智能卡技术

王爱英　主编

清华大学出版社

目　录

前言 …… I
第1章　智能卡概论 …… 1
1.1　智能卡基础知识 …… 1
1.1.1　什么是智能卡 …… 1
1.1.2　IC卡的接口设备 …… 2
1.2　金融卡的应用基础 …… 3
1.2.1　IC卡提供的信息 …… 3
1.2.2　举例——在自动柜员机上实现取款 …… 3
1.2.3　IC卡存储区的分配和功能简介 …… 4
1.2.4　接口设备存储器内容简介 …… 4
1.2.5　使用智能卡完成一次购物的操作过程 …… 5
1.2.6　发展智能卡与人有关的因素 …… 5
1.2.7　智能卡的种类 …… 6
1.3　智能卡的安全问题 …… 6
1.3.1　影响智能卡安全的若干基本问题 …… 6
1.3.2　安全措施 …… 7
1.3.3　密钥与认证 …… 7
1.3.4　卡片的作弊问题 …… 7
1.4　识别卡的国际标准 …… 8
1.4.1　磁卡的国际标准 …… 8
1.4.2　IC卡(接触型)的国际标准 …… 8
1.5　金卡工程(电子货币工程) …… 9
1.5.1　金卡工程的总体设想 …… 9
1.5.2　银行卡基本业务需求 …… 11
1.5.3　金卡工程总体结构 …… 12
1.5.4　应用软件设计要求和设备功能 …… 20
1.5.5　安全与保密 …… 22
1.5.6　技术标准与规范 …… 22
1.6　智能卡的诞生与发展 …… 23
1.7　本书内容简介 …… 24
第2章　磁卡 …… 26
2.1　概述 …… 26
2.2　金融交易卡第1磁道的格式及内容 …… 31

2.3 金融交易卡第2磁道的格式及内容 …… 32
2.4 金融交易卡第3磁道的格式及内容 …… 33
2.5 主帐号格式 …… 40
2.6 金融交易内容 …… 42
2.7 磁卡存在的问题 …… 45
2.8 与磁卡有关的国际标准 …… 45
第3章 IC卡国际标准(一) …… 47
3.1 ISO 7816-1,接触型集成电路卡的物理特性 …… 47
3.2 ISO 7816-2,接触型集成电路卡的触点尺寸和位置 …… 48
3.3 ISO/IEC 7816-3,接触型集成电路卡的电信号和传输协议 …… 48
3.3.1 触点的电特性 …… 49
3.3.2 IC卡的操作过程 …… 52
3.3.3 卡的复位 …… 52
3.3.4 异步传输的复位应答(Answer To Reset) …… 54
3.3.5 同步传输的复位应答(Answer To Reset) …… 58
3.3.6 协议类型选择PTS(Protocol Type Selection) …… 58
3.3.7 异步半双工字符传输协议(T=0) …… 59
3.4 ISO/IEC 7816-3 AMENDENT 1 异步半双工分组传输协议(T=1) …… 61
3.4.1 分组基本组成——分组帧(Block frame) …… 61
3.4.2 专用接口参数 …… 62
3.4.3 协议操作 …… 63
第4章 IC卡国际标准(二) …… 67
4.1 ISO/IEC 7816-4(行业间交换用命令)规定的范围 …… 67
4.2 数据结构 …… 67
4.2.1 文件组织 …… 67
4.2.2 数据访问(存取)方式 …… 68
4.2.3 文件控制信息(FCI) …… 70
4.3 卡的安全结构 …… 71
4.3.1 安全状态 …… 71
4.3.2 安全属性 …… 72
4.3.3 安全机制 …… 72
4.4 应用协议数据单元(APDU)的信息结构 …… 72
4.4.1 命令APDU …… 73
4.4.2 应答APDU …… 74
4.4.3 命令头部、数据字段和应答尾部的代码约定 …… 74
4.5 基本行业间命令 …… 79
4.6 历史字节 …… 98
4.6.1 目的和一般结构 …… 98

4.6.2 类型指示符(必有的) …… 98
4.6.3 可选的 COMPACT-TLV 对象 …… 98
4.6.4 状态信息 …… 102
4.6.5 DIR 数据访问 …… 103
4.7 与应用无关的卡服务 …… 103
4.7.1 定义和范围 …… 103
4.7.2 卡识别服务 …… 103
4.7.3 应用选择服务 …… 104
4.7.4 数据对象检索服务 …… 104
4.7.5 文件选择服务 …… 104
4.7.6 文件 I/O 服务 …… 105
4.8 ISO/IEC 7816-5 应用标识符的编号系统和注册过程 …… 106
4.8.1 定义和缩写 …… 106
4.8.2 数据单元 …… 106
4.8.3 检索 ASN.1 对象 …… 108
4.8.4 数据单元的使用 …… 109
4.8.5 标识符的注册 …… 109
第5章 智能卡的安全和鉴别 …… 112
5.1 对智能卡安全的威胁 …… 112
5.2 物理安全 …… 112
5.3 逻辑安全 …… 113
5.3.1 用户鉴别 …… 113
5.3.2 存储区域保护 …… 115
5.3.3 智能卡的通信安全与保密 …… 116
5.4 密码技术 …… 118
5.4.1 对称密码体制 …… 119
5.4.2 非对称密码体制 …… 125
5.4.3 密钥管理 …… 129
5.5 鉴别体制 …… 129
5.5.1 对称鉴别体制 …… 129
5.5.2 非对称鉴别体制 …… 131
第6章 IC卡及其专用芯片 …… 134
6.1 IC卡的存储器芯片 …… 134
6.2 逻辑加密卡分析 …… 141
6.2.1 名词解释 …… 141
6.2.2 功能框图 …… 142
6.2.3 芯片内部存储区域分配 …… 143
6.2.4 AT88SC102 分析 …… 144

6.2.5 SLE4404 分析 …… 151
6.2.6 几种典型电路分析 …… 154
6.3 智能卡的硬件环境 …… 157
6.4 智能卡的操作系统——COS …… 159
6.4.1 COS 概述 …… 159
6.4.2 COS 的体系结构 …… 160
6.4.3 COS 的命令系统 …… 166
6.5 智能卡举例(MC68HC05SC 系列) …… 170
第7章 IC 卡接口设备技术 …… 181
7.1 IC 卡接口设备的组成 …… 181
7.2 IC 卡适配插座(IC 卡座) …… 182
7.2.1 IC 卡适配插座的结构形式 …… 182
7.2.2 选择 IC 卡适配插座时的几个重要的指标 …… 183
7.3 IC 卡的接口电路和读写控制 …… 183
7.3.1 IC 卡的接口电路 …… 183
7.3.2 IC 卡的控制与读写技术 …… 185
7.4 IC 卡的应用设备 …… 194
7.4.1 专用的 IC 卡应用设备 …… 195
7.4.2 通用型 IC 卡应用设备 …… 197
第8章 自动柜员机 ATM 和销售点终端 POS …… 200
8.1 ATM 的功能和结构 …… 200
8.1.1 ATM 的硬件构成 …… 200
8.1.2 ATM 的软件 …… 204
8.1.3 ATM 的机械结构 …… 205
8.1.4 ATM 应用流程 …… 206
8.1.5 ATM 应用现状与前景 …… 207
8.2 POS 和 POS 系统 …… 207
8.2.1 POS 结构和功能 …… 207
8.2.2 POS 终端的三种类型 …… 209
8.2.3 POS 系统的构成与应用 …… 209
第9章 IC 卡应用技术 …… 213
9.1 IC 卡的应用概况与技术优势 …… 213
9.2 IC 卡的应用模式与特点 …… 214
9.3 IC 卡的应用领域 …… 216
9.3.1 IC 卡在金融领域的应用 …… 216
9.3.2 IC 卡在非金融领域的应用 …… 219
9.4 IC 卡应用系统的开发 …… 222
9.5 IC 卡应用系统的安全性和可靠性 …… 225

附录 A　有关识别卡的国际组织及识别卡标准 …… 227
附录 B　台湾 IC 金融卡规格(参考) …… 230
附录 C　T=0 的 APDU 传输 …… 236
附录 D　T=1 的 APDU 传输 …… 242
附录 E　RSA 密码算法的实现 …… 245
附录 F　智能卡的设计、制造、个人化和发行 …… 250
附录 G　英文缩写词 …… 255
参考文献 …… 258

第1章 智能卡概论

1.1 智能卡基础知识

1.1.1 什么是智能卡

智能卡的名称来源于英文名词“smart card”，又称集成电路卡，即IC卡(Integrated Circuit Card)。它将一个集成电路芯片镶嵌于塑料基片中，封装成卡的形式，其外形与覆盖磁条的磁卡相似。

IC卡的概念是70年代初提出来的，法国布尔(BULL)公司于1976年首先创造出IC卡产品，并将这项技术应用到金融、交通、医疗、身份证明等多个行业，它将微电子技术和计算机技术结合在一起，提高了人们生活和工作的现代化程度。

IC卡芯片具有写入数据和存储数据的能力，IC卡存储器中的内容根据需要可以有条件地供外部读取，或供内部信息处理和判定之用。根据卡中所镶嵌的集成电路的不同可以分成以下三类：

1. 存储器卡　卡中的集成电路为EEPROM(可用电擦除的可编程只读存储器，也可写作E^2PROM。)

2. 逻辑加密卡　卡中的集成电路具有加密逻辑和EEPROM。

3. CPU卡　卡中的集成电路包括中央处理器CPU、E^2PROM、随机存储器RAM以及固化在只读存储器ROM中的片内操作系统COS(Chip Operating System)。

严格地讲，只有CPU卡才是真正的智能卡，但在本书中，为了论述全面，更为了应用的需要，我们将研究讨论上述三种IC卡。

按应用领域来分，IC卡有金融卡和非金融卡两种。金融卡又有信用卡(credit card)和现金卡(debit card)等。信用卡主要由银行发行和管理，持卡人用它作为消费时的支付工具，可以使用预先设定的透支限额资金。现金卡可用作电子存折和电子钱包，不允许透支。非金融卡往往出现在各种事物管理、安全管理场所，如身份证明、健康记录和职工考勤等。

按卡与外界数据传送的形式来分，有接触型IC卡和非接触型IC卡两种。当前使用广泛的是接触型IC卡，在这种卡片上，IC芯片有8个触点可与外界接触。非接触型IC卡的集成电路不向外引出触点，因此它除了包含前述三种IC卡的电路外，还带有射频收发电路及其相关电路。

在IC卡推出之前，从世界范围来看，磁卡已得到广泛应用，为了从磁卡平稳过渡到IC卡，也是为了兼容，在IC卡上仍保留磁卡原有的动能，也就是说在IC卡上仍贴有磁条，因此IC卡也可同时作为磁卡使用，图1.1为IC卡的外观图，正面中左侧的小方块中有8个触点，其下面为凸型字符，背面有磁条。正面还可印刷各种图案，甚至人像。卡的尺寸、触点的位置与用途、磁条的位置及数据格式等均有相应的国际标准予以明确规定。

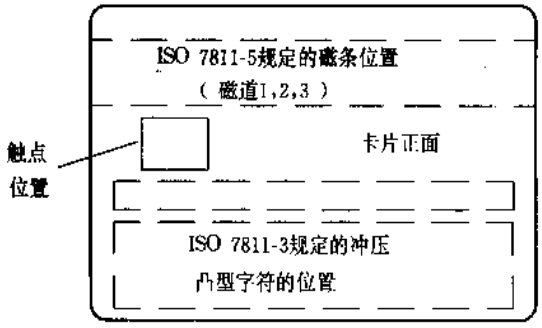


图 1.1　IC 卡的外观图

无论是磁卡还是 IC 卡，卡上都有唯一的发行人和持卡人的识别标志，这种卡有时称之为识别卡。

1.1.2　IC 卡的接口设备

为了使用卡片，还需要有与 IC 卡配合工作的接口设备 IFD(InterFace Device)，或称为读写设备。IFD 可以是一个由微处理器、键盘、显示器与 I/O 接口组成的独立设备，该接

