软件的数据库信息不能实现共享，用户只能到被指定的营业网点去购电，而不能做到根据实际情况在任何一个网点实现缴费购电。从电力公司的角度来讲，如果在所有的营业网点都安装了独立的单机版 IC 卡收费管理软件，如何将各个网点的购电交易、收费情况统计出来也是一个工作量非常大的事情，不容易实现对所有营业网点的有效管理。

因此，建立网络版的 IC 卡电表收费管理系统是十分必要的。这样既能够满足用户异地随时缴费购电写卡的要求，也能够满足供电公司数据统计汇总的要求。在网络版 IC 卡电表收费管理系统中，核心是建立一个统一的收费数据库系统，利用电力公司内部的网络，将收费数据库系统和各个营业网点的售电写卡终端建立实时连接，售电写卡终端完成对用户前端的缴费写卡服务，而所有的交易记录都实时保存在统一的收费数据库系统中。同样，电力公司的其他管理终端也可以在授权的情况下访问收费数据库，进行各种查询统计业务。

4.3 智能卡电表的功能和结构

4.3.1 智能卡电表的功能

1. 智能控制功能

IC 卡电表使用机电一体式 IC 卡电表，采用光电脉冲采样方式自动计量用户电量，当用户购电量用完时，自动切断用户用电。

2. 预报警功能

当用户 IC 卡电表中所剩电量小于报警电量时，能够给予用户报警提示，以便用户尽快购电。

3. 电量返读功能

用户每次将电卡插入 IC 卡电表后，IC 卡电表将自动把剩余电量等信息回写到电卡中，以供售电管理系统查询。

4. 安全保护功能

采用 CPU 卡作为购电卡，在 IC 卡电能表内安装有 ESAM，与 CPU 卡相互做密钥认证，具有高度安全性，严格保证一户一表一卡，每次购电卡只一次输入有效。

5. 补卡功能

当用户购电卡丢失时，可以通过售电网络为用户补发电卡。

6. 检查功能

售电网络可以发行检查卡，定期对用户 IC 卡电表运行情况进行检查。

7. 通信功能

售电部门可以通过建立一定的数据通信信道，对居民使用的 IC 卡电表中的所有数据及时进行抄收。

8. 电量冻结功能

售电部门可以通过数据通信信道对 IC 卡电表下发电量冻结指令，并将冻结电量数据抄回进行线损统计和电费核算。

9. 负荷统计功能

售电部门可以通过数据通信信道对 IC 卡电表下发负荷冻结指令，IC 卡电表能够根据指令计算用户某一时刻的功率并加以冻结传输给售电部门进行居民用电负荷分析。

4.3.2　智能卡电表的结构

1. 智能卡电表的构成

IC 卡电表结构如图 4-2 所示。对机电一体式智能卡电表，可采用双路光电探头进行脉冲采样计量，为保证计量的准确性，要求光电探头采用透射式结构，应能够有效解决由于圆盘抖动造成的计量误计现象。IC 卡电表上采用数码管显示用户表内的剩余电量以及提示信息，采用发光二极管指示 IC 卡电表运行状态，对用户用电的控制功能由 IC 卡电表外的断路器完成，IC 卡电表内置小电流继电器通过表尾输出断路器的控制信号。IC 卡电表内 CPU 与 CPU 卡以及 ESAM 通信均采用 T = 0 协议，IC 卡电表的安全认证由 CPU 卡和 ESAM 共同完成，表内 CPU 只起通信传递作用，无需增加加密算法。IC 卡电表在结构上应考虑设计安全、操作方便的数据通信接口，以便售电部门进行数据抄收使用。

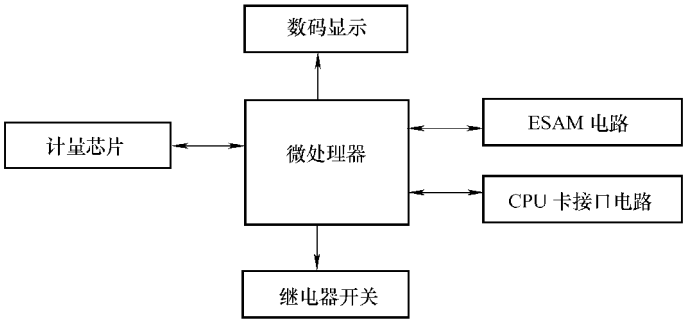


图 4-2　IC 卡电表结构

2. ESAM 接口

ESAM 和 CPU 卡硬件连接电路图（MCS51）如图 4-3 所示。

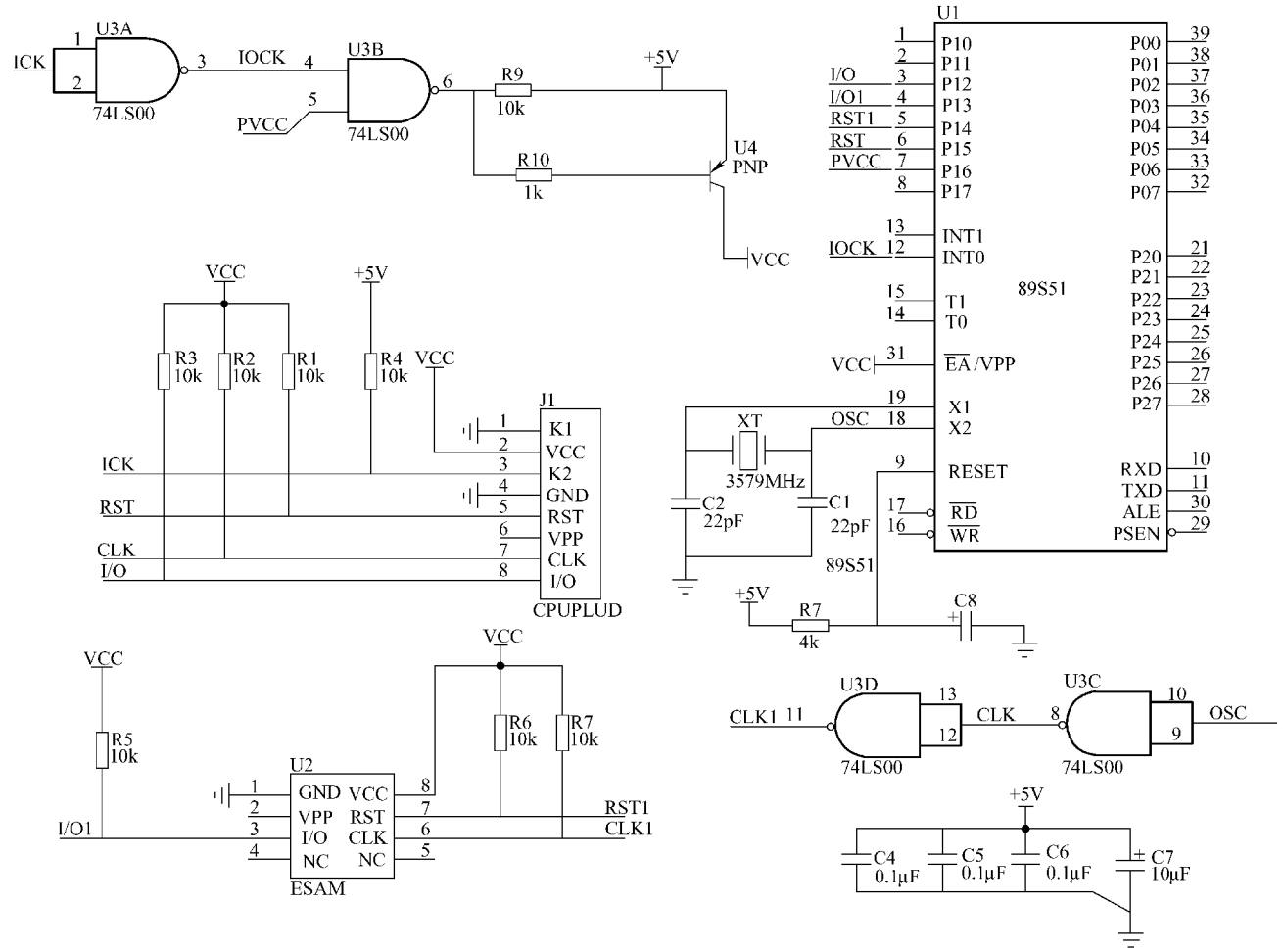


图 4-3　ESAM 和 CPU 卡硬件连接电路图

4.3.3　智能卡电表的数据项设计

1. 户号

电力公司在开户报装时为每一用户分配的编号，为压缩 BCD 码，严格做到一户一号不重复。在用户第一次购电时通过电卡将户号传递到 IC 卡电表，作为今后一表一卡的判断依据。

2. 电表表号

电表表号为 IC 卡电表出厂编号，为压缩 BCD 码，由三部分组成：

电表表号 = 厂家编号 + 版本号 + 电表流水号

其中厂家编号为 2 位 1 字节，版本号为 2 位 1 字节，由各厂家根据情况而定，初始值均为 01。电表流水号为 6 位 3 字节。为各厂家生产时 IC 卡电表的流水号，应保证一表一号不重复。IC 卡电表铭牌编号应与电表表号严格一致。

3. 电卡类型

电卡类型为营业购电卡的类型编号，规定如下：01—初始化卡；02—用户购电卡；03—检查卡；04—补卡；05—居民不记名卡；06—修改主密钥卡；07—商业不记名。

4. 剩余电量

剩余电量为用户 IC 卡电表中允许用户还能使用的电量。用户每次将购电卡插入 IC 卡电表中时将剩余电量返写至电卡中。

5. 购电量

购电量为用户每次到银行网点交款所购电量。IC 卡电表从电卡中读入本次购电量应与表中剩余电量相加作为当前实际剩余电量。

6. 购电次数

购电次数为用户从开户起到银行网点交款购电总次数，每购一次电购电次数加 1，若购电次数为 9999，则下次加 1 翻为 0000。

7. 报警电量

报警电量为提醒用户尽快购电的报警门限电量，为压缩 BCD 编码。具体划分为报警电量 1 和报警电量 2，各为 6 位 3 字节，其中报警电量 1 的值大于报警电量 2 的值。当用户 IC 卡电表中剩余电量小于等于报警电量 1 时，用户 IC 卡电表的数码显示部分处于常亮状态，给予用户第一次光报警。当用户 IC 卡电表中剩余电量小于等于报警电量 2 时，切断用户用电提醒用户，用户此时将电卡插入 IC 卡电表后可恢复用电，但此后数码管仍保持为常点亮状态，两次报警电量值可任意设置。

8. 充值限额

充值限额为限制用户将购电量输入 IC 卡电表的门限电量。当用户 IC 卡电表中剩余电量大于等于限购电量时，不接受用户本次所购电量；只有当用户 IC 卡电表

中剩余电量小于限购电量后才能接受用户所购买的电量，以免造成用户囤积电量。不接受用户购电卡时，数码管显示剩余电量并闪烁给予用户提示，延时 10s 后自动消失。

9. 累计购电量

累计购电量为用户自开户起累计所购电量。用户每次购电时，银行主机将比较从用户电卡中返写的累计购电量与银行所存数据是否一致，一致时才能进行下次购电。当累计购电量超过 999999 时自动滚屏为 000000。

10. 累计应急购电量

累计应急购电量为用户使用不记名卡累计所购电量。当累计购电量超过 999999 时自动滚屏为 000000。

11. 累计用电量

累计用电量为用户自开户起累计所用电量。当累计用电量超过 999999 时自动滚屏为 000000。

12. 过零电量

当 IC 卡电表中剩余电量为零后应断开断路器切断用户用电，若此时 IC 卡电表未能切断用户用电，则用户到下次购电前所使用的电量称为过零电量。银行售电网点每次购电前需读入此单元并上传电力公司营业中心，营业中心依据过零电量决定对用户的处理流程。

13. 脉冲常数

脉冲常数为每记录 1kW · h 电能电子部分所接收到的脉冲数，为 IC 卡电表状态数据。

14. IC 卡电表状态字

电表状态字为反映 IC 卡电表运行状态的单元，如 EEPROM 错、执行机构错等。

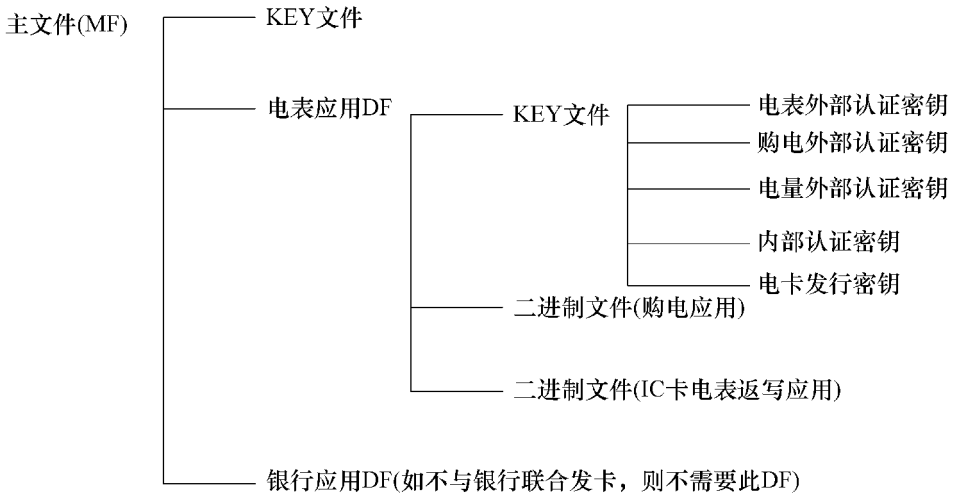
4.4 电卡设计

4.4.1 电卡分类及结构

根据其功能以及使用环境不同，可以划分为用户卡、检测卡、生产测试卡、不记名卡、修改主密钥卡、ESAM 卡和 PESAM 卡七类，具体定义如下：

1. 用户卡

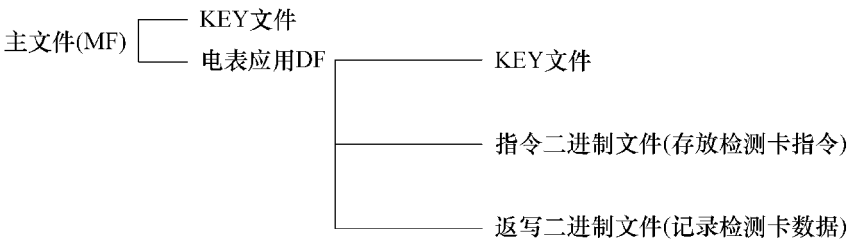
用户卡是指用户用来完成购电以及向 IC 卡电表中追加购电量的电卡。其结构定义如下：



考虑到与银行应用接轨，将 IC 卡电表应用设计为一个 DF，MF 结构保留，开放给银行应用。在设计中做到不经过 MF 级就可直接访问电表应用 DF 目录。在电表应用 DF 目录中包含三个文件，其中购电应用二进制文件是银行写购电信息的文件，IC 卡电表返写应用二进制文件是 IC 卡电表返写数据的文件。对它们的写操作分别由 KEY 文件中购电外部认证密钥、电表外部认证密钥和电量外部认证密钥控制，用户卡必须通过内部认证以及相应的外部认证后才可以进行写操作，但对用户卡所有二进制文件的读操作则不需任何认证即可进行。电卡发行密钥与售电流程操作无关，是电力公司在初始化电卡时的外部认证密钥，通过此认证才可以更改电卡中的密钥。

2. 检测卡

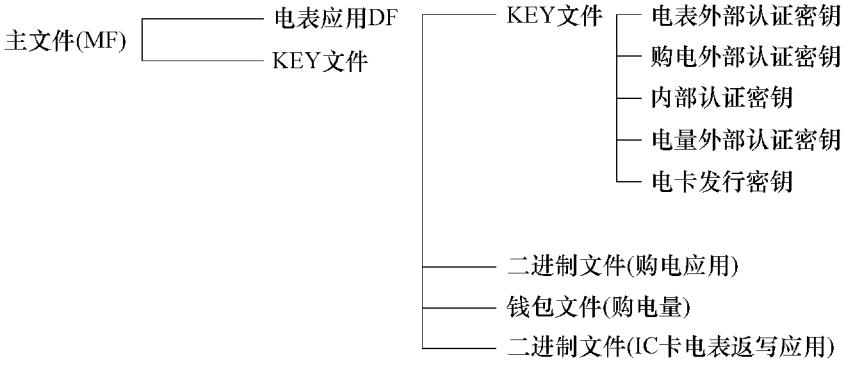
检测卡是电力公司和 IC 卡电表生产厂家用来对 IC 卡电表进行检测用的电卡。此卡对所有 IC 卡电表通用，插入 IC 卡电表后将返回 IC 卡电表内所有计量和状态信息，其结构如下：



由于检测卡是通用的工具卡，所以在其结构中只有一个空的 KEY 文件，不含有任何密钥，这样就可以很方便地制作和使用检测卡。指令二进制文件存放的是检测卡指令，返写二进制文件用来记录 IC 卡电表返回的数据。

3. 不记名卡

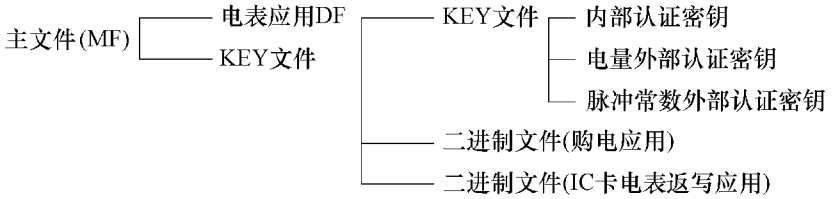
不记名卡是电力公司单独在社会上发行的一次性购电卡。当用户 IC 卡电表电量用完且不能立即到银行储蓄网点进行下次购电时，可以购买不记名卡作应急用。其结构如下：



其中购电应用二进制文件用来存放不记名卡指令，钱包文件存放不记名卡购电量，该文件无存款权限，IC 卡电表密钥认证通过后一次扣减为零。IC 卡电表返写应用二进制文件用来返写 IC 卡电表表号备查。

4. 生产测试卡

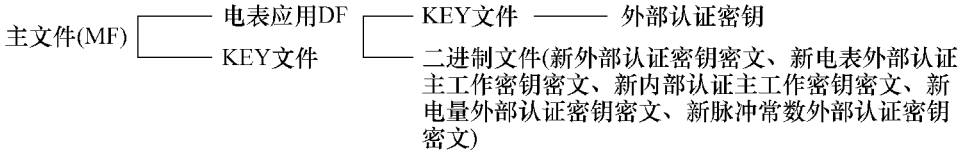
生产测试卡是为了方便 IC 卡电表生产厂家在生产过程中进行检测的一组卡，其内容由各 IC 卡电表生产厂家自定。具体结构如下：



与用户卡的区别有两点：一是不考虑银行应用，取消购电外部认证和电表外部认证；二是增加脉冲常数外部认证密钥，如果需修改脉冲常数，必须经过此认证，否则 ESAM 不接受，这也就意味着出厂后脉冲常数将不可更改。生产测试卡中的密钥均为公开密钥，IC 卡电表生产厂家可以根据需要随意制卡。

5. 修改主密钥卡

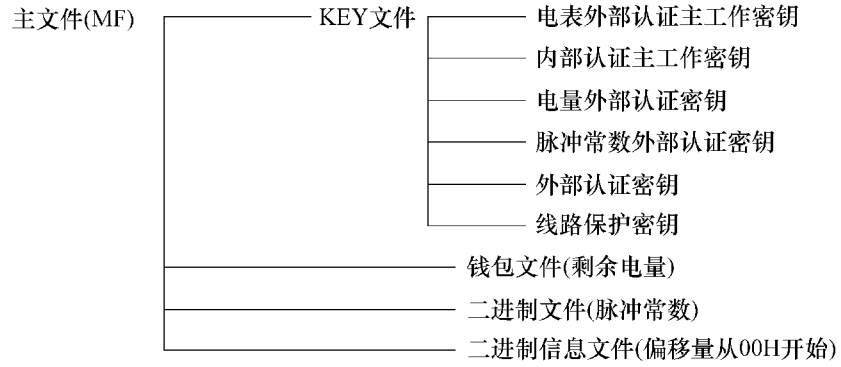
在 IC 卡电表生产过程中，为方便 IC 卡电表生产厂家测试，ESAM 中的主密钥是公开的，IC 卡电表出厂前，利用电力公司提供的修改主密钥卡将 IC 卡电表内 ESAM 的主工作密钥修改为实际运行过程中的主密钥，IC 卡电表主密钥修改后也就意味着 IC 卡电表生产厂家使用的电卡不可能进入电力公司售电管理系统，此主密钥由电力公司掌握，IC 卡电表生产厂家不可知。其结构如下：



将修改主密钥卡插入后，首先由 ESAM 对电卡进行外部认证，认证通过后将电卡中的五个密钥的密文读入，ESAM 利用线路保护密钥对它们进行解密，然后逐一替换 ESAM 中的主工作密钥。需特别指出，替换后由于主密钥改变，生产测试卡将不能再修改脉冲常数，而用户卡中不含脉冲常数外部认证密钥，也不能对脉冲常数进行修改。

6. ESAM 卡

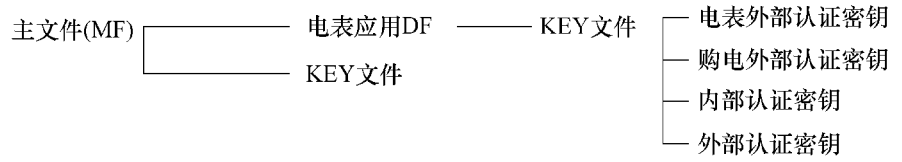
所谓 ESAM 卡即 IC 卡电表中的 ESAM，ESAM 在 IC 卡电表中有两个作用：一是进行一表一卡的安全认证工作；二是作为 IC 卡电表内数据存储区，其结构如下：



在 ESAM 中，KEY 文件中的电表外部认证主工作密钥和内部认证主工作密钥用于一户一表安全认证；外部认证密钥和线路保护密钥用于更换 IC 卡电表应用主工作密钥；电量外部认证密钥用来对钱包文件进行认证，剩余电量增加时必须经过认证才能写入 ESAM，剩余电量递减时不需通过认证；脉冲常数外部认证密钥用来对脉冲常数二进制文件进行安全认证，修改脉冲常数必须通过认证，但读操作则不需认证；二进制信息文件用于存放 IC 卡电表内部数据，不需认证可自由读写，其格式可由各 IC 卡电表生产厂家自定。

7. PESAM 卡

PESAM 卡是由供电部门发行的供银行储蓄网点售电使用的认证卡，无此卡不能进行正常的售电操作，PESAM 卡中无数据操作文件，只存放认证密钥，其结构如下：



4.4.2 电卡应用文件和密钥

1. 电卡应用文件

（1）购电应用二进制文件

购电应用二进制文件存放用户购电信息。在 CPU 卡中，二进制文件为一个连续存储区，用户可对其中任意一个存储单元进行读写操作。

（2）IC 卡电表返写应用二进制文件

IC 卡电表返写应用二进制文件存放从 IC 卡电表返回的信息。当用户把所购电量写入 IC 卡电表的同时 IC 卡电表把表内的信息写入用户卡，下次购电时由 POS 机读入银行售电系统。

（3）购电量钱包文件

购电量钱包文件存放用户购电量，分为存款和扣款两个交易过程，可用不同的密钥分别控制其权限。在 IC 卡电表应用中主要用于对 IC 卡电表中购电量的控制，以防非法窃取电量。

2. 电卡密钥类型

（1）用户卡电表外部认证密钥

用户卡电表外部认证密钥控制对用户卡上 IC 卡电表返写应用文件的写操作。售电网络通过电表外部认证密钥的认证，可以擦除卡上的电卡返写应用文件；IC 卡电表通过电表外部认证密钥的认证，可以向电表返写二进制文件中返写数据。

（2）用户卡购电外部认证密钥

用户卡购电外部认证密钥控制对用户卡上购电应用文件的操作。售电网络通过购电外部认证密钥的认证，可以在卡上写入购电量等相关信息。

（3）用户卡电卡发行密钥

用户卡电卡发行密钥控制对用户卡上密钥的更新。售电网络通过电卡发行密钥认证后可以修改用户卡上的密钥组。

（4）用户卡内部认证密钥

用户卡内部认证密钥控制对用户卡的操作。只有通过对用户卡的内部认证，用户卡才被认可是本系统所发行卡，才能进行进一步的操作。

（5）用户卡电量外部认证密钥

用户卡电量外部认证密钥控制对 IC 卡电表中 ESAM 中电量钱包文件的存款操作。通过对 ESAM 的电量外部认证密钥的认证，IC 卡电表允许将新增加的购电量写入 ESAM 中。

（6）ESAM 线路保护密钥

ESAM 线路保护密钥控制对 ESAM 密钥组的更新。修改主密钥卡中存放的被线路保护密钥加密的新密钥密文在传输到 ESAM 后，ESAM 使用线路保护密钥对密文

数据进行解密，得到真正的密钥组用于修改 ESAM 的密钥。线路保护密钥使被更新的密钥在传输过程中，以加密保护的方式传送，直到被更新的 ESAM 内部以后，才得到真正的密钥数据。该数据在传送过程中如果被窃取，由于窃取者不知道线路保护密钥，也不可能得到真正的密钥。

（7）ESAM 脉冲常数认证密钥

ESAM 脉冲常数认证密钥控制对 IC 卡电表脉冲常数的修改。只有通过该密钥的认证后，才可以修改 IC 卡电表中的脉冲参数。

4.4.3　电卡密钥安全体系

1. 电卡相关业务初始化流程（见图 4-4）

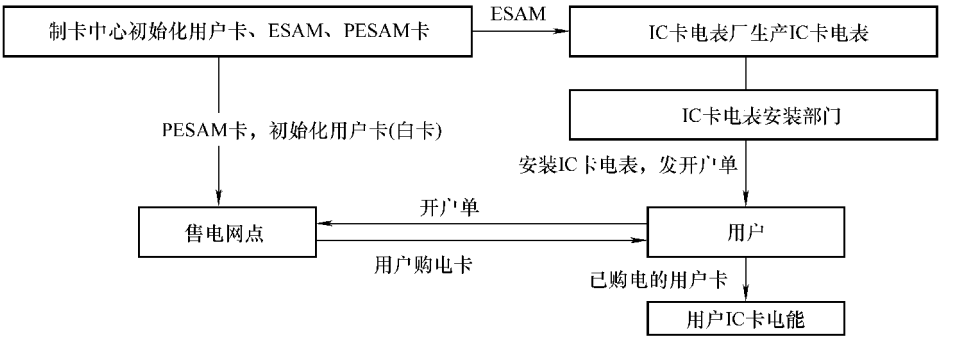


图 4-4　电卡相关业务初始化流程

2. 电卡密钥生成流程（见图 4-5）

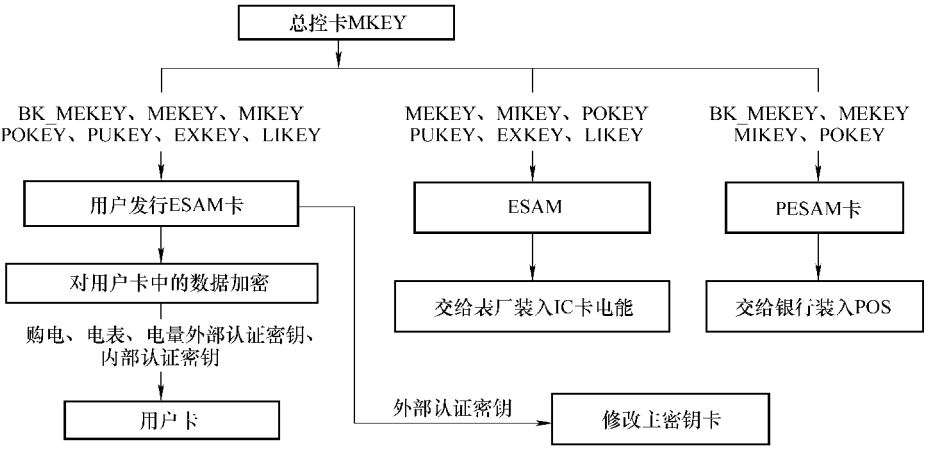


图 4-5　电卡密钥生成流程

4.5 智能卡电表和智能卡的接口文件

4.5.1 电卡数据文件结构

1. 电卡数据文件结构

（1）用户卡购电应用二进制文件

数据类型	值	数据长度/B
起始命令	* *	1
命令字节	* *	1
数据长度		1
用户号		4
电卡类型	* *	1
购电量		3
购电次数		2
报警电量 1		3
报警电量 2		3
充值限额		3
校验和		1
结束码	* *	1

（2）用户卡电表返写应用二进制文件

数据类型	值	数据长度/B
起始命令	* *	1
命令字节	* *	1
数据长度		1
剩余电量		3
累计购电量		3
累计用电量		3
过零电量		3
非法插卡次数	* *	2
表的状态字		1
电表表号		5
累计应急购电量		3
校验和		1
结束码	* *	1

（3）检测卡二进制文件

数据类型	值	数据长度/B
起始命令	* *	1
命令字节	* *	1
数据长度		1
电卡类型	* *	1
校验和		1
结束码	* *	1

（4）检测卡返写二进制文件

数据类型	值	数据长度/B
起始命令	* *	1
命令字节	* *	1
数据长度		1
剩余电量		3
累计购电量		3
累计用电量		3
过零电量		3
电表状态字		1
电表表号		5
累计应急购电量		3
购电次数		2
脉冲常数		2
报警电量 1		3
报警电量 2		3
充值限额		3
校验和		1
结束码	* *	1