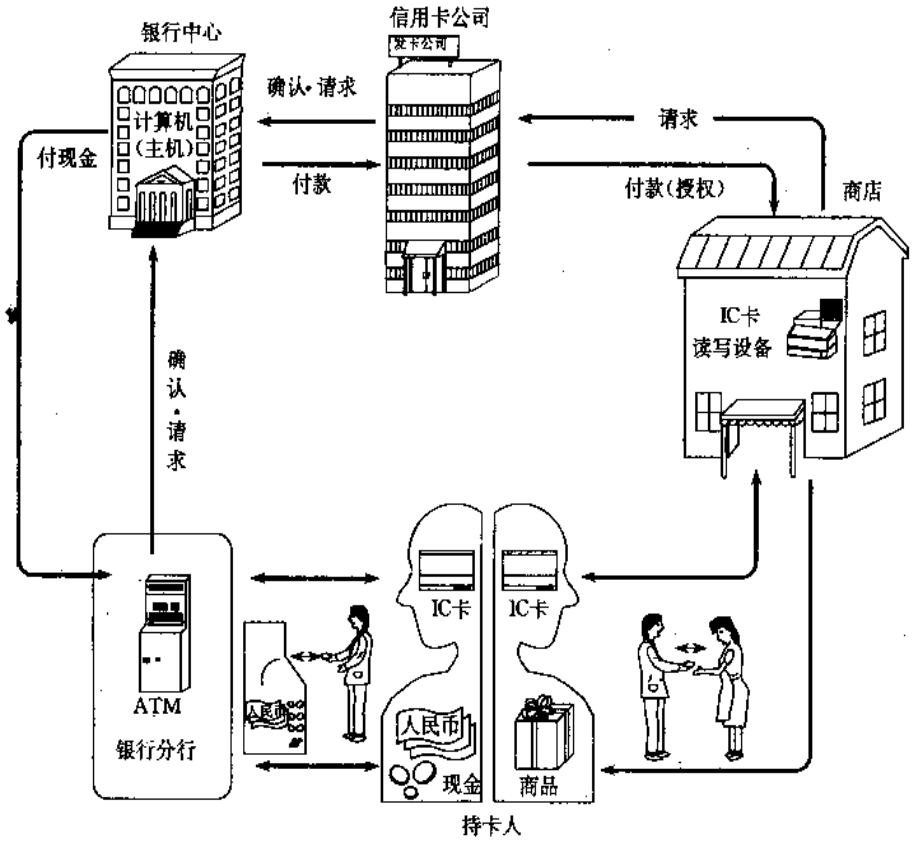


图 1.2　IC 卡应用过程

口设备通过IC卡上的8个触点向IC卡提供电源并与IC卡相互交换信息。IFD也可以是一个简单的接口电路，IC卡通过该电路与通用微机相连接。无论是磁卡或IC卡，在卡上能存储的信息总是有限的，因此大部分信息需要存放在接口设备或计算机中。当用信用卡购物时，如在允许透支范围内，则可以先取走商品，事后再结算；如需一笔大款，则需经银行确认，授权于商店后，才能取走商品。由于银行、发放信用卡的公司以及商店不在同一处，因此需要经过通信线路和计算机(主机)联系才能实现上述过程。

图1.2(右半部)示出使用信用卡购物的过程。

为了快速而又可靠地进行处理，计算机网络与通信线路的安全与响应时间是关键。

图1.2(左半部)是在ATM(自动柜员机)上自动取款(稍后说明)。

1.2 金融卡的应用基础

IC卡主要用作金融卡，金融卡的主要功能是存储数据和处理数据。

1.2.1 IC卡提供的信息

1. 印在卡上的可供人阅读的信息　用以标识卡发行人的标志、使用期限、客户姓名、帐号和签名等，这些信息是卡能作为金融交易中的支付工具的基础。

2. 机器可读数据　卡上的凸出字符用于压印帐单，以便向售货商和客户提供交易凭证。卡上还可提供金融交易的帐目。

3. 提供机器可读的授权和数据收集系统的标识符。

1.2.2 举例——在自动柜员机上实现取款

下面以自动柜员机ATM为例进行说明。

自动柜员机是放在银行或商店大堂中供客户自动提款的机器(有的ATM还有自动存款功能)。执行从ATM提取现金的操作仅需十几秒钟，总共只需要作出4个输入动作：

1. 插入金融卡；
2. 输入个人标识码(PIN)；
3. 选择交易类型(取款)；
4. 给出申请提取的金额。

当ATM判别没有问题时，自动输出卡和现金，并打印凭证。由此可见，ATM是一种操作方便的信息处理系统，可以24小时提供服务。

ATM是安装在柜里的计算机系统，它要处理卡片、货币、收据和信封(存款用)四种介质，并能与相连接的远程计算机相互通信。它的内部有严密的可靠的物理和逻辑安全措施。它的每一笔交易通常接受正确的授权和严格的控制，因此ATM系统既是一个操作简单的系统，又是一个构造复杂的系统。

ATM将磁条上(对磁卡)的数据，诸如发行人和客户帐号识别码(用来获取自动授权信息的基础)通过通信线路与发卡单位的计算机及其帐户数据库相连，用以检查金融卡的编号(查对黑名单)，以防止他人使用已挂失的或偷窃来的金融卡，同时核对客户的帐面记

录，以查明可供支用的金额，并根据交易的金额随即更新帐面记录，供金融卡下次使用。此外，为了避免某些可能发生的弊端(如已挂失但尚未列入黑名单)，还要限制金融卡在一天内允许使用的次数和一天内允许提取现金的总金额。

绝大多数ATM机取款时还需输入个人标识符PIN，并将PIN送到计算机，用来核对持卡人是否是卡的主人。如在通信线路上明文传送PIN，存在被窃听的危险，为此需对PIN进行加密，这就要提供一个加密算法和"密钥"，让经过加密后的PIN在通信线路上传送，在接收端解密，因此在接收端提出了密钥的管理和保护的要求(参考第5章)。

1.2.3 IC卡存储区的分配和功能简介

IC卡的存储量比磁卡大得多，一般分四个存储区。

1. 公开的(不保密的)存储区　内含公用信息，诸如发行标识符，持卡人的帐号等。

2. 外部不可读的存储区　存储的内容是供内部决策用的，如PIN值，该值是在卡片发行时进行个人化处理写入的，用户在输入正确的PIN值后，允许输入新PIN值进行修改，但在任何情况下，都不允许将存储在卡中的PIN值向外界传送。在本存储区内还可能存放密钥。

3. 保密存储区　内含帐面余额、允许卡使用的服务类型及限额等。当持卡人输入正确的PIN值后，允许读取本存储区数据，并根据应用情况写入正确数据(如修改余额)。

4. 记录区　内含每次交易细节，称为日志，可供查询。

除了存储器卡外，在其它IC卡中还有逻辑电路或微处理器，提供安全可靠的服务。

1.2.4 接口设备存储器内容简介

与智能卡配合使用的接口设备(或称为读写设备、读卡器)应该提供附加的存储器和逻辑电路，它本身可能就是一台微机。

用于商店中的接口设备的存储器中包含如下内容：

1. 交易数据　内含每次交易记录，一般于每天晚上将当天交易细节汇总后传送到开户银行或发卡银行，供转帐和清算之用。银行应保证及时将应付款存入售货商帐户。

2. 非法卡表(或称为黑名单、止付名单)　列出所有挂失、被窃或透支超过限额的帐户清单，在每天向银行递交交易细节时，也递交此清单。同时银行经汇总后，应将修改后的黑名单提供给售货商。凡登在黑名单上的帐户或透支超额的帐户要进行交易时，须由售货商用专用电话和银行进一步授权核实后，方可受理。也可拒绝处理，甚至可根据实际情况将卡没收。

3. 保密数据　密钥和授权电话号码即属于保密数据，密钥用以生成校验码以防交易日志被修改。至于授权电话，在售货商希望成交某些超额交易时，用它接通用户银行，经银行授权后方可受理，如果电话通信线路很忙，那么等待授权的时间可能很长，甚至能让客户觉得无法容忍，这就会影响到金融卡的推广应用。较先进的系统应靠计算机网络和通信线路来完成授权功能。

1.2.5 使用智能卡完成一次购物的操作过程

操作顺序如下：

1. 客户拿着金融卡和购买的商品来到付款处。并将金融卡插入能输入 PIN 的小键盘设备中。

2. 售货员通过他本人工作的键盘输入交易金额。

3. 交易金融显示在小键盘设备的显示板上。

4. 客户在小键盘上按下某个指定键，表示对交易金额的认可。

5. 小键盘设备的显示板上指示客户输入 PIN。然后客户输入 PIN。输入后自动与卡中的 PIN 比较，如一致，就将金融卡自身打开，准备受理交易。

6. 接着接口设备内部进行一连串处理，如查对黑名单、核实资金是否够用、计算交易后的余额，将它登入交易日志记录里并计算出安全校验码加在日志记录中以保证数据的安全。同时把这笔交易记录也写到金融卡中。最后给客户打印收据。

7. 显示板指示交易结束，客户取走商品和卡。

1.2.6 发展智能卡与人有关的因素

参与智能卡操作的相关方面有：持卡人或用户，商店，卡片的发行者及销售部门，卡片的设计者、出售商及安全维护。

1. 持卡人或用户

用户要求：

- 使用方便：装置的地点、使用的时间和操作的步骤等力求方便。操作一学就会。
- 启用手续简易：发行和基于 PIN 号的卡片个人化处理手续简易。
- 加快交易时间：进行一次交易或授权等待时间尽量缩短。
- 安全可靠：每次交易正确无误，操作错误后的重新启动方便可靠，卡片的丢失、被窃和 PIN 值的更换等容易处理。
- 清楚简单的操作提示：卡片上清楚表明接口方向，显示屏幕清楚易读，避免使用计算机术语和复杂的交互式操作。

2. 商店

商店期望：

- 人员培养容易，操作过程和例外处理简单。
- 故障处理简单：故障处理包括出错后的重新启动，例外情况或交易被拒绝时的处理，以及在正常的解决办法失灵时，其他可供选择的措施。
- 安全可靠：对丢失、被窃以及未付帐款的卡片处理办法简单且安全，对各类不安全因素易于检测。

3. 卡片的发行者和销售部门

除了满足商店和用户的要求以外，应做好有关方面(银行、商店、用户)之间的信息交换工作，以及用户忘了 PIN 后的处理工作等。

4. 设计者、出售商及安全维护

设计目标应满足用户及商店的要求。电子设备应保证能够每天 24 小时不间断工作，并能很容易测试判断智能卡是否工作正常。机械设计要保证设备和零件工作可靠。设计好对例外情况的处理办法，并能迅速排除故障。

1.2.7 智能卡的种类

1. 信用卡　卡中预先建立允许透支的限额，即预先设置好可借用的资金额度，承诺到期归还并支付利息的责任。根据持卡人信用程度的不同，有两种信用卡：金卡和普通卡。前者的透支限额高。

2. 现金卡(付款卡)　供储蓄帐户使用，持卡使用的资金是客户已经存放在银行中的存款。

3. ATM 卡　只能在 ATM 中使用的现金卡或信用卡。

4. 预付卡　按卡面价值购买，先购买，后使用，例如电话和公共系统用的预付卡，电表预付卡等。

另外还有诸如大饭店内部使用的卡，客人进入饭店后，住宿、用餐、娱乐等都可凭卡记帐，离开饭店时结帐。

1.3 智能卡的安全问题

智能卡的作用是替代流通领域中的现金或支票，随着智能卡的推广使用，利用它进行欺诈或作弊的行为也会不断增加，对于出现的不安全问题的解决办法需要在提供合理的效果和防护的保证与所需的成本和投资之间进行平衡，从而提出一个折衷的解决办法。

1.3.1 影响智能卡安全的若干基本问题

在众多智能卡安全问题中有下列基本问题需要解决：

1. 智能卡和接口设备之间的信息流通　这些流通的信息可以被截取分析，从而可被复制或插入假信号。

2. 模拟智能卡(或伪造智能卡)　模拟智能卡与接口设备之间的信息，使接口设备无法判断出是合法的还是模拟的智能卡。

3. 在交易中间更换智能卡　在授权过程中使用的是合法的智能卡，而在交易数据写入之前更换成另一张卡，因此将交易数据写入替代卡中。

4. 修改信用卡中控制余额更新的日期　信用卡使用时需要输入当天日期，以供卡判断是否是当天第一次使用，即是否应将有效余额项更新为最高授权余额(也即是前面讲到的，允许一天内支取的最大金额)，如果修改控制余额更新的日期(即上次使用的日期)，并将它提前，则输入当天日期后，接口设备会误认为是当天第一次取款，于是将有效余额更新为最高授权余额，因此利用窃来的卡可取走最高授权的金额，其危害性还在于(在银行提出新的黑名单之前)可重复多次作弊。

5. 商店雇员的作弊行为　接口设备写入卡中的数据不正确，或雇员私下将一笔交易写成两笔交易，因此接口设备不允许被借用、私自拆卸或改装。

1.3.2 安全措施

为了安全防护，一般采取以下措施：

1. 对持卡人、卡和接口设备的合法性的相互检验。

2. 重要数据加密后传送。

3. 卡和接口设备中设置安全区，在安全区中包含有逻辑电路或外部不可读的存储区，任何有害的不合规范的操作，将自动禁止卡的进一步操作。

4. 有关人员明确各自的责任，并严格遵守。

5. 设置止付名单(黑名单)。

1.3.3 密钥与认证

1. IC 卡系统中常用的两种密码算法

(1) 对称密钥密码算法或秘密密钥密码算法(DES)

(2) 非对称密钥密码算法或公共密钥密码算法(RSA)