（5）不记名卡购电应用二进制文件

数据类型	值	数据长度/B
起始命令	* *	1
命令字节	* *	1
数据长度		1
电卡类型	* *	1
校验和		1
结束码	* *	1

（6）不记名卡电表返写应用二进制文件

数据类型	值	数据长度/B
起始命令	* *	1
命令字节	* *	1
数据长度		1
电表表号		4
校验和		1
结束码	* *	1

（7）修改主密钥卡二进制文件

数据类型	值	数据长度/B
起始命令	* *	1
命令字节	* *	1
数据长度		1
电卡类型	* *	1
数据块长度		1
新外部认证密钥密文		8
加密数据块		7
数据块长度		1
新电表外部认证主工作密钥密文		8
加密数据块		7
24H 数据块长度		1
新内部认证主工作密钥密文		8
加密数据块		7
34H 数据块长度		1
新电量外部认证密钥密文		8
加密数据块		7
数据块长度		1
新脉冲常数外部认证密钥密文		8
4DH ~ 53H 加密数据块		5
校验和		1
结束码	* *	1

（8）继电器测试卡应用二进制文件

数据类型	值	数据长度/B
起始命令	* *	1
命令字节	* *	1
数据长度		1
校验和		1
结束码	* *	1

（9）增加电量卡应用二进制文件

数据类型	值	数据长度/B
起始命令	* *	1
命令字节	* *	1
数据长度		1
增加电量		3
校验和		1
结束码	* *	1

（10）快速测试卡应用二进制文件

数据类型	值	数据长度/B
起始命令	* *	1
命令字节	* *	1
数据长度		1
剩余电量		3
脉冲常数		2
报警电量 1		3
报警电量 2		3
充值限额		3
校验和		1
结束码	* *	1

（11）预置卡应用二进制文件

数据类型	值	数据长度/B
起始命令	* *	1
命令字节	* *	1
数据长度		1
剩余电量		3
脉冲常数		2
报警电量		3
报警电量 2		3
充值限额		3
校验和		1
结束码	* *	1

（12）修改表号卡应用二进制文件

数据类型	值	数据长度/B
起始命令	* *	1
命令字节	* *	1
数据长度		1
电表表号		4
预置电量		3
用户类型		1
校验和		1
结束码	* *	1

注：表格中的 * * 表示自定义的控制字段。

2. 智能卡电表数据文件的数据格式

数据在购电卡中采用不定长格式存放，在与购电卡进行数据交换或与数据抄收装置进行数据传输时均采用数据串的形式进行，具体格式如下：

起始	命令	长度	数据	校验	结束

起始：1B，固定为 68H，为数据串的开始标识。

命令：1B，不同的命令表示与 IC 卡电表进行数据交换的流程不同，它决定了数据串中数据的长度。

长度：1B，压缩 BCD 码，为数据串中数据区的长度。

数据：字节数不定，为前面介绍数据项的组合，组合方式与命令有关。

校验：1B，为命令、长度、数据三部分的累加和去除高字节自然溢出后得到，

为十六进制数。

结束：1B，固定为 16H，代表数据串结束。

对数据串是否有效的判别依据为起始、结束字节必须正确；长度与数据区字节数必须相等；校验必须正确。

4.5.2　智能卡电表和智能卡的安全认证流程

智能卡电表和智能卡的安全认证都是通过智能卡电表中的 ESAM 完成的，智能卡电表中的 CPU 在认证过程中只起到数据传输的作用，不参与数据加密和解密运算。

1. 用户卡和智能卡电表 ESAM 的内部认证流程

1）智能卡电表读取用户卡上的卡序列号，送 ESAM。

2）ESAM 用内部认证主工作密钥对卡序列号进行加密，生成内部认证工作密钥。

3）智能卡电表送加密指令及随机数给用户卡，用户卡用内部认证密钥加密，并将加密结果 D1 送回智能卡电表。

4）智能卡电表送加密指令及随机数给 ESAM，ESAM 将加密结果 D2 送回智能卡电表。

5）智能卡电表比较 D1 与 D2，若相等，则内部认证成功；否则不成功。

2. 用户卡和智能卡电表 ESAM 的外部认证流程（电表外部认证）

1）智能卡电表取用户卡的卡序列号，送 ESAM。

2）ESAM 用电表外部认证主工作密钥对卡序列号进行加密，生成电表外部认证工作密钥。

3）智能卡电表从用户卡取随机数。

4）智能卡电表将随机数送 ESAM，ESAM 用工作密钥对随机数加密，并将加密结果返回。

5）智能卡电表送加密结果给用户卡，并发外部认证指令。

6）用户卡告诉智能卡电表认证是否成功，若成功则将电卡状态置为相应外部认证密钥规定的状态。

3. IC 卡电表 ESAM 的外部认证流程（外部认证、电量外部认证、脉冲常数外部认证）

1）智能卡电表从 ESAM 中取随机数。

2）智能卡电表将随机数送用户卡，用户卡用相应的工作密钥对随机数进行加密，并将加密结果送回 IC 卡电表。

3）智能卡电表将加密结果送 ESAM，并发外部认证指令。

4）ESAM 告诉智能卡电表认证是否成功，并允许智能卡电表对 ESAM 作相应

的操作。

4.5.3 智能卡电表和智能卡的操作流程

1. 智能卡电表读取电卡购电量流程

1）智能卡电表从用户卡中读取卡序列号和用户号，并比较用户号是否一致，不一致则拒绝读卡。

2）用户号一致，智能卡电表将卡序列号送 ESAM，ESAM 对卡序列号进行加密，生成相应的工作密钥。

3）智能卡电表用内部认证密钥对电卡作内部认证。

4）智能卡电表用电表外部认证密钥对电卡作外部认证。

5）智能卡电表从电卡购电应用二进制文件中读取购电数据，判断其完整性，同时判断购电次数是否与智能卡电表内一致，不一致则向智能卡电表返写应用二进制文件返写数据退出。

6）若判断一致，智能卡电表用电量外部认证密钥对 ESAM 进行外部认证，若一致则将购电量及状态数据存入 ESAM，并返写数据退出；否则只返写数据退出。

2. IC 卡电表和电卡实现一户一表的流程

用户卡密钥初始化完成后，由电力公司发给银行各储蓄网点；电力公司将智能卡电表安装完毕并将开户信息登录后，向用户提供开户单。用户持开户单到银行储蓄网点办理开户以及购电手续，银行储蓄网点根据用户开户单上的户号从电力公司传给银行主机的数据库中调出用户信息，按规定格式写入已初始化的用户卡，完成用户卡的开户工作。同时根据用户的要求进行售电操作，将售电量同时写入用户卡中。

用户将用户卡插入智能卡电表后，智能卡电表将用户号读入，存入智能卡电表 ESAM 中，然后读入用户的购电量，完成首次购电操作，同时将智能卡电表表号返写给电卡。

当用户第二次购电时，银行储蓄网点从电卡中读取智能卡电表表号，通过银行主机返传到电力公司营业中心，完成用户智能卡电表的资产登记管理；当用户第二次购电插卡时，智能卡电表将用户号读入，首先与 ESAM 中的用户号进行比较，若相同则进行读入购电量操作，不同则拒绝读卡。这样就完成了一户一表的认证工作。

3. 不记名卡与智能卡电表操作流程

因银行目前实现自动售电尤其是夜间无人售电流程较为复杂，所以为解决用户在非工作时间购电的矛盾采取了发行不记名卡的方法。不记名卡的结构与用户卡基本相同，密钥管理也基本相同，但电表应用和购电应用两个二进制文件的内容与用户卡完全不同。

不记名卡作为整个售电系统中较为特殊的一个组成部分，具有以下几个特点：

1）具有通用性，在任何一块智能卡电表上都可以使用。

2）使用次数只有一次，不能重复使用。

3）不能去银行购电。

4）不记名卡中没有任何个人信息，完全由电力公司发行、管理，在一般的商店、超市等商业网点都可以购买到。

智能卡电表处理不记名卡的流程如下：

1）智能卡电表首先从电卡中电表返写应用二进制文件读取电表表号，若有电表表号（未使用时电表表号单元均为 FFH），说明此卡已经使用过则退出。

2）智能卡电表若读到电表表号单元均为 FFH，则从电卡中读入卡序列号和购电应用二进制文件，判断数据的完整性，不对则退出。

3）数据完整则将卡序列号送 ESAM，ESAM 对卡序列号进行加密生成相应的工作密钥。

4）智能卡电表用内部认证密钥电卡进行内部认证。

5）智能卡电表用电量外部认证密钥对 ESAM 进行外部认证，通过后将购电量读入智能卡电表，然后将电卡钱包文件中的购电量一次扣除。

6）智能卡电表用电表外部认证密钥对电卡作外部认证，并向电卡返写二进制文件中返写该智能卡电表表号。

7）智能卡电表再从电卡中读取电表表号进行比较，若比较不正确，此卡作废，电量不写入 ESAM；比较正确，智能卡电表将购电量和状态信息存入 ESAM。

4. 检测卡操作流程

检测卡主要在生产过程中检测智能卡电表中的继电器通断是否正常。将继电器检测卡插入智能卡电表中，继电器将切换到与目前状态相反的工作状态，对智能卡电表内的数据无影响。

5. 增加电量卡操作流程

增加电量卡主要在生产过程中向智能卡电表中追加电量，在校表和走字过程中使用。将增加电量卡插入智能卡电表中，可以将一定数量的电量值与智能卡电表中的剩余电量值相加。

6. 快速测试卡操作流程

快速测试卡主要用来在生产过程中快速测试智能卡电表的功能。将快速测试卡插入到智能卡电表中，智能卡电表将快速测试卡中的数据读入到相应数据单元，并以当前脉冲常数进行电量处理，当测试完毕掉电后，当前脉冲常数自动失效，智能卡电表将以正常的脉冲常数进行电量处理。

7. 预置卡操作流程

预置卡主要用来在生产过程中对智能卡电表的参数进行初始化，其数据结构与

快速测试卡相同，但在脉冲常数的处理上不同，将预置卡插入到智能卡电表中后，智能卡电表将脉冲常数保存到 ESAM 中的脉冲常数二进制文件中，掉电后该数据不会自动失效。

8. 修改表号卡操作流程

修改表号卡主要用来在智能卡电表出厂前对参数进行初始化，主要将电表表号输入到智能卡电表中，同时可在智能卡电表内为用户预留一定的剩余电量，并在智能卡电表内输入用户类型标志，同时将智能卡电表内有关数据单元清零，购电次数设为 1，报警电量设为 000000，充值限额设为 999999。

第 5 章　智能卡水表

智能卡水表以 CPU 智能卡以及嵌入式安全控制模块（ESAM）作为数据信息存储和传递介质，具备很高的安全性和抗攻击性。CPU 智能卡的文件结构和操作应完全符合中国人民银行金融卡规范（PBOC 规范），可与金融系统实现一卡通，同时也可实现一卡多表应用。本章阐述了智能卡水表的功能、设计原理；根据智能卡片的不同类型，给出了其文件系统的具体设计、智能卡水表 ESAM 文件系统及智能卡读写接口设计实例。

5.1　智能卡水表功能

1. 一卡多表收费功能

一张用户卡上可以完成多种不同水表类型（如冷水表、热水表、中水表、纯水表）的收费工作，同时也可以完成多块同种水表类型的收费工作。

2. 预付费功能

可以通过用户卡向 CPU 卡水表中写入购水量，当购水量使用完毕，即剩余水量为零时，阀门自动关闭切断用户用水；用户只有再次缴费购水并将购水量通过用户卡写入 CPU 卡水表后才能自动打开阀门恢复继续用水。

3. 显示功能

用户可以通过 CPU 卡水表上的按键或者插入用户卡查看表中的剩余水量、累计购水量以及累计用水量信息。

4. 报警功能

当用户剩余水量小于设定值时，水表液晶显示屏处于常显状态，同时剩余水量每减少 $1m^3$，蜂鸣器会给出报警提示音，提示用户尽快购水。

5. 可选择的透支功能

在 CPU 卡水表中设置透支水量值后，当剩余电量为零、阀门关闭时，可以通过按键或插卡使阀门打开进入透支状态继续用水，当继续使用水量超过透支水量值后，自动关闭阀门停止用户用水。

6. 应急购水功能

在特殊情况下，用户可以购买一次性使用的应急购水卡将一定的购水量追加到 CPU 卡水表中，并且不会影响正常用户卡的使用。

7. 参数设置功能

用户可以根据自己的实际需要，通过用户卡购水时改变 CPU 卡水表中的一些设定参数。

8. 防止水量囤积功能

当 CPU 卡水表中的剩余水量大于充值限额时，拒绝用户将新的购水量输入到 CPU 卡水表中，只有当表中的剩余水量小于充值限额时，才允许将新的购水量输入到 CPU 卡水表中。

9. 补卡功能

当用户不慎将用户卡丢失后，可以通过管理系统为用户重新补发一张用户卡，并将最近一次购水记录补写到用户卡中，CPU 卡水表可以自动判别最后一次购水记录是否对表有效。

10. 数据返回功能

可以通过用户卡将 CPU 卡水表中的计量数据和工作状态数据返回到管理部门，供结算统计处理使用。

11. 阶梯水量统计功能

在 CPU 卡水表中可以自动计量冻结 12 个月的累计用水量，并可以通过用户卡带回到管理系统，管理系统可以根据累计用水量对用户进行阶梯水量收费计算。

12. 检查功能

可以在 CPU 卡水表中插入检查卡，将水表中的数据全部读出，供检查分析使用。

13. 回收转移功能

可以在旧表中插入回收转移卡将表中的相关数据读出，并通过回收数据转移卡将这些数据转移到新表中去。

14. 校时功能

可以利用校时卡对 CPU 卡水表中的日历和时钟进行校准和修改。

5.2 智能卡水表原理

为实现上述功能，智能卡水表的电路模块应包括微控制器、电源模块、计量模块、IC 卡接口模块、LCD 显示模块、阀门控制开关模块、ESAM 和实时时钟模块等，以实现先付费后用水的功能。当用户购买水量后，将卡插入水表，就可以开阀用水。当剩余水量等于规定的关阀报警水量时，将给用户提示信息并自动关闭阀门，并允许插卡恢复供水。当剩余水量为零时，自动关阀。若允许用户透支，则插卡恢复供水直至使用完透支水量后才关阀。用户每次将卡插入水表后，水表 LCD

显示模块将显示剩余水量，并将剩余水量等用水信息及水表状态信息返写到用户卡中，以供售水管理系统入库查询统计。图 5-1 是智能卡水表的原理图。

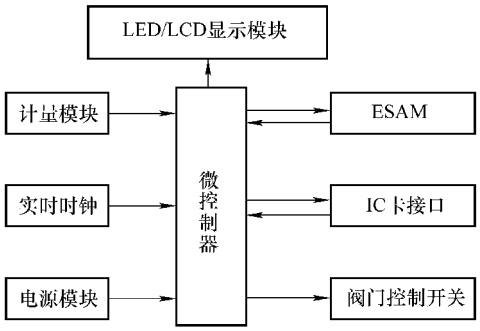


图 5-1　智能卡水表的原理图

5.3　智能卡水表卡片类型

智能卡水表系统中卡的种类有多种，分别实现不同的功能，应用于不同的阶段，满足不同的需求。

1. 用户卡

用户卡是在用户安装完 CPU 卡水表后开始使用，根据需要它可以分为四种类型：首次购水卡；普通购水卡；可以进行参数设置的购水卡；可以进行密钥修改的购水卡。

（1）首次购水卡

用户在安装完 CPU 卡水表及开户手续后，首次缴费购水的用户卡称为首次购水卡。首次购水卡除了将购水量输入水表外，同时将用户户号信息传递到水表，完成用户卡与水表的对应关系，同时可以将必要的运行参数写入到水表中。

（2）普通购水卡

普通购水卡是用户正常使用的购水卡，在将购水量读入到 CPU 卡水表之前，要首先判断用户卡中的户号和 CPU 卡水表中的是否相同，相同则可将购水量读入，否则拒绝读入，同时将 CPU 卡水表中的运行数据信息返传到用户卡中。

（3）可进行参数设置的购水卡

根据需要，在完成正常购水过程的同时，还可以通过用户卡对 CPU 卡水表的运行参数进行修改，参数包括报警水量、透支限额、充值限额和扣卡水量。

（4）可进行密钥修改的购水卡

根据需要，在完成正常购水的同时，还可以通过用户卡对 CPU 卡水表中的运行密钥进行更新和替换，用新的密钥值继续进行安全认证。

2. 生产设置卡

CPU 卡水表在生产过程中主要使用生产设置卡。生产设置卡根据需要可以划分为三种类型：普通设置卡、带表号的设置卡和初始化卡。

（1）普通设置卡

普通设置卡是在 CPU 卡水表装配完毕后，对水表的基本参数进行设置的卡，包括：预置水量、用水种类、报警水量、透支限额、充值限额、扣卡水量、表累计量小数位等基本参数，参数设置在表内采用的是数据更新覆盖的方式，不对原有的数据进行累加。普通设置卡可以多次重复使用。

（2）带表号的设置卡

带表号的设置卡除了能够对上述基本参数进行设置外，还可以对检验合格的水表进行出厂表号的设置工作。带表号的设置卡只能使用一次，只能对一块水表进行设置。

（3）初始化卡

初始化卡是在 CPU 卡水表出厂前，将水表内的数据设置成出厂状态，出厂状态的数据可以根据需要事先规定。初始化卡可以多次重复使用。

3. 修改密钥卡

修改密钥卡用于将处于生产测试状态的 CPU 卡水表的公开测试密钥修改为运行密钥，或者将处于运行状态的 CPU 卡水表的运行密钥更换为新密钥。此卡可以多次重复使用，由 CPU 卡水表的管理部门发行。

4. 校时卡

校时卡用于在生产状态和运行状态下对 CPU 卡水表内的时钟和日历进行设置，运行状态的校时卡由 CPU 卡水表的管理部门进行发行，在使用时一般需要有手持设备在现场制卡。

5. 检查卡

检查卡用于在生产状态和运行状态下对 CPU 卡水表中的所有计量数据和状态数据进行检测。将检查卡插入 CPU 卡水表中，可以将所有数据全部读出。检查卡可以多次重复使用。

6. 回收转移卡

回收转移卡用于在运行状态下将一块旧 CPU 卡水表中的计量数据和状态数据全部读出，再将这些数据转移到一块新的 CPU 卡水表中去，主要在换表过程中使用。

7. 应急购水卡

当用户由于各种原因不能及时持用户卡进行购水时，可以通过购买应急购水卡向 CPU 卡水表中加入一定数量的应急购水量。应急购水卡只能使用一次，不进行用户户号核对，可以在任何一块 CPU 卡水表上使用，它是面向社会公开发行的。

5.4 卡片文件系统设计

5.4.1 用户卡

用户卡文件系统的结构可考虑将不同收费的项目设计在不同的应用目录中，以实现不同行业管理之间的一卡多用，每个应用目录下的文件结构和密钥结构均相同，这样不同应用的水表可以使用相同的程序模块，减少开发工作量。图 5-2 是用户卡文件系统结构图。

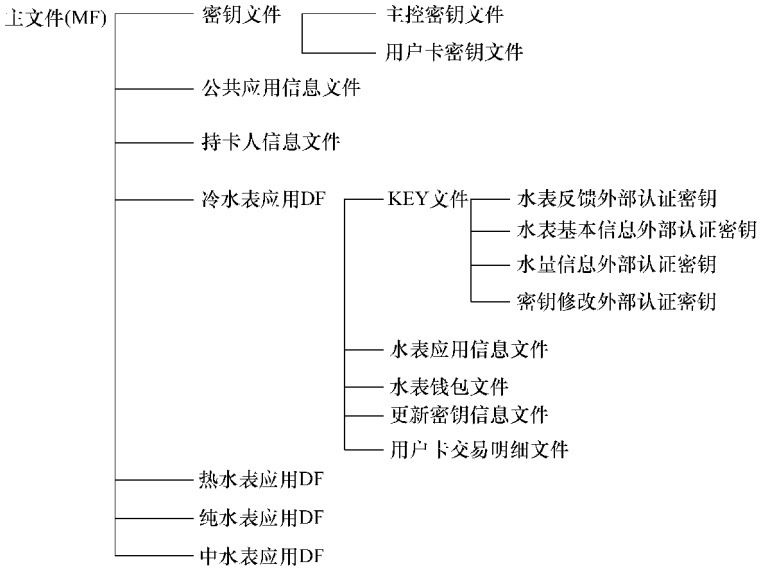


图 5-2　用户卡文件系统结构图

用户卡文件系统是一个三层结构。

第一层为 MF（主文件），实质是一个 DDF（目录专用文件），通常将 MF 开放给银行。

第二层是水表应用。考虑到不同类型的用水，设计了四种水表应用目录，即冷水表应用目录、热水表应用目录、纯水表应用目录、中水表应用目录，以满足不同的需求。同时，在第二层还建立公共应用信息文件和持卡人信息文件，公共应用信息文件采用二进制文件，用来存储发行商和应用版本的信息；持卡人信息文件采用二进制文件，用来存储持卡人的个人信息，如用户姓名、身份证、电话、住址等。这两个文件中的内容只与卡片管理应用有关，与水表应用设计无关。其数据内容和空间大小可根据卡片实际调整。

第三层为各种水表应用目录。以冷水表应用目录为例，设置了三种类型的文件，第一种是二进制文件，用来存储用户的用户号、购水时间、购水次数，以及设置参数如报警水量、透支限额、充值限额、扣卡水量等，该文件内容可以自由读取，修改时必须通过密钥认证并以加密写入的方式进行。第二种是钱包文件，考虑到与金融系统的兼容性，可采用标准的金融电子钱包存储本次购水量，向钱包中写入本次购水量使用圈存交易，从钱包中取出本次购水量追加到水表使用消费交易。第三种文件是循环文件，用来存储交易过程数据，可根据需要存储多笔交易过程数据。

1. 用户卡文件

★用户卡文件

文件	内容说明	标识
MF	主文件	3F00
MKF	主密钥文件	0000
EF1	公共应用信息文件	0015
EF2	持卡人信息文件	0016
DF01	冷水表应用目录文件	3F03 或 WATER3
DKF	水表应用密钥文件	0000
EF1	水表应用信息文件	0001
EF2	水表钱包文件	0002
EF3	水表反馈信息文件	0003
EF4	更新密钥信息文件	0004
EF18	用户卡交易明细文件	0018
DF02	热水表应用目录文件	3F04 或 WATER4
DF03	纯水表应用目录文件	3F05 或 WATER5
DF04	中水表应用目录文件	3F06 或 WATER6

为保证目录文件选择的灵活性，对冷水表应用目录文件可采用目录标识符 3F03 和目录名称 WATER3 两种方式（其余方式类推），建议采用目录名称方式选择水表应用目录。

冷水表应用目录文件中，水表应用信息文件用来将后台管理系统的信息传递到水表中，后台管理系统采用密文写入，水表采用明文读出。水表反馈信息文件用来将水表中的信息传递到后台管理系统中，水表采用明文写入，后台管理系统采用明文读出。更新密钥信息文件用来在需要时用密文传递的方式对水表 ESAM 中的密钥进行更新，后台管理系统采用密文写入，水表采用明文读出。操作时首先将所有的密钥密文读入到 ESAM 临时信息文件，然后再分别进行密钥解密更换工作。

2. 密钥文件

★用户卡主控密钥文件（MKF）

标识	名　　称	标识	名　　称
00	用户卡主控密钥	01	持卡人信息外部认证密钥

★用户卡密钥文件（DKF）

标识	名　　称	标识	名　　称
00	水表主控密钥	03	文件线路保护密钥
00	TAC 内部密钥	04	水表应用外部认证密钥
00	口令密钥	05	水表反馈外部认证密钥
00	口令重装密钥	06	水表基本信息外部认证密钥
01	系统内部认证密钥	07	水量信息外部认证密钥
02	圈存密钥	08	密钥修改外部认证密钥
02	消费密钥		

用户卡主控密钥由卡片发行方进行明文安装，认证过程中可使用不同的加密算法（如 3DES 运算）。

持卡人信息外部认证密钥使用用户卡主控密钥进行密文安装，水表应用目录中的其他密钥使用水表主控密钥进行密文安装。考虑与金融系统的兼容性，水表应用目录中的密钥长度均为 16B。

TAC 内部密钥用来在圈存和消费过程中计算 TAC 码，与 ESAM 配对使用。安装时采用线路保护方式进行。

口令密钥用于在银行做圈存操作时进行认证，认证通过后才能进行圈存操作，使用时口令密钥值由用户自行输入。注意符合 PBOC 规范的口令密钥为 2～6B。

口令重装密钥用于在重装口令密钥时计算 MAC 码，卡片发行时一次写入。

系统内部认证用来验证是否和 ESAM 是一个系统发行的，与 ESAM 配对使用。安装时采用线路保护方式进行。

圈存密钥用来验证将本次购水量按圈存交易方式写入水表钱包文件的过程，与售水卡（PSAM 卡）配对使用。安装时采用线路保护方式进行。

消费密钥用来控制水表将水表钱包文件中的本次购水量按消费交易方式写入水表中的过程，与 ESAM 配对使用。安装时采用线路保护方式进行。

文件线路保护密钥主要用于对水表应用信息文件进行操作，完成对数据的加密写入。与售水卡配对使用，安装时采用线路保护方式进行。

水表应用外部认证密钥主要用于对水表应用信息文件进行操作，认证通过后可以对数据进行改写，与售水卡配对使用。安装时采用线路保护方式进行。

水表反馈外部认证密钥主要用于对水表反馈信息文件进行操作，认证通过后可以对数据进行改写，与 ESAM 配对使用。安装时采用线路保护方式进行。

水表基本信息外部认证密钥与 ESAM 配对使用，安装时采用线路保护方式进行。

水量信息外部认证密钥与 ESAM 配对使用，安装时采用线路保护方式进行。

密钥修改外部认证密钥与 ESAM 配对使用，安装时采用线路保护方式进行。

用户卡中需要分散的密钥在发行时采用其主密钥与卡片序列号进行加密产生。

3. 水表应用信息文件

★水表应用信息文件（文件标识符：0001）

数据项	长度/B	数据项	长度/B
用户卡命令码	1	透支限额	3
卡标识	1	充值限额	3
本次购水时间	3	扣卡水量	3
用户号	6	校验和	1
报警水量	3		

管理软件在写水表应用信息文件时，用文件线路保护密钥加密写入数据，而用明文读出数据。

水表是否进行参数设置或进行密钥修改由卡标识单元决定，程序根据卡标识的内容进行选择。如果要对密钥进行修改时，约定首先处理购水量和参数设置，最后进行密钥修改，密钥修改成功后，将水表工作状态字中的密钥更新标志置 1。用户卡中的密钥更新在用户下次购水时进行。下次购水时，后台管理系统首先查询水表反馈信息文件中的水表工作状态字中的密钥更新标志，若为 1，则进行用户卡密钥更新，若为 0，不进行密钥更新。在下次用户卡与水表交易完成后，将水表工作状态字中的密钥更新标志清 0。

正常用户卡插入后，水表首先应该判断用户卡中卡标识单元中的用户卡类型，如果用户卡为首次购水卡，则将用户号写入水表 ESAM；若为正常用户卡，则从 ESAM 中读出用户号进行比较，若不相同，则拒绝此卡，不进行购水交易。

4. 水表钱包文件

★水表钱包文件（文件标识符：0002）

数据项	长度/B
水表本次购水量	8

在 PBOC 金融规范中，钱包文件固定为 8B，但其中交易数据为 4B。

5. 水表反馈信息文件

★水表反馈信息文件（文件标识符：0003）

数据项	长度/B	数据项	长度/B
起始码	1	水表工作状态字	1
水表表号	7	磁干扰次数	1
表累计用水量	3	读卡错次数	1
表内水量	4	低电压次数	1
表本次购水量	3	表月累计用水量	36
购水时间	3	当前日期	3
表累计购水量	3	校验和	1
累计应急购水量	3		

每次当用户卡插入水表后，水表在完成扣水交易过程后将上述信息写入到水表反馈信息文件中。如果插入的是其他的用户卡，则不进行返写。

6. 更新密钥信息文件

★更新密钥信息文件（文件标识符：0004）

数据项	长度/B	数据项	长度/B
消费主密钥	24	水表基本信息外部认证密钥	24
系统内部认证主密钥	24	水量信息外部认证密钥	24
水表反馈外部认证主密钥	24	密钥修改外部认证密钥	24
生产设置外部认证密钥	24		

在进行密钥更新时，微控制器必须首先将更新密钥信息文件中的内容一次全部读入保存，然后逐个进行密钥更新。若读取数据不完整，不进行密钥更新。

7. 用户卡交易明细文件

★用户卡交易明细文件（文件标识符：0018）

数据项	长度/B	数据项	长度/B
交易序号	2	终端机编号	6
透支限额	3	交易日期	4
交易量	4	交易时间	3
交易类型标识	1		

根据金融规范，每次交易过程完成后，都必须将交易内容存放在交易明细文件中，交易明细文件的格式是固定的。对于用户卡，其交易明细文件至少应该存放两笔记录。

5.4.2　生产数据设置卡

生产数据设置卡主要在生产过程中对水表的参数进行设置，为保证系统的安全性，现场运行的水表如果进行参数修改，应由用户卡进行，不允许使用生产数据设置卡进行。图 5-3 是生产数据设置卡结构图。