对持卡人、智能卡和接口设备之间的相互认证以及数据的加密均可采用这两种密码算法中的一种。

与加密有关的还有解密和密钥管理，密钥管理包括：密钥的生成、分配、保管和销毁等。

对传输的信息进行加密，以防被窃取、更改，从而避免造成损失。对存储的信息进行加密保护，使得只有掌握密钥的人才能读取信息。

2. 认证

为防止信息被篡改、伪造或过后否认，特别是对被传输的信息，加密认证就显得更为重要。

(1) 信息验证　防止信息被篡改，保护信息的完整性，要求在接收时能发现被篡改的数据，例如可采用一定的算法产生附加的校验码，在接收点进行检验。

(2) 数字签名(电子签名)　要求：收方能确认发方的签名；发方签名后，不能否认自己的签名；发生矛盾时，公证人(第三方)能仲裁收发方的问题。

为实现数字签名，一般要求用公共密钥解决。

(3) 身份认证：用 password 或个人身份号 PIN 进行认证，更可靠的是利用生物特征。

本处讨论的密钥与认证问题将在第 5 章详细讨论。

1.3.4 卡片的作弊问题

从磁卡使用情况来看，造成发卡行损失的有两种情况：

1. 呆帐　持卡人到时不付帐。

2. 作弊　是由于犯罪行为引起的，因此在塑料卡上采取了一些防范措施。例如 VISA 卡采取了以下措施：正面有全息飞鸽图形；精细的底版印刷；非凸形的标识号；卡片上有签字条，当签字被更改时，签字条立即显示出 VOID(作废)。

其他根据需要还可以作出照片、指纹等个人标识。

除了卡片外，磁条也是很有问题的，例如磁条上的记录具有以下特点：可读出，可更改，可伪造，可模拟，可擦掉。

为了避免由于作弊造成的损失，因此磁卡使用时（尤其是超过现额时）需经过授权验证。

读取IC卡中的信息较磁卡为难，尤其是智能卡，可通过加密验证等手段使得冒用或伪造变得困难起来，因此与磁卡相比可使用在脱机情况下。但是实际上没有绝对的秘密可言，因为客观上存在着能力很强的对手，既使有加密方法，也肯定能找到解密的方法，只不过是要耗费多大代价，是否值得的问题，即使是好的设计也会存在不同程度的易被击破的弱点。

1.4 识别卡的国际标准

由于信用卡可在国内各地使用，某些还能在国外使用，因此制定国际和国家标准是迫切需要的，国家标准应该尽量与国际标准一致。

识别卡是一种可识别其发行者和持有者的卡。金卡支付业务中用得最多的是信用卡，它是一种识别卡。识别卡分磁卡和IC卡两类。

1.4.1 磁卡的国际标准

1. 物理特性　包括卡的材料、构造、特性、标称尺寸等均应符合国际标准ISO 7810：1985。

2. 凸印　卡正面显著地凸起的字符称为凸印，用于数据传送，这种传送可以通过压印机，也可以用目视或机器阅读。凸印字符包含标识号，持卡人的姓名和地址。常用的ID-1型卡上凸印字符的位置应符合国际标准ISO 7811-3：1985的规定。

凸印字符及其字体的选择应符合ISO 1073-1和ISO 1073-2和ISO 7811-1附录B、附录C描述的7B字体的规定，凸印字符的字符间距、高度等符合国际标准ISO 7811-1：1985的规定。凸印字符的印刷规范符合ISO 1831：1980的规定。

3. 磁条　磁条上磁性材料的物理特性和性能特性、编码技术和编码字符集有相应的国际标准ISO 7811-2：1985。磁条上共有三个磁道，第一、二磁道为只读磁道，第三磁道为读写磁道，分别有国际标准ISO 7811-4：1985和ISO 7811-5：1985。

有关磁卡的较为详细的介绍请见本书第2章。

1.4.2 IC卡（接触型）的国际标准

1. 物理特性　符合ISO 7810：1987中规定的各类识别卡的物理特性和ISO 7813中规定的金融交易卡的全部尺寸要求，此外还应符合国际标准ISO 7816-1：1987规定的附加特性、机械强度和静电测试方法。

2. 触点尺寸与位置。

应符合国际标准ISO 7816-2：1988中的规定。

3. 电信号与传输协议。

IC 卡与接口设备之间电源及信息交换应符合 ISO/IEC 7816-3:1989 的规定。

4. 行业间交换用命令。

有相应的国际标准 ISO/IEC 7816-4：1994。但该版本尚未正式通过。

5. 应用标识符的编号系统和注册过程　应符合国际标准 ISO/IEC 7816-5:1994 中的规定。

IC 卡的国际标准是本书重点之一，将在第 3 章和第 4 章中描述。

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，读者应注意国际标准的最新版本。

1.5　金卡工程(电子货币工程)

金卡工程(电子货币工程)是我国金融电子化建设的重要组成部分。电子货币是现代化货币流通的形式，它集计算机、通信、金融和商业专用机具为一体，以金融交易卡(信用卡和现金卡)为介质，并通过电子信息转帐形式实现货币流通。金卡工程就是为实现电子货币大范围流通的跨部门、跨地区和跨世纪的系统工程。

金卡工程的实现可减少社会上现金的流通量和货币的发行量，加强国家对资金的宏观调控和决策能力。这对国家掌握各种金融活动和资金的流动情况，加速资金的周转提供了现代化技术手段；并对抑制通货膨胀、稳定社会治安、减少经济犯罪起良好作用。

本节内容未经核实，纯按技术问题讨论，仅供参考。

1.5.1　金卡工程的总体设想

1. 金卡工程的发展

先从金融卡(银行卡)起步，用 10 年(1994 年—2003 年)时间，在全国 400 个城市及部分经济发达的县城推广使用。在 3 亿城市人口地区，计划发卡量达到 2 亿张。

将 10 年时间划分成 3 个阶段：试点阶段(3 年)、推广阶段(3 年)和普及阶段(4 年)。

(1) 试点阶段　选择 12 个省市进行金卡工程试点。这 12 个省市是：北京、上海、广州、杭州、江苏省、青岛、厦门、天津、辽宁省、海南省、大连和山东省。具体目标为：

- 制定发展信用卡市场的规划，建立以金融部门为主体的信用卡业务管理体系。
- 建立法律法规，统一银行卡标准，实现信用卡跨地区、跨部门通用。
- 建立全国金卡信息交换服务中心和各试点城市金卡信息交换服务中心，并与人民银行国家处理中心联网。实现同城或异地授权信息的即时转接和资金的适时结算。
- 全国计划发卡量为 3000 万张。

(2) 推广阶段　具体目标为：

- 进一步完善试点城市的发卡、联网、应用和服务环境。
- 选择一些城市推广，分别建立城市(区域)金卡信息交换服务分中心，并联网。
- 全国计划发卡量为 6000 万张。

(3) 普及阶段　具体目标为：

- 完善有关银行卡业务的法律、法规、制度和监督体系。
- 全国 400 个城市联网，实现即时授权和适时结算。
- 相当多城市将信用卡业务推广到周围经济较发达的县、镇。
- 到 2003 年，全国计划发卡量超过 2 亿张。

2. 金卡工程的实现技术

建立现代化银行卡电子货币系统，银行卡通用，可凭卡在同城或异地购物、消费、存取款和转帐结算，要达到这一目标，需建立先进的信用卡技术支撑系统，主要指信用卡授权清算系统、计算机网络、通信系统、卡及其读写机具。

(1) 建立信用卡授权系统　这是加强信用卡管理、减少信用卡风险的一项重要措施。信用卡授权是指发卡银行授予特约商户向持卡人支付资金(商品)的权力，即授权单位对支付行为负责，因此必须是经营信用卡业务的金融机构或其代理才有资格授权。目前我国信用卡授权还处在用电话、传真等人工授权阶段，授权时间长、安全性差，因此需建立全国性的电子授权中心，例如设立全国和城市(或区域)两级授权交换中心。

(2) 信用卡资金清算系统　信用卡资金清算是指银行通过同行业间的资金往来，按照一定程序，将持卡人使用的资金完成最终支付的一个资金流动过程。目前我国信用卡业务仅有同城资金清算系统，异地跨行清算尚未开办。

(3) 技术装备

- 通信网络：可以采用中国国家金融网络(CNFN)，邮电部中国公用分组交换数据网 CHINAPAC 和国家公用经济信息通信网(金桥网)，实现互连、互为备份。
- 各专业银行的入网前置机应该尽早统一标准，以实现跨行授权。
- 计算机系统：根据业务量确定规模，尽量采用开放式系统。
- 信用卡终端设备：ATM(自动柜员机)和 POS(销售点终端)推广使用。
- 磁卡和 IC 卡：目前我国发行的信用卡还是磁卡，优点是价格便宜，但易伪造、安全性差。智能卡的优点是安全，可脱机处理，对通信网络的要求较低，但价格高。我国考虑同时发展磁卡和 IC 卡，并选定试点城市，一开始就用 IC 卡。

3. 金卡工程的效益目标

提高银行卡结算业务在全社会资金结算中的比例，扭转现金结算总额上升的趋势，减少现金流通量。

4. 金卡工程的管理体系

建立和完善以金融部门为主的银行卡业务管理体系。

人民银行加强对银行卡业务的指导、管理和监督。建立并健全各商业银行联营银行卡的联合组织，并制定规章。

制定有关的法律、法规，促进银行卡业务发展。

5. 其他

依托金卡工程促进商业和旅游服务业等领域的信息化，带动配套电子信息产业的发展。

1.5.2 银行卡基本业务需求

银行卡有信用卡和现金卡两种。

1. 信用卡

是银行或金融机构发给信用良好人士使用的一种凭证，持卡人可用它来购物消费、信用借款、转帐结算、汇兑和储蓄等。国内按发卡银行不同有牡丹卡、长城卡、金穗卡和龙卡等；按使用对象不同分单位卡和个人卡；按持卡人信誉程度不同有金卡和普通卡；按还款先后不同分借记卡和贷记卡；按信用卡国际组织不同有 MASTER 卡和 VISA 卡。

发卡银行加入信用卡国际组织后发行的、可在全球使用的、以本币或外币进行结算的信用卡称为国际卡。一般在国内消费时以本币或外币结算，在国外消费时以所在国货币或美元结算。

银行卡的业务范围和应用范围包括：发卡中心业务处理、在国内外商店购物消费、在银行自动柜员机(ATM)上存取现金和转帐，以及在销售点终端(POS)上付款或转帐等。

银行卡发卡中心业务处理范围包括：

(1) 银行卡业务档案资料管理：包括持卡人档案、商户档案、发卡机构档案、止付名单(黑名单)档案、储蓄所档案、ATM 和 POS 等有关机具的档案等。

其业务包括档案资料的收集、整理、储存和使用。

(2) 帐户管理：包括单位卡活期和定期帐户、个人卡活期和定期帐户、商户活期和定期帐户、银行内部帐户等。

其业务包括开户、查询、帐务处理、冻结、清户和开出有关清单等。

(3) 发卡和换卡：对新开户或过期、遗失、被窃、损坏的卡进行发放或更换。

(4) 帐务处理

- 日间业务处理：本地卡和异地卡现金和转帐收付业务处理；透支和还款处理；错帐冲正和帐户调整；查询。
- 日、月、年终业务处理：轧帐、借贷款利息计算、生成报表等。

(5) 授权：商户或取现金点对超过消费限额或取现金限额的银行卡交易，必须通过发卡或代理行授权同意后，才能受理，无论是否同意用卡，均应产生答复信息。

(6) 止付：银行卡信息交换中心应储存所有银行的止付名单，不联网的商户或取现金点应保存可在本处使用的止付信用卡名单。每笔交易都应该查对止付名单。

(7) 清算：本系统资金清算由发卡银行自行处理，跨系统清算由中央银行处理中心处理。

(8) 事后监督和统计打印报表。

2. 现金卡

由于持卡人不能透支，所以不涉及持卡人信誉，发行手续简便，只要领卡人在银行有一定存款，银行即可发卡。持卡人用卡时银行应对卡的真伪进行认证。用户正确输入密码后可对密码进行修改。IC 卡上可以带有帐户存款余额，因此可以脱机操作，不需要授权。

3. 银行卡信息交换中心

为了处理本地和异地的跨系统授权业务，应成立全国银行卡信息交换中心和地区银

行卡信息交换中心，本地跨系统的授权需通过地区银行卡信息交换中心转给发卡银行处理、异地跨系统授权通过全国银行卡信息交换中心转给地区银行卡信息交换中心，再由其转给发卡银行处理。

1.5.3 金卡工程总体结构

1. 金卡信息交换中心

我国金卡工程信息交换可能采用两级(国家和城市)交换，发卡单位最终授权的机制。具体可按以下规定执行：

- 银行卡在同城(区域)范围内的跨行交易，需要经过同城(区域)交换中心的转接。
- 银行卡跨地区交换，通过本地城市信息交换中心→国家信息交换中心→异地城市信息交换中心，转至发卡行(见图 1.3)。