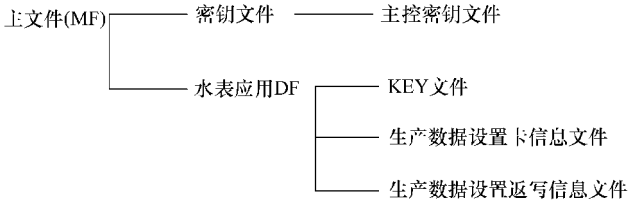


图 5-3　生产数据设置卡结构图

1. 生产数据设置卡文件

★生产数据设置卡文件

文件	内容说明	标识
MF	主文件	3F00
MKF	主密钥文件	0000
DF01	水表应用目录文件	3F03 或 WATER3
DKF	水表应用密钥文件	0000
EF1	生产数据设置卡信息文件	0001
EF2	生产数据设置返写信息文件	0002

在用生产数据设置卡对水表进行参数设置时，水表还没有进入运行状态，此时水表只选择 DF01 应用目录进行数据操作。

2. 密钥文件

★密钥文件（DKF）

标识	名　　称	标识	名　　称
00	生产数据设置卡主控密钥	02	生产数据设置卡外部认证密钥
01	系统内部认证密钥	03	生产设置外部认证密钥

生产数据设置卡主控密钥采用明文装载方式，用来控制和传输其他密钥的装载过程。

系统内部认证密钥在使用前首先用用户卡序列号进行分散，用来验证是否和 ESAM 是一个系统发行的，与 ESAM 配对使用。安装时采用线路保护方式进行。

生产数据设置卡外部认证密钥主要用于控制对生产数据设置卡信息文件的操作，认证通过后可以对数据进行修改，与生产操作员卡配对使用。安装时采用线路保护方式进行。

生产设置外部认证密钥与 ESAM 配对使用，安装时采用线路保护方式进行。

3. 生产数据设置卡信息文件

★生产数据设置卡信息文件（文件标识符：0001）

数据项	长度/B	数据项	长度/B
生产数据设置卡命令码	1	透支限额	3
卡类别标识	1	充值限额	3
水表表号	7	扣卡水量	3
预置水量	3	表累计量小数位	1
用水种类	1	校验和	1
报警水量	3		

使用生产数据设置卡时，如果卡类别标识不为 30H，可以对多块水表的参数进行设置，水表表号单元填零；如果卡类别标识为 30H，只能对一块水表的参数进行设置。设置成功后，要将水表表号写入生产数据设置卡返写信息文件。水表在接受表号设置时，要首先判断生产数据设置卡返写信息文件是否为空，若不为空，则拒绝接受表号设置。

如果卡类别标识为 50H，只进行预置水量和用水种类的参数设置，生产数据设置卡其余数据单元填零。表内数据自动恢复为初始值，并且只能接受首次购水卡的操作。

如果此时使用运行密钥，可以起到现场初始化卡的作用。作为现场初始化卡使用时，其水表应用目录可以根据实际情况为 3F03、3F04、3F05、3F06 中的任一个，水表会根据用水种类自动进行应用目录选择。

4. 生产数据设置卡返写信息文件

★生产数据设置卡返写信息文件（文件标识符：0002）

数据项	长度/B	数据项	长度/B
起始码	1	水表表号	7
表号设置成功标志	1	校验和	1

5.4.3　检查卡

检查卡主要在现场或生产过程中对水表的数据进行检查核对的卡片，为保证检查卡使用的方便性，检查卡对数据进行操作时不进行一卡一表的数据认证，这样检查卡就可以对任何一块水表进行数据检查工作。图 5-4 是检查卡文件结构图。

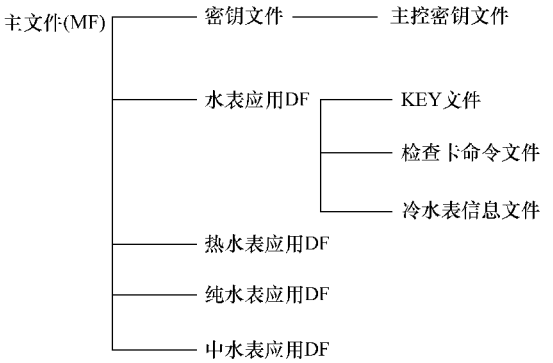


图 5-4　检查卡文件结构图

1. 检查卡文件

★检查卡文件

文件	内容说明	标识
MF	主文件	3F00
MKF	主密钥文件	0000
DF01	冷水表应用目录文件	3F03 或 WATER3
DKF	气表应用密钥文件	0000
EF1	检查卡命令文件	0001
EF2	冷水表信息文件	0002
DF02	热水表应用目录文件	3F04 或 WATER4
DF03	纯水表应用目录文件	3F05 或 WATER5
DF04	中水表应用目录文件	3F06 或 WATER6

2. 密钥文件

★主控密钥文件（MKF）

标识	名　　称
00	检查卡主控密钥

检查卡主控密钥采用明文装载方式，用来控制和传输其他密钥的装载过程。

★密钥文件（DKF）

标识	名称	标识	名称
00	水表主控密钥	01	系统内部认证密钥

水表主控密钥在检查卡主控密钥的控制下进行密文装载，用来控制和传输其他密钥的装载过程。系统内部认证密钥在使用前首先用用户卡序列号进行分散，用来验证是否和 ESAM 是一个系统发行的，与 ESAM 配对使用。安装时采用线路保护方式进行。

3. 检查卡命令文件

★检查卡命令文件（文件标识符：0001）

数据项	长度/B	数据项	长度/B
检查卡命令码	1	校验和	1

4. 冷水表信息文件

★冷水表信息文件（文件标识符：0002）

数据项	长度/B	数据项	长度/B
起始码	1	应急卡本次购水量	3
水表表号	7	表累计用水量	3
用户号	6	表内水量	4
用水种类	1	计量脉冲数	1
报警水量	3	水表工作状态字	1
透支限额	3	磁干扰次数	1
充值限额	3	读卡错次数	1
扣卡水量	3	低电压次数	1
表累计量小数位	1	表月累计用水量	36
表本次购水量	3	当前日历	3
购水时间	3	当前时钟	3
累计购水量	3	校验和	1
累计应急购水量	3		

5.4.4　修改密钥卡

修改密钥卡主要在生产过程中对水表的生产测试密钥进行修改，将生产过程使用的公开测试密钥更换为运行密钥。为保证系统的安全性，现场运行的水表如果进行密钥修改，一定要通过用户卡进行，不允许使用修改密钥卡进行。图 5-5 是修改密钥卡文件结构图。

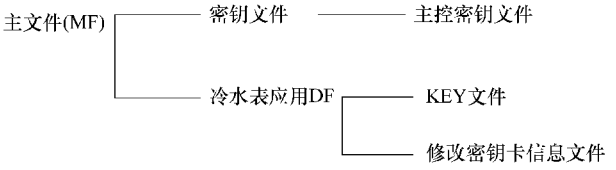


图 5-5　修改密钥卡文件结构图

1. 修改密钥卡文件

★文件系统定义

文件	内容说明	标识
MF	主文件	3F00
MKF	主密钥文件	0000
DF01	冷水表应用目录文件	3F03 或 WATER3
DKF	水表应用密钥文件	0000
EF1	修改密钥卡信息文件	0001

2. 密钥文件

★密钥文件（DKF）

标识	名称	标识	名称
00	修改密钥卡主控密钥	02	密钥修改外部认证密钥
01	系统内部认证密钥		

修改密钥卡主控密钥采用明文装载方式，用来控制和传输其他密钥的装载过程。

系统内部认证密钥在使用前首先用用户卡序列号进行分散，用来验证是否和ESAM是一个系统发行的，与ESAM配对使用。安装时采用线路保护方式进行。

密钥修改外部认证密钥与ESAM配对使用。安装时采用线路保护方式进行。

修改密钥卡信息文件的内容在建立卡片文件结构时一次写入，在使用过程中其内容将不可更改，不需要通过外部认证密钥对其写权限进行控制。

3. 修改密钥卡信息文件

★修改密钥卡信息文件（文件标识符：0001）

数据项	长度/B	数据项	长度/B
修改密钥卡命令码	1	生产设置外部认证密钥	24
消费主密钥	24	水表基本信息外部认证密钥	24
系统内部认证主密钥	24	水量信息外部认证密钥	24
水表反馈外部认证主密钥	24	密钥修改外部认证密钥	24

修改密钥卡可以重复使用，对多块水表进行密钥更新。进行密钥修改时，应先将所有密钥值全部从修改密钥卡中读入水表，然后再逐个替换。

5.4.5 回收转移卡

回收转移卡主要用于在现场进行换表操作时将旧表中的数据一次全部转移到新表中（水表表号除外）。根据现场实际使用情况，水表应用目录可以是3F03、3F04、3F05、3F06中的任意一个，水表会根据用水种类自动进行选择，如果卡的应用目录与水表不符，水表自动退出，不进行回收转移操作。图5-6是回收转移卡文件结构图。

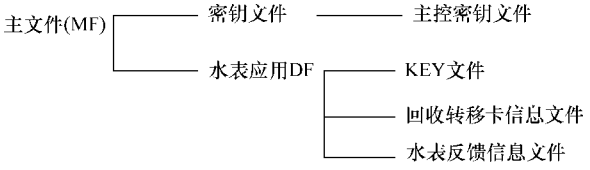


图5-6 回收转移卡文件结构图

1. 回收转移卡文件

★文件系统定义

文件	内容说明	标识
MF	主文件	3F00
MKF	主密钥文件	0000
DF01	水表应用目录文件	3F03 或 WATER3
DKF	水表应用密钥文件	0000
EF1	回收转移卡信息文件	0001
EF2	水表反馈信息文件	0002

2. 密钥文件

★密钥文件（DKF）

标识	名称	标识	名称
00	回收转移卡主控密钥	02	水表反馈外部认证密钥
01	系统内部认证密钥	03	生产设置外部认证密钥（运行值）

回收转移卡主控密钥采用明文装载方式，用来控制和传输其他密钥的装载过程。

系统内部认证密钥在使用前首先用用户卡序列号进行分散，用来验证是否和 ESAM 模块是一个系统发行的，与 ESAM 配对使用。安装时采用线路保护方式进行。

水表反馈外部认证密钥主要用于控制对水表反馈信息文件的操作，认证通过后可以对数据进行修改，与旧表中的 ESAM 配对使用。安装时采用线路保护方式进行。

生产设置外部认证密钥（运行值）与新表中的 ESAM 配对使用，安装时采用线路保护方式进行。

3. 回收转移卡信息文件

★回收转移卡信息文件（文件标识符：0001）

数据项	长度/B	数据项	长度/B
回收转移卡命令码	1	校验和	1

回收转移卡在使用时有两个过程，首先从旧表中读出数据，然后再将回收转移卡中的数据转移到新表中。从旧表中读出的数据包括旧表表号，旧表表号不转移到新表中，但应移到 POS 机中。进行回收转移操作时，更换的水表必须处于初始化状态，数据回收转移完毕后，用户继续进行老用户购水操作。

4. 水表反馈信息文件

★水表反馈信息文件（文件标识符：0002）

数据项	长度/B	数据项	长度/B
水表转移字	1	应急卡本次购水量	3
水表表号	7	表累计用水量	3
用户号	6	表内水量	4
用水种类	1	计量脉冲数	1
报警水量	3	水表工作状态字	1
透支限额	3	磁干扰次数	1
充值限额	3	读卡错次数	1
扣卡水量	3	低电压次数	1
表累计量小数位	1	表月累计用水量	36
表本次购水量	3	当前日历	3
购水时间	3	当前时钟	3
累计购水量	3	校验和	1
累计应急购水量	3		

在数据转移时，旧表中的水表表号不进行转移。如果在进行系统密钥更换过程中换表，换上的水表为更新密钥后的新表，更换完毕后，用户到管理系统进行用户卡密钥的更换。

5.4.6 校时卡

校时卡主要用于在生产过程中或在现场运行状态下对水表中的时钟和日历进行调校。在生产中，水表自动选择 3F03 水表应用目录。根据现场实际使用情况，水表应用目录可以是 3F03、3F04、3F05、3F06 中的任意一个，水表会根据用水种类自动进行选择，如果卡的应用目录与水表不符，水表自动退出，不进行回收转移操作。图 5-7 是校时卡文件结构图。

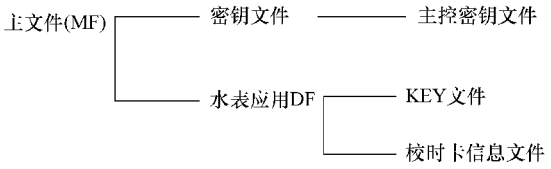


图 5-7 校时卡文件结构图

1. 校时卡文件

★校时卡文件

文件	内容说明	标识
MF	主文件	3F00
MKF	主密钥文件	0000
DF01	水表应用目录文件	3F03 或 WATER3
DKF	水表应用密钥文件	0000
EF1	校时卡信息文件	0001

2. 密钥文件（DKF）

★密钥文件（DKF）

标识	名称	标识	名称
00	校时卡主控密钥	02	校时卡信息外部认证密钥
01	系统内部认证密钥		

校时卡主控密钥采用明文装载方式，用来控制和传输其他密钥的装载过程。

系统内部认证密钥在使用前首先用用户卡序列号进行分散，用来验证是否和 ESAM 是一个系统发行的，与 ESAM 配对使用。安装时采用线路保护方式进行。

3. 校时卡信息文件

★校时卡信息文件（文件标识符：0001）

数据项	长度/B	数据项	长度/B
校时卡命令码	1	新时钟	3
新日期	3	校验和	1

新日期三字节分别为年、月、日，新时钟三字节分别为时、分、秒。这样相当于日历修改范围是 2001 ~ 2100 年。

5.4.7　应急购水卡

当用户由于各种原因不能及时持用户卡进行购水时，可以通过购买应急购水卡向 CPU 卡水表中加入一定数量的应急购水量。图 5-8 是应急购水卡文件结构图。

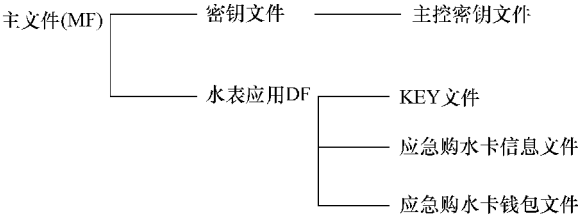


图 5-8　应急购水卡文件结构图

1. 应急购水卡文件

★应急购水卡文件

文件	内容说明	标识
MF	主文件	3F00
MKF	主密钥文件	0000
DF01	水表应用目录文件	3F03 或 WATER3
DKF	水表应用密钥文件	0000
EF1	应急购水卡信息文件	0001
EF2	应急购水卡钱包文件	0002
EF3	水表反馈信息文件	0003
EF18	应急购水卡交易明细文件	0018

2. 密钥文件（DKF）

★密钥文件（DKF）

标识	名称	标识	名称
00	应急购水卡主控密钥	02	圈存密钥
00	TAC 内部密钥	02	消费密钥
00	口令密钥	03	水量信息外部认证密钥
01	系统内部认证密钥	04	水表反馈外部认证密钥

应急购水卡主控密钥采用明文装载方式，用来控制和传输其他密钥的装载过程。

TAC 内部密钥用来在圈存和消费过程中计算 TAC 码，与 ESAM 配对使用。安装时采用线路保护方式进行。

口令密钥用来提升状态寄存器的值为非零，从而达到圈存初始化的权限。

系统内部认证密钥用来验证是否和 ESAM 模块是一个系统发行的，与 ESAM 配对使用。安装时采用线路保护方式进行。

圈存密钥用来在发行应急购水卡时，验证将应急购水量按圈存交易方式写入应急购水卡钱包文件的过程，与应急售水卡（PSAM 卡）配对使用。安装时采用线路保护方式进行。

消费密钥用来控制水表将应急购水卡钱包文件中的应急购水量按消费交易方式写入水表中的过程，与 ESAM 配对使用。安装时采用线路保护方式进行。

水量信息外部认证密钥与 ESAM 配对使用，用于完成对 ESAM 相关文件进行操作的认证过程。安装时采用线路保护方式进行。

3. 应急购水卡信息文件

★应急购水卡信息文件（文件标识符：0001）

数据项	长度/B	数据项	长度/B
应急购水卡命令码	1	校验和	1
用水种类	1		

水表在插入应急购水卡后，首先读入用水种类进行用户类别判别，若卡中的用户类别与水表中不同，则拒绝接收此应急购水卡。应急购水卡中的应急购水量只有在表内水量为零或透支状态时才能加入水表中。

4. 应急购水卡钱包文件

★应急购水卡钱包文件（文件标识符：0002）

数据项	长度/B
应急购水卡本次购水量	8

在 PBOC 金融规范中，钱包文件固定为 8B，但其中交易数据为 4B，由于规定应急卡本次购水量为 3B，在数据处理过程中，可在其前面补 1 字节 00H。

5. 应急购水卡交易明细文件

★应急购水卡交易明细文件（文件标识符：0018）

数据项	长度/B	数据项	长度/B
交易序号	2	终端机编号	6
透支限额	3	交易日期	4
交易量	4	交易时间	3
交易类型标识	1		

根据金融规范，每次交易过程完成后，都必须将交易内容存放在交易明细文件中，交易明细文件的格式是固定的。对于应急购气卡，其交易明细文件至少应该存放两笔记录。

交易序号记录的是交易发生的次数。透支限额对于应急购水卡不存在，其值固定为 000000H。交易量对于圈存交易来讲，是应急购水卡本次购水量，高字节填 00H。交易类型标识对于圈存交易为 02H。终端机编号对于圈存交易为售卡终端的编号。

6. 水表反馈信息文件

★水表反馈信息文件（文件标识符：0003）

数据项	长度/B	数据项	长度/B
起始码	1	水表工作状态字	1
水表表号	7	磁干扰次数	1
表累计用水量	3	读卡错次数	1
表内水量	4	低电压次数	1
表本次购水量	3	表月累计用水量	36
购水时间	3	当前日期	3
表累计购水量	3	校验和	1
累计应急购水量	3		

不记名卡消费交易完成后，水表将当前表内数据信息返写到不记名卡中的水表反馈信息文件中。

5.5 智能卡水表设计实例

根据卡片的文件系统，可以相应地设计出水表中 ESAM 的数据项内容和文件系统。

5.5.1 水表 ESAM 设计

1. ESAM 数据项

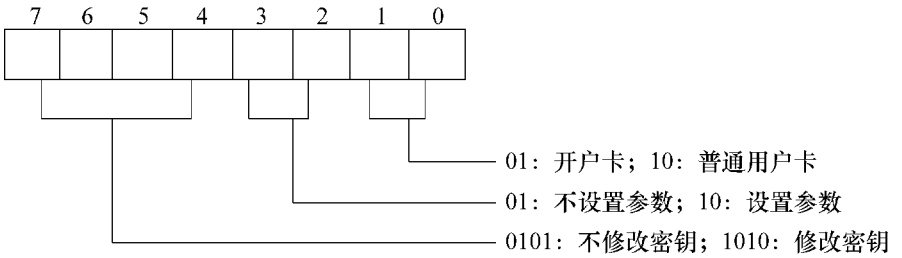
★ESAM 数据项

数据项	长度/B	数据项	长度/B
水表表号	7	**********	***
用户号	6	报警水量	3
卡标识	1	透支限额	3
用水种类	1	充值限额	3
**********	***	扣卡水量	3
表累计购水量	3	水表工作状态字	1
表本次购水量	3	当前日期（上次插卡日期）	3
购水时间	3	**********	***
表内水量	4	磁干扰次数	1
表累计用水量	3	读卡错次数	1
表累计量小数位	1	低电压次数	1
计量脉冲数	1	**********	***
应急购水卡购水量	3	表月累计用水量	36
累计应急购水量	3		

1）水表表号由 7 字节 BCD 码组成，分别为厂商标识、表型标识、版本标识和表序列号，其中前三项各为 1B，表序列号为 4B。其中厂商标识由应用方统一制订，表型标识和版本标识由厂商自行定义。数据存放格式为高字节在前，低字节在后，以下所有数据项未经说明，均采用此格式。

2）用户号由 6 字节 BCD 码组成，由应用方统一制订。

3）卡标识由 1 字节 HEX 码组成，表示当前用户卡的性质，规定如下：



实际使用时可以是以上三种情况的组合（其余情况为非法）。

4）用水种类由 1 字节 BCD 码组成，表示当前用户使用水的类别，规定 0X 代表居民用户，8X 代表工业用户，在低 4 位中 1 代表冷水表，2 代表热水表，3 代表纯净水表，4 代表中水表，依次进行扩展。用户种类不同的表卡不能建立对应关系。由于可能出现一卡多表的情况，水表按照低 4 位的类型进入用户卡中不同的应用目录。

5）表累计购水量由 3 字节 HEX 码组成，表示水表内用户累计购买的水量。6B 整数，以下数据同。

6）表本次购水量由 3 字节 HEX 码组成，表示水表内用户当前购买的水量。

7）购水时间由 3 字节 BCD 码组成，表示用户当前购水的具体日期，分别为年、月、日。

8）表内水量由 4 字节 HEX 码组成，表示水表内还可以使用的水量，当表内水量为零时，如果设置了透支限额，水表将自动进入透支状态，但要关闭阀门为用户报警，用户这时将用户卡插入或按键即可打开阀门继续用水，当表内水量超过透支限额时，关闭阀门切断用户用水；如果透支限额为零，则当表内水量为零时，直接关闭阀门切断用户用水。表内水量数据为3B，用高字节代表表内水量的极性，为0表示表内水量为正数，为 1 表示表内水量为负数，有透支情况发生。当累计用水量发生变化时，需重新计算表内水量。

9）表累计用水量由 3 字节 HEX 码组成，表示水表内累计计量使用的水量。

10）表累计量小数位由 1 字节 HEX 码组成，表示水表记录的用户用水量的小数位，规定 00H 为整数计量，01H 为 1 位小数计量，10H 为 2 位小数计量。该项选择取决于计量传感器安装在哪个计度轮上。

11）计量脉冲数由 1 字节 HEX 码组成，表示水表在进行用水量进位之间所记录的脉冲数。如果为整数计量，每来一个脉冲表累计用水量加 1；如果为 1 位小数计量，每来 10 个脉冲表累计用水量加 1；如果为 2 位小数计量，每来 100 个脉冲表累计用水量加 1。计量脉冲数平时存放在 RAM 中，只有检测到电池失效时，才将其值存放到 ESAM 中。

12）应急卡购水量由 3 字节 HEX 码组成，表示水表内通过应急购水卡加入的

水量。

13）累计应急购水量由 3 字节 HEX 码组成，表示水表内通过应急购水卡累计加入的水量。这样，表内水量 = 表累计购水量 + 累计应急购水量 – 表累计用水量。

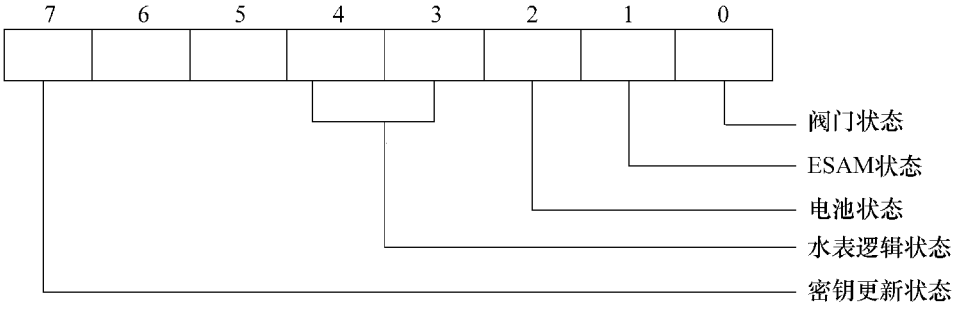
14）报警水量由 3 字节 HEX 码组成，当表内水量小于报警水量时，水表将自动给予用户报警提示。

15）透支限额由 3 字节 HEX 码组成，当水表进入透支状态且表内水量超过透支限额时，水表将自动关闭阀门，切断用户用水。

16）充值限额由 3 字节 HEX 码组成，当水表中表内水量大于充值限额时，水表拒绝将本次购水量输入到水表内。表内最大水量 = 充值限额 + 最大一次购水量。

17）扣卡水量由 3 字节 HEX 码组成，表示当用户卡每次插入水表后，水表从用户卡中扣到水表内的购水量。如果用户卡中的购水量小于扣卡水量，则水表将购水量一次扣清。如果扣卡水量设置为 FFFFFFH，则表示当用户卡插入到水表后，水表一次将用户卡中的购水量一次扣清。扣卡水量的扣取采用两种方式，第一种方式是每次将用户卡插入水表时，水表按扣卡水量的值从用户卡上扣取一次。第二种方式是每次将用户卡插入水表后，每按一次水表上的按键从用户卡上扣取一次。

18）水表工作状态字由 1B 组成，记录水表的运行状态，每位为 0 表示工作正常，为 1 表示错误，定义如下：



水表逻辑状态采用 2 位表示，01 代表初始化状态，10 代表运行状态。

19）当前日期由 3 字节 BCD 码组成，记录水表内时钟所记录的当前年、月、日，各占 1B。当用户卡插入后，水表将当前日期返写到水表反馈信息文件中，数据名称定义为上次插卡日期。

20）磁干扰次数由 1B 组成，记录水表被磁性物质干扰的次数，记录到 FFH 时自动翻滚为 00H。

21）读卡错次数由 1B 组成，记录水表插卡操作出错的次数，记录到 FFH 时自动翻滚为 00H。

22）低电压次数由 1B 组成，记录水表电池低于正常工作电压的次数，记录到

FFH 时自动翻滚为 00H。

23）表月累计用水量由 3 字节 HEX 码组成，记录表内每个月的累计用水量，最大可记录 12 个月的月累计用水量。记录时间段为自然月，即当时钟跳变到每月 1 日零点时进行月累计用水量记录。

2. 水表 ESAM 文件

★水表 ESAM 文件

文件	内容说明	标识
MF	主文件	3F00
MKF	密钥文件	0000
EF1	累计用水量文件	0001
EF2	水表基本信息文件	0002
EF3	水量信息文件	0003
EF4	水表运行信息文件	0004
EF5	临时信息文件	0005

临时信息文件主要用于微控制器在进行数据处理时作为数据临时存储单元使用。

3. ESAM 密钥文件（MKF）

★ESAM 密钥文件（MKF）

标识	名称	标识	名称
00	水表主控密钥	04	生产设置外部认证密钥
01	消费主密钥	05	水表基本信息外部认证密钥
02	系统内部认证主密钥	06	水量信息外部认证密钥
03	水表反馈外部认证主密钥	07	密钥修改外部认证密钥

1）水表主控密钥用来对 ESAM 中的其他密钥进行密文安装和密文修改。

2）消费主密钥在使用前首先用 IC 卡序列号进行分散，用来在消费交易中对 MAC1 码进行校验时使用，与用户卡配对使用。

3）系统内部认证主密钥在使用时首先利用 IC 卡序列号进行密钥分散，生成系统内部认证工作密钥，用来认证 IC 卡和 ESAM 是否是同一个地方发行的，与 IC 卡上的系统内部认证密钥配对使用。

4）生产设置外部认证密钥主要用于对累计用水量钱包文件进行清零操作，认证通过后可以对累计用水量钱包文件进行增款操作，与生产设置卡配对使用。

5）水表基本信息外部认证密钥主要用于对水表基本信息文件进行操作，认证通过后可以对数据进行改写，与用户卡配对使用。

6）水量信息外部认证密钥主要用于对水量信息文件进行操作，认证通过后可以对数据进行改写，与用户卡配对使用。

7）水表反馈外部认证主密钥在使用时首先利用用户卡序列号进行密钥分散，生成水表反馈外部认证工作密钥，与用户卡配对使用。

8）密钥修改外部认证密钥主要用于控制对 ESAM 中除水表主控密钥外其他密钥的更新，认证通过后利用水表主控密钥对其他密钥进行密文修改，与用户卡配对使用。

4. 累计用水量文件

★累计用水量文件（文件标识符：0001）

数据项	长度/B
表累计用水量	2×3

由于表累计用水量文件为“钱包文件”类型，存储动态表累计用水量的绝对值的反，数值类型为 6 位 3 字节二进制数。初始值为 FFFFFFH，最大计数递减为 000000H，转换为 BCD 码为 16777215，若按每天使用 1000m^3 水计算，可记录约 45 年的用水量。该水量可以被自由扣减和读取，但必须通过生产设置外部认证后才能够进行增款操作。

5. 水表基本信息文件

★水表基本信息文件（文件标识符：0002）

数据项	长度/B	数据项	长度/B
水表表号	7	透支限额	3
用户号	6	充值限额	3
用水种类	1	扣卡水量	3
报警水量	3	表累计量小数位	1

水表基本信息文件中的数据不一定每次插卡都进行更改，只有在修改基本参数的命令存在时，才进行更改。

用户卡不能对水表基本信息文件中的水表表号和表累计量小数位进行修改，这两项数据必须通过设置卡进行设置或更改，但设置卡可以对所有数据进行修改。

6. 水量信息文件

★水量信息文件（文件标识符：0003）

数据项	长度/B	数据项	长度/B
表本次购水量	3	未完成 MAC2 码	4
购水时间	3	未完成 TAC 码	4
累计购水量	3	未完成购水量	4
累计应急购水量	3	应急购水卡未完成交易序号	2
应急购水卡本次购水量	3	应急购水卡未完成 MAC2 码	4
表消费交易序号	2	应急购水卡未完成 TAC 码	4
未完成交易序号	2	应急购水卡未完成购水量	4

1）初始化后累计购水量和累计应急购水量单元数据为零，本次购水有效后，将本次购水量累加到累计购水量单元。

2）在水量信息文件中保留由于意外插卡造成交易未完成时的交易记录，以便在下次将用户卡插入时，水表可以根据实际情况将上次未完成的交易补充完成。在设计中为用户卡和应急购水卡各保留一次机会。