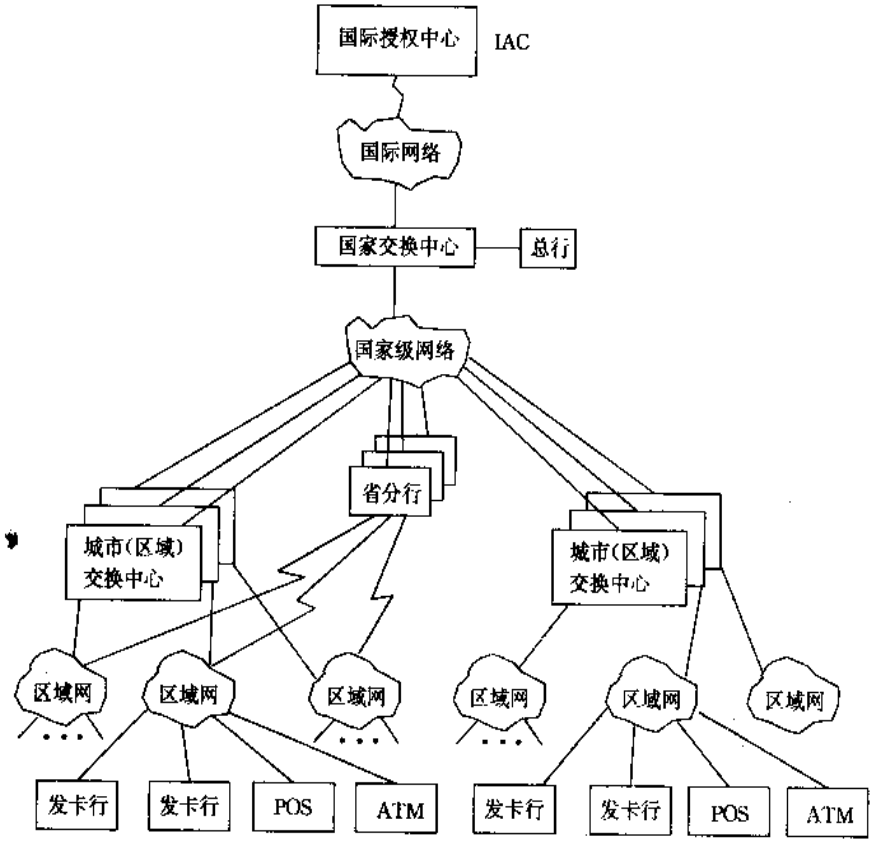


图 1.3 金卡信息交换服务网络系统

- 银行卡在本行系统内交易，使用本银行系统内的网络，如图 1.4 所示。

图 1.3 中的国家信息交换中心对内连接各城市信息交换中心，对外统一与国际信用卡处理中心连接，其功能有：跨城市授权信息转接；分发全国止付名单；与国际统一接口，生成并分发结算报表；提供跨城市信用卡业务的统计、分析和预测资料。

国家信息交换中心出现故障时，可考虑由一个中心城市(例如上海、广州)接替其

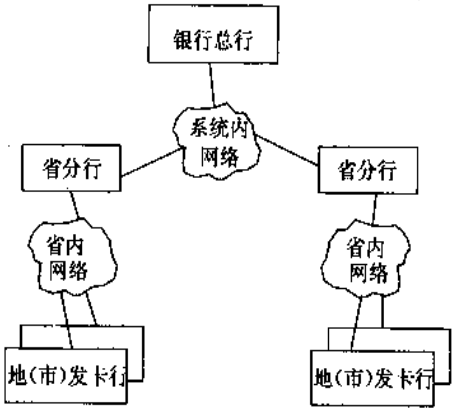


图 1.4　银行本系统的网络结构

职能。

城市信息交换中心对上与国家信息交换中心连接，对下与城市各发卡银行及 ATM/POS 中心相连，其功能有：银行卡同城跨行使用的信息转发；银行卡异地使用的信息转发；统一并分发本市止付名单；向城市清算中心提供信用卡同城跨行使用产生的清算资料；统计、生成报表等。

发卡行信用卡处理中心向上与城市信息交换中心相联或区域内非中心城市信用卡信息交换转发集结点相联，向下与本行信用卡营业网点(包括 ATM 和 POS 等)相连。

图 1.4 中的银行总行是银行卡业务的主管单位，发卡行也可以是为数众多的地方分行。

2. 通信网络

充分利用现有资源，以先进、可靠、方便、安全和经济为原则，选用中国国家金融通信网(CNFN)、中国国家公用数据网(CHINAPAC)和国家公用经济信息网(金桥网)为主干网。上述网络互连互通、互为备份。在城市内，优先选用电信管理部门已建成的区域性网络。不应再重新组建专用网。

今将三个主干网的情况简介如下：

(1) 中国国家金融通信网 CNFN

在规划 CNFN 之前的几年中，各金融部门的数据通信网建设，已取得了可喜的成绩，例如：

① 中国人民银行卫星通信网：1989 年开始筹建中国人民银行的卫星通信网，实现全国范围内异地资金转帐信息的传输与交换。目前已建成一个在北京中央主站控制下，接全国 400 多个城市用户站的卫星通信网络(星型结构)，并与计算机联网，每天运行电子联行信息交换业务。主站的 IBM 4381 处理机担任通信管理、控制和联行业务处理。用户站(清算分中心)使用微机系统。租用亚洲一号卫星的转发器。

目前已提供的通信服务系统有：电子联行系统，人民银行管理信息系统，中国证券交易系统和全国增值税稽核系统等。

② 中国工商银行 SNA 专线网：共用邮电部门提供的专线通信网，采用 IBM ES

9000/260 作为主处理机和网控，连接全国 44 个一级分行，运行联行付帐、信贷统计、管理信息系统和信用卡黑名单等多种业务。地区级主处理机为 IBM 4381(正在升档为 ES 9000)和日立 M680。采用 SNA 网络体系结构。

③ 中国人民建设银行 X.25 分组交换网：以邮电部 X.25 公用数据通信网为依托，组成建设银行的连接全国 44 个省市分行的虚拟专用网络及其网络管理控制中心。开展联行对帐、国内清算、统计报表传输等业务。

④ 中国银行 SWIFT 网络接口：已实现了 IBM 4381(正在升档为 ES 9000)、S 系列小型机和 B 系列微型机之间的专线文件传输，以及总行与对外清算银行之间的连接。通过总行的环球银行间金融通信系统(SWIFT)标准接口，加入 SWIFT 系统网络，参与纽约、东京、伦敦和香港外汇清算。

中国人民银行和其它专业银行虽然都建立了规模不同、采用各种通信线路的城市和全国通信网络，但除了中国人民银行的卫星通信网初具规模、并有综合性通信支持服务功能以外，其它专业银行的通信网络规模较小，基本上采用专线，技术水平和系统的安全可靠性都不能适应我国金融发展的要求，因此于 1991 年正式规划筹建中国国家金融网络 CNFN。

中国国家金融网络 CNFN 由两级网络和三个层次的节点构成，如图 1.5 所示。

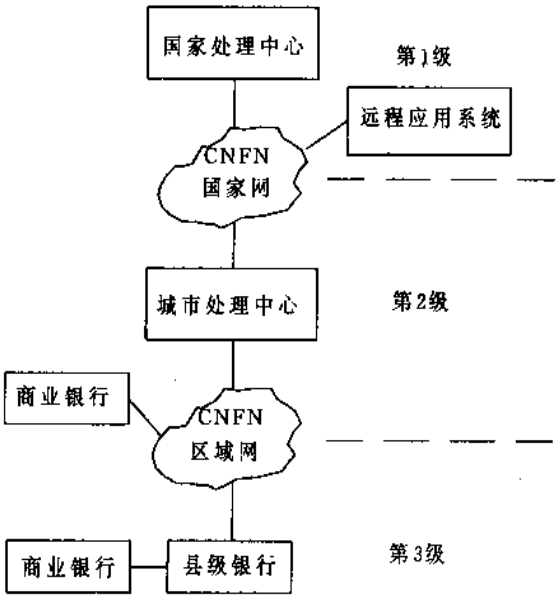


图 1.5 CNFN 组成

国家级网(CNFN 国家网)是一级处理节点(国家处理中心)与二级处理节点(城市处理中心)之间的广域网络，由中国人民银行卫星通信网和邮电部 X.25 公用数据网共同构成，实行“天”、“地”互为备份。区域级网(CNFN 区域网)是二级处理节点(城市处理中心)与三级处理节点(县级银行)之间的广域网络，原则上采用邮电部提供的 X.25 公用数据传输网，又可由区域中心城市所在地的城市网和连接市属县的“市-县”网组成。

国家处理中心由全国应用处理中心、应用系统控制中心、网络管理控制中心和数据库中心组成。要求处理功能强、可靠性高，所以采用成熟的主机系统和互为备份的双桥局域网进行系统集成。

城市处理中心和县级银行处理节点，采用客户机/服务器结构。

CNFN 拓扑结构如图 1.6 所示。

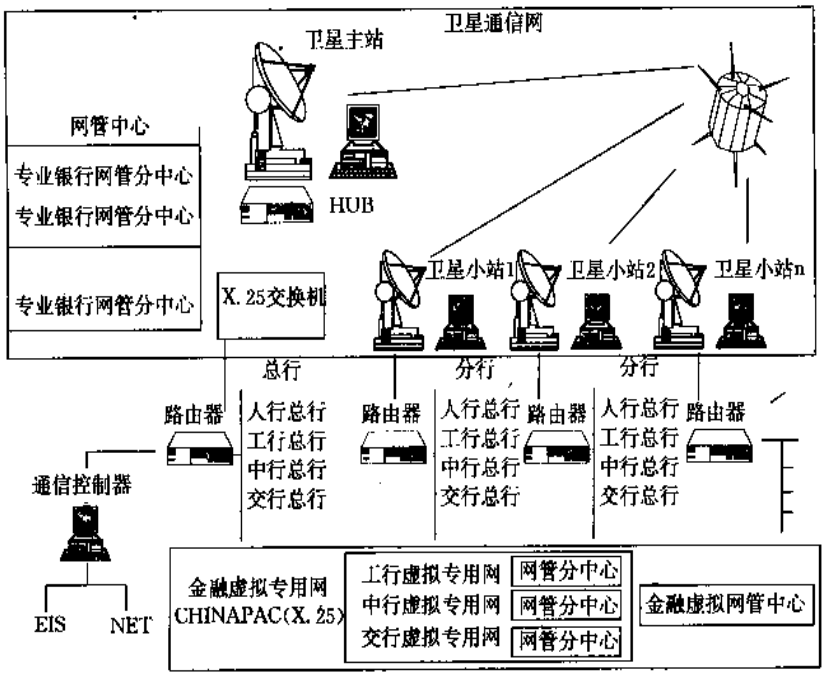


图 1.6 CNFN 网络拓扑结构

中国国家金融网络(CNFN)包含以下应用服务系统：

- 同城清算所(LCH)
- 支付资金结算系统(PFSS)
- 银行卡授权服务系统(BCASS)
- 政府债券簿记系统(GSES)
- 金融管理信息系统(FMIS)

采用国际标准化组织建议的 OSI 开放式系统互连模型，作为中国国家金融网的网络协议标准。

(2) 中国国家公用数据网(CHINAPAC)

邮电部在大力发展电话业务、加强通信基础设施建设的同时，加快开发数据通信及其增值业务。目前我国城乡电话网的总容量已达 6134 万门，网络的规模已排在世界电信网的第 6 位。“九五”将完成覆盖中国大陆的光缆网，此外，还加快了微波和卫星通信的建设步伐。为了适应社会对信息通信的需求，尤其是为了满足国家经济信息化工程的需要，邮电部在加快电话网建设的同时，加快了数据通信网的建设。重点抓了公用数据通信网络的建设。四通八达的光缆网是各种电信网的物理基础，为了将一部分光缆网用于数据通信而

建立了数字数据网(DDN),这个网的主要任务是灵活方便地向用户提供永久性或半永久性的数字电路出租业务。电信部门利用 DDN 所提供的电路构成各种数据网或业务网,中国公用分组交换数据网 CHINAPAC 即为其中之一。

中国公用分组交换数据网具有智能化网络管理功能,能自动统计、分析业务流量、流向,自动提供网络优化方案;能自动检测、分析、显示网内各种故障,并提出解决方法。

图 1.7 示出 CHINAPAC 主干网拓扑结构,北京、上海、广州、武汉、沈阳、南京、成都、西安为汇接节点,汇接节点之间采用全连通结构。在分组网上还开设多种增值业务,如电子邮件(E-mail)、可视图文(Videotex)、电子数据交换(EDI)、数据库检索和传真、存储转发等业务,以满足不同用户的通信需求。