7. 水表运行信息文件

★水表运行信息文件（文件标识符：0004）

数据项	长度/B	数据项	长度/B
计量脉冲数	1	低电压次数	1
水表工作状态字	1	表月累计用水量	36
磁干扰次数	1	当前日历	3
读卡错次数	1		

计量脉冲数和水表工作状态字都在电池进行更换时进行写入 EEPROM 的工作，平时数据存放在 RAM 中，当前日历每天在日历变化时写入一次。表月累计用水量在每个自然月开始时将表累计用水量写入相应的月累计用水量单元。

8. 临时信息文件

★临时信息文件（文件标识符：0005）

数据项	长度/B
自定义	1

临时信息文件主要用来在数据处理过程中对数据进行暂态存储使用，可以根据实际编程情况自行定义。

5.5.2　CPU 卡读写接口设计

以美国 TI 公司的 MSP430 单片机为例实现对 CPU 卡的读写操作。

1. CPU 卡的读写接口硬件设计

CPU 卡的外部引脚有 8 根，实际用到的有 5 根，即 VCC、RST、CLK、GND 和 I/O 口线，卡座上还有一根引脚 KEY 用来判断 IC 卡是否插入卡座。MSP430F413 是 64 脚封装，有 48 根通用 I/O 引脚。这里采用 P6 端口的部分口线作为 I/O 线与 CPU 卡通信。

从安全性和低功耗方面考虑，CPU 卡的电源和时钟是受单片机控制的，在 CPU 卡未插入卡座时，不应给卡座供电，也不应输出时钟信号。在电路中，晶体管 V13、V16 用来保证对电源和时钟的控制。单片机 P6.0 引脚用来控制给 CPU 卡上电及内部时钟输出，该引脚平时为高电平，当有卡插入时输出低电平。

引脚 P1.1/TA0/MCLK 用来提供 CPU 卡的时钟信号，当不需要外围元器件工作时，可以关闭该时钟信号以降低功耗。

引脚 P6.1 用来控制 CPU 卡的复位。CPU 卡采用的是低电平复位方式，当 CPU 卡工作时引脚 P6.1 平时为高电平。

引脚 P6.2 用来实现 CPU 卡和单片机的双向数据通信，由于 CPU 卡的 I/O 口线采用的是集电极开路方式，使用时要在口线外接上拉电阻 R44。

引脚 P6.3 用来检测是否有卡插入卡座，当有卡插入时，单片机给出电源和时钟信号，与 CPU 卡进行数据传输。

CPU 卡座的接口电路如图 5-9 所示。

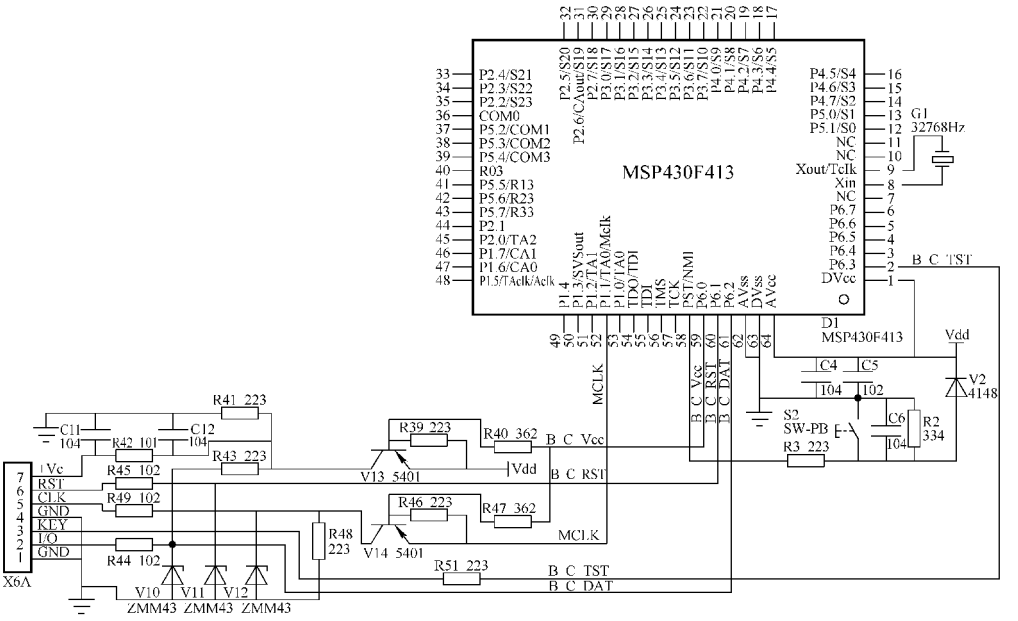


图 5-9　CPU 卡座的接口电路

2. CPU 卡的读写接口软件设计

CPU 卡在数据传输方式上采用的是串行异步半双工方式，在对 CPU 卡进行读写设计时，需要计算出在 I/O 口线上数据的位宽，以保证通信的正确。MSP430 单片机由于采用了数字控制振荡器（DCO）技术，系统提供的时钟频率是可调的，所以可根据系统要求的时钟频率对基础时钟模块进行设置，以得到准确的时钟信号。在设计读写程序时，应遵循 ISO/IEC 7816 标准规定的流程进行编程，保证正确地接收复位信号，正确地发送命令并根据每条命令的格式接收到正确的返回数据或状态标志。

（1）基本时间单位（ETU）

由于 CPU 卡是采用串行异步半双工方式与终端通信，由终端向 CPU 卡提供时钟信号，并以此来控制数据传输的时序，所以在程序设计前应先计算出准确的基本时间单位（ETU），它是指 I/O 口线上传输的数据位宽度，其计算公式为

$$\mathrm{ETU} = 372/f \tag{5-1}$$

式中，f 为时钟频率，一般在 1 ~ 5MHz 之间选择。当时钟频率为 3.57MHz 时，传输的速率为 9600 波特率。

（2）对 MCLK 的软件设置

MCLK 可用来给 CPU 卡提供时钟信号。MCLK 的时钟源来自数字控制振荡器（DCO），MSP430 的 DCO 被集成在 FLL（锁频环）+时钟模块中，该模块产生的时钟信号 f_{DCOCLK} 可以作为 MCLK 或 SMCLK。f_{DCOCLK} 的计算公式为

$$f_{\mathrm{DCOCLK}} = f_{\mathrm{CRYSTAL}} \cdot D \cdot (N+1) \tag{5-2}$$

或者

$$f_{\mathrm{DCOCLK}} = f_{\mathrm{CRYSTAL}} \cdot (N+1) \tag{5-3}$$

式中，D 的取值分别为 0，2，4，8。当 $D=0$ 时，f_{DCOCLK} 由式（5-2）得到；其他情况由式（5-3）得到。

N 的默认值为 31，最大值为 127，可根据 MCLK 的需要进行设定。

f_{CRYSTAL} 是晶振频率，电路图中给出的是 32768Hz。

MCLK 的值是由以上三个参数确定的。当 $D=2$，$N=63$ 时，MCLK 的值为 4.196MHz，以充分利用 MSP430 和 CPU 卡的高速性能。

（3）CPU 卡的上电复位

在对 CPU 卡读写操作前，必须对它进行正确复位。CPU 卡的复位操作要严格按照 ISO/IEC 7816 的时序要求进行，其上电复位时序如图 5-10 所示。

具体的复位过程是，VCC 信号先有效，在 200 个时钟周期内加上 CLK 时钟

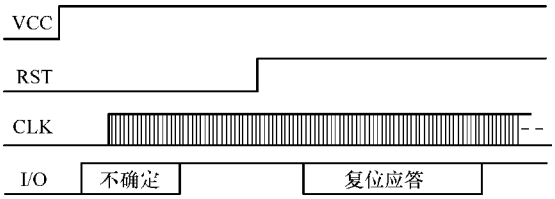


图 5-10 CPU 卡的上电复位时序

信号；之后，在 200 个 CLK 内，I/O 口线应被置于接收状态；CLK 有效后，RST 应保持至少 400 个 CLK 的低电平状态，之后卡复位，RST 被置为高电平。I/O 口线给出的复位应答信号应在 RST 的上升沿之后 400 ~ 40000 个时钟周期内开始。

需要注意的是，当加上 CLK 信号后，RST 的低电平保持时间至少要保持 400 个时钟周期；当 RST 变为高电平后，要延迟 400 个时钟周期才能开始接收复位应答信号；否则将不能收到正确的复位应答字节。

CPU 卡复位应答的源程序如下：

```
; ***************P6 端口定义*****************
ICPOWER    SET    1H          //IC 卡的电源引脚
ICRST      SET    2H          //IC 卡的复位引脚
ICIO       SET    4H          //IC 卡的数据引脚
Ic_ Ok     SET    8H          //IC 卡插到位引脚
; ********YGICFLAG0、1 标志位定义*********
#DEFINE  CARDPRO_ ERR  02H, &YGICFLAG0     //0—读写卡操作正常；1—
                                             读写卡错误
#DEFINE  ICXOR  40H, &YGICFLAG1            //卡传来的校验和
#DEFINE  MXOR  80H, &YGICFLAG1            //CPU 计算的校验和
; **************定义特殊寄存器**************
#define    CNTREG    R5            //发送或接收数据的位数（常为 8 位）
; ***************用户寄存器*****************
sfrB        YGICFLAG0 =200h        //标志寄存器 0
sfrB        YGICFLAG1 =201H        //标志寄存器 1
sfrb        RESETCNT =206H         //复位应答计数器
sfrb        ERRCNT =207H           //错误计数器
```

```
sfrb        TRDATA = 20AH            //收发字符寄存器
sfrw        DELAYCNT = 24AH          //延时寄存器

RSTDATABUF    SET    2A0H           //复位信号存放的区域，共 13B
; ****************************************
; CARDRESET：复位应答子程序
;              接收 13 个应答信号，存放在 RSTDATABUF 开始的区域
; ****************************************
CARDRESET:
    CLR.B  YGICFLAG1
    MOV.B  #8, CNTREG
    CLR.B  &TRDATA
    MOV    #RSTDATABUF, BX
    MOV.B  #13, &RESETCNT
RST_ IC:
    BIS.B  #ICPOWER, &P6OUT          //引脚状态初始化
    BIS.B  #ICIO, &P6OUT
    BIC.B  #ICRST, &P6OUT
    BIS.B  #ICPOWER + ICIO + ICRST, &P6DIR
    BIC.B  #IC_ OK, &P6DIR
    BIC.B  #CARDPRO_ ERR

    CALL   #DELAY1ETU

    MOV.B  #0FH, &SCFI1               //对时钟频率进行设置
    BIS.B  #DCOPLUS, &053H
    MOV.B  # (64 -1), &SCFQCTL        //MCLK = 4.196MHz
    MOV.B  #40H, &SCFI0
    BIS.B  #02H, &P1DIR               //使 P1.1 为时钟输出
    BIS.B  #02H, &P1SEL
    BIC.B  #ICPOWER, &P6OUT          //上电
    BIS.B  #ICPOWER, &P6DIR
```

```
    CALL   #DELAY05ETU

    BIC.B  #ICIO, &P6DIR              //把口线置为接收状态
    CALL   #DELAY1ETU
    CALL   #DELAY1ETU
    CALL   #DELAY1ETU

    BIS.B  #ICRST, &P6OUT             //把 RST 置高
    CALL   #DELAY1ETU

RST_A:
    CALL   #RECCHAR                   //接收 13 个复位字符
    BIT.B  #C, SR                     //判断错误标志位，为低表示正常
    JNZ    RST_ERR
    MOV.B  &TRDATA, 0 (BX)
    INC    BX
    DEC.B  &RESETCNT
    JNZ    RST_A
    RET
RST_ERR:
    BIS.B  #CARDPRO_ERR               //将错误标志置 1
    RET

; ****************************************
; DELAY1ETU：延时 1 个 ETU 子程序
; ****************************************
DELAY1ETU:                            //TOTAL:   372 (INCLUDE CALL)
    MOV  #120, DELAYNUM               //2
DLY_WAIT:
    DEC    DELAYNUM                   //1
    JNZ DLY_WAIT                      //2
    NOP
```

```
    NOP
    RET                                 //3
; ****************************************
```

（4）CPU 卡的下电

CPU 卡正确复位后，就可以开始执行各种交易。在交易结束后，要对卡执行下电操作，以正确地释放各触点。在下电过程中，首先要将 RST 置为低电平，然后将 CLK 置低，之后将 I/O 口线置低，最后 VCC 被置低。其下电时序如图 5-11 所示。

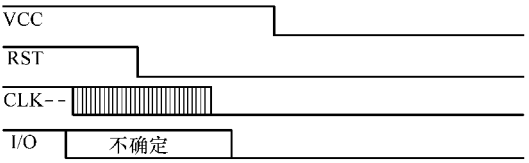


图 5-11　CPU 卡的下电时序

```
; ****************************************
; CARDDOWN：CPU 卡下电子程序
; ****************************************
CARDDOWN:
    BIS.B  #ICPOWER, &P6DIR
    BIC.B  #ICRST, &P6OUT
    NOP
    NOP
    BIC.B  #ICIO, &p6DIR
    BIS.B  #ICPOWER, &P6OUT
    RET
; ****************************************
```

（5）接收字符程序

按照 ISO/IEC 7816 标准，CPU 卡的字符帧格式为 1 个起始位、8 个数据位、1 个奇偶校验位和 1 个停止位，其中起始位为低电平，停止位为高电平。在接收字符时应注意，应把接收到的校验位和本地计算的校验位进行比较，相一致则继续接收字符，否则转为发送态，要求重发字符。错误次数不超过 3 次。其流程如图 5-12 所示，可以根据该流程设计出一个完整的接收字符程序。

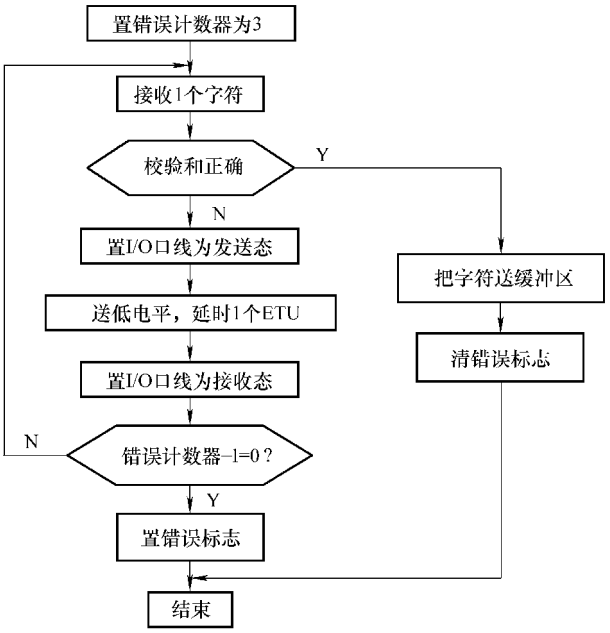


图 5-12　CPU 卡接收字符流程

该接收字符的源程序如下：

```
;* * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * *
;RECCHAR:接收字符子程序
;          收到的字符存放在 TRDATA 寄存器中
;* * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * *
RECCHAR:
    MOV.B   #3,&ERRCNT          //错误计数器赋值
RECCHAR1:
    CLR.B   YGICFLAG1           //清标志
    MOV.B   #8,CNTREG
    CLR.B   &TRDATA
    MOV.W#40000,&DELAYCNT
RECC_IC:
    BIC.B   #ICIO,&P6DIR        //将数据口设为输入口
    BIT.B   #ICIO,&P6IN         //判断起始位,不超过 40000 个 CLK
    JZ      RECC_WAITIC05
    JMP     RECC_DEL
RECC_WAITIC05:
```

```
    CALL    #DELAY05ETU
    BIT.B   #ICIO,&P6IN
    JZ      RECC_BEGIN
RECC_DEL:
    DEC.W   &DELAYCNT
    JNZ     RECC_IC
    BIS.B   #C,SR                   //超时,置 C=1
    RET

RECC_BEGIN:
    CALL    #RECONEBYTE             //接收一个字符,存入寄存器 TRDATA 中
    BIT.B   #ICXOR                  //判断校验和
    JNZ     RECC_CMP1
    BIT.B   #MXOR
    JZ      RECC_OK
    JMP     RECC_CMPERR

RECC_CMP1:
    BIT.B   #MXOR                   //MXOR=1?
    JZ      RECC_CMPERR             //=0,ERR

RECC_OK:                            //校验和正确,延时 1 个 ETU,清标志,子程序
                                      返回
    CALL#DELAY1ETU
    CLRC
    RET

RECC_CMPERR:                        //校验和错误
    BIS.B   #ICIO,&P6DIR            //置 I/O 口线为发送态
    BIC.B   #ICIO,&P6OUT            //送低电平
    CALL    #DELAY1ETU              //延时 1 个 ETU
    BIS.B   #ICIO,&P6OUT

RECC_AGAIN:
    CALL    #DELAY1ETU
```

```
    DEC. B   &ERRCNT
    CMP. B   #0,&ERRCNT          //错误计数器不为 0,重新接收字符
    JNZ      RECCHAR1
    SETC                         //错误计数器为 0,置错误标志,子程序返回
    RET
;* * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * *
```

(6) 发送字节程序

在发送字符时，要根据 ISO/IEC 7816 标准的规定，在发送完校验位后，转为接收态，在下一个 ETU 时，若 I/O 口线为高电平，则表明字符已正确的发送，可以转为发送态发下一个字符；若 I/O 口线为低电平，则表明通信错误，应重发原字符。超过 3 次错误，则退出发送状态。发送字符的流程如图 5-13 所示。

有了发送和接收字符程序，就可以很容易地设计出发送和接收字符串程序，进而根据 CPU 卡的各种操作命令流程设计出各交易程序。

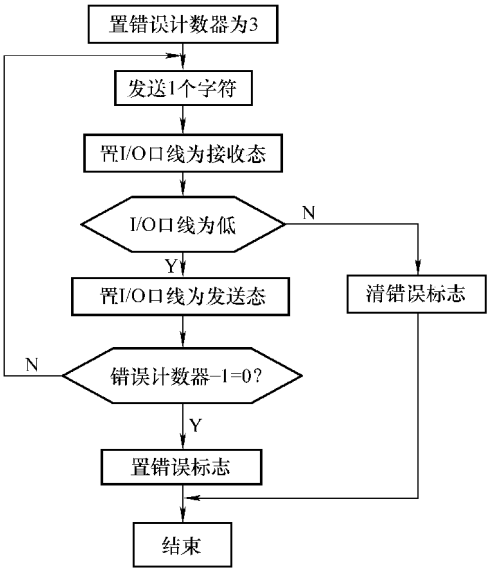


图 5-13 CPU 卡发送字符流程

该发送字符的源程序如下：

```
;* * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * *
;SENDCHAR:发送字符子程序
;                发送的字符存放在 TRDATA 寄存器中
```

```
;* * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * *
    SENDCHAR:
    MOV.B  #3,&ERRCNT          //错误次数为 3 次
SCHAR1:
    CLR.B  YGICFLAG1           //清标志
SCHAR_IC1:
    BIS.B  #ICIO,&P6DIR        //将数据口设为输出口
    BIC.B  #ICIO,&P6OUT
    CALL   #DELAY1ETU
    BIS.B  #ICIO,&P6DIR
    CALL   #SENDONEBYTE        //发送 1 个字符
    BIC.B  #ICIO,&P6DIR        //将数据口设为输入口
    CALL   #DELAY05ETU
    BIT.B  #ICIO,&P6IN         //判断 I/O 口线,为高则正确发送
    JZ     SCHAR_ERR

SCHAR_OK:
    CALL   #DELAY05ETU         //1 个字节发送完毕
    CALL   #DELAY1ETU
    CLRC
    RET

SCHAR_ERR:                     //发送错误
    CALL   #DELAY1ETU
    BIS.B  #ICIO,&P6DIR        //将数据口设为输出口
    CALL   #DELAY1ETU
    DEC.B  &ERRCNT
    JNZ    SCHAR1              //错误计数器不为 0,重新发送
    SETC                       //错误计数器为 0,将错误标志置 1,子程序返回
    RET
;* * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * *
```

5.5.3 CPU 卡水表管理信息系统

CPU 卡水表管理信息系统（MIS）是集用水计量、统计管理和售水操作为一体的计算机管理系统。

1. 对 CPU 卡水表管理信息系统的要求

1）对操作员的管理：操作员在登录和使用管理系统时必须使用 PKEY（电子钥匙）进行安全认证，通过后才能进入和使用管理系统，同时还可以实现对操作员的使用权限进行有效控制和管理。

2）对交易进行控制：使用双卡座读写器，在对用户卡进行交易写卡过程时必须通过 PSAM 卡对用户卡进行安全认证后才能进行，以有效杜绝非法用户卡及对用户卡的非法操作。

3）数据库的安全保证：选用关系型数据库，对数据库的读写操作进行权限控制，保证黑客不能够通过其他操作环境非法改写数据库。对数据库的操作只能在计费管理系统中进行，并且每项操作都有工作日志记录。

4）良好的数据交换接口：可以根据需要，将计费管理系统中的各种数据查询统计报表转换输出，便于与其他管理信息系统进行数据交换。

5）安全的数据库导出和导入措施：为防止数据丢失和损坏，提供对数据库的备份和恢复，管理方可以根据需要采用定时数据库备份导出，一旦发现硬盘介质损坏，可以方便地进行数据库导入。

6）良好的人机交互形式：系统界面设计应简明易懂，便于用户学习操作。

2. CPU 卡水表管理信息系统的组成

CPU 卡水表管理信息系统由计算机、PKEY（电子钥匙）、IC 卡读写器、CPU 用户卡以及 CPU 卡水表五个部分组成。组成示意图如图 5-14 所示。

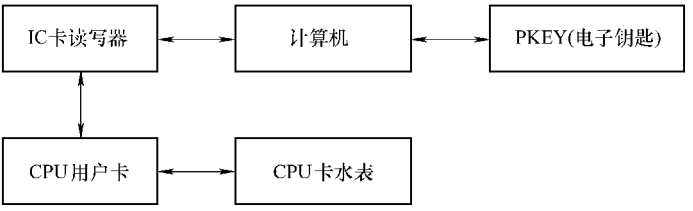


图 5-14 CPU 卡水表管理信息系统组成

计算机是整个 CPU 卡水表管理信息系统的核心，主要完成对用户以及表数据信息的管理、数据的查询统计、交易信息记录等功能。

PKEY（电子钥匙）通过计算机的串行口或 USB 口进行连接，主要用来对操作员进行身份认证，不同的操作员有不同的 PKEY，操作员只有插入 PKEY 才能登录 CPU 卡水表管理信息系统。

IC 卡读写器通过计算机的串行口进行连接，通过 IC 卡读写器可以对各种不同用途的 CPU 卡进行安全认证和数据读写操作。

CPU 用户卡由用户持有，是管理系统与 CPU 卡水表进行数据交换的介质。用户卡将用户交易信息以及参数设置信息传递到 CPU 卡水表，将表的计量信息和运行状态信息传递到管理信息系统。

CPU 卡水表用来完成对用户计量以及控制的功能，当用户购买的水量用完后，自动关闭阀门，切断供应。

3. CPU 卡水表管理信息系统软件的主要功能

CPU 卡水表管理信息系统软件主要包括五个功能模块：用户管理模块、设备和水价管理模块、查询模块、统计模块和系统维护模块，如图 5-15 所示。

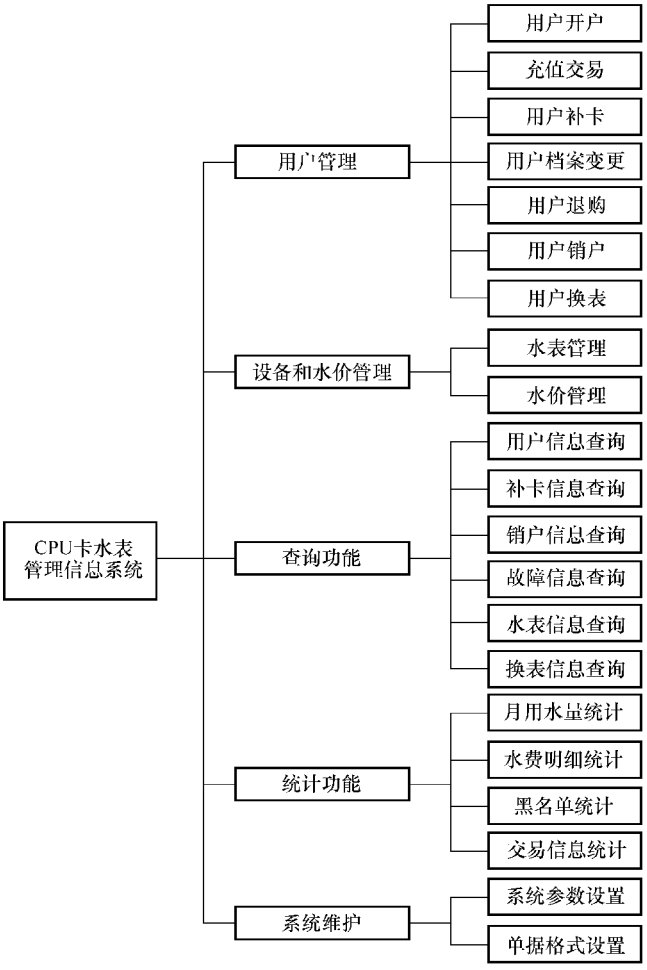


图 5-15　CPU 卡水表 MIS 软件功能

（1）用户管理模块

用户管理模块包括开户、充值交易、结算阶梯水价、用户档案变更、补卡、退购、销户和换表操作。

1）开户：在系统中未存有信息的新用户，必须先执行开户操作，才能进行其他的操作。开户功能在系统的数据库和用户卡中保存了新用户的相关信息。

2）用户档案变更：开户时，若用户信息输入有误，可将错误的用户信息改正过来。

3）充值交易：为用户完成购水交易，根据用户的购水量计算销售金额并为用户打印收据，并将购水量信息以及相关参数信息写入用户卡，同时将用户卡中表计量信息和工作状态信息读回管理系统中。

4）退购：用户卡购水后，如果再要求改变其购水量，可通过退购来折合金额。

5）补卡：用户丢失用户卡后，可购买新的用户卡，将原有的用户信息补写进新卡中。

6）销户：此功能在用户脱离本系统的管理范围时，销除用户信息并对用户水量进行结算。

7）换表：此功能用来记录用户的水表出现故障或有其他原因时，必须进行更换新表操作的相关信息。

（2）设备和水价管理模块

对管理方所拥有的 CPU 卡水表和现行的水价进行管理。

1）水表管理：管理方对已购买的 CPU 卡水表进行统一固定资产管理，包括增加、删除和修改功能。

2）水价管理：可以通过此功能设置各种所需的价格、进行调价和删除操作。

（3）查询模块

查询模块包括用户信息查询、补卡信息查询、销户信息查询、故障信息查询、用户水表信息查询和换表信息查询等操作。

1）用户信息查询：查询在本系统中已开户的用户相关信息。

2）补卡信息查询：查询用户补卡的信息。

3）销户信息查询：查询在本系统销户的用户、日期和退还的金额。

4）故障信息查询：查询用户水表目前阀门、电池和 ESAM 的状态。

5）用户水表信息查询：查询在本系统中已有记录的用户水表信息。

6）换表信息查询：查询用户使用水表更换情况。

（4）统计模块

对月用水量、水费明细、黑名单、当前余额以及交易信息进行统计并生成报表打印输出，提供采用多种查询方式，使用方便灵活。

（5）系统维护模块

系统维护模块是对包括系统参数、水表参数和打印单据格式等的设置操作。

1）系统参数：

① 基本参数设置：对读写卡器端口及表内的预置值、报警水量、限购水量、充值限额等参数的设置。

② 水表参数：可以新增、保存、删除水表的相关参数。

③ 水表位置：记录水表安装的默认位置。

2）设置单据格式：能够对要打印的单据包括开户单、补卡单、销户单、退购单等进行格式设置和项目选择。

第 6 章　智能卡燃气表

本章从安全因素角度考虑，介绍了智能卡燃气表的操作规程；给出了智能卡和 ESAM 卡的文件设计；分析了远传抄表的通信协议；设计了基于 NEC 单片机的远传燃气卡表，阐述了其系统架构、系统各部分的硬件电路和软件模块，给出了系统测试结果。

6.1　智能卡燃气表可操作性

与智能卡电表一样，影响智能卡燃气表安全性的因素可以分为卡片介质的安全性、表计生产过程的安全性和运行管理的安全性。考虑到这些安全因素，对智能卡燃气表的可操作性体现在四个方面：用户卡开户过程、用户卡操作过程、补卡过程和故障表维护过程。

1. 用户卡开户过程

用户卡开户过程要完成用户信息、燃气表信息以及用户卡的对应。这个过程应尽量流程简便，以避免用户在银行和燃气管理部门之间的多次往返。由于是银行发卡，考虑到银行的使用对象是个人，而燃气表的使用对象是户，为方便用户，应该考虑一表多卡的情况。如果仅从方便性来讲，可以取消户号，在用户卡中也用钱包文件存储购气量，用户可以根据自己的需要，将所购气量输入到任何一块表中；如果考虑表计信息回传或补卡需要，可以设置户号，但允许一户中多个成员使用一个户号以便任何人都可以持卡购气。在用户卡上用钱包文件存储购气量的好处是可以根据限制条件一次或多次将购气量输入到燃气表中，从而有效防止用户囤积气量。用户户号由燃气集团编制，通过开户单传给用户，每一个用户中的成员都可以持开户单到银行申请办理用户卡业务并进行购气，在银行数据库中，以户号为索引为每个成员分别建立账务信息。