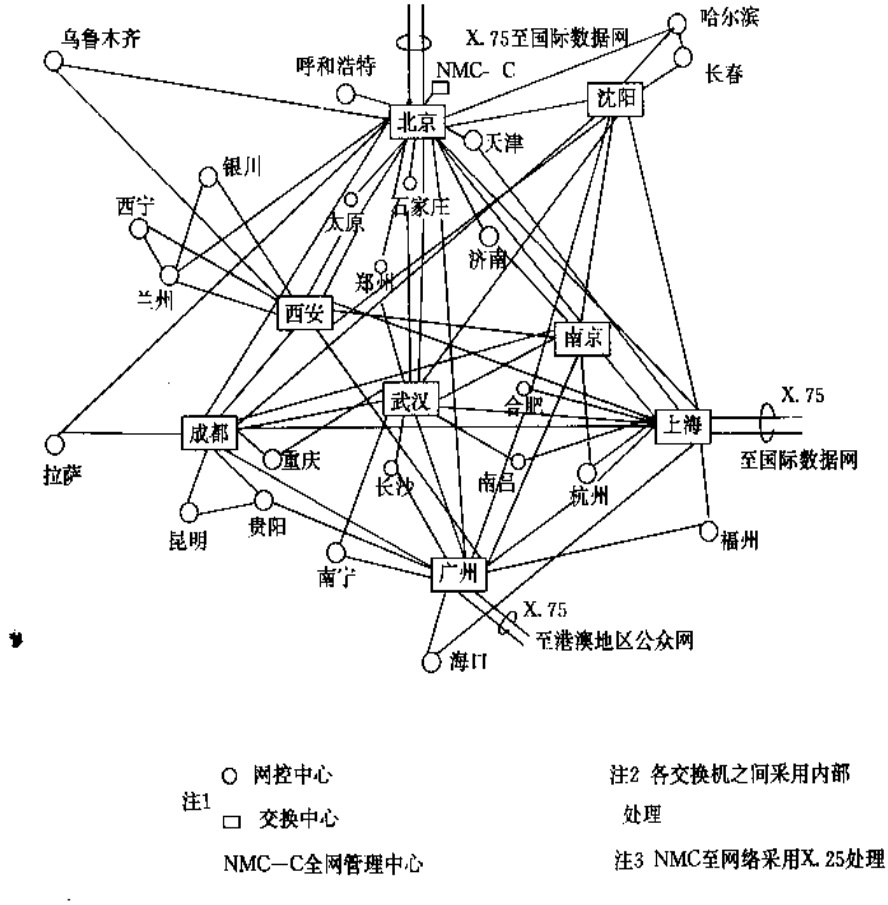


图 1.7 CHINAPAC 主干网拓扑结构

在主干网建设的同时,各省(区、市)也加快了省(区、市)内网络的建设。

CHINAPAC 是利用 DDN 网提供的物理电路(中继电路和用户电路)和普通的用户电话线,加上分组交换设备和网管设备而建立起来的具有信息交换功能、可以进行异种计算机间通信的网络。

(3) 国家公用经济信息通信网(金桥工程)

① 国家公用经济信息通信网(金桥工程)的建设方针：统筹规划，联合建设，统一标准，专通结合(专用网和通用网结合)。

这也是充分利用现有信息资源和通信资源、扩大网络规模、有利于资源共享的方针。

② 金桥工程的初期建设：金桥工程首先支持国家经济信息系统的建设，目前国家经济信息系统在全国各地的信息中心已有 1500 多个，总投资约 13 亿元，但过去由于缺少信息通信支持环境，这些信息中心未能连接起来而影响了作用的发挥。

金桥工程网控中心现已基本建成，24 个省、市建站联网工作于 1995 年开动。

③ 金桥工程的总体框架和特点：金桥工程由信息通信网络、计算机系统、信息源(数据库、资料库、图象库等)组成。采用"天地一体"网络结构，即卫星网和地面光缆网在统一的网管系统下实行互联互通、互为补充、互为备用。光缆网由邮电部数字数据网 DDN 的若干专线构成。在现阶段，不新建自成体系的区域网，主要利用邮电部的分组交换网(CHINAPAC)和数字数据网(CHINADDN)，也可利用广电部的有线电视网(CATV)。

金桥网的一期工程覆盖全国 400 多个城市，与各部门、各地方专用网(现有 100 多个专用网)实行异构网互联，并通过直接或间接方式与上万个信息源(大中型企业、重点工程、高等院校、科研基地)相联，与国家综合管理部门相联，并实现国际联网。

金桥工程能传输数据、语音、文字、图象，提供廉价的综合业务数字网(ISDN)服务。

金桥网是增值业务网，可以提供电子邮件(E-mail)、电子数据交换(EDI)、多媒体业务和可视图文、电视会议业务。

金桥网具有对网络错误信息记录、分析和处理的功能，以及对网络进行诊断、测试和预防故障的功能；具有对网络运行状态进行实时监测，并根据监测结果动态调整路由表的功能；具有自动计费管理的功能；具有防止信息被篡改和加密等安全机制。

通过上面介绍，可以看到这三个主干网都有很强大的功能，可以应用到金卡工程中。

金卡工程涉及的数据通信网有三种类型：

- 广域网(WAN)
- 城域网或区域网
- 局域网(LAN)

分别构成三级网络结构中的第一级、第二级和第三级。

图 1.8 示出金卡工程计算机网络的结构，是利用国家现有主干网(CHINAPAC、金桥网和 CNFN)和地区网组成的金卡工程虚拟专用网。

3. 金卡工程与国家支付系统(CNPS)

金卡工程是中国国家支付系统 CNPS 的重要组成部分。金卡工程的主干网、区域网必须与金融专用网相结合。金卡工程与支付系统的逻辑关系如图 1.9 所示。

支付系统使用的通信网络与同级的金卡工程使用的通信网络实际上都是在同一个网络上。这样为银行卡跨行清算提供了方便条件。

4. 金卡工程持卡消费运行流程

用图表示持卡消费运行流程：图 1.10 为城市级(同城)金卡支付业务流程；图 1.11 为异地支付业务流程；图 1.12 为国际支付业务流程。

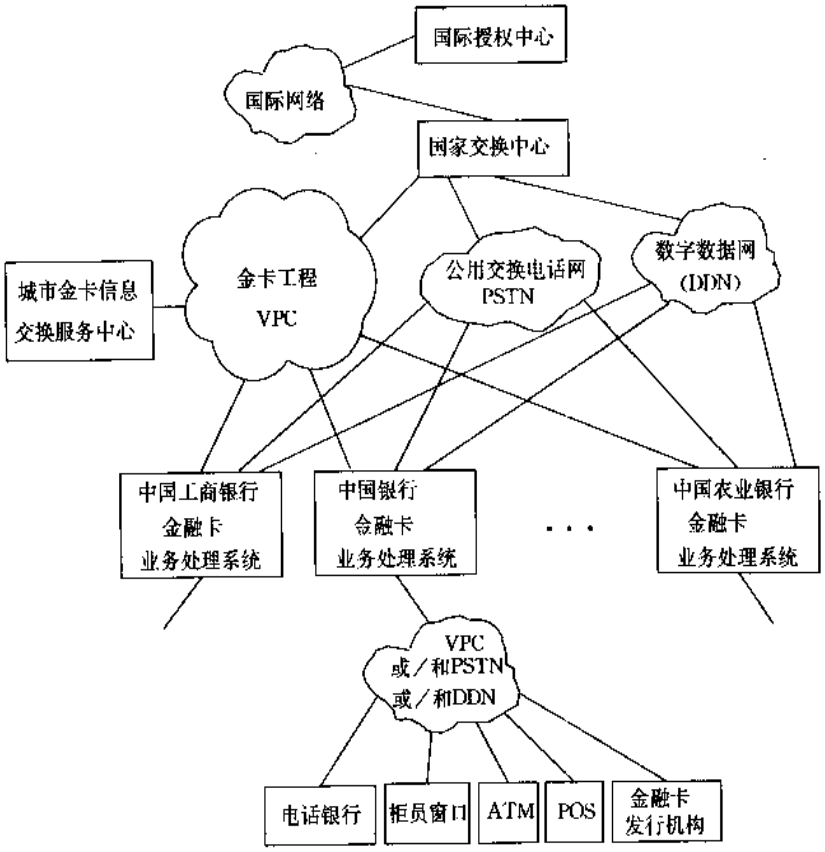


图 1.8　金卡工程计算机网络结构

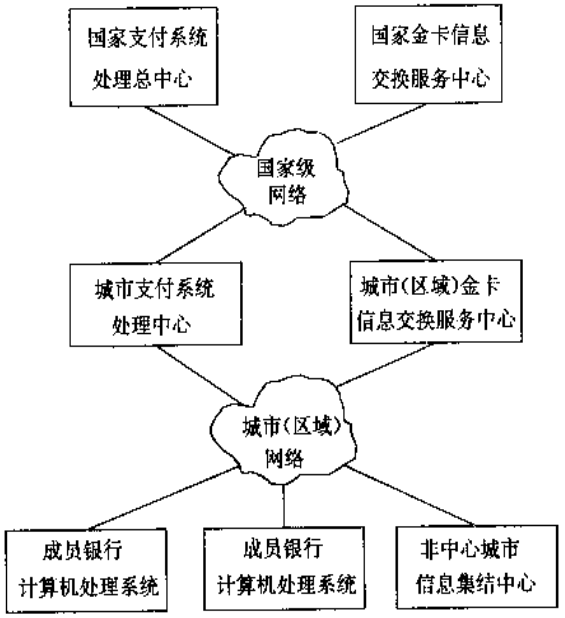


图 1.9　金卡工程与支付系统逻辑关系图

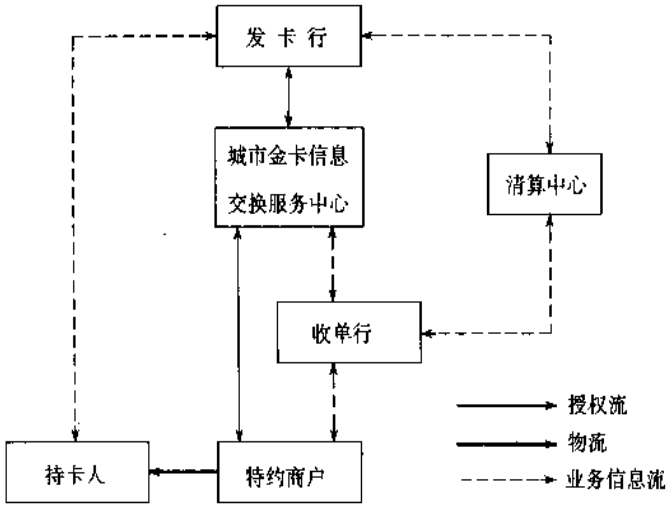


图 1.10　城市级(同城)金卡支付业务流程

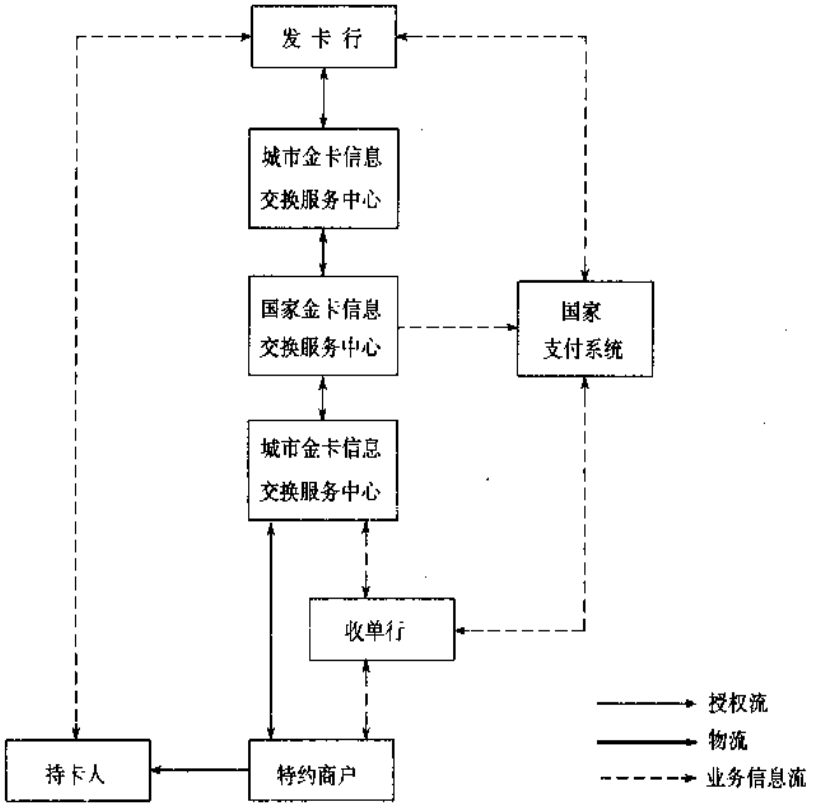


图 1.11　金卡异地支付业务关系图

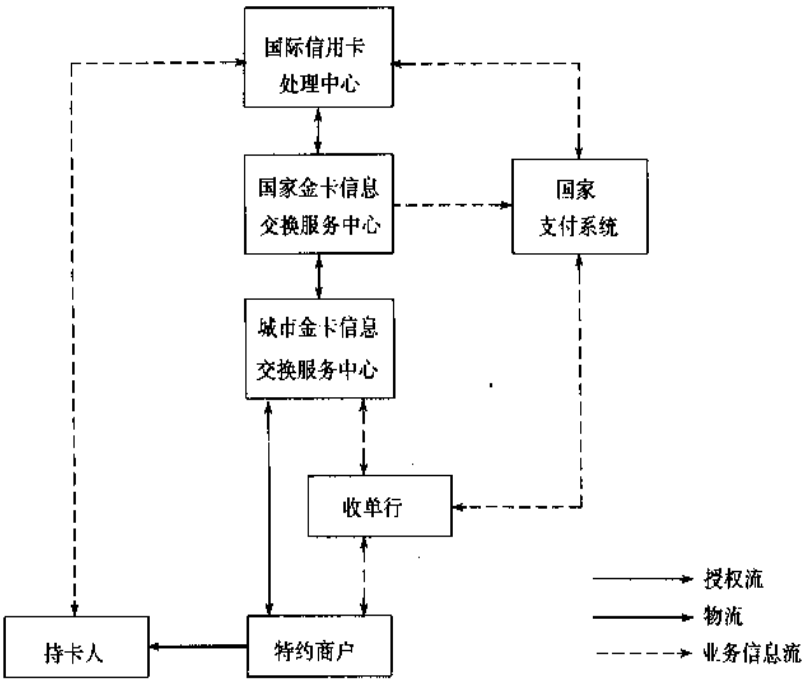


图 1.12　金卡国际支付业务关系图(国外卡国内消费)

1.5.4　应用软件设计要求和设备功能

1. 应用软件设计要求

金卡工程软件是在网络环境下运行的,为了实现基本功能至少提出下述设计要求:

(1) 完成交易处理:包括查黑名单、授权、存款、取款、记帐、查询余额、结算、清算、打印报表、生成黑名单等。

(2) 网络管理和应用软件。

(3) 设备管理软件。

(4) 安全和加密:个人身份(PIN)验证、卡与读写设备(接口设备)真伪认证。数据保护(防非法删除、非法数据进入、非法修改等),尤其是在网络上传送的数据应先加密、后传送。为了安全运行要做好加密/解密密钥的管理工作。

(5) 系统灵活性:软件模块化,便于修改和扩充,能适应多种硬件平台。

(6) 应用软件具有防止、隔离及纠正各类错误的机制,采取预防及故障后恢复运行的措施。

(7) 系统具有可移植性和可维护性。

下面讨论信用卡终端设备功能。

目前主要采用磁卡,但应同时考虑 IC 卡。

2. 自动取款机设备功能

(1) 基本功能

① 取款:自动取款机将取款信息送往发卡行主机,检查此卡是否已列入黑名单以及

是否超出当天取款限额，如可受理，则送出磁卡和现金；如检查出磁卡非法、无效或过期，则自动将磁卡没收。如发现磁卡非本行发行，拒绝使用。

② PIN 验证：当持卡人连续三次(或四次)输入个人标识号(PIN)不正确，则自动停止付款。

③ 日结总帐打印。

④ 脱机处理：可根据存放在本机上的黑名单处理取款业务。

⑤ 汉字显示。

⑥ 回收介质：在一定时间内客户未取走磁卡、现金或凭证，将其自动收回。

⑦ 回收残钞。

⑧ 钱箱现金不够拒绝取款。

(2) 可选功能

① 查询余额：向发卡行查询帐户余额。

② 更改密码：持卡人输入密码，如正确，允许修改密码。

③ 咨询服务：诸如咨询外币兑换率等。

④ 结帐单打印。

3. 脱机 ATM(自动柜员机)功能

(1) 基本功能：除了增加存款功能以外，其余同自动提款机。

存款：由 ATM 打印客户通知单，输出存款信封，持卡人将现金与通知单一起装入信封，加以密封后送入 ATM。

(2) 可选功能

① 中止运转：因存款袋容器装满而中止存款。

② 取款使用其它票证支付：取款时除使用现金支付外，可以根据客户要求使用邮票、旅行支票、票券等支付。

③ 语音提示。

其余的可选功能同自动提款机。

4. 联机 ATM 设备功能

(1) 基本功能：基本与脱机 ATM 设备相同，但增加两项功能：更改磁卡密码和查询帐户信息。

(2) 可选功能：基本与脱机 ATM 设备相同，但可实现转帐，如代收水电费、代发工资等多帐号自动转帐。

5. ATM 的维护功能

(1) 备份当天的流水帐和存取款明细帐。

(2) 检查钱箱，及时补充钞票。

(3) 清理废钞箱。

(4) 维护性测试：包括对钱箱、出钞机、读卡器和通信线路的测试运转。

(5) 清点没收的磁卡。

(6) 检查打印纸是否快用完。

1.5.5 安全与保密

1. 安全与保密策略

(1) 实体安全：包括卡片的制造、发放、管理和服务等安全体系的建立；卡基安全质量保证；本单位员工与来访者的出入管理与访问控制；设施的选址和建设；实体对环境和对自然灾害或破坏性活动的防御措施；安全报警与探测系统。

(2) 人事安全：工作人员的招聘与任用策略；安全意识的培训。

(3) 信息系统的安全：逻辑访问控制；检查跟踪；通信网络线路与信息传输的安全性；密码密钥的设置与安全；信息电磁发射泄漏问题等。

(4) 持卡人安全

为保证持卡人经济上不受损失，应做到：对卡片的被盗或丢失有快速处理办法；加强识别伪卡的能力。

制定安全措施，处理持卡人经济情况发生变化时的帐务风险。

2. 设备威胁和风险种类

威胁有：偷窃，硬件故障，配置出错，故意破坏或设备被改装，数据或软件被拷贝，数据或软件被修改，未经授权而更换设备。

对于保密设备的威胁可能来自：

(1) 隐含功能：可能被"攻击者"利用设备中的隐含功能来获取密钥或 PIN 或其它可供攻击的信息。

(2) 设计缺陷：攻击者可能利用设计上的缺陷来获取密钥或 PIN 等。

(3) 破译：如密钥被识破就应立即更换。

(4) 接口管理：不允许在未经允许情况下向设备发送一系列可能导致敏感信息泄漏的信号，保密设备不允许出错。

(5) 窃听。

(6) 伪造设备替换掉保密设备。

3. 传输安全——加密

参见本书 1.3.3 及第 5 章。

4. 操作系统安全

一般的通用系统软件不能满足安全条件，需要附加安全保密软件。

1.5.6 技术标准与规范

金卡工程根据《中华人民共和国标准化法》和我国有关标准化方针政策开展工作。凡是我国已有的国家标准，要认真贯彻实施；如我国还没有此国家标准，但已有国际标准，则按国际标准贯彻实施；如国际、国内都还没有形成相应的标准，则积极参照 VISA、MASTER 等国际信用卡组织的规范。与 IC 卡有关的国际标准和国家标准请参见附录 A。

1.6 智能卡的诞生与发展

1977年，Motorola与它的一个计算机客户合作开发了世界上的第一张智能卡，形成了第一代智能卡产品，将一个可编程的微控制器及一个非易失性的存储器集成在一个模块内，然后嵌入一张符合ISO 7810标准的信用卡中。该产品在法国的Blois进行了试点，目的是为了对进行脱机(Off-line)交易所需的技术予以评估。自此以后，智能卡开始迅猛发展，智能卡所采用的技术也日新月异地发生着变化。1979年产生了世界上第一片专为智能卡所设计的单片机芯片。从而形成了第二代的智能卡产品，并在法国、瑞士、斯堪的那维亚得到应用。当时主要是用作银行卡(Bank card)。进入90年代后，在通信、健康、交通等方面，智能卡的应用也开始蓬勃发展。例如在远东地区，随着经济的飞跃，智能卡正以每年34%的速度增长。仅在台湾地区，据预测，从1994年到1997年，智能卡的流通量就将增加8倍；而同时基于智能卡的交易则将增长110倍。在美国，1994年有超过100万张的银行卡在使用。在1994年，全球共生产了5.8亿张存储器卡，其中包括了6300万张微处理器卡。根据法国Solaic公司的分析，到2000年，世界范围内IC卡的产量将达到13亿张，其中将有80%用于通信、12%用于银行、8%用于交通/政府部门；而IC卡的销售额将达到50亿法国法郎(9亿美元)，其中欧洲将占60%、北美洲25%、世界其它地方15%。

目前，智能卡已经在以下领域中获得或即将获得广泛的应用：

- 金融服务(financial services)
- 通信及信息服务(telecommunications and Information services)
- 医疗保健(health care)
- 教育(education)
- 旅游与娱乐(travel and entertainment)
- 政府(government/EBT)
- 交通(transportation)
- 付费电视(pay TV)

从上面的划分可以看出，当前的智能卡还基本上是一种单功能卡，即一般一张卡只适用于某一种应用。以后的智能卡则将向着多功能卡的方向发展。例如可以发行城市卡(city card)，这种卡将包括用户在一个城市中可能经常需要接触的大部分应用功能，诸如作为电子钱包(electronic purses)使用、作为电话卡(phone card)使用、作为信用卡使用、作为医疗保健卡使用等。另外，未来的智能卡还将与通信更为紧密地结合，在网络管理等方面得到应用。

为了实现多功能卡的功能，现有的智能卡技术还必须加以改进。因为对于多功能卡而言，通常的要求是：16K—256K的ROM；大于256Bytes的RAM；3K—128K的EEPROM(或是与Flash EEPROM的合成)；可选用的协处理器部件(主要用于加密/解密的处理)；生物特征识别等。要在不超过25mm^{2}的硅芯上集成所有这些内容，就意味着必须要使用1.0μ—0.65μ的微电子集成技术，这还有待于智能卡芯片的制造商们对现有技术进行改进。据预测，到90年代后期，这样的芯片就可以进行批量生产了。

对未来的芯片有两种截然不同的要求，其一是继续向更小、更便宜、更通用的方向发展；其二是向更复杂、支持多种应用或支持实时数据处理的应用方向发展。

在技术上希望达到以下指标：

1. 降低工作电压(<2V)、降低功耗，这样可降低手持设备(如移动电话)中所用电池的重量，从而减轻手持设备的重量和延长电池使用时间。

2. 增加 EEPROM 的容量，减少 EEPROM 的编程时间(<2ms)。

3. 提高执行加密/解密算法时间，这意味着要增加芯片的运算能力和增加 RAM 的容量，而 RAM 所占芯片的面积比其他存储器大得多(参阅 6.5 节)。

4. 发展非接触卡，将标准的 HCMOS 技术与射频技术结合起来，从而用一个芯片完成非接触型卡的功能。这里的射频技术是为了完成非接触型卡的收发功能而采用的。

1.7 本书内容简介

本书的第 1 章为概论，对智能卡(对芯片到系统)作了较为全面的描述，说明了磁卡、IC 卡(存储器卡、逻辑加密卡、智能卡)和金融交易卡(金融卡)等的含义与功能，并以自动柜员机 ATM 和销售点终端 POS 为例说明一次交易的操作过程。文中突出了卡的安全问题和标准化问题。并重点介绍了金卡工程，因为在我国，智能卡技术的发展将随着金卡工程的实施而迅速发展。通过以上这些论述，希望读者和我们对智能卡将涉及哪些领域达成共识。建议读者阅读本书时，先阅读第 1 章。

从第 2 章到第 9 章，是按专题进行论述。

第 2 章介绍了与磁卡有关的国际标准以及金融卡的国际标准。因为智能卡是从磁卡发展而来的，而且目前世界上除了法国以外，其他国家仍以使用磁卡为主，因此发展智能卡时仍需兼顾磁卡。

第 3 章和第 4 章主要介绍了接触型 IC 卡的国际标准，涉及卡的物理特性、触点尺寸和位置、电信号和传输协议、行业间交换用命令以及应用标识符的编号系统和注册过程等。由于 IC 卡需要在全国或全球通用，因此标准化工作非常重要。

第 5 章智能卡的安全和鉴别推荐了两种在智能卡中常用的密码算法：对称密钥密码算法(DES)和非对称密钥密码算法(RSA)，讲述了基本原理、算法及其应用。本章是实现智能卡安全的数学基础，同时也是实用技术。此外智能卡的安全与鉴别也是本章的重点。

第 6 章 IC 卡及其专用芯片讨论了三种类型的 IC 卡：存储器卡、逻辑加密卡和带微处理器的智能卡。描述了各类卡中的 IC(集成电路)的组成、工作原理、性能、特点和适用范围。尤其是智能卡内还含有 CPU 和操作系统，可以进行各种管理及运算，提高了卡的安全性，扩大了应用范围。

第 7 章 IC 卡的接口设备是 IC 卡与外界接触的窗口，将讨论接口电路、设备的组成、对卡的控制信号的生成以及应用实例。

第 8 章中介绍的 ATM 和 POS 是金融卡应用的主要场所，该章对 ATM 和 POS 的结构、组成、工作原理以及与系统网络的连接逐一加以说明。

第 9 章对 IC 卡的各类应用作概括性介绍。

最后为附录。

思 考 题

1. 什么是智能卡和 IC 卡?
2. 磁卡与 IC 卡的主要差别是什么?
3. 什么是信用卡和现金卡?
4. ATM(自动柜员机)和 POS(销售点终端)的用途各是什么? 两者在功能和结构上有什么主要差别?
5. 金卡工程的主要目标是什么? 为什么金卡工程又称为电子货币工程?
6. 计算机网络在金卡工程中的重要性如何? 请说出金卡工程中准备采用的主干网名称,这些网是否是金卡工程专用的?
7. 智能卡与安全有什么关系? 磁卡与智能卡在安全性方面有什么主要差别?
8. 什么叫授权? 并简述授权的重要性及授权过程。
9. 在 IC 卡应用系统中,常用的密码算法是什么?
10. PIN 主要用于验证持卡人的身份,保护卡主人的利益,这种说法对吗?
11. 一个现代化的信用卡应用系统的硬件应包括哪些主要部件和设备?
12. 信用卡系统的标准化有什么意义?
13. 对于磁卡与 IC 卡,有哪些国际标准?
14. IC 卡的存储器一般可划分成几个存储区? 简单说明各区的作用。
15. 什么是接口设备(或读写设备)? 其功能是什么? 是否允许商店的雇员对接口设备进行改装?
16. 凭你日常生活的经验,你感到 IC 卡可应用在哪些场合?
17. 请画出国际流通的信用卡(国外发行)在国内消费时的最简单的流程图。