2. 用户卡操作过程

考虑到用户使用过程中，插拔用户卡的随意性，应该尽量使用户卡与燃气表进行数据交换的时间降到最短，以避免由于用户在数据处理过程中将卡拔出而造成的数据错误，给用户购气过程造成不方便。从这个角度来讲，应尽量减少数据项(尤其是从表中返传的数据项)，并尽可能地将数据一次读取或一次写入。

用户在使用过程中，如果由于购气量用完造成不能继续用气，而当时用户又不能方便地购气，应该允许用户采用应急透支的方式暂时继续用气，可以根据需要设

定透支门限，在用户下次购气时将透支值扣除。

考虑到燃气表在应用过程中存在参数修改的可能性，可以将某些参数通过用户卡进行传递，在用户购气过程中对燃气表进行修改。

3. 补卡过程

当用户卡遗失后，应该能够重新给用户补发用户卡。最简单的方式是直接补给用户一张卡片，对用户遗失卡片中的购气数据不再补发，损失部分用户自己负责，这样用户补完卡就同时可以进行下次购气。如果要为用户将遗失卡片的购气数据补回，则需要用户补完卡后将卡插入燃气表，根据带回的数据进行运算，补写上次购气量并同时进行本次购气。这样操作流程则复杂一些，需要用户跑两次。折中一点的方案是用户补完卡后就进行下次购气，不核算补写购气量，等用户再次购气时，由于用户卡已经将燃气表中数据带回，这时再替用户核算补写购气量并进行新的购气交易。

4. 故障表维护过程

在燃气表安装过程或在运行时由于某种原因都有可能造成需要对现场燃气表中的数据进行修改，这时需要有工具卡对燃气表进行操作，这种操作应该有别于燃气表生产厂家在生产过程中修改燃气表数据的操作。要杜绝生产卡未经授权可以在运行现场使用。应该设计一种现场数据设置卡，这种卡使用运行密钥，里面的设置参数可以灵活设置，插卡一次就应该将燃气表数据修改完毕。

6.2　智能卡燃气表卡片文件设计

6.2.1　用户卡文件

用户卡由于要通过银行完成购气交易，并有可能和银行联名发卡，因此可以考虑选择容量较大的卡片，并预留较大的空间拓展其他应用。

1. 卡片结构

用户卡片结构如图 6-1 所示。

2. 文件说明

用户卡由用户持有，主要用来将用户购买的气量传递到燃气表中，并将燃气表中的信息回传到管理中心。同时完成两种辅助功能，在管理系统需要的时候，还可以进行燃气表参数设置和燃气表密钥更新操作。

由于涉及与银行联名发卡，因此将燃气表应用开辟为一个应用目录，主文件由银行进行操作管理。

在主文件下有两个应用文件。

1）用户基本信息文件用来存储用户姓名、身份证号等信息。

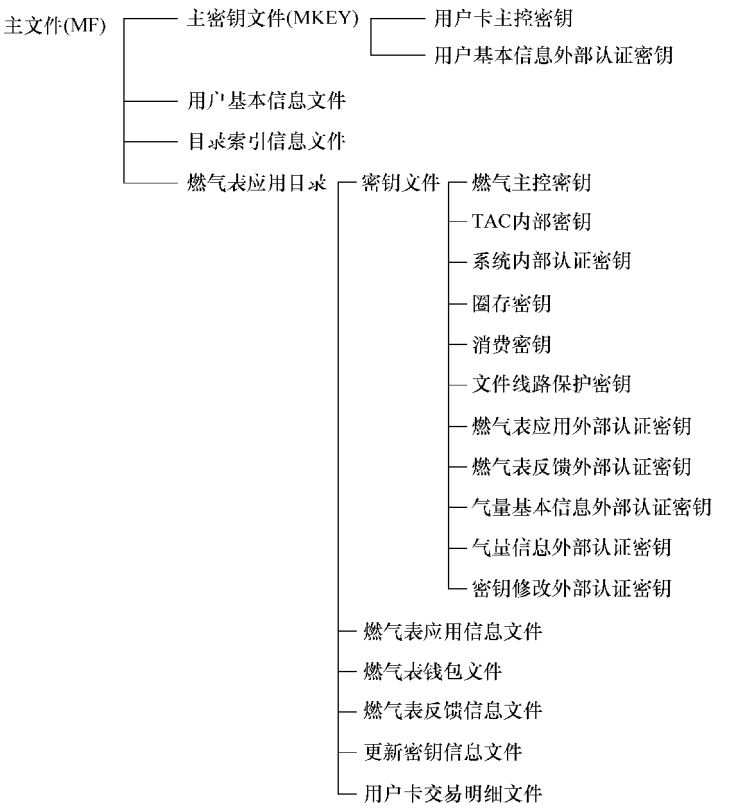


图 6-1　用户卡结构

2）目录索引信息文件用来存储在主文件下开通的目录文件的目录标识符或目录名称，以便管理系统对目录应用进行选择。

在燃气表应用目录下有五个应用文件。

1）燃气表应用信息文件用来存放用户号、卡标识、购气信息以及燃气表参数设置信息等内容。

2）燃气表钱包文件采用标准金融钱包，用来存放本次用户的购气量，在管理系统以圈存交易方式存入用户卡钱包文件，在燃气表中以消费交易方式读入燃气表 ESAM 中。

3）燃气表反馈信息文件用来存放燃气表返回到管理系统的数据信息，包括燃气表表号、相关购气信息、相关用气信息、燃气表工作状态信息等内容。

4）更新密钥信息文件用来存放通过用户卡更新密钥的密文信息，它只在需要的时候使用，平时内容为空。燃气表将密钥密文内容读入后将其内容擦除。

5）用户卡交易明细文件用来存放燃气表进行圈存和消费交易的历史数据，便于进行数据查询和数据恢复。

为了保证数据传输的安全性，用户卡中燃气表应用信息文件的数据在更新时使用文件线路保护密钥进行加密写入，这样可以有效杜绝第三方对用户卡片内容的攻击和篡改。

3. 密钥说明

密钥系统根据文件的定义划分为两级，即主文件下的主密钥文件和燃气表应用目录下的密钥文件。

主文件的主密钥文件下有两条密钥。

1）用户卡主控密钥由发卡方采用明文进行安装，而卡片上其他密钥的安装都需要在主控密钥的控制下进行密文安装。

2）用户基本信息外部认证密钥用于对主文件下用户基本信息文件和目录索引信息文件内容的操作进行控制，只有通过该密钥认证后才能对数据进行写入和更新。在用户卡主控密钥的控制下进行密文安装。

燃气表应用目录的密钥文件下有 11 条密钥。

1）燃气主控密钥在用户卡主控密钥的控制下进行密文安装，用来控制燃气表应用目录下其他密钥的安装。

2）TAC 内部密钥用于在用户卡进行圈存交易和消费交易时进行 TAC 码计算。在燃气主控密钥的控制下进行密文安装。

3）系统内部认证密钥用来验证是否和 ESAM 是一个系统发行的。在燃气主控密钥的控制下进行密文安装。

4）圈存密钥用于在用户卡进行圈存交易时计算 MAC1 码。在燃气主控密钥的控制下进行密文安装。

5）消费密钥用于在用户卡进行消费交易时计算 MAC1 码。在燃气主控密钥的控制下进行密文安装。

6）文件线路保护密钥用于对燃气表应用信息文件的数据进行加密写入。在燃气主控密钥的控制下进行密文安装。

7）燃气表应用外部认证密钥用于对燃气表应用信息文件内容的操作进行控制，只有通过该密钥认证后才能对数据进行写入和更新。在燃气主控密钥的控制下进行密文安装。

8）燃气表反馈外部认证密钥用于对燃气表反馈信息文件内容的操作进行控制，只有通过该密钥认证后才能对数据进行写入和更新。在燃气主控密钥的控制下进行密文安装。

9）气量基本信息外部认证密钥与 ESAM 配对使用。在燃气主控密钥的控制下进行密文安装。

10）气量信息外部认证密钥与 ESAM 配对使用。在燃气主控密钥的控制下进行密文安装。

11）密钥修改外部认证密钥与 ESAM 配对使用。在燃气主控密钥的控制下进行密文安装。

6.2.2 ESAM 文件

ESAM 由于安装在卡式燃气表中，是一个专用芯片，只负责完成密钥安全认证和表中数据存储，因此可以选择较小容量的芯片。

1. ESAM 结构

ESAM 结构如图 6-2 所示。

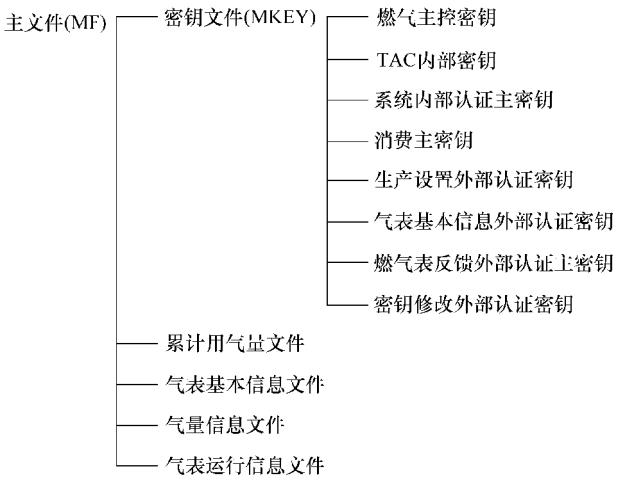


图 6-2 ESAM 结构

2. 文件说明

ESAM 安装在燃气表中，主要用来存放燃气表中的所有数据，并对数据的存放进行安全认证。

1）累计用气量文件用来动态存储燃气表的累计用气量信息。

2）气表基本信息文件用来存储燃气表表号、用户号、卡标识、燃气表运行参数、燃气表逻辑状态等信息。

3）气量信息文件用来存储燃气表中各个应用的本次购气量、累计购气量以及整个燃气表的累计购气量和应急购气量信息。根据北京燃气的需要，在一个燃气表中最多可以进行三个应用的操作，即可以做到一表对应三卡。

4）气表运行信息文件用来存储燃气表中表内气量、燃气表工作状态字、运行状态信息、12 个月累计用气量等信息。

3. 密钥说明

1）燃气主控密钥采用明文方式进行安装，用来控制 ESAM 中其他密钥的安装和更新。

2）TAC 内部密钥用于在燃气表进行消费交易时计算 TAC 码。

3）系统内部认证主密钥在使用时首先利用用户卡序列号进行密钥分散，生成工作密钥，与用户卡配对使用。

4）消费主密钥在使用时首先利用用户卡序列号进行密钥分散，生成工作密钥，与用户卡配对使用。

5）生产设置外部认证密钥用于对累计用气量钱包文件内容的操作进行控制，只有通过该密钥认证后才能对数据进行写入和更新。

6）气表基本信息外部认证密钥用于对气表基本信息文件内容的操作进行控制，只有通过该密钥认证后才能对数据进行写入和更新。

7）燃气表反馈外部认证主密钥首先利用用户卡序列号进行密钥分散，生成工作密钥，与用户卡配对使用。

8）密钥修改外部认证密钥用于对燃气表中密钥更改的操作进行控制，只有通过该密钥认证后才能对密钥进行更新。

6.3　远传抄表通信协议

燃气表远传抄表是指将用户燃气表中的数据抄出传递到管理方，对于管理方，最终需要建立一个管理平台，包含人工抄表数据、远传抄表数据以及 IC 卡预付费管理系统数据。因此设计远传抄表系统必须注意要有良好的兼容性和开放性。

各种远传抄表系统都需要数据采集器、数据集中器、手持抄表器等各种类型的中间设备，这些中间设备的功能要求大致相同，但各个厂家设计的完全不同，导致完全互不兼容，为此需要制定中间设备的设计规范，统一接口、尺寸、安装方式、数据协议，做到通用的中间设备可以在各种不同的远传抄表系统中使用。

这里提供一种远传抄表的数据通信协议，该协议分为三个层次，分别是物理层、数据链路层和应用层。

1. 物理层

采集器与远传燃气表之间的通信连接采用 RS485 串行通信电气接口，主从网络结构形式。RS485 接口的一般性能应符合下列要求：

驱动与接收端耐静电放电（ESD）：±15kV（人体模式）。

共模输入电压：－7 ~ ＋12V。

差模输入电压：大于 0.2V。

在传输速率为 1200bit/s 时，单用户点对点有效传输距离不小于 1200m。

2. 数据链路层

本协议为主从结构的半双工通信方式，通信波特率初始值为 1200，如果要调整，可以下发波特率变更指令，调整范围最高为 9600。传输字节格式采用 1 个起始位、8 个数据位，1 个校验位，1 个停止位，共 11 位。其位传输顺序为先传低位，后传高位。

采集器与燃气表之间的通信采用帧（数据包）的形式。帧格式如下：

起始标志	命令字	长度	数据	校验	结束标志

起始标志：1B，为数据包的开始标志。

命令字：1B。

长度：1B，十六进制整数，最大为 255，为数据区的长度。

数据：字节数由长度字节确定。

校验：1B，为命令、长度、数据三部分累加和计算所得的数据，为十六进制数。

结束标志：1B，代表数据包的结束。

传输控制：采集终端对燃气表发出指令后，若间隔 5s 没有收到响应，再次下发指令，若三次仍无响应，则标记此燃气表通信故障。

所有指令（除广播指令外），若燃气表未正确执行，一律返回如下格式的报错数据包：

数据项	长度/B	数据项	长度/B
起始字符	1	错误命令码	1
命令码	1	校验	1
数据长度	1	结束字符	1
燃气表表号	7		

3. 应用层

应用层主要描述采集器与燃气表之间进行数据交换的指令。

（1）实时抄收指令

将远传燃气表内的所有数据一次全部抄回。当远传燃气表接收到实时抄收指令后，首先核对燃气表表号，不对则不返回数据，若燃气表表号正确则返回数据帧。

★实时抄收指令：

数据项	长度/B	数据项	长度/B
起始	1	燃气表表号	7
命令	1	校验	1
长度	1	结束	2

★返回数据帧格式：

数据项	长度/B	数据项	长度/B
起始	1	大流量次数	1
命令	1	超小流量次数	1
长度	1	低电压次数	1
燃气表表号	7	磁干扰次数	1
累计用气量	3	燃气表工作状态字	1
冻结气量	3	校验	1
气量冻结日期	3	结束	1
表月累计用气量	3		

采集终端对远传燃气表进行数据抄收时，若发出的抄收指令未收到返回数据，则间隔 10s 再次下发抄收指令，若三次未收到响应，则标记此块远传燃气表通信故障，进行相应的处理。

（2）气量冻结指令

将远传燃气表内累计用气量进行冻结并进行存储。气量冻结指令如下：

起始标志　命令字　长度　燃气表表号　气量冻结日期　校验　结束标志

当远传燃气表接收到气量冻结指令后，将当前累计用气量数据存储到表内冻结气量单元，同时保存接收到的气量冻结日期。在处理时，远传燃气表首先判断燃气表表号，若燃气表表号为 FFFFFFFFFF 时表示为广播地址，接收到指令的远传燃气表都要执行气量冻结操作，执行完毕后无返传数据；当为固定的燃气表表号时，要进行表号比较，表号不对则不进行气量冻结操作，只有表号对应的远传燃气表才执行冻结操作指令，并将冻结结果返回。冻结正确返回数据格式为

起始标志　　命令字　　长度　　55　　校验　　结束标志

冻结错误返回数据格式为

起始标志　　命令字　　长度　　AA　　校验　　结束标志

冻结错误时将远传燃气表状态字中相应错误标志置 1。

（3）燃气表表号抄收显示指令

远传燃气表接收到此指令时，将燃气表表号返传。抄收指令格式如下：

起始标志　　命令字　　长度　　校验　　结束标志

远传燃气表返传数据格式如下：

起始标志　命令字　长度　燃气表表号　校验　结束标志

采集终端在接收到远传燃气表返回的数据帧后，将燃气表表号进行查新存储，并下发正确接收指令，远传燃气表收到采集终端的指令后，在显示器上显示燃气表表号的后 4 位，延时 10s 后自动熄灭。

正确接收指令格式如下：

起始标志　命令字　长度　55　校验　结束标志

此指令主要在燃气集团对用户进行开户时登录燃气表表号使用，以实现燃气表表号和用户户号的一一对应。

（4）燃气表表号预置指令

此指令用于在远传燃气表出厂前向远传燃气表内输入燃气表表号和累计用气量初值，并将远传燃气表内相关数据单元置为初始值。指令格式如下：

起始标志　命令字　长度　燃气表表号　累计用气量　校验　结束标志

远传燃气表正确接收该指令并完成操作后，返回格式如下：

起始标志　命令字　长度　55　校验　结束标志

若处理错误则返回格式如下：

起始标志　命令字　长度　AA　校验　结束标志

（5）预置累计用气量指令

当需要对用户正在使用的远传燃气表进行更换时，需将当前表计中的累计用气量输入到新更换的远传燃气表中，指令格式如下：

起始标志　命令字　长度　燃气表表号　累计用气量　校验　结束标志

远传燃气表接收并正确处理后返回格式如下：

起始标志　命令字　长度　55　校验　结束标志

若错误则返回格式如下：

起始标志　命令字　长度　AA　校验　结束标志

6.4　智能卡远传燃气表实例

6.4.1　基本功能

智能卡远传燃气表应具有以下基本功能：

1. 正确计量功能

系统的最终目标是准确计量。要确保用户每用单位气量时，气表计量一次。另外，在计量方式上，燃气营销公司可以根据需要设置用户购买的是金额或用气量（单位是元或 m^3），当选用金额计量方式时，加入了阶梯价格，以节约资源。

2. 预付费及用气控制功能

当燃气表内剩余气量（或金额）低于预设报警值时，系统将关闭阀门，液晶显示购气标志且蜂鸣器鸣叫，以提醒用户购气，此时只有插入用户卡才能打开阀门，恢复供气；当剩余气量减少到透支值时，燃气表将自动关阀、停止供气。只有当用户通过 IC 卡购买燃气并插卡后，可将购买量与燃气表内的剩余气量进行累加，自动恢复供气。

3. 阀门驱动及反测功能

主要实现阀门的开关控制，同时对阀门的到位信号进行反测，判断阀门是否工作正常。

4. 读写 IC 卡功能

应能正确地识别本系统 IC 卡，并对其进行读写。

5. 低电压检测功能

燃气表是采用电池供电，为了确保系统正常工作，在使用过程中需要对电池进行电压检测。当电池电压达到预设报警值或被取出时，系统应关闭阀门，声音报警并显示换电池标志，以提示用户更换电池。

6. 阶梯价格设置功能

可以通过参数设置卡或数据远传模式对燃气表中的价格进行设置和修改，并可以根据实际需要设置多级气价。

7. 数据掉电存储功能

当电池电压过低或被取出时，燃气表中的重要数据不能丢失，必须准确无误地保存下来，确保系统复位后，能被重新读入。

8. 报警功能

当燃气表中剩余气量不足、电池电压低、存在磁干扰、读卡错误等情况时，进行蜂鸣器报警和液晶显示报警。

9. 防窃功能

当有强磁场干扰燃气表正常采样时，系统将关闭阀门，停止供气。当强磁场消失后，用户插入 IC 卡方可重新打开阀门恢复用气。

10. 防气量囤积功能

当燃气表中的剩余值和本次购买值之和大于等于充值限额时，拒绝将当前购买值读入到燃气表中，避免用户过多购气囤积购买值。

11. 低功耗功能

考虑到燃气表的防爆安全性，不能用 220V 的市电供电。应采用电池供电，为了延长电池的使用寿命，系统应具有低功耗功能。

12. 数据远传功能

为实现数据的实时传输，采用远程通信方式实现数据远传功能。

6.4.2　系统总体架构

智能卡远传燃气表系统设计了两种数据通信方式实现燃气表与监控中心的数据交互：一种是远传通信方式，燃气表采用 RS485 总线与数据集中器相连，通过通信网络与互联网的无缝连接，监控中心接收燃气表中的用户数据并对之进行分析处理；另一种方式是 IC 卡通信方式，通过 IC 卡将用户数据送给工作站，再由网络将用户数据传输到监控中心，如图 6-3 所示。

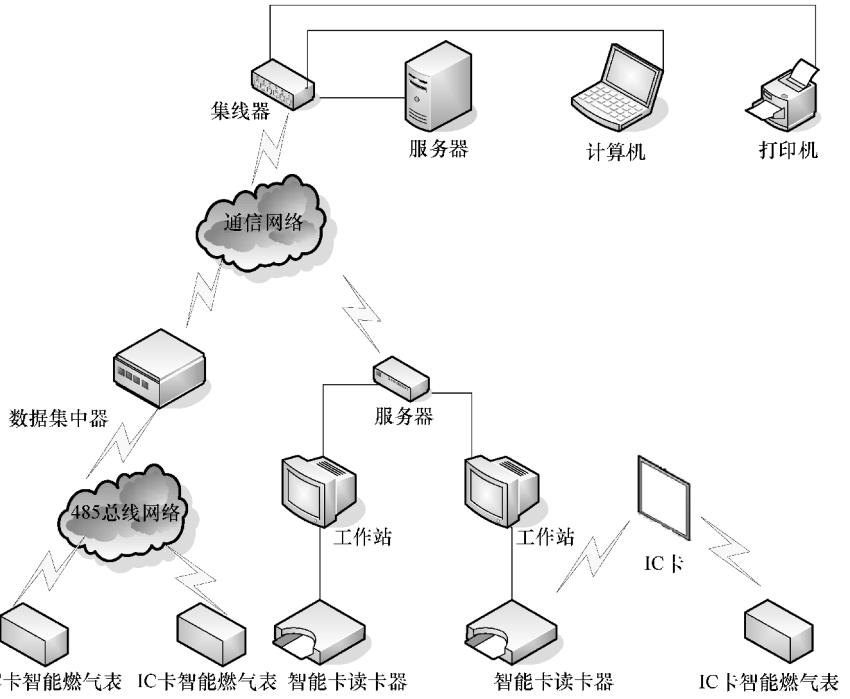


图 6-3　系统总体架构

6.4.3　系统硬件设计

6.4.3.1　系统工作原理

IC 卡远传燃气表以机械式燃气表为基表，由光电或霍尔元件采样将基表的气体流量信号送给单片机进行处理，单片机将该信号与表内燃气量或金额进行计算，并与设定报警值进行比较，当减至设定报警值后，将发出提示信号并关阀一次以提醒用户提前购气；当用户再次插入空卡时气表会重新恢复供气，直到剩余气量（或金额）为零关闭阀门。如果燃气公司设置该系统具有透支功能，则即使剩余气量（或金额）减为负数后，只要未达到系统设定的透支值，用户可继续用气，当

用户重新购买燃气后，系统会自动减去已透支部分。由于在设计中加入了对金额的扣除功能，随着燃气供需关系的变化，可以在表内对用户的用气量进行阶梯计价，以及实时更新价格，有利于燃气资源的合理有效使用。

系统硬件电路包括低功耗单片机、计量传感器电路、阀门控制电路、卡座控制电路、电压测试电路、液晶显示屏、声音报警电路和通信接口模块等，如图 6-4 所示。

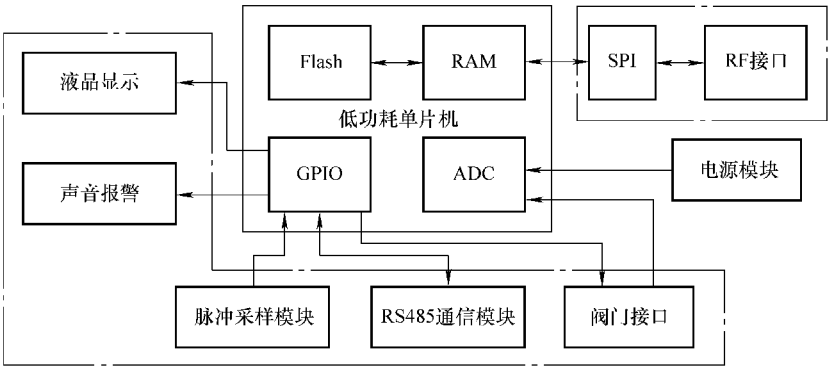


图 6-4　IC 卡智能燃气表硬件框图

6.4.3.2　低功耗单片机

低功耗单片机是燃气表中的核心部件，此处采用 NEC 公司的 μ78F0451，它是一款常用于家用电器、仪器仪表的高性价比单片机，指令最短执行时间可以在高速 0.2μs（时钟频率为 10MHz）和超低速 122μs（副系统时钟频率为 32.768kHz）之间改变；具有 16KB Flash 程序存储器和 768B RAM；具有自编程及片上调试功能；内部集成液晶控制器和驱动器；在 32768Hz 工作频率下，HALT 待机模式工作电流为 2.4μA（典型值），STOP 模式下工作电流为 1μA（典型值）。其引脚如图 6-5 所示。

6.4.3.3　电源模块

考虑到其防爆安全性，不能用 220V 的市电供电，应采用电池供电方式，但电池的使用寿命即燃气表的功耗要认真考虑。系统中电源模块采用 3 节碱性电池串联方式提供 6.5V 的电压，通过 XC6201T332P 稳压芯片，将 6.5V 的电压稳压到 3.3V，为单片机供电。该模块电路设计如图 6-6 所示，其中 C28 为超级电容，容量为 0.47F，在电池电压过低或更换电池时作为后备电池，以保证燃气表内数据及阀门状态的正确，防止掉电后数据丢失以及阀门的不关闭，造成用户数据紊乱、窃气或危险事件的发生。

6.4.3.4　脉冲采样模块

此模块主要完成对气流脉冲的正确计量，此模块采用双干簧管作为脉冲采集器件，其工作原理是：在普通转盘计数的燃气表中安装两个干簧管和磁铁，干簧管固

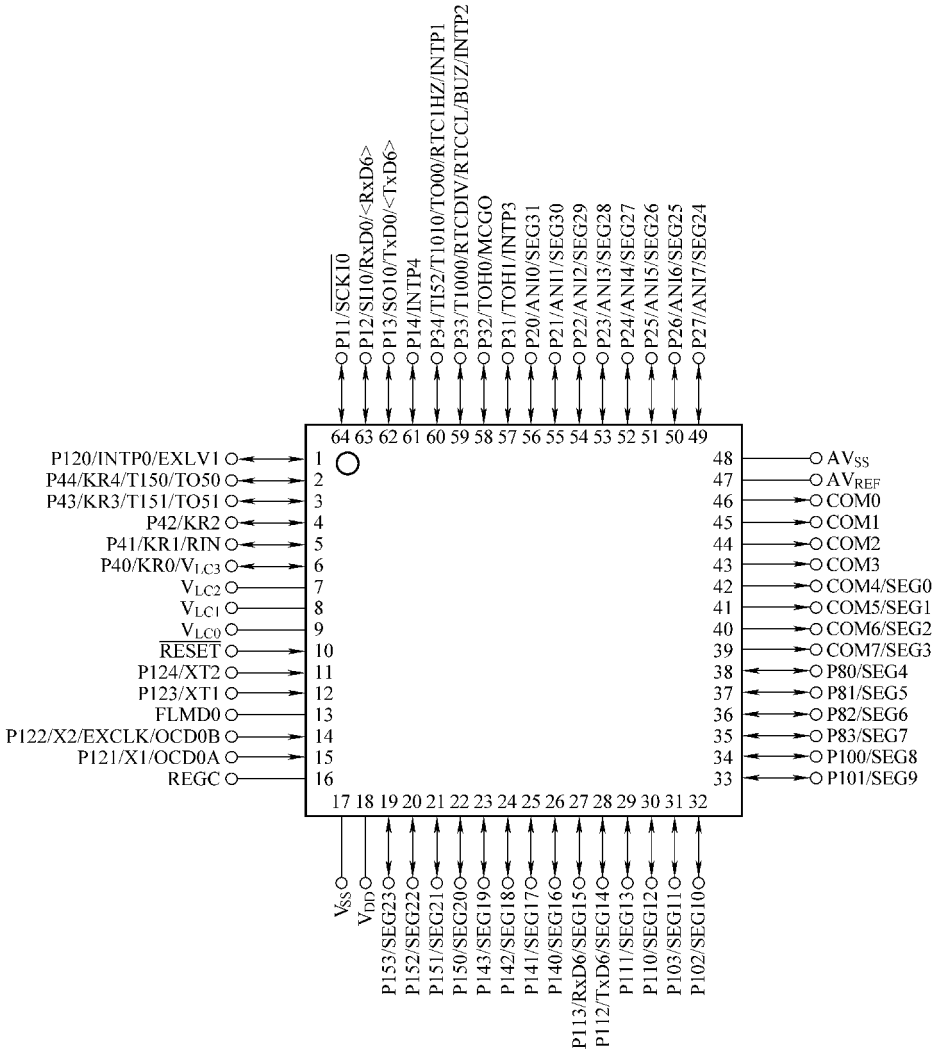


图 6-5　μ78F0451 引脚图

定安装在计数转盘附近，磁铁安装在计数盘（例如 0.1m^3）位上，当燃气表中有气流通过时，燃气表内部气囊膨胀，从而推动磁体靠近干簧管并与之吸合，当磁铁依次分别吸合两个干簧管，则为一个有效的气流脉冲。脉冲采样模块如图 6-7 所示，P4.2 为脉冲采样模块供电，P3.1 为其中一个干簧管的脉冲采样接口，P12.0 为另外一个干簧管的脉冲采样接口，当收到一组有效脉冲时，用气量增加 0.1m^3。

6.4.3.5　卡座控制电路

卡座控制电路采用 MFRC522 芯片来实现对卡片的读和写。MFRC522 是高度集成的非接触式（13.56MHz）读写卡芯片，支持 ISO 14443A/MIFARE 卡，并可实现

各种不同主机接口的功能，如 SPI、UART 及 I^2C。

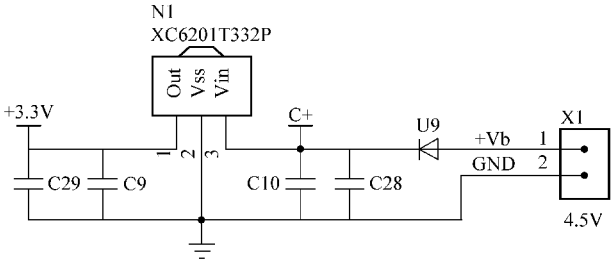


图 6-6　电源模块

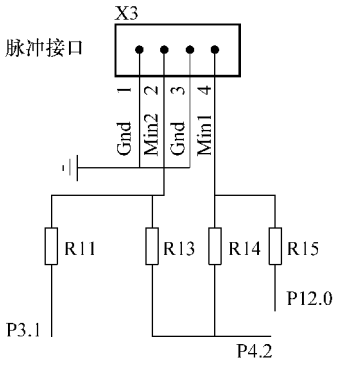


图 6-7　脉冲采样模块

1. MFRC522 芯片

该器件为 32 脚 HVQFN 封装，其引脚排列如图 6-8 所示。器件使用了 3 个独立电源以实现在 EMC 特性和信号退耦方面达到最佳性能。表 6-1 对各个引脚进行了描述。

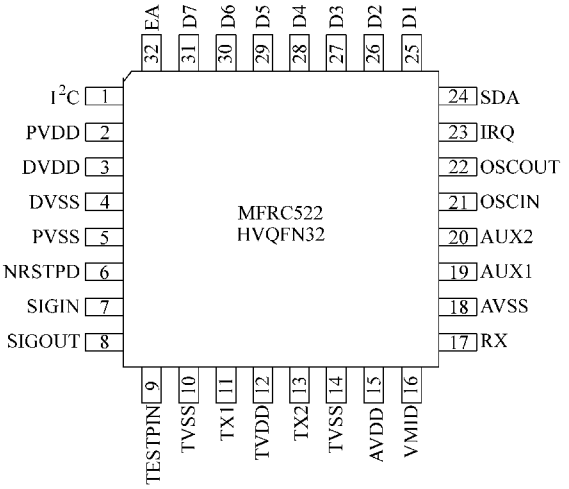


图 6-8　MFRC522 引脚图

表 6-1　MFRC522 引脚描述

符号	HVQFN32	类型	描　　述
OSCIN	21	I	晶振输入：振荡器的反相放大器的输入。它也是外部产生的时钟的输入（f_{osc} = 27.12MHz）
IRQ	23	O	中断请求：输出，用来指示一个中断事件

（续）

符号	HVQFN32	类型	描　　述
SIGIN	7	I	信号输入
SIGOUT	8	O	信号输出
TX1	11	O	发送器 1：传递调制的 13.56MHz 的能量载波信号
TVDD	12	PWR	发送器电源：给 TX1 和 TX2 的输出级供电
TX2	13	O	发送器 2：传递调制的 13.56MHz 的能量载波信号
TVSS	10，14	PWR	发送器地：TX1 和 TX2 的输出级的地
DVSS	4	PWR	数字地 不同接口的数据引脚（测试端口、I^2C、SPI、UART）
D1	25	I/O	
D2	26	I/O	
D3	27	I/O	
D4	28	I/O	
D5	29	I/O	
D6	30	I/O	
D7	31	I/O	
SDA	24	I	串行数据线
EA	32	I	外部地址：该引脚用来编码 I^2C 地址
I^2C	1	I	I^2C 使能
DVDD	3	PWR	数字电源
AVDD	15	PWR	模拟电源
AUX1	19	O	辅助输出：这两个引脚用于测试
AUX2	20	O	
AVSS	18	PWR	模拟地
RX	17	1	接收器输入：接收的 RF 信号引脚
VMID	16	PWR	内部参考电压：该引脚提供内部参考电压
NRSTPD	6	1	不复位和掉电：引脚为低电平时，切断内部电流吸收，关闭振荡器，断开输入引脚与外部电路的连接。引脚的上升沿来启动内部复位阶段
OSCOUT	22	O	晶振输出：振荡器的反相放大器的输出
TESTPIN	9		不连接：三态引脚
PVDD	2	PWR	引脚电源
PVSS	5	PWR	引脚电源地

注：引脚类型：I—输入；O—输出；PWR—电源。

2. 卡座控制电路

卡座控制电路如图 6-9 所示。连接 27.12MHz 的晶振为 MFRC522 提供时钟频率，单片机引脚 P1.1（SCK）、P1.2（MISO）、P1.3（MOSI）、P4.4（NSS）实现与 MFPC522 芯片的 SPI 接口，其中，单片机作为主机，MFRC522 作为从机。为了降低系统功耗，该电路采用了分时供电的方法：只有当检测到有 IC 卡靠近时，控制单片机引脚 P2.1 输出低电平，导通 U7，为 MFRC522 芯片提供电源，其他情况下不为其提供电源。另外，该电路部分中的 RF 接口也通过控制单片机引脚 P4.3 的电平采用分时供电的方法，只有当需要检测是否有 IC 卡靠近时才为其提供电源，P1.4 用来采样 IC 卡到位信号。

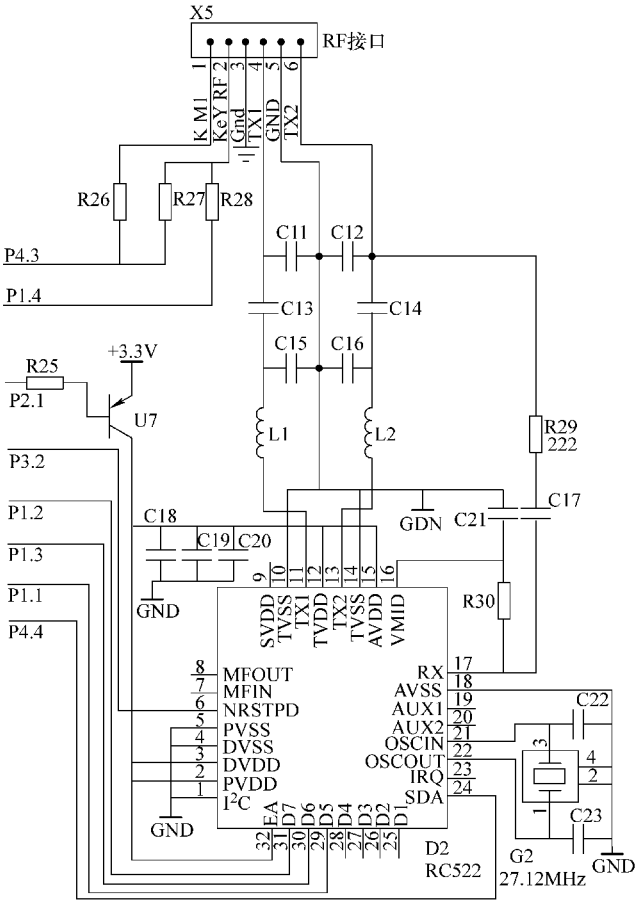


图 6-9　卡座控制电路

6.4.3.6　阀门控制模块

此模块由阀门驱动与反测阀门到位信号两部分构成，如图 6-10 所示。电动机

接口处接燃气表的阀门，其中，Driv1 和 Driv2 分别作为驱动阀门开和关的信号引脚；单片机引脚 P4.0 和 P4.1 则用来控制电动机接口中 Driv1 和 Driv2 的信号，实现阀门的开关；P2.4 和 P2.5 分别作为阀门开和关到位信号输入引脚；P3.4 为阀门控制模块供电，该模块同样采用了分时供电的方式，以降低功耗。

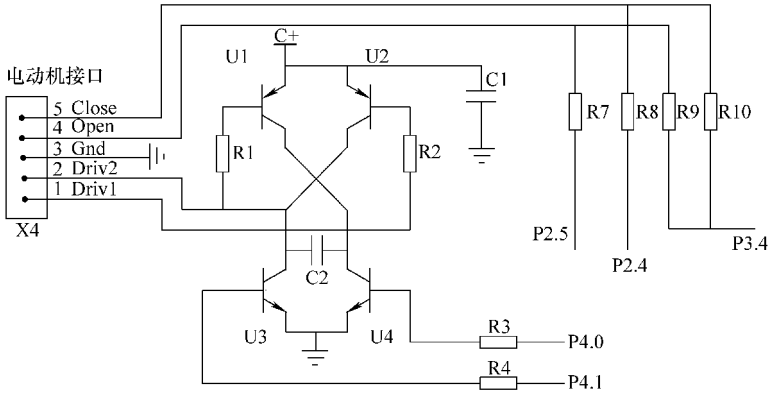


图 6-10　阀门控制模块

其工作原理为：当单片机引脚 P4.0 输出低电平且 P4.1 输出高电平时，U3 导通，使 Driv2 端口为低电平；U3 的导通也使 U2 导通，从而使 Driv1 端口为高电平，为电动机接口提供打开阀门的运行信号；而阀门的运行状态则是通过反测引脚 P2.5 的输入信号来确定，若在设定时间内为低电平的话，说明阀门已正常打开，否则阀门异常；关闭阀门的驱动通过单片机引脚 P4.0 输出高电平且 P4.1 输出低电平来提供运行信号，阀门是否关闭通过反测引脚 P2.4 来确定，其工作原理同开阀。

6.4.3.7　通信模块

系统包含一个 RS485 总线接口，作为一种抗共模干扰能力强、接收灵敏度高的总线技术，RS485 总线使用一对双绞线作为传输介质，采用半双工的通信方式，并可形成一对多或多对多形式的通信网络，可实现几十米到上千米的短中程距离通信，它具有硬件简单、成本低廉、控制方便等优点。

通信模块采用 3082E/3485CN 芯片，它是一款低功耗 RS485 收发器，它的电源电压为 5V，在失效关闭方式中，电源电流跌至毫微安培。通信模块如图 6-11 所示，XC62FP502PR 为稳压芯片，将 RS485 总线上的电压稳压到 5V，为收发器提供电源，单片机引脚 P11.1 用来使能接收或发送，P11.2 为接收数据端，P11.3 为发送数据端。通过 RS485 总线，燃气公司可以向燃气表发送命令帧，将燃气表中的计量和状态数据抄出，也可以对燃气表进行参数设置以及开关阀控制。

6.4.3.8　电池电压检测模块

电池电压检测模块每隔一定时间将 P2.2 的输出电平置高，导通 U6 对电池放电，如图 6-12 所示；同时，将 P4.2 的输出电平置高，导通 U8，利用单片机内部

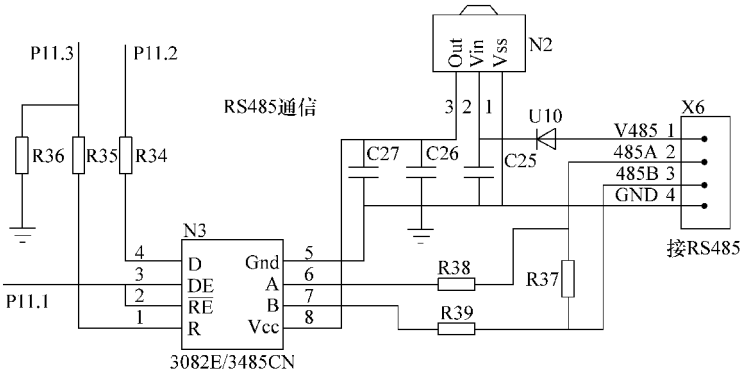


图 6-11　通信模块

的 A – D 转换通道 P2.7，采样放电后的电池电压信号，来判断电池电压是否能为系统提供正常的工作电压，如图 6-13 所示。当电池电压低或电池被取出时，关闭阀门，蜂鸣器报警，用来提醒用户尽快更换燃气表中的电池，保证燃气表的正确计量。此模块同样采用分时供电的方式，以降低系统功耗。

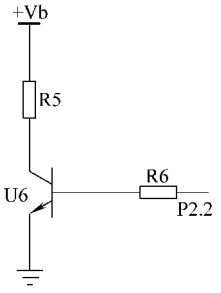


图 6-12　电池放电电路

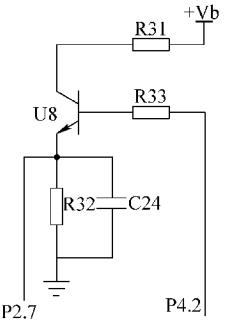


图 6-13　电池电压检测模块

6.4.3.9　液晶显示

液晶显示内容设计如图 6-14 所示。

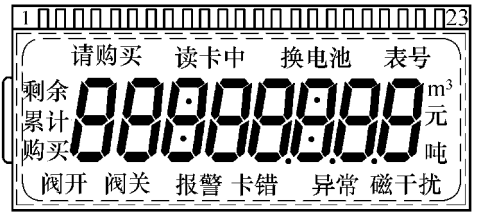


图 6-14　液晶显示屏

6.4.3.10　声音报警电路

声音报警电路如图 6-15 所示，通过控制单片机引脚 P2.6 的输出电平实现蜂鸣器的鸣叫。当 P2.6 输出低电平时，U5 导通，从而使蜂鸣器鸣叫；反之，当 P2.6 输出高电平时，U5 截止，蜂鸣器停止鸣叫。

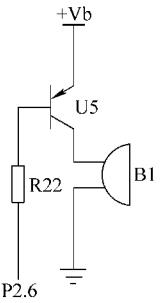


图 6-15　声音报警电路

6.4.4　系统硬件测试

系统测试包括软件和硬件两部分，而软件部分的设计必须建立在稳定的硬件基础之上，所以在软件设计之前必须对硬件进行测试。系统硬件测试的主要包括：

1. 电源测试

拿到电路板后，首先测试电源和地是否短路，如果没有短路焊接电源模块部分，焊接完成后用万用表测试电压是否正常，如正常，继续焊接。

2. 单片机程序写入测试

在完成单片机的程序写入后，给特定的引脚（如计量、插卡等）以信号，测试是否有输出信号。如有相应的输出信号，则表示单片机已正常工作。

3. 阀门测试

对于阀门的测试主要测试阻塞和打滑的情况，因为该部分可直接通过电平信号驱动来实现，所以可以单独进行测试。阀门测试主要有两项：一是当控制阀门打开或关闭的引脚有信号输出时，检测电机接口是否有电压；二是当阀门打开或关闭后检测是否有到位信号。

6.4.5　系统软件设计

6.4.5.1　软件总体结构

系统软件主要包括四部分：电源管理部分、IC 卡部分、RS485 通信部分以及燃气表功能部分，电源管理部分主要实现电源的掉电、上电检测以及电池电压的采集，IC 卡部分主要实现 IC 卡的读写，RS485 通信部分主要实现燃气表与燃气公司之间的 RS485 通信，燃气表功能部分主要实现燃气公司要求的功能，如图 6-16 所示。

6.4.5.2　卡片数据结构定义

系统卡片采用 MIFARE 1 卡，有 8kbit 存储容量，16 个扇区，每个扇区有 4 个数据块。每一块燃气表占用 4 个扇区，其中第 1、2 个扇区为指令区，第 3、4 个扇区为返写区，见表 6-2。卡片数据的读写都需要进行密码认证，为 6B 密码。

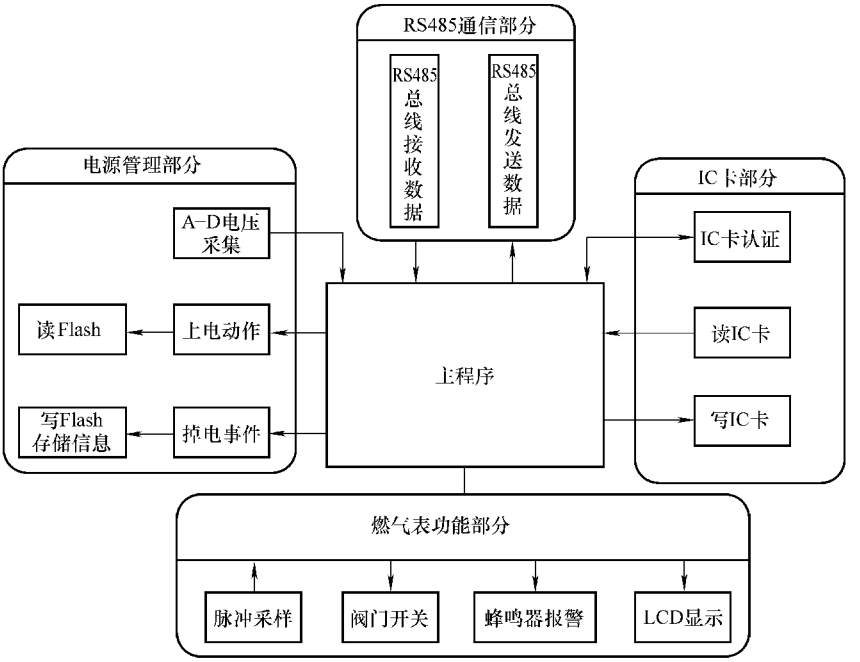


图 6-16　IC 卡智能燃气表软件功能模块图

表 6-2　卡片数据结构说明

扇区 0	不使用	数据块 0
		数据块 1
		数据块 2
	密码块	数据块 3
扇区 1	燃气表指令区	数据块 0
		数据块 1
		数据块 2
	密码块	数据块 3
扇区 2	燃气表指令区	数据块 0
		数据块 1
		数据块 2
	密码块	数据块 3
扇区 3	燃气表返写区	数据块 0
		数据块 1
		数据块 2
	密码块	数据块 3

（续）

扇区 4	燃气表返写区	数据块 0
		数据块 1
		数据块 2
	密码块	数据块 3

一套预付费燃气系统中卡的种类有很多种，主要有两大类：用户卡和管理卡。用户卡是消费者使用的卡片；管理卡是燃气公司管理时使用的卡片，一般包括参数设置卡、检查卡、退气卡、转移卡、校时卡、密钥修改卡等。下面以用户卡为例对 MIFARE 1 卡的数据结构进行描述。

用户卡由用户持有，用来完成缴费购气，包含的数据有分区号、用户号、报警值、充值限额、透支限额、最低消费额、购买值等，见表 6-3；通过用户卡返回的数据有燃气表表号、剩余值、累计用气量、表工作状态字、月用气量等，见表 6-4。

表 6-3 用户卡指令区数据项定义

数据项	长度/B	数据项	长度/B
用户卡命令码	1	阶梯价格	25
分区号	2	新价格启动日期	3
用户号	5	购气次数	2
报警值	4	购买值	4
充值限额	4	特征字	2
透支限额	4		

表 6-4 用户卡返写区数据项定义

数据项	长度/B	数据项	长度/B
起始码	1	表工作状态字	1
燃气表表号	5	磁干扰次数	1
表累计购买值	4	月用气量	36
购买次数	2	当前日期	3
表内剩余值	4	特征字	2
表累计用气量	3		

由图 6-9 所示，有关卡的读写程序如下。

```
#DEFINE  P_RC522_NSS    P4.4  ;RC_522 SDA
# DEFINE  P_RC522_SCK    P1.1  ;RC_522SPI SCK
# DEFINE  P_RC522_MISO   P1.2  ;RC_522 SPI MISO 主机输入从机输出
# DEFINE  P_RC522_MOSI   P1.3  ;RC_522 SPI MOSI 主机输出从机输入
# DEFINE  P_RC522_RST    P3.2  ;RC_522 NRSTPD
# DEFINE  K_ACTIVE       P2.1  ;RC_522 POWER ON 低有效

BLOCK_CNT         EQU    0fed8h
BLOCK_START_NUM   EQU    0fed9h

BlockNum:    DS   1
RC522Buf:    DS   2            ;RC522 发送或接收缓冲区

;- - - -从0fd00H 到0fd3fH 为发送或接收缓冲区(64B) - - - - - - -
data_buf   EQU    0fd3fh       ;发送或接收数据区
                               ;复位信息存放区,64B
;- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
;RC522 CONTROLLING REGISTER
;- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
#DEFINE    ComIrqReg       4h
#DEFINE    ErrorReg        6h
#DEFINE    FIFODataReg     9h
#DEFINE    FIFOLevelReg    0Ah

#DEFINE    mOK             #01h
#DEFINE    mFALSE          #00h
```

1. 读 MIFARE 1 卡

```
;* * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * *
;CARD_RD:读 MIFARE 1 卡
;* * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * *
CARD_RD:
    WDTE = #0ACh              ;清看门狗
    SET1  P_RC522_NSS
    SET1  P_RC522_SCK
    SET1  P_RC522_MOSI
```

```
    SET1  P_RC522_RST          ;复位引脚初始化
    SET1  PM1.2                ;设置 P_RC522_MISO 引脚为输入模式
    CLR1  P_RC522_MISO
    CLR1  P_RC522_NSS

    CLR1  K_ACTIVE             ;RC522 上电
    CALL  ! Delay30ms          ;延时 30ms
    CALL  ! RC522_RST          ;复位 RC522
    CALL  ! halRC522Initial    ;初始化 RC522 的寄存器
    A = D
    BF  A.0,$CARD_RD_E         ;初始化失败跳转 CARD_RD_E 处执行

    CALL  ! halRC522Request    ;RC522 发请求信号寻找感应区中的卡片
    A = D
    BF  A.0,$CARD_RD_E         ;请求失败跳转 CARD_RD_E 处执行

    CALL  ! halRC522GetUID     ;读卡序列号识别卡
    A = D
    BF  A.0,$CARD_RD_E         ;序列号错误跳转 CARD_RD_E 处执行

    CALL  ! halRC522SelectTag  ;选择卡片
    A = D
    BF  A.0,$CARD_RD_E         ;卡片错误跳转 CARD_RD_E 处执行


    A = #4
    BLOCK_START_NUM = A

READ_CARD:
    A = #3                     ;读取扇区 1 中的三个数据块
    BLOCK_CNT = A
    HL = #DATA_BUF
    CALL  ! READ_FILE

    A = ! BLOCK_START_NUM      ;读取扇区 2 中的三个数据块
```

```
    A + = #4
    ! BLOCK_START_NUM = A
    BLOCK_CNT = #3
    CALL  ! READ_FILE

    A = ! BLOCK_START_NUM      ;读取扇区 3 中的第一个数据块
    A + = #4
    ! BLOCK_START_NUM  = A
    BLOCK_CNT = #1
    CALL  ! READ_FILE
CARD_RD_E:
    RET
```

2. 读文件

```
;* * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * *
;READ_FILE:读扇区的数据
;输入:BLOCK_START_NUM(4,8,c,10h....);
      BLOCK_CNT( < =4)
      HL(data_buf pointer)
;输出:D = mOK,or D = mFALSE
      Databuf(file data)
;相关寄存器:A,HL,C,B
;* * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * *
READ_FILE:
    A = BLOCK_START_NUM
    ! BlockNum = A

    PUSH  HL
    CALL  ! halRC522Authentication      ;校验扇区密码
    POP  HL
    A = D
    BF  A.0,$READ_FILE_END              ;密码校验失败,程序返回
READ_NEXT_BLOCK:
    CALL! halRC522ReadBlock
    A = D
    BF  A.0,$READ_FILE_END
```

```
    A = ! BlockNum
    A + = #1
    ! BlockNum = A

    DBNZ  BLOCK_CNT,$READ_NEXT_BLOCK     ;读下一个数据块

READ_FILE_END:
    RET
```

3. 读卡扇区中的数据块

```
;* * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * *
;halRC522ReadBlock:读扇区中的数据块
;输入:HL,FmBlockNum(block numble)
;输出:D = mOK,or D = mFALSE
      HL (databuf)
;相关寄存器:AX,BC,DE
;* * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * *
halRC522ReadBlock:
    PUSH HL
    A = #ComIrqReg
    E = #80H
    CALL ! ClearBitMask
;//WRITE BLOCK NUMBLE AND EXECUTE command Transceive
FMREADBLOCKJMP1:
    A = #30h
    ! RC522Buf = A
    A = ! BlockNum
    ! (RC522Buf - 1) = A
    C = #02h                          ;把命令长度送给 C
    E = #Transceive                   ;把命令字送给 E
    CALL  ! halRC522CommandSend;发送发数据命令
    A = D
    BT  A.0,$FMREADBLOCKJMP2     ;命令发送成功转下一步,否则退出
    POP  HL
    RET
```

```
;// READ ERROR FLAG REGISTER
FMREADBLOCKJMP2:
    A = #ErrorReg
    CALL  ! ReadRC522Reg          ;读错误标志寄存器
    ! RC522Buf = A
    A = D
    BT  A.0,$FMREADBLOCKJMP3      ;读成功转下一步,否则退出
    POP  HL
    RET
;// ReadBlock Execute OK?
FMREADBLOCKJMP3:
    A = ! RC522Buf
    AND  A,#0Eh                   ;ollErr,CRCErr, ParityErr
    BZ  $FMREADBLOCKJMP4          ;无错误标志转下一步,否则退出
    POP  HL
    D = mFALSE
    RET
;// READ FIFO
FMREADBLOCKJMP4:
    POP  HL
    CALL  ! halRC522ReadFIFO      ;
    A = D
    BT  A.0,$FMREADBLOCKJMP5
    RET
      ;// COUTER = 16?
FMREADBLOCKJMP5:
    A = B
    SUB  A,#10h
    BZ  $FMREADBLOCKJMP6
    D = mFALSE
    RET
FMREADBLOCKJMP6:
    D = mOK
    RET
```

4. 读卡中 FIFO 缓冲区

```
;* * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * *
;halRC522ReadFIFO:读卡中 FIFO 缓冲区的数据
;输入:无
;输出:D = mOK,or D = mFALSE
      RC522Buf,B(DATA LENGTH)
;相关寄存器:AX,BC,DE
;* * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * *
halRC522ReadFIFO:
    ;//READ FIFO LENGHT REGISTER
    A = #FIFOLevelReg
    CALL ! ReadRC522Reg          ;读操作,得到长度数据
    ! RC522Buf = A               ;读到的数据送 RC522Buf 缓冲区
    A = D
    BT A.0,$FMREADFIFOJMP1       ;读成功则跳转下一步
    RET

FMREADFIFOJMP1:                  ;判断缓冲区数据长度是否为 0
    A = ! RC522Buf               ;READ LENGTH
    C = A
    B = A                        ;暂存数据长度
    ADD A,#00
    BNZ $FMREADFIFOJMP2          ;长度不为 0 则跳转下一步
    D = mFALSE
    RET
FMREADFIFOJMP2:                  ;缓冲区数据长度不为零,读数据
    HL = #RC522Buf
FMREADFIFOJMP3:
    A = #FIFODataReg             ;读 FIFO 的数据
    CALL ! ReadRC522Reg
    [HL] = A                     ;
    DECW HL
    DBNZ C,$FMREADFIFOJMP3       ;未读完,继续读
    D = mOK                      ;数据读完,置标志,返回
    RET
```

5. 读字节操作

```
;* * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * *
;ReadRC522Reg:读字节操作
;输入:A(address)
;输出:A(register value) D = mOK, D = mFALSE
;* * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * *
ReadRC522Reg:
    D = mOK;
    CLR1 CY
    ROLC A,1
    OR   A,#80h                    ;最高位置 1,读操作
    AND   A,#0FEh
    X = A
    CLR1   P_RC522_NSS             ;NSS = 0 ,ENABLE
    SET1   CSIE10                  ;ENABLE 串行操作
FMSPIREADLOOPa:
    A = X                          ;SEND ADDRESS
    SOTB10 = A                     ;数据写入发送缓冲寄存器 SOTB10
    while(CSIM10.0)                ;等待串行通信结束
    endw
    A = #00h
FMSPINORMALREAD:
    SOTB10 = A
    while(CSIM10.0)
    endw

    A = SIO10                      ;将收到的串行移位寄存器的值送给 A
    CALL ! Delay5us
    SET1 P_RC522_NSS               ;NSS DISABLE
    RET
```

6.4.5.3　主程序

当系统上电后，执行主程序。首先进行系统初始化；然后将 Flash 中的本机数据读出，并判断是否满足打开阀门的条件，满足条件后打开阀门，在 LCD 上显示本机参数；最后系统进入低功耗模式，等待气流脉冲、插卡等中断唤醒。图 6-17 所示为主程序流程。

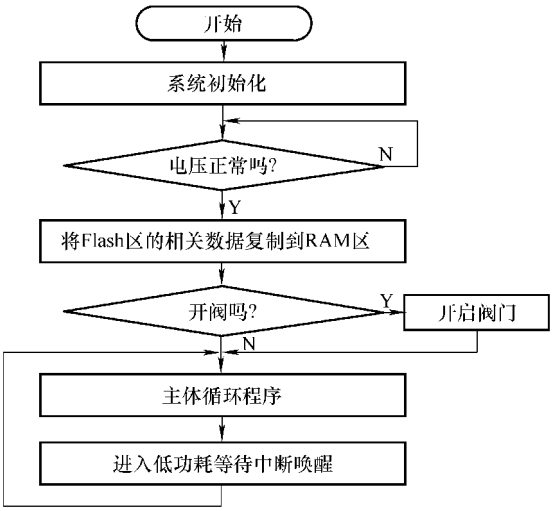


图 6-17　主程序流程图

（1）系统初始化

其中包含了对堆栈的设置，时钟设置，内存初始化、A－D 寄存器设置，定时器以及端口的初始设置等。

（2）判别电压是否正常

此功能的判定过程如下：

1）判断电池电压低达到 30 天标志位是否置位，若是，则跳转 2）执行；否则跳转 3）执行；

2）通过检测电池是否取出来判断是否更换了新的电池，若是，则跳转 3）执行；否则，等待更换新的电池；

3）通过检测低电压检测引脚判断电池电压是否能为系统提供满足要求的稳定电压，如果满足要求则跳转（3）处执行，否则一直等待更换满足要求的电池。在此等待过程中 LCD 上将会显示换电池标志，提醒用户更换电池。

（3）将 Flash 区的相关数据读入到相应的 RAM 区

将燃气表表号、剩余气量（或金额）、阶梯价格、燃气表工作状态字等数据读入到相应的 RAM 区，方便系统对其数据进行读取、计算和存储。

（4）判别是否要开阀

这一过程主要根据从 Flash 区复制到 RAM 区的数据判断用户购气量或剩余金额是否已经达到关阀值，如果是，则不开阀；否则开阀。

（5）主体循环程序

主循环主要实现 RS485 通信、磁干扰、IC 插卡、电池电压检测、开关阀以及更新 Flash 的检测和处理。

（6）低功耗设置

由于系统采用电池作为电源，因此具有低功耗的特点。低功耗有两种模式，即 HALT 和 STOP 模式。在 HALT 模式中，CPU 操作时钟停止。如果设置 HALT 模式前，高速系统时钟振荡器、内部高速振荡器、内部低速振荡器或副系统时钟振荡器正在使用，则设置后时钟的振荡继续，工作电流不如 STOP 模式中下降得多；而在 STOP 模式中，高速系统时钟振荡器和内部高速振荡器停止操作，整个系统操作停止，这样 CPU 工作电流将会大幅下降（比 HALT 模式小很多）。所以采用 STOP 模式能使系统功耗更低，进入 STOP 模式后等待中断唤醒。

6.4.5.4　燃气流量脉冲采样模块

功能：采样燃气表气流脉冲信号，实现两个功能：一是采样双干簧管的闭合状态，判断是否有一个有效的气流脉冲信号到来，二是判断在用户用气的同时是否存在磁干扰信号，如图 6-18 所示，描述如下：

（1）为脉冲采样模块上电

将 P4.2 端口的输出电平置 1，为脉冲采样模块供电。

（2）判断干簧管 1 的状态

检测 P12.0 端口的输出电平，若为高电平，则表明干簧管 1 未采样到一个气流脉冲，清零和干簧管 1 相关的标志位，跳到（3）执行；若为低电平，则表明干簧管 1 采样到一个气流脉冲，判断干簧管 1 的初次闭合状态标志是否为 1，若为 1，则表明此次为干簧管 1 二次闭合，将干簧管 1 的二次闭合状态标志置 1；否则，表明此次为干簧管 1 初次闭合，将干簧管 1 的初次闭合状态标志置 1。

（3）判断干簧管 2 的状态

检测 P3.1 端口的输出电平，若为高电平，则表明干簧管 2 未采样到一个气流脉冲，清零和干簧管 2 相关的标志位，跳到（4）执行；若为低电平，则表明干簧管 2 采样到一个气流脉冲，判断干簧管 2 的初次闭合状态标志是否为 1，若为 1，则表明此次为干簧管 2 二次闭合，将干簧管 2 的二次闭合状态标志置 1；否则，表明此次为干簧管 2 初次闭合，将干簧管 2 的初次闭合状态标志置 1。

（4）判断是否存在磁干扰

判断干簧管 1、2 的二次闭合状态标志，若同时为 1，则表明存在磁干扰，当磁干扰持续 5s 后，要立即存脉冲，关闭阀门，并通过液晶显示器显示磁干扰标志；否则，跳到（5）执行。

（5）判断是否采样到一个有效的气流脉冲信号

判断干簧管 1、2 的二次闭合状态，若在有时间间隔的情况下采样到它们都闭合，则表明采样到一个有效的气流脉冲，置位相应的标志位；否则，没有采样到有效脉冲，跳到（6）执行。

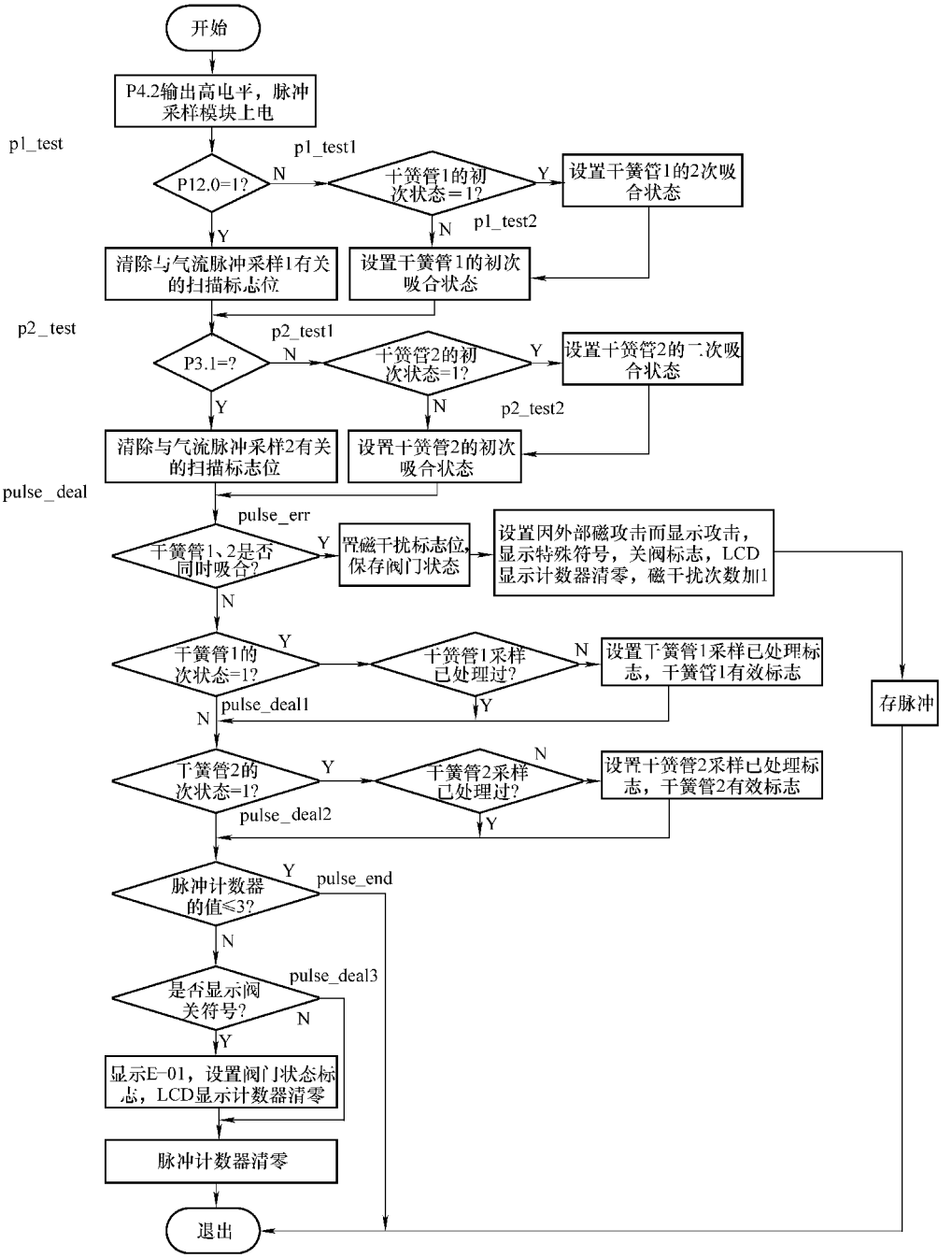


图 6-18　燃气流量脉冲采样流程图

（6）停止脉冲采样模块供电

将 P4. 2 端口的输出电平置 0，停止为脉冲采样模块供电。

6. 4. 5. 5　剩余气量计算模块

功能：当采样到一个有效的气流脉冲信号（0. 1m^3）时，首先计算剩余气量或金额，然后再判断其值是否已达到预设的报警值。

（1）累计用气量递增

当采样到一个有效的气流脉冲信号（0. 1m^3）时，燃气表中的累计用气量递增，表示用户又用了 0. 1m^3 燃气。

（2）计算当月累计用气情况

通过判断当前计量方式来决定对当月累计用气情况的计算方式，若当前计量方式为按金额计量，则读取当前的计量价格，加上相应的价格，计算当月的累计用气值；否则，当月的累计用气量加 1。

（3）计算剩余气量情况

通过判断当前计量方式来决定对剩余气量的计算方式，若当前计量方式为按金额计量，则读取当前的计量价格，减去相应的价格，计算剩余金额；否则，剩余气量减 1。

（4）剩余气量是否小于 0

根据系统功能，该系统具有透支功能，通过剩余气量的最高位可以知道系统是否已经透支。若剩余气量为负，则跳转至步骤（5）；否则跳转至步骤（6）。

（5）剩余气量绝对值大于透支气量判断

如果剩余气量绝对值小于透支量，系统保持开阀状态继续供气，但是系统会声音报警，并显示购气，以提醒用户；否则，系统将关闭阀门停止供气，直到用户再次购气。

（6）剩余气量（非负）是否小于预设报警值

在剩余气量为非负时，判断剩余气量是否小于预设报警值，若是，则进行步骤（7），否则退出。

（7）剩余气量是否等于 0

如果剩余气量小于报警气量，系统会声音报警并在液晶显示屏上显示请充值，提醒用户及时充值，另外，还要对剩余气量是否等于 0 作出判断：若是，则进行步骤（8），否则退出。

（8）透支限额是否等于 0

如果剩余等于 0，还要对透支限额是否等于 0 作出判断：如果条件成立，则说明系统已经透支，关闭阀门，同时声音报警并在液晶显示屏上显示购气，以提醒用户购气，否则退出。

6. 4. 5. 6　IC 卡认证模块

功能：对插卡操作做出判断，本系统中燃气表必须接收和处理多种 IC 卡，包

括用户卡、检查卡、参数设置卡和校时卡等。IC 卡的认证过程如下：

1）从卡中读出卡的命令码。

2）根据卡的命令码判断卡的类型，并跳转到相应的卡处理子程序处执行，若没有匹配的命令码，说明插入的卡片非本系统卡，系统报错，不做任何处理。

6.4.5.7 用户卡处理模块

功能：对插入的用户卡进行处理。首先判断插入的卡是否为与该燃气表绑定的用户卡，然后实现用户再次购气与充值，IC 卡返写等功能。图 6-19 所示为用户卡处理程序流程，对其描述如下：

（1）判断燃气表是否插入过回收转移卡

判断燃气表是否插过回收转移卡，若插过，系统报错退出，不对卡作任何处理；否则继续执行。

（2）判断从卡中读取的分区号是否与燃气表中存储的分区号一致

判断从卡中读取的分区号是否与燃气表中存储的分区号一致，若一致，则跳转（3）处执行，否则，非本系统卡，系统报错退出，不对卡作任何处理。

（3）判断读取的数据是否正确

对卡中读取的密文进行解密，并将从卡中读取的数据进行累加和计算，判断是否与卡中读取的累加和一致，若一致，说明读取数据正确，则跳转（4）处执行，否则，读取数据有误，系统报错退出，不对卡作任何处理。

（4）判断燃气表是否已开户

判断燃气表中的购买次数是否为 0，若是，则表示该燃气表仍未开户，跳转（5）执行；否则，表示已开户，跳转（6）执行。

（5）判断卡中的购买次数是否为 1

判断卡中读取的购买次数是否为 1，若是，则表明此卡为开户卡，将卡中读取的用户号保存到燃气表中，跳转（6）执行，否则，系统报错退出，不对卡作任何处理。

（6）判断燃气表中的用户号是否与从卡中读取的用户号一致

判断燃气表中的用户号是否与从卡中读取的用户号一致，若是，表明此卡为本燃气表的用户卡，跳转到（7）处执行；否则，非本系统卡，系统报错退出，不对卡作任何处理。

（7）判断从卡中读取的购买次数是否比燃气表中的购买次数多 1

判断从卡中读取的购买次数是否比燃气表中的购买次数多 1，若是，则表明用户购买了新的燃气，跳转到（8）处执行；否则，表明用户没有购买新的燃气，跳转（9）处执行。

（8）判断是否允许增加气量

将燃气表中剩余气量与购买燃气量相加，判断是否允许增加气量，若是，进行

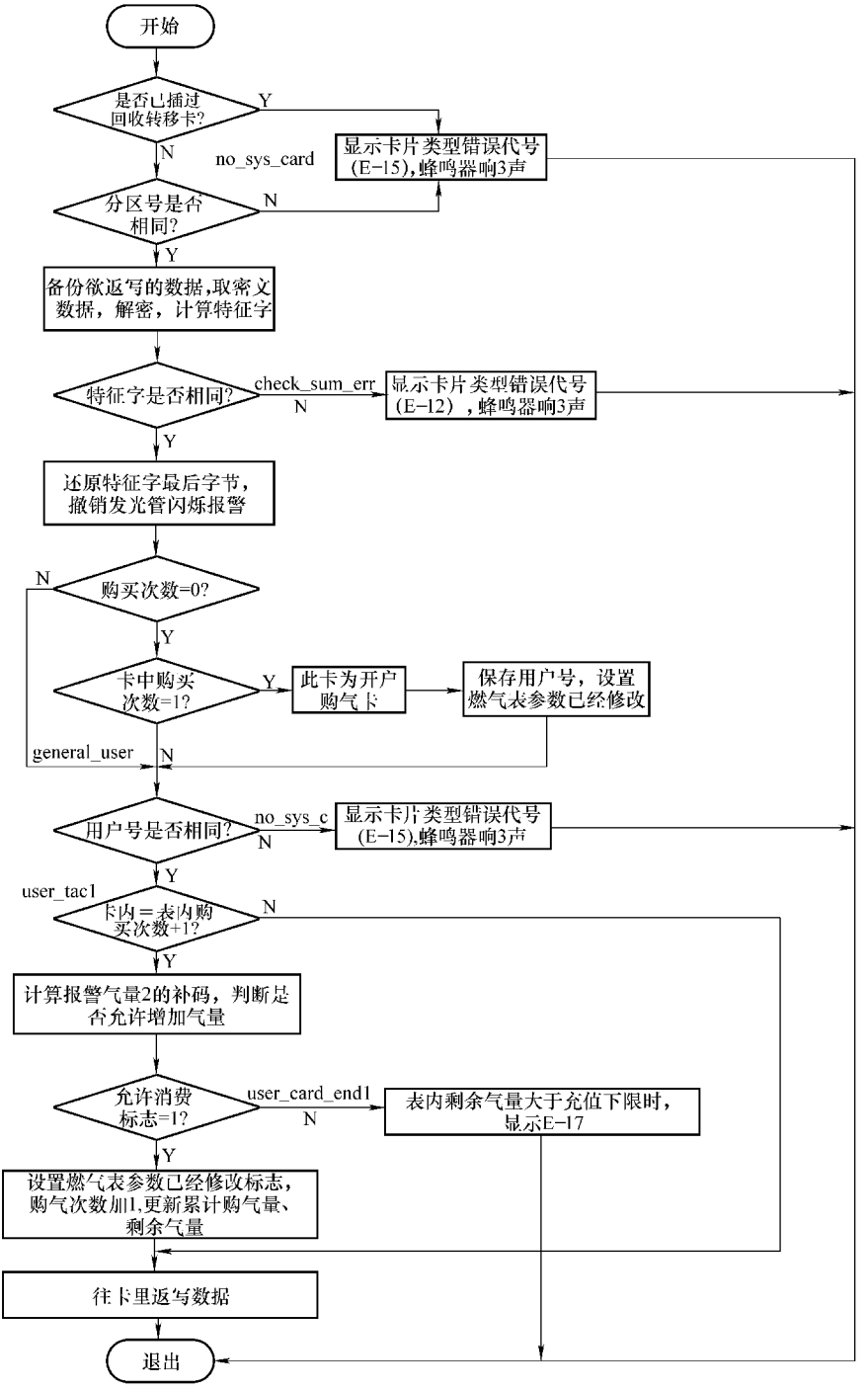


图 6-19　用户卡处理程序流程图

充值，对剩余气量、购买燃气量等数据进行更新，跳转（9）处执行；否则，不进行充值，直接退出。

（9）返写数据至 IC 卡中

将燃气表中已经被更新的数据写到 IC 卡中，实现燃气公司与用户之间的信息交互。

6.4.5.8 RS485 通信模块

功能：对接收到的 RS485 通信帧做出判断，本系统中燃气表必须接收和处理多种 RS485 通信帧，包括抄收数据帧、参数设置帧、冻结指令帧、冻结数据抄收帧和阀门控制帧等。对 RS485 通信帧的认证过程如下：

1）从接收到的 RS485 通信帧中识别出通信帧的命令码。

2）根据通信帧的命令码判断接收帧类型，并跳转到相应的 RS485 通信帧处理子程序处执行，若没有匹配的命令码，说明接收到非本系统命令帧，不作任何处理。

6.4.5.9 开关阀模块

功能：实现阀门的开关。

打开阀门的原因有：用户再次插卡购气、更换了满足要求的电池或磁干扰消失等。关闭阀门原因有：剩余气量小于报警气量或透支气量、电池被拆卸或电池电压低、有磁干扰信号影响等。单片机能否可靠控制阀门的开和关，影响着燃气表的供气情况，设计时应重点考虑。本系统从软硬件两方面进行了设计：

1）在硬件方面，用单片机引脚 P4.0 和 P4.1 来控制阀门开和关的同时，用单片机引脚 P2.4 和 P2.5 来反测阀门的开关到位信号。

2）在软件方面，经过多次实验，得出了阀门到位所需时间约为 4.5s，若在此时间内检测到阀门到位信号，则说明阀门正常；否则说明阀门异常，如打滑、阻塞或损坏等。

6.4.5.10 电池电压检测模块

功能：检测电池是否被取出或电压过低。

一方面，程序每秒钟对电池电压进行检测判断电池是否被取出，若是，则关闭阀门停止供气，直到电池被插上且电压正常，系统才复位重新开始运行；另一方面，程序每隔 12 天对电池进行放电，并检测电池电压是否过低，若是，则关闭阀门停止供气，用户插入用户卡可以重新打开阀门供气，若检测到电池电压低持续 30 天，则永久关阀，直到用户更换电池且电压正常，系统才复位重新开始运行。

6.4.6 系统测试

系统测试其实就是检验本设计中燃气表能否实现预期功能，主要包括功能测试、低功耗测试和强度测试三个方面。

6.4.6.1　功能测试

1. 燃气用气控制测试

通过用户卡或参数设置卡为燃气表输入一定气量（m^3）或金额（元），燃气表应能够正确读入预购气量（或金额），并计算剩余气量（或金额），同时打开阀门；采样有效的气流脉冲，当燃气表剩余气量（或金额）降至预设报警值时，检查燃气表的阀门状态，此时燃气表应能够自动关闭阀门，停止供气，同时声音报警，并显示购气，以提醒用户；当重新购买并读入一定气量（或金额）后，燃气表将会自动打开阀门，为用户供气。

2. 数据保持与恢复测试

通过用户卡或参数设置卡为燃气表输入一定气量（m^3）或金额（元），阀门打开，采样气流脉冲一段时间后，假设剩余气量为输入气量或金额的一半，此时切断电源，停止为燃气表供电，5min 之后恢复供电，燃气表恢复正常工作状态，并且表内剩余气量或金额和掉电前一致。

3. 电池低电压测试

将稳压电源调整至低于燃气表所要求的工作电压，燃气表上电后，发出声音报警，并在液晶显示屏上显示换电池标志，阀门保持关闭；将稳压电源的电压调到高于预设的低电压报警值，燃气表上电后，阀门自动打开，此情况下需要进行两方面的测试，测试一：缓慢下调稳压电源的电压，使其低于预设的低电压报警值，将校时卡时间设置为 23：59：58，刷校时卡 12 次模拟 12 天，电池开始放电并进行电压检测，此时燃气表关闭阀门，发出声音报警，并能在显示屏上显示换电池标志；测试二：拔出稳压电源，燃气表将关闭阀门，发出声音报警，并在显示屏上显示换电池标志。

4. 气量或金额累积功能测试

通过用户卡或参数设置卡为燃气表输入一定气量（m^3）或金额（元），阀门打开，采样气流脉冲一段时间后停止用气，假设此时表内剩余气量为输入气量或金额的一半，然后再通过用户卡向燃气表输入一定气量（m^3）或金额（元）时，此时检查燃气表的剩余气量值为原剩余量和新输入量之和，表明该系统具有气量或金额累积功能。

5. 磁干扰测试

通过用户卡或参数设置卡向燃气表输入高于预定值的气量或金额使其正常工作，用强磁场靠近燃气表，系统将关闭阀门，并报警提示，显示相应的错误提示，当磁场消失后，系统将重新开阀供气。

6. 误操作测试

将非本系统卡插入燃气表时，系统会发出声音报警，并在液晶显示屏上显示相应的错误提示。

6.4.6.2 低功耗测试

1. 各模块能量消耗

通过对燃气表进行多次测试，系统中各模块的能量消耗见表 6-5。

表 6-5 系统各模块能量消耗

状态	控制器	读卡	脉冲采样	电源放电检测	LED	阀门	蜂鸣
工作	13μA	48mA	8 ~ 14μA	400μA（实时） 60mA（放电）	11 ~ 16μA	47mA	16mA
休眠	8μA	无	无	无	无	无	无

可以看出，当燃气表中所有模块都正常工作时系统最大电流消耗约为 80 mA。其中电源电压检测模块消耗最大，它由两部分组成：一部分是实时检测电池电压，以检测电池是否被取出，电流消耗约为 400μA；另一部分是放电检测电压，电流消耗约为 60mA，放电检测电压每 12 天检测一次，能耗可以忽略；其余模块中，卡座和阀门模块能耗消耗最大，约为 47 ~ 48mA，它们也只在少数时间处于工作状态；蜂鸣、LCD 显示模块等都仅在需要的情况下才使用，在实际应用中其能量消耗微乎其微。因此，在工作状态下，系统的电流消耗约为

$$I_{\text{active}} \approx 13\mu\text{A} + (8+14)/2\mu\text{A} + 400\mu\text{A} = 424\mu\text{A} \tag{6-1}$$

2. 系统整体功耗分析

（1）脉冲采样模块功耗

该模块采用中断处理方式，当有气流脉冲到来时，该模块的电流消耗主要由两部分组成，一部分为该模块本身的能耗，另一部分为中断唤醒单片机并进行相应处理时的能耗。

$$I_{\text{pulse}} = (8+14)/2\mu\text{A} + 400\mu\text{A} = 411\mu\text{A} \tag{6-2}$$

其中断处理程序每次仅进行脉冲采样及磁干扰检测工作，工作周期小于 3μs，即 $T_{\text{pulse}} \approx 3 \times 10^{-6}\text{s}$。而当双干簧管依次采样到脉冲时，才为一个有效脉冲，累计用气 0.1m³，采样到气流脉冲频率的高低和用户的燃气使用情况密不可分，假设用户一个月使用大约 10m³ 的燃气，可计算得出每个月中断 2×10^4 次，每秒的平均中断频率为 $F_{\text{interrupt}} = 0.0077$ 次 / s。根据上面的分析，可以计算出该模块在一个周期内（1h）的电流消耗为

$$E_{\text{pulse}} = I_{\text{pulse}} T_{\text{pulse}} F_{\text{interrupt}} \times 3600\text{s} = 3.149 \times 10^{-9}\text{mAh} \tag{6-3}$$

由此可见，该模块上的功耗极低，几乎为 0，可以忽略不计。

（2）电源电压检测模块功耗

电源电压检测模块通过每 12 天对电池放电并利用 A－D 采集电池电压来进行检测，持续时间约为 10s；电流消耗约为 60mA，则可以计算出该模块在一个周期内（1h）的电流消耗为

$$E_{AD} = I_{AD} t_{AD} = 5.66 \times 10^{-4} \text{mAh} \tag{6-4}$$

（3）卡座模块功耗

该模块采用中断处理方式，实现 IC 卡与卡座之间的通信，工作时间小于 1s，电流消耗约为 48mA。假如用户一个月购买一次燃气并将购买值读入燃气表，则可以计算出该模块在一个周期内（ 1h）的电流消耗为

$$E_{card} = I_{card} t_{card} \div 30 \div 24 = 0.067 \text{mAh} \tag{6-5}$$

（4）其他模块功耗

蜂鸣器和 LCD 仅在存在磁干扰以及电池电压过低等异常情况时才工作，大部分时间都处于关闭状态，其电流消耗接近 0μA，可以忽略不计。

（5）系统整体功耗

根据（1） ~（4）可以计算出整个系统一天的功耗为

$$E_{day} < （E_{pulse} + E_{AD} + E_{card}） \times 12 = 0.810792 \text{mAh} \tag{6-6}$$

系统一年的功耗为

$$E_{year} = E_{day} \times 365 = 295.939 \text{mAh} \tag{6-7}$$

本系统采用 3 节碱性电池串联方式来提供电源，单节电池放电到 1.2V 左右时系统就不能正常工作了，假设此时，3 节电池的放电量分别为 1000mAh、1500mAh、2000mAh，可以计算出燃气表可以工作的天数分别为 1233 天、1850 天和 2467 天。

6.4.6.3　强度测试

强度测试总是迫使系统在异常情况下运行。对于燃气表，主要是在比一般气流脉冲信号高几倍频率的基础上进行测试。经过多次测试表明，系统依然能够正确计量气流信号。

本设计已在实际中得到成功应用。

第 7 章　智能卡表的一卡通设计

随着新技术的发展，在城市范围内实现居民生活水、电、气、热表一卡通已经可以成为现实，本章对城市水、电、气、热表一卡通的技术规范提出设想，分别从总体设计、IC 卡表、IC 卡、IC 卡表和 IC 卡接口、银行业务流程五部分对应该遵循的标准进行描述。

7.1　总体设计

1. 建立高度安全的收费管理机制

首先，城市水、电、气、热表一卡通中 IC 卡传输介质采用 CPU 智能卡，其安全认证机制建立在密钥认证的基础上，而不再是存储卡和逻辑加密卡所使用的密码认证，相比而言，密钥破译难度极大，外人很难进行非法攻击。这样采用 CPU 智能卡将有效保证整个收费管理系统中数据交换的安全性；其次，在水表、电表、气表、热表以及相应的 IC 卡读写机中安装 ESAM 或使用 PSAM 卡，使得密钥认证的过程只在 ESAM（或 PSAM 卡）与 IC 卡之间进行，而与表计以及读写器的设计无关，ESAM（或 PSAM 卡）与 IC 卡的初始化以及发行管理将直接由城市 IC 卡领导小组统一进行管理，与表计和读写器的生产单位以及使用单位无关。采用这种方式可以使整个收费管理系统具有高度的安全性。

2. 建立方便灵活的收费网络

收费系统充分利用银行储蓄网点，用户所有的持卡缴费操作都可通过银行储蓄网点进行，这样可以实现就近持卡缴费和异地持卡缴费，极大地方便了用户。

3. 提供方便的辅助售卡

除银行储蓄网点正常售卡外，还可以在社会上发行一定数量固定面值的不记名卡，当用户由于各种原因不能及时到银行储蓄网点购卡时，可以购买不记名卡作应急用。

4. 符合 IC 卡标准的售卡系统

售卡系统采用了符合 IC 卡国际标准的 CPU 卡，便于进行升级，从而保证售卡系统不会由于 IC 卡的更新而被改变，使系统的适应性大为增加，可以保证一卡通工程能够长期稳定地进行。

5. 可扩展的售卡系统

采用 CPU 卡后，在 IC 卡结构上设计有金融系统使用的文件区域，并且在售卡系统设计中保留有与银行系统接口的功能，具备与银行发行联名卡的条件，为将来实现一卡多用打下基础。

7.2　智能卡表部分

7.2.1　智能卡表的功能

1. 智能控制功能

智能卡表使用机电一体式 IC 卡表，采用脉冲采样方式自动计量用户表计的使用量，当用户使用量用完时，自动切断用户用电。

2. 预报警功能

当用户 IC 卡表中所剩使用量小于报警使用量时，能够给予用户报警提示，以便用户尽快购卡。

3. 使用量返读功能

用户每次将 IC 卡插入智能卡表后，智能卡表将自动把剩余使用量等信息回写到 IC 卡中，以供售卡管理系统查询。

4. 安全保护功能

采用 CPU 卡作为用户卡，在智能卡表内安装有 SAM，与 CPU 卡相互做密钥认证，具有高度安全性，严格保证一户一表一卡，每次用户卡只一次输入有效。

5. 补卡功能

当用户 IC 卡丢失时，可以通过售卡网络为用户补发 IC 卡。

6. 检查功能

售卡网络可以发行检查卡，定期对用户智能卡表运行情况进行检查。

7. 通信功能

表计管理部门可以根据需要在表计上建立一定的数据通信信道，对居民使用的相关智能卡表中的所有数据及时进行抄收。

7.2.2　智能卡表的安全控制

1. SAM 卡认证功能

智能卡表内有一个 ESAM 对 CPU 卡进行安全认证，同时存储智能卡表内的计量和状态数据。

2. 智能卡表通信功能

智能卡表内 CPU 与 CPU 卡以及 ESAM 通信均采用 T = 0 协议，智能卡表的安全认证由 CPU 卡和 ESAM 共同完成，表内 CPU 只起通信传递作用，不参与进行密钥加密计算的过程。

7.2.3 智能卡表数据项内容说明

1. 户号（10 位 5 字节）

表计管理部门在开户报装时为每一用户分配的编号，为压缩 BCD 码，严格做到一户一号不重复。在用户第一次购电时通过 IC 卡将户号传递到表号卡表，作为今后一表一卡的判断依据。

2. 表号（10 位 5 字节）

表号为智能卡表出厂编号，为压缩 BCD 码，由三部分组成：

表号 = 厂商编号 + 版本号 + 表计流水号

其中厂商编号为 2 位 1 字节，版本号为 2 位 1 字节，由各厂家根据情况而定，初始值均为 01。表计流水号为 6 位 3 字节。为各厂家生产时 IC 卡表的流水号，应保证一表一号不重复。智能卡表铭牌编号应与表号严格一致。

3. IC 卡类型（2 位 1 字节）

IC 卡类型即营业 IC 卡的类型编号，规定为

01—初始化卡；02—用户卡；03—检查卡；04—补卡；05—居民不记名卡；06—修改主密钥卡；07—商业不记名卡。

4. 剩余使用量（6 位 3 字节）

剩余使用量即智能卡表中允许用户还能使用的量。用户每次将 IC 卡插入智能卡表中时将剩余使用量返写至 IC 卡中。

5. 所购使用量（6 位 3 字节）

所购使用量即用户每次到银行网点交款所购使用量。智能卡表从 IC 卡中读入本次所购使用量应与表中剩余使用量相加作为当前实际剩余使用量。

6. 购卡次数（4 位 2 字节）

购卡次数即用户从开户起到银行网点交款购卡总次数，每购一次购卡次数加 1，若购卡次数为 9999，则下次加 1 翻为 0000。购卡次数对应不同的表计各不相同，各自独立。

7. 报警量（12 位 6 字节）

报警量即提醒用户尽快购卡的报警门限量。具体划分为报警量 1 和报警量 2，各为 6 位 3 字节，其中报警量 1 的值大于报警量 2 的值。当用户 IC 卡表中剩余使用量小于等于报警量 1 时，智能卡表的数码显示部分处于常亮状态，给予用户第一

次光报警。当智能卡表中剩余使用量小于等于报警量 2 时，切断用户水或电或气或热供应提醒用户，用户此时将 IC 卡插入智能卡表后可恢复供应，但此后数码管仍保持为常点亮状态，两次报警量值可任意设置。

8. 下限量（6 位 3 字节）

下限量即限制用户将所购使用量输入智能卡表的门限量。当智能卡表中剩余使用量大于等于限购量时，不接受用户本次所购使用量；只有当智能卡表中剩余使用量小于限购量后才能接受用户所购买的使用量，以免造成用户囤积使用量。不接受用户 IC 卡时数码管显示剩余使用量并闪烁给予用户提示，延时 10s 后自动消失。

9. 累计所购使用量（6 位 3 字节）

累计所购使用量即用户自开户起累计所购使用量。用户每次购买时，银行主机将比较从用户 IC 卡中返写的累计所购使用量与银行所存数据是否一致，一致才能进行下次购卡。当累计所购使用量超过 999999 时自动滚屏为 000000。

10. 累计应急所购使用量（6 位 3 字节）

累计应急所购使用量即用户使用不记名卡累计所购使用量。当累计所购使用量超过 999999 时自动滚屏为 000000。

11. 累计使用量（6 位 3 字节）

累计使用量即用户自开户起累计所用的量。当累计使用量超过 999999 时自动滚屏为 000000。

12. 过零使用量（6 位 3 字节）

当智能卡表中剩余使用为零后应断开用户供应，若此时智能卡表未能切断用户供应，则用户到下次购卡前所使用的量称为过零使用量。银行售卡网点每次购卡前需读入此单元并上传相应的表计管理中心，管理中心依据过零使用量决定对用户的处理流程。

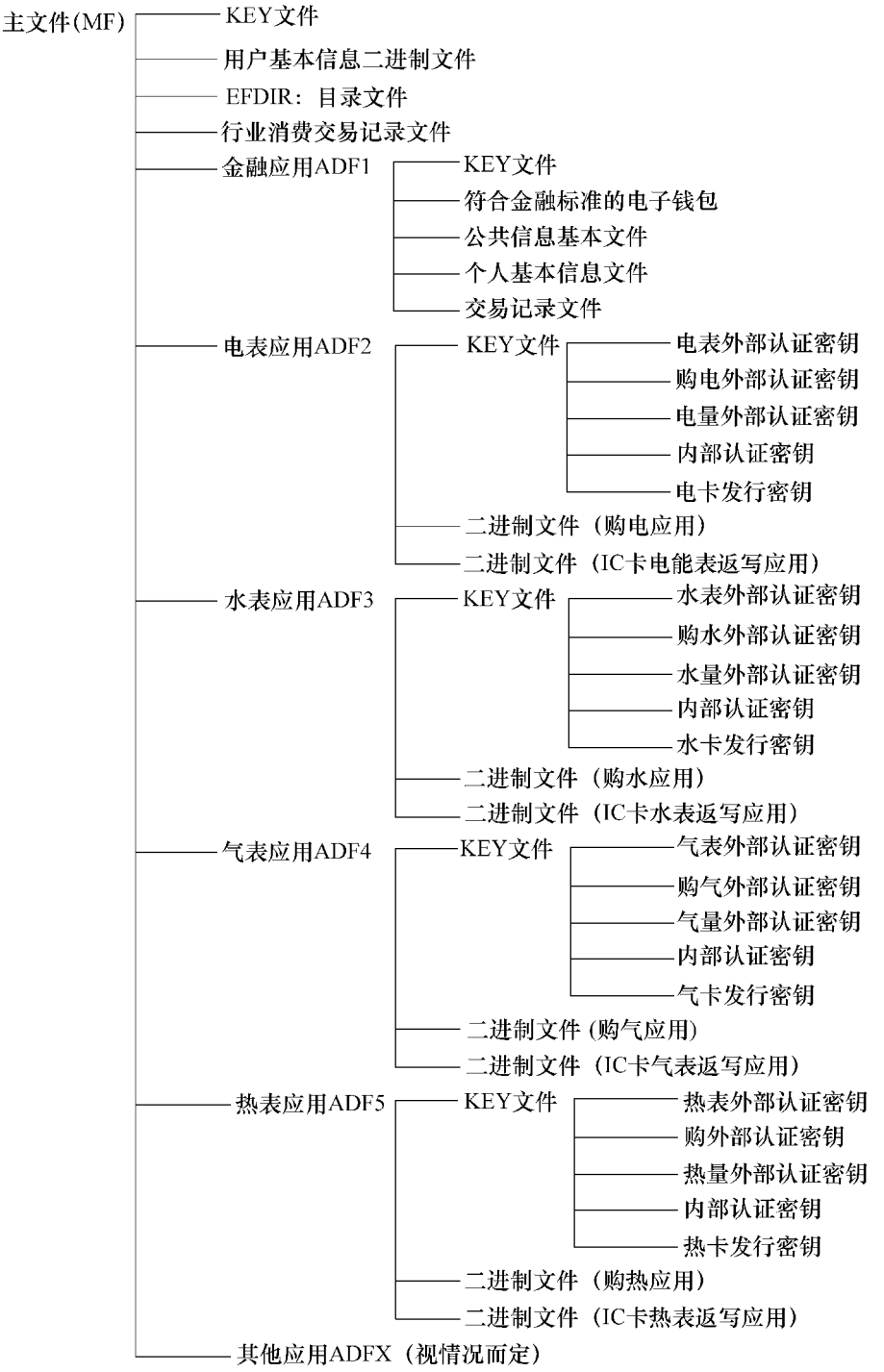
7.3　智能卡部分

7.3.1　智能卡分类及结构

智能卡为 CPU 卡，根据其功能以及使用环境不同，可以划分为用户卡、检测卡、不记名卡、修改主密钥卡、ESAM 卡和 PSAM 卡具体定义如下：

1. 用户卡

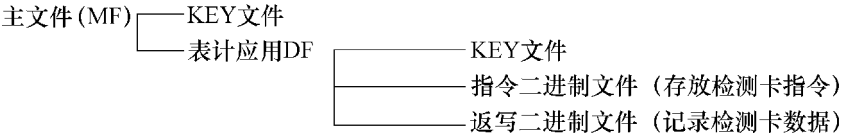
用户卡是指用户用来完成购卡以及向智能卡表中追加所购使用量的 IC 卡。其结构定义如下：


主文件(MF)
KEY文件
用户基本信息二进制文件
EFDIR：目录文件
行业消费交易记录文件
金融应用ADF1
KEY文件
符合金融标准的电子钱包
公共信息基本文件
个人基本信息文件
交易记录文件
电表应用ADF2
KEY文件
电表外部认证密钥
购电外部认证密钥
电量外部认证密钥
内部认证密钥
电卡发行密钥
二进制文件（购电应用）
二进制文件（IC卡电能表返写应用）
水表应用ADF3
KEY文件
水表外部认证密钥
购水外部认证密钥
水量外部认证密钥
内部认证密钥
水卡发行密钥
二进制文件（购水应用）
二进制文件（IC卡水表返写应用）
气表应用ADF4
KEY文件
气表外部认证密钥
购气外部认证密钥
气量外部认证密钥
内部认证密钥
气卡发行密钥
二进制文件（购气应用）
二进制文件（IC卡气表返写应用）
热表应用ADF5
KEY文件
热表外部认证密钥
购外部认证密钥
热量外部认证密钥
内部认证密钥
热卡发行密钥
二进制文件（购热应用）
二进制文件（IC卡热表返写应用）
其他应用ADFX（视情况而定）

为考虑与银行应用接轨，将智能卡表应用设计为几个不同的 DF，主文件（MF）结构保留给城市 IC 卡管理中心使用。在设计中做到不经过 MF 级就可直接访问表计应用 DF 目录。第一级目录文件开放作为金融应用，可以设置电子钱包进行消费交易和充值交易。在表计应用 DF 目录中包含三个文件，其中购卡应用二进制文件是银行写购卡信息的文件，智能卡表返写应用二进制文件是智能卡表返写数据的文件。对它们的写操作分别由 KEY 文件中购卡外部认证密钥、表计外部认证密钥和使用量外部认证密钥控制，用户卡必须通过内部认证以及相应的外部认证后才可以进行写操作，但对用户卡所有二进制文件的读操作则不需任何认证即可进行。用户卡发行密钥与售卡流程操作无关，是表计管理部门在初始化 IC 卡时的外部认证密钥，通过此认证才可以更改 IC 卡中的密钥。

2. 检测卡

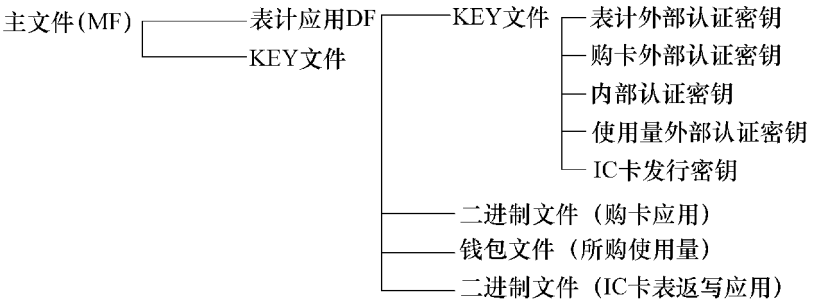
检测卡是表计管理部门和智能卡表生产厂家用来对智能卡表进行检测用的 IC 卡。此卡对所有智能卡表通用，插入智能卡表后将返回智能卡表内所有计量和状态信息，其结构如下：



由于检测卡是通用的工具卡，所以在其结构中只有一个空的 KEY 文件，不含有任何密钥，这样就可以很方便地制作和使用检测卡。指令二进制文件存放的是检测卡指令，返写二进制文件用来记录智能卡表返回的数据。

3. 不记名卡

不记名卡是表计管理部门单独在社会上发行的一次性使用的 IC 卡。当用户 IC 卡表中使用量用完且不能立即到银行储蓄网点进行下次购卡时，可以购买不记名卡作应急用。其结构如下：

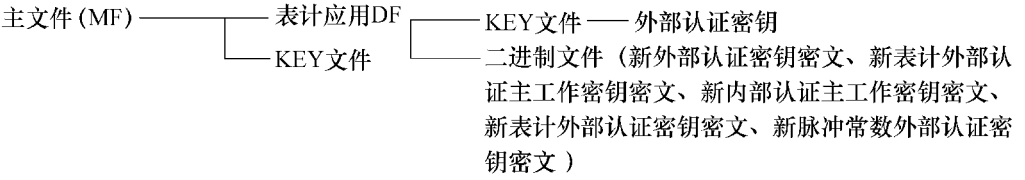


其中购卡应用二进制文件用来存放不记名卡指令，钱包文件存放不记名卡所购

使用量，该文件无存款权限，智能卡表密钥认证通过后一次扣减为零。IC 卡表返写应用二进制文件用来返写智能卡表表号备查。各表计管理部门在发行不记名卡时，应首先到城市 IC 卡管理中心领取本行业的不记名卡密钥主控卡，然后统一进行密钥分解制作本行业的不记名卡。

4. 修改主密钥卡

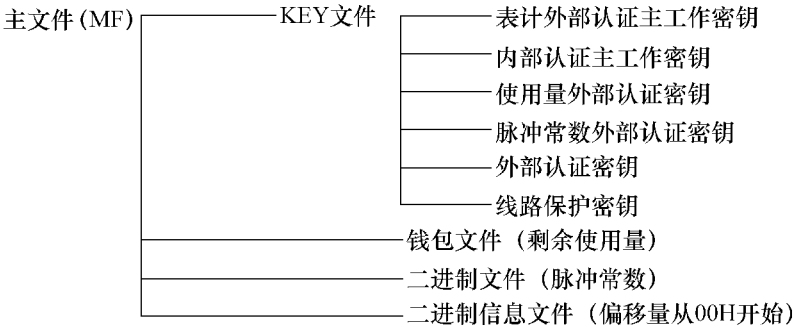
在智能卡表生产过程中，为方便智能卡表生产厂家测试，ESAM 中的主密钥是公开的，智能卡表出厂前，利用表计管理部门提供的修改主密钥卡将智能卡表内 ESAM 的主工作密钥修改为实际运行过程中的主密钥，智能卡表主密钥修改后也就意味着智能卡表生产厂家使用的 IC 卡不可能进入表计管理部门的管理系统，此主密钥由表计管理部门掌握，智能卡表生产厂家不可知。其结构如下：



将修改主密钥卡插入后，首先由 ESAM 对 IC 卡进行外部认证，认证通过后将 IC 卡中的五个密钥的密文读入，ESAM 利用线路保护密钥对它们进行解密，然后逐一替换 ESAM 中的主工作密钥。

5. ESAM 卡

所谓 ESAM 卡即智能卡表中的 ESAM，ESAM 在智能卡表中有两个作用：一是进行一表一卡的安全认证工作；二是作为 IC 卡表内数据存储区，其结构如下：

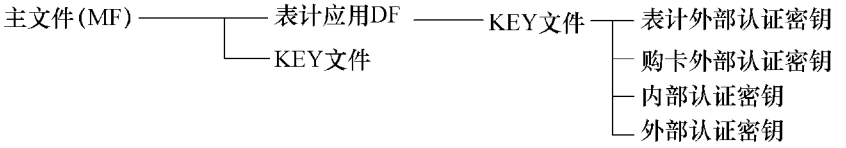


在 ESAM 中，KEY 文件中的表计外部认证主工作密钥和内部认证主工作密钥用于一户一表安全认证；外部认证密钥和线路保护密钥用于更换智能卡表应用主工作密钥；使用量外部认证密钥用来对钱包文件进行认证，剩余使用量增加时必须经过认证才能写入 ESAM，剩余使用量递减时不需通过认证；脉冲常数外部认证密钥用来对脉冲常数二进制文件进行安全认证，修改脉冲常数必须通过认证，但读操作

则不需认证；二进制信息文件用于存放智能卡表内部数据，不需认证可自由读写，其格式由各智能卡表生产厂家自定。

6. PSAM 卡

PSAM 卡是由城市 IC 卡管理中心发行的可以用于各种表计管理部门对用户卡进行充值和消费的认证卡，主要是作为各金融储蓄网点售卡时使用的认证卡，无此卡不能进行正常的售卡操作，PSAM 卡中无数据操作文件，只存放认证密钥。PSAM 卡制作完毕后，直接由城市 IC 卡管理中心提供给金融行业，安装在各金融储蓄网点的 POS 机中。其结构如下：



7.3.2　卡的密钥安全体系

1. 卡相关业务初始化流程（见图 7-1）

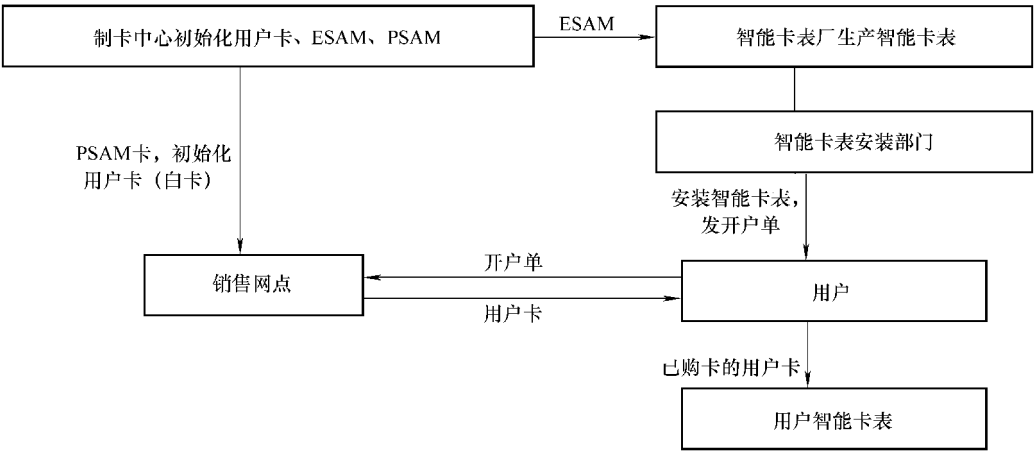


图 7-1　卡相关业务初始化流程

2. 卡密钥的种类、存储及生成关系

系统通过总控卡完成用户卡、ESAM 和 PSAM 卡的密钥初始化。总控卡存储 DES 加密密钥 MKEY，MKEY 是由若干位操作人员输入密钥初值，通过总控卡生成程序对特定的代码 D0 加密生成的。总控卡的 MKEY 通过对七个特定代码（D1，D2，D3，D4，D5，D6，D7）加密不同的主密钥。主密钥分别写入三种 ESAM 卡：

用户卡发行 ESAM 卡、ESAM 和 PSAM 卡。七个主密钥以 DES 加密密钥方式写入用户卡发行 ESAM 卡；购卡外部认证主密钥 BK_ MEKEY、表计外部认证主密钥 MEKEY、内部认证主密钥 MIKEY 以主工作密钥方式写入 PSAM 卡；表计外部认证主密钥 MEKEY、内部认证主密钥 MIKEY 以主工作密钥方式写入 ESAM，使用量外部认证密钥 POKEY、脉冲常数外部认证密钥 PUKEY、外部认证密钥 EXKEY、线路保护密钥 LIKEY 以密钥方式写入 ESAM。

修改主密钥卡只存有外部认证密钥，它用来对智能卡表 ESAM 进行 DES 加密用。此外部认证密钥是由用户卡发行 ESAM 卡以密钥方式写入的，因此所有修改主密钥卡上的外部认证密钥均相同。认证时，首先由智能卡表从 ESAM 取随机数送修改主密钥卡，修改主密钥卡对随机数进行 DES 加密后将加密结果送回智能卡表，智能卡表再将加密结果送 ESAM，并发外部认证指令，ESAM 认证通过后可以接受 IC 卡中的新密钥。

7.3.3 智能卡表数据文件的数据格式说明

数据在 IC 卡中采用不定长格式存放，在与 IC 卡进行数据交换或与数据抄收装置进行数据传输时均采用数据串的形式进行，具体格式如下：

起始	命令	长度	数据	校验	结束

起始：1B，为数据串的开始标识。

命令：1B，不同的命令表示与智能卡表进行数据交换的流程不同，它决定了数据串中数据的长度。

长度：1B，压缩 BCD 码，为数据串中数据区的长度。

数据：字节数不定，为前面介绍数据项的组合，组合方式与命令有关。

校验：1B，为命令、长度、数据三部分的累加和去除高字节自然溢出后得到，为十六进制数。

结束：1B，代表数据串结束。

对数据串是否有效的判别依据为起始、结束字节必须正确；长度与数据区字节数必须相等；校验必须正确。

利用数据抄收装置进行数据抄收时，采用串行通讯方式，通讯波特率为 1200，1 个启动位，8 个数据位，1 个偶校验位，1 个停止位，传送数据时低位在前。

7.4 表计管理部门和银行业务流程

7.4.1 业务流程组成

整个业务流程分为表计管理部门和银行两大部分，如图 7-2 所示。表计管理部

门侧由营业中心和各分局管理中心组成，通过电话拨号网络连接。各分局管理中心负责两项业务，一是用户报装，二是用户购卡结算统计；营业中心负责将各分局管理中心上传的用户报装数据进行打包整理发送给银行，并且根据上传数据为各分局制作用户卡，同时营业中心还负责将银行传来的交易数据进行解包整理下发给各分局管理中心，供分局管理中心进行收费统计，制作各种营业报表；银行侧由银行计算中心和各储蓄网点组成，通过银行专线连接成网络。银行计算中心负责进行每笔交易的计算和存储，并将购卡交易数据传给不同的表计管理部门营业中心。银行各储蓄网点负责为用户进行购卡以及补发 IC 卡业务，由于银行各储蓄网点已经实现网络化，因此可以实现用户异地购卡，即用户可以方便地在各个储蓄网点进行购卡。购卡时将用户所购使用量写入用户卡的购卡二进制文件中，同时将用户卡中表计返写二进制文件中的数据读出上传银行主机存储。银行主机与不同的表计管理部门营业中心主机通过专线（DDN、ISDN 等形式）连接，每天交换一次数据，营业中心将新开户、故障维修户、特殊处理户、价格变更情况传给银行主机；银行主机将当天购卡交易数据及购卡户表计返写信息传给不同的表计管理部门营业中心。

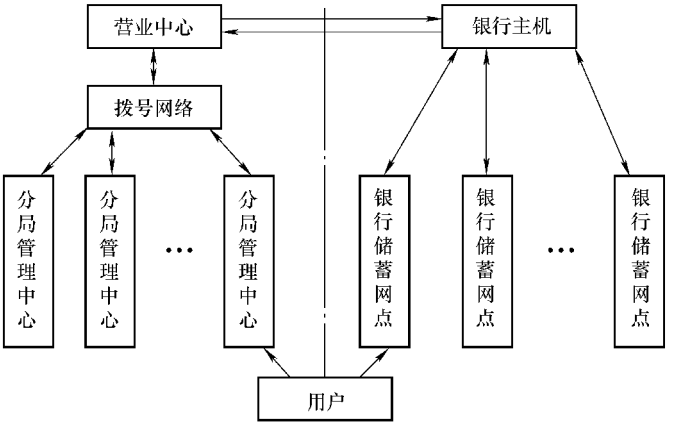


图 7-2　业务流程

7.4.2　表计管理部门营业中心密钥管理流程

1）营业中心由专人到城市管理中心领取本行业的密钥总控卡一张，并妥善管理。

2）营业中心由专人以特定程序通过专用设备用密钥总控卡生成 ESAM 发行卡、用户卡发行卡、PSAM 卡发行卡、修改主密钥卡发行卡、不记名卡发行卡各一张，并分别交专人管理。

3）根据使用需要，营业中心由专人持 PSAM 卡发行卡制作一批 PSAM 卡交银行发放给各储蓄网点使用。

4）根据使用需要，营业中心由专人持 ESAM 发行卡初始化 ESAM、持修改主

密钥卡发行卡制作一批修改主密钥卡供表计生产厂家使用。

5）根据市场需要，营业中心由专人持不记名卡发行卡制作一批不记名卡在市场上发行。

7.4.3 表计管理部门分局管理中心业务流程

1）用户 IC 卡表安装完毕后根据安装单开始报装业务，在售卡系统中登录用户表计信息及用户信息，给用户分配户号，设置相应的价格。

2）将当天开户的信息进行数据打包操作，并将打包后的数据上传给营业中心。

3）打印当日开户信息，制作用户开户单，并随用户卡发放给用户。

4）接收每天从营业中心传回的用户购卡交易数据并整理统计生成各种业务报表。

5）故障表处理、使用量增补扣减处理、换表及过户处理。

在表计管理部门分局管理中心所处理的业务中，与制卡、售卡等实际操作流程严格划开，只进行与系统内部收费营业相关的业务。

7.4.4 表计管理部门营业中心业务流程

1）负责本行业各级密钥的管理与使用，为智能卡表生产厂家提供修改主密钥卡及 SAM，为银行系统提供 PSAM 卡，为各分局管理中心提供初始化的用户卡。

2）每日将分局管理中心上传数据进行打包处理并传给银行主机。

3）每日将银行主机传来的购卡交易数据进行解包处理并下发分局管理中心。

4）对每日传递的数据进行监控及各种汇总分析处理，负责系统的安全运行。

7.4.5 银行储蓄网点业务流程

1）负责为用户进行购卡交易，并将购卡交易上传银行主机。交易过程中，储蓄网点终端通过 POS 机完成对用户卡的读写及安全认证工作。

2）负责为用户进行补卡交易操作。

3）负责将用户 IC 卡中的返写数据上传银行主机。

所有的购卡业务均在银行储蓄网点完成，与表计管理部门的业务管理系统严格分开。

7.4.6 银行主机业务流程

1）接收不同的表计管理部门营业中心信息，更新替换数据库内容。

2）与银行储蓄网点进行数据传递，完成用户购卡的相关交易，并将交易数据添加到数据库。

3）将每日交易数据及用户表计返写数据传输到不同的表计管理部门营业中心。

4）负责整个数据库的安全及备份工作。

参 考 文 献

[1] ISO/IEC 7816 – 1 Cards with contact – Physical Characteristics, 1998.

[2] ISO/IEC 7816 – 2 Cards with contact – Dimensions and Location of the Contacts, 1999.

[3] ISO/IEC 7816 – 3 Cards with contact – Electrical Interface and Transmission Protocols, 1997.

[4] ISO/IEC 7816 – 4 Organization, Security and Commands for Interchange, 2005.

[5] ISO/IEC 14443 – 1 Physical Characteristics, 2008.

[6] ISO/IEC 14443 – 2 Radio Frequency Power and Signal Interface, 2001.

[7] ISO/IEC 14443 – 3 Initialization and Anticollision, 2001.

[8] ISO/IEC 14443 – 4 Transmission Protocol, 2008.

[9] 王卓人，邓晋钧，刘宗洋. IC 卡的技术与应用［M］. 北京：电子工业出版社. 1998.

[10] 王爱英. 智能卡技术——IC 卡［M］. 2 版. 北京：清华大学出版社，2000.

[11] 杨振野. IC 卡技术及其应用［M］. 北京：科学出版社，2011.

[12] 刘守义. 智能卡技术［M］. 西安：西安电子科技大学出版社，2004.

[13] 张之津，李胜广，薛艺泽. 智能卡安全与设计［M］. 北京：清华大学出版社，2012.

[14] 张井合，吴今培，张其善. CPU 卡中 T = 0 通讯协议的分析与实现［J］. 电子技术应用，2002（10）.

[15] 邓赟. 智能卡操作系统（COS）安全管理研究［J］. 硅谷，2010（2）.

[16] 刘玉珍，涂航，张焕国，等. 实用智能卡操作系统的设计与实现［J］. 武汉大学学报：自然科学版. 2000（3）.

[17] 吴叶兰，陈红军. 智能卡表的安全技术研究［C］. 第二十三届中国控制会议，2004.

[18] 陈红军. 智能卡表的安全性分析［J］. 中国防伪报道，2006（11）.

[19] Yelan Wu, Shufang Zheng, Hongjun Chen. Low – Power Gas Meter Design and Implement Based on NEC MCU［C］. 2nd International Conference on Electric Information and Control Engineering (ICEICE 2012).

[20] NEC uPD78F0451 User's Manual: 78K0/LE3 8 – Bit Single – Chip Microcontrollers. 2007.

[21] MFRC522 Data sheet http://www.nxp.com/documents/data_sheet/MFRC522.pdf. 2010.

[22] 严雄武，梁楚樵. MIFARE 非接触式 IC 卡读卡器的设计架构研究［J］. 武汉理工大学学报，2004，26（12）：89 – 91.

[23] 王洪庆. 低功耗预付费智能燃气表的研制［J］. 制造业自动化，2009，31（12）：185 – 188.

[24] 崔洋，姜宇. 数字远传燃气表的低功耗设计与实现［J］. 传感技术学报，2010，23（2）：209 – 214.

ZHINENG KABIAO JISHU YU YINGYONG

地址：北京市百万庄大街22号
邮政编码：100037
电话服务
社服务中心：010-88361066
销售一部：010-68326294
销售二部：010-88379649
读者购书热线：010-88379203
网络服务
教材网：http://www.cmpedu.com
机工官网：http://www.cmpbook.com
机工官博：http://weibo.com/cmp1952
封面无防伪标均为盗版

上架指导：工业技术／仪器仪表
ISBN 978-7-111-39929-2
策划编辑◎牛新国/ 封面设计◎赵颖喆

ISBN 978-7-111-39929-2
9 787111 399292 >
定价：29.90元