第2章 磁　卡

磁卡广泛地应用于金融、邮电、航空等领域，它是利用贴在卡上的磁条来记录持卡人的帐户、姓名等信息的。磁条表面涂有磁性材料，当读卡设备的磁头掠过磁条时，就可以对磁条进行读写操作。

2.1 概　述

磁卡一般作为识别卡用。所谓识别卡，是指一种标识其持卡人和发行者的卡，卡上载有进行该卡预期应用所要求输入的数据。作为一种识别卡，磁卡也应具备识别卡的一般特性。例如，在卡的功能没有损害的前提下，允许磁卡正常使用过程中承受一定程度的变形（弯曲而未折损），允许因为记录或打印而使卡的弹性变小。又如，在环境温度－35℃和50℃（－30°F 和 120°F）之间，卡的结构应保持可靠和可用，等等。

磁卡还有一些它自身的特性和应遵循的规定。磁卡的材料不应含有可能渗入或改变磁性材料性质的成分，以免卡在正常使用时，磁性材料变得不能满足识别卡的国际标准所规定的特性。磁条的信息，因为污染可能失效。卡暴露在强磁场中，记录的数据也易于破坏。

磁卡尺寸有三种规格，见表 2.1。

表 2.1　三种规格的磁卡尺寸

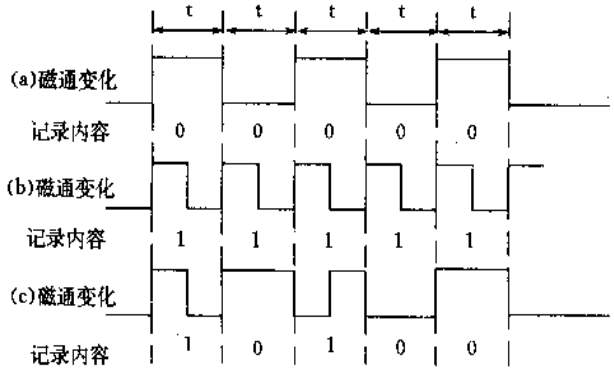
卡类型	宽　度		高　度		厚　度	
	mm	in	mm	in	mm	in
ID—1	85.6	3.370	53.98	2.125	0.76	0.030
ID—2	105	4.134	74	2.913	0.76	0.030
ID—3	125	4.921	88	3.465	0.76	0.030

注：mm　毫米，　in　英寸，下同。

一般将磁条贴在磁卡的背面，磁条可读表面高度应该从 0mm（0in）到 0.038mm（0.0015in）。

磁条上记录的信息采用调频制编码技术，具有自同步能力。图 2.1 示出采用这种编码技术的例子。在每个时钟周期，磁通至少变化一次。如在每个周期中间产生磁通变化表示逻辑“1”；如无磁通变化表示逻辑“0”。

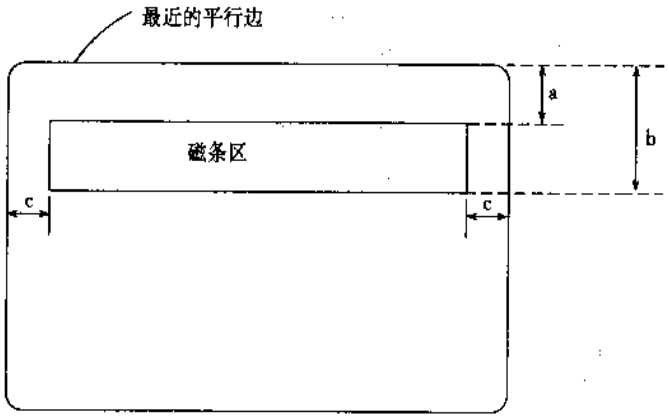
国际标准 ISO 7811/2 规定，磁道 1 记录字母数字型数据，磁道 2 记录数字型数据，两者都是只读磁道。磁道 3 记录数字型数据，它是读写磁道。三条磁道在卡上的位置在国际标准 ISO 7811/4 和 ISO 7811/5 中有严格的定义。



t 表示时钟周期

图 2.1 调频制编码示例

磁卡的磁性材料(磁条)所占区域见图 2.2。



a 最大 5.54mm(0.218in)

b 最小 11.89mm(0.468in)

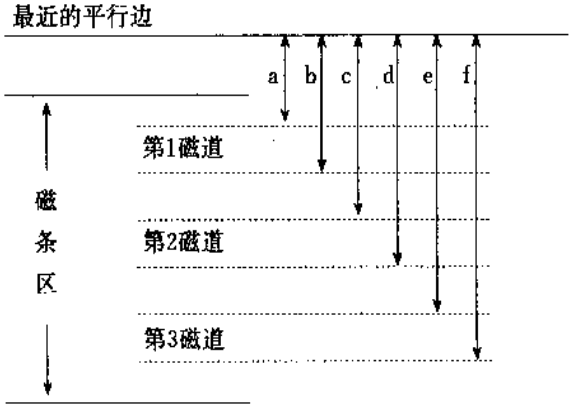
c 最大 2.92mm(0.115in)

图 2.2 磁条区域的位置

三个编码磁道在卡上的位置见图 2.3。

编码时,各磁道都是从右侧顶端开始编码,每个字符的位结构都是首先编码最低有效位(b_1),最后编码奇偶校验位。磁道 1 和磁道 2 第一个数据位的中心线在离卡右边线 7.44±0.51mm(0.293±0.020in)处,如图 2.4。磁道 1 和磁道 2 所记录的最后一数据位的中心线不能超过离卡左边线为 6.93mm(0.273in)的线(如图 2.4)。磁道 3 未定义左边界,其编码的右边界为 7.44±1.00mm(0.293±0.040in)。

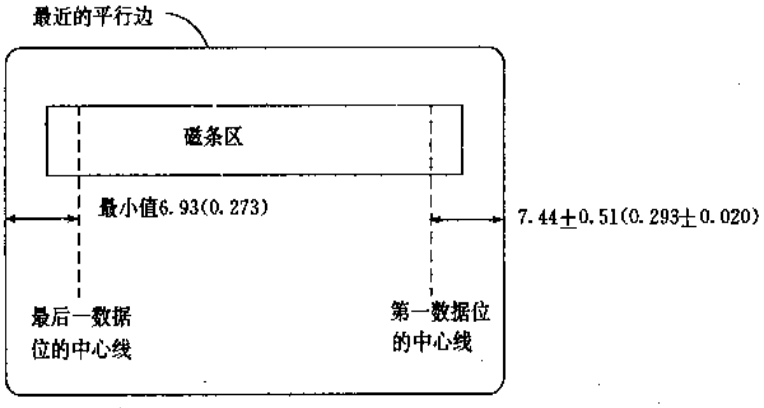
磁道1采用的编码字符集见表2.2,其代码是字母数字型的,6位字符并带奇校验位。



a 最大值 5.66(0.223)，单位mm,括号里尺寸单位是in
b 最小值 8.46(0.333)，最大值8.97(0.353)
c 最大值 8.97(0.353)，最小值8.46(0.333)
d 最小值 11.76(0.463)，最大值12.27(0.483)
e 最小值 12.01(0.473)，最大值12.52(0.493)
f 最小值 15.32(0.603)，最大值15.82(0.623)

注：若有多个磁道被编码时，各磁道的位置不能相互重叠，即使各磁道的毛边也不允许相互影响。

图 2.3 磁道的位置



注：尺寸单位mm(括号中尺寸单位为in)

图 2.4 磁道 1 和磁道 2 编码数据的限制范围

表 2.2　第 1 磁道用的编码字符集

				b_6	0	0	1	1
				b_5	0	1	0	1
b_4	b_3	b_2	b_1	列 / 行	0	1	2	3
0	0	0	0	0	SP	0	ⓐ	P
0	0	0	1	1	ⓐ	1	A	Q
0	0	1	0	2	ⓐ	2	B	R
0	0	1	1	3	ⓒ	3	C	S
0	1	0	0	4	$	4	D	T
0	1	0	1	5	%ⓓ	5	E	U
0	1	1	0	6	ⓐ	6	F	V
0	1	1	1	7	ⓐ	7	G	W
1	0	0	0	8	(	8	H	X
1	0	0	1	9	)	9	I	Y
1	0	1	0	10	ⓐ	ⓐ	!	Z
1	0	1	1	11	ⓐ	ⓐ	K	ⓑ
1	1	0	0	12	ⓐ	ⓐ	L	ⓑ
1	1	0	1	13	-	ⓐ	M	ⓑ
1	1	1	0	14	.	ⓐ	N	ⓓ
1	1	1	1	15	/	? ⓓ	O	ⓐ

ⓐ 这些字符位置仅适用于硬件控制并且不包含信息字符。

ⓑ 这些字符位置保留给附加国家字符用，国际上不通用。

ⓒ 字符位置保留给任选附加图形符号用。

ⓓ 这些字符对本应用具有下列含义：

位置　0/5　%表示“起始标记”(x/y 表示表中的第 x 列，第 y 行位置，下同)

1/15　? 表示“结束标记”

3/14　表示“分隔符”

磁道 2 和磁道 3 采用的编码字符集都是数字型的，其字符代码是 BCD(4 位)代码并带有奇校验位 P，如表 2.3 所示。

表 2.3　第 2 和第 3 磁道的编码字符集

位					行	字符
P	b_4	b_3	b_2	b_1		
1	0	0	0	0	0	0
0	0	0	0	1	1	1
0	0	0	1	0	2	2
1	0	0	1	1	3	3
0	0	1	0	0	4	4
1	0	1	0	1	5	5
1	0	1	1	0	6	6
0	0	1	1	1	7	7
0	1	0	0	0	8	8
1	1	0	0	1	9	9
1	1	0	1	0	10	ⓐ
0	1	0	1	1	11	$ⓑ^1$
1	1	1	0	0	12	ⓐ
0	1	1	0	1	13	$ⓑ^2$
0	1	1	1	0	14	ⓐ
1	1	1	1	1	15	$ⓑ^3$

注：ⓐ 这些字符位置仅适用于硬件控制并且不应包含信息字符(数据内容)。

$ⓑ^1$ 起始标记(起始字符)。

$ⓑ^2$ 分隔符。

$ⓑ^3$ 结束标记(结束字符)。

三条磁道都采用两种错误检测技术：奇偶校验和纵向冗余校验(Longitudinal Redundancy Check—LRC)。每一编码字符都含有一奇偶校验位，三条磁道都采用奇校验，即奇偶位保证每一字符(包括奇偶位在内)"1"的总数是奇数。每条数据信息都应包含纵向冗余校验(LRC)字符。按照卡的起始标记、数据、结束标记的读卡方向，LRC 字符应紧跟在结束标记之后编码。LRC 字符的位结构与数据字符的位结构相同，都是先编码低有效位，再编码高有效位，最后编码奇偶校验位。LRC 字符的计算方法分两步：

第一步：不包括奇校验位，LRC 字符的每一位使数据信息(包括起始标记、数据、结束标记、LRC 字符)对应位上的位编码为"1"的总数是偶数。即，所有数据信息字符第 1 位的"1"的个数是偶数，第 2 位的"1"的个数也是偶数，……。

第二步：求 LRC 字符的奇校验位。LRC 字符的奇校验位与其他数据字符奇校验位的求法一样，奇校验位使得 LRC 字符本身所有位"1"的总数是奇数。

三条磁道的格式及内容因应用而异。随后各节分别阐述在磁卡的一个主要应用领域——金融交易卡(FTC)上对各磁道的格式及内容的规定。以后不经特别说明，本章所述信息内容都是针对金融交易卡而言的。

2.2 金融交易卡第1磁道的格式及内容

磁道1的标准记录密度为8.3bpmm(210bpi)±5%,其每个字符的长度为7个比特(包括校验位)(注意,bpmm 位/毫米 bpi 位/英寸)。磁道1信息最大长度为79个字母数字字符。

国际标准ISO 7813:1987规定第1磁道有二种结构,其中结构A留给发卡者规定,结构B见表2.4。

表2.4 FTC卡磁道1格式

1	1	最多19个数字	1	3	2—26个字符	1	4	1	2		1	1
STX	FC	PAN	FS	CC	NM	FS	ED	ID	SC	DD	ETX	LRC

最大记录长度 79个字符

STX 起始字符(起始标记),在编码字符集(表2.2)中位于位置0/5处,是"%"。

FC 格式代码,在这儿应是"B",表明是格式B,位于字符集位置2/2处。

PAN 个人标识号码(主帐号),代表持卡人的号码,由发卡者标识号码、个人帐户标识、校验数字三部分构成,详见第2.5节的主帐号格式。

FS 分隔符。位于编码字符集位置3/14处。

CC 国家代码。3个数字,当主帐号的主要行业标识符是"59"(金融行业)时,这个字段按ISO 3166强制编码。在所有其他情形下,没有该字段。

NM 持卡人的姓名,2—26个字符。最小编码数据应为一个字符(作为姓氏)加上姓氏分隔符。除姓以外,姓名字段的其他逻辑元素要求用空格分隔,最后一逻辑元素后不必有空格。姓名字段格式如下:

- 姓氏
- 姓氏分隔符 "/",位于字符集0/5处
- 第一个名字或简写
- 空格 (当后面还有中间名字时需要),位于字符集0/0处。
- 中间名字(第二个名字)或简写
- 圆点"." (当后面还有头衔时存在),位于字符集0/14处。
- 头衔

例如:

Stewart/richard. Mr (无中间名字)

Stewart/ (只有姓氏)

Stewart/Richard Tom. Mr (全称)

Stewart/Richard Tom (无头衔)

在姓名字段代码的最后一个逻辑元素之后,应跟一分隔符(FS)来分隔姓名字段和后续字段。

ED　失效日期。格式为 YYMM，用 4 个数字表示卡的有效期限(YY 表示年，MM 表示月)。如果不定义失效日期，该字段应为一分隔符(位于字符集 3/14 处)。

ID　交换指示符，见 SC。

SC　服务代码。ID 和 SC 用来表示发卡者对持卡人提供的服务范围和类别。如果这两项内容不存在或不用指定，这两个字段以一个分隔符(FS)代替。

交换指示符(ID)是 1 个数字，它由 ISO 技术组织指定。目前已指定的有：

1　适用于国际交换

5　只适合于发卡国家内的交换

7　不适用于一般交换(在发行者之间的特定协议不受此限制)

9　系统测试卡

服务代码(SC)由 2 个数字组成：

00—49　是由 ISO 技术组织指定、发布的代码

50—59　是由国家标准组织指定和发布的代码

60—99　是可由民间指定的代码

当交换指示符(ID)为 1 时，SC 只能指定在 00—49 之间；当交换指示符为 5 或 7 时，所有 SC 代码都有效。目前指定的服务代码有：

01　无限制

02　无 ATM 服务

03　只有 ATM 服务

10　无现金预支

11　既无现金预支又无 ATM 服务

20　要求授权，即所有交易都必须经过发行者或其代理授权

DD　自由数据，或称随意数据。可包括卡的启用日期、平衡字符，等等。该字段的长度应使整个磁道信息长度不超过总长 79 个字符。

ETX　结束标记(结束字符)，位于字符集 1/15 处。

LRC　纵向冗余校验字符。

2.3　金融交易卡第 2 磁道的格式及内容

磁道 2 的记录密度比磁道 1 低得多，为 3bpmm(75bpi)±3%，每个字符长度为 5 个比特(含校验位)，其信息最大长度为 40 个数字字符。

ISO 7813 规定了第 2 磁道的标准结构(表 2.5)。

表 2.5　FTC 卡磁道 2 格式

1	最多 19 个数字	1	3	4	1	2		1	1
STX	PAN	FS	CC	ED	ID	SC	DD	ETX	LRC

最大记录长度　40 个字符

STX　起始标记(起始字符),其编码为 BCD 码的 11(见表 2.3)。

PAN　主帐号。它是用来标识发行卡片的行业、卡片发行人以及带有一位校验位的客户标识号,详见第 2.5 节的主帐号格式。

FS　分隔符。其编码为 BCD 码的 13。

CC　国家代码。3 个数字。同磁道 1 一样,当主帐号 PAN 的主要行业标识符是"59"(金融行业)时,这个字段强制按 ISO 3166 编码。而在所有其他情形下,没有该字段,后一字段紧跟终结主帐号的分隔符。

ED　失效日期(终止日期)的格式为 YYMM。如果无失效日期,该字段为一分隔符(BCD 码 13)。

ID　交换指示符,见 SC。

SC　服务代码。

ID 和 SC 的含义和内容的规定与第 1 磁道一样。如果这两项内容不用指定,这两字段以一分隔符(FS)代替。

DD　随意数据,由卡的发行者自行决定。该字段长度应使整个磁道信息长度不超过总长 40 个数字字符。

ETX　结束标记(结束字符),其编码是 BCD 码的 15。

LRC　纵向冗余校验字符。

比较第 1 磁道和第 2 磁道可以发现,两磁道的区别在于第 1 磁道比第 2 磁道多一个姓名字段,可以记录持卡人的姓名。第 1 磁道的编码字符集是字母数字的,字母主要提供给姓名字段用,第 2 磁道的编码字符集是数字的。除此之外,两个磁道其他字段的含义、格式及长度基本上是一样的。第 1 磁道因为信息内容多,磁道比第 2 磁道密。实际应用时,发卡者可以根据实际需要确定选用哪条磁道,也可以将两磁道配合起来使用,提供更丰富的信息。

2.4　金融交易卡第 3 磁道的格式及内容

第 3 磁道的记录密度为 8.3bpmm(210bpi)±8%,每个字符长度与第 2 磁道一样为 5 个比特(含校验位),其信息最大长度为 107 个数字字符。

第 3 磁道的信息有两种标准格式(参见 ISO 4909):格式代码为 01 和格式代码为 02,见表 2.6 和表 2.7。

表 2.6　格式代码为 01 的第 3 磁道信息布局

字段		M=强制 O=可选	D=动态(见注 1) S=静态	F=固定 V=可变	长度
号	内容				
1	起始标记	M	S	F	1
2	格式代码	M	S	F	2
3	主帐号(PAN)	见注 4	S	V	见注 3

续表

字段		M=强制	D=动态	F=固定	长度
			见注 1		
号	内　容	O=可选	S=静态	V=可变	
4	字段分隔符	M	S	F	1
5	国家代码	M	S	F	3
		见注 6			
6	货币	M	S	F	3
7	金额指数	M	S	F	1
8	周期授权额	M	S	F	4
9	本周期余额	M	D	F	4
10	周期起始	M	D	F	4
11	周期长度	M	S	F	2
12	密码输入次数	M	S	F	1
13	PINPARM	M	S	F	6
		见注 5			
14	交换控制符	M	S	F	1
15	PAN 帐户类型 TA 和服务限制 SR	M	S	F	2
16	SAN-1 的 TA 和 SR	M	S	F	2
17	SAN-2 的 TA 和 SR	M	S	F	2
18	失效日期	M	S	F	4
		见注 5			
19	卡顺序号	M	S	F	1
20	卡保密号	M	D	F	9
		见注 5			
21	SAN-1	O	S	V	见注 2
22	字段分隔符	M	S	F	1
23	SAN-2	O	S	V	见注 2
24	字段分隔符	M	S	F	1
25	传送标记	M	S	F	1
26	CCD	M	D	F	6
		见注 5			
27	附加数据	O	D	V	见注 2
28	结束标记	M	S	F	1
29	LRC	M	D	F	1
			最大长度		107

注：1. 动态字段可以被适当的交换方更新，静态字段仅由发卡行更新。

2. 第 3 磁道上总的字符数不能大于 107。

3. 主帐号的最大长度依赖于前 2 位数字。

4. 在双磁道操作中(即磁道 2 和磁道 3 配合使用)，PAN 在第 2 磁道上编码，此时 PAN 在第 3 磁道上的编码是可选择的。然而，当 PAN 在第 3 磁道上编码时，其各组成部分都应出现。

5. 如果不使用，用 1 个 FS 代替。

6. 当 PAN 以主要行业标识符 59 开始时，字段 5 应该包含国家代码；否则，它仅包含一个 FS。

表 2.7　格式代码为 02 的第 3 磁道信息布局

字段		M=强制 O=可选	D=动态 见注 1 S=静态	F=固定 V=可变	长度
号	内　容				
1	起始标记	M	S	F	1
2	格式代码	M	S	F	2
3	主帐号(PAN)	见注 4	S	V	见注 3
4	字段分隔符	M	S	F	1
5	国家代码	M 见注 6	S	F	3
6	货币	M	S	F	3
7	金额指数	M	S	F	1
8	周期授权额	M	S	F	4
9	本周期余额	M	D	F	4
10	周期起始	M	D	F	4
11	周期长度	M	S	F	2
12	密码输入次数	M	S	F	1
13	PINPARM	M 见注 5	S	F	6
14	交换控制符	M	S	F	1
15	PAN 帐户类型 TA 和服务限制 SR	M	S	F	2
16	SAN-1 的 TA 和 SR	M	S	F	2
17	SAN-2 的 TA 和 SR	M	S	F	2
18	失效日期	M 见注 5	S	F	4
19	卡顺序号	M	S	F	1
20	卡保密号	M 见注 5	D	F	9
21	SAN-1	O	S	V	见注 2
22	字段分隔符	M	S	F	1
23	SAN-2	O	S	V	见注 2
24	字段分隔符	M	S	F	1
25	传送标记	M	S	F	1
26	CCD	M	D	F	6
27	附加数据	见注 5			
27.1	交易日期	M 见注 5	D	F	4
27.2	附加校验值	M 见注 5	S	F	8
27.3	备选的卡顺序号	O 见注 7	S	F	3
27.4	国际网络标识码	M 见注 5	S	F	3
27.5	随意数据	O	D	F	见注 2

续表

字段		M=强制	D=动态	F=固定	长度
号	内容	O=可选	见注1 S=静态	V=可变	
28	结束标记	M	S	F	1
29	LRC	M	D	F	1
			最大长度		107

注：1. 动态字段可以被适当的交换方更新，静态字段仅由发卡行更新。

2. 第3磁道上总的字符数不能大于107。

3. 主帐号的最大长度依赖于前2位数字。

4. 在双磁道操作中(即磁道2和磁道3配合使用)，PAN在第2磁道上编码，此时PAN在居第3磁道上的编码是可选择的。然而，当PAN在第3磁道上编码时，其各组成部分都应出现。

5. 如果不使用，用1个FS代替。

6. 当PAN以主要行业标识符59开始时，字段5应该包含国家代码；否则，它仅包含一个FS。

7. 字段19为1个FS时表明该字段存在。

表中第1列为字段号，第2列是字段的名称。第3列，M表示该字段是强制存在的，O表示该字段是可选的，可有可无。第4列，D表示该字段是动态字段，其内容可在交易时更新；反之，S字段(静态字段)的内容只能被发行卡的机构(发卡者)更改，在卡的使用期间是不变的。第5列，从卡的角度说明该字段的内容是固定的还是可变的。固定(F)字段的内容是确定的、不变的，不管发卡者、使用者是谁；而可变(V)字段的内容可以随发行者或使用者的不同而不同。例如：PAN字段，它是静态字段，因为它由发卡者分配给使用人——持卡者，其内容由发卡者确定，在持卡人使用卡进行交易期间，其帐号是不变的(除非发卡者进行修改或重新指定)；但从卡的角度来看，一张卡可以是这个帐号，也可以是那个帐号，也就是说该字段的内容是可变的，因卡不同而不同，该字段是可变(V)字段。

字段1：起始标记。用于标明数据的起始，是磁道上编码的第一个数据字符，其值为BCD码的11(见表2.3)。

字段2：格式代码。用于确定磁道的数据格式。其内容定义如下：

00—— 不适用于国际交换

01——磁道格式见表2.6

02——磁道格式见表2.7

03—89——保留供ISO以后分配

90—99——供独立发卡者定义格式使用，不适用于国际交换。

字段3：主帐号(PAN)。长度详见第2.5节。该字段用来标识可以处理交易的发卡者和持卡人。当第3磁道和第2磁道配合使用时，PAN必须在第2磁道上编码，在第3磁道上的编码是可选的(可有可无)。当只有第3磁道独立使用时，PAN必须在此磁道上编码。

字段4：字段分隔符(FS)。用于标明PAN字段的结束，其值为BCD码的13(见表2.3)。

字段 5：国家代码。如果存在，应为CCC 格式的 3 个数字，否则为 1 个 FS 字符。该字段用于标明可以处理卡上交易数据的国家。

字段 6：货币类型。标明进行更新计算时所使用的货币类型。该字段的代码定义见 ISO 4217。

字段 7：金额指数。用于决定一个周期内授权金额（见字段 8）和本周期余额（见字段 9）的基值。

字段 8：每周期授权金额。该字段规定了一个周期内所允许使用（或称交易）的金额总数。这里（包括所有字段）所指的周期是指交易周期，即交易有效的一个固定或预先规定的时间期限（见字段 11）。

字段 9：本周期余额。该字段记录了当前周期内余留下来的可使用金额总数。在新的一周期开始时，应将每周期授权额（字段 8）的值赋给该字段；以后，每次交易后，交易量从该字段中减去，该字段将包含本周期的余额量。

字段 6 到字段 9 提供了一种表示货币的完整的方法。一个完整的金额量表示为：

$$\text{金额数（字段 8 或字段 9 内容）} \times 10^{\text{金额指数}} \text{货币类型}$$

例如，每周期授权 1995 美元表示为：字段 6 的 3 个数字代表美元；字段 7 的值＝0；字段 8 的值＝1995。如果不是 1995 美元而是 19950 美元，那么字段 7 的内容就等于 1，如此类推。

字段 10：周期起始。用于表明新周期开始时的日期，或者表示卡开始有效的日期。用 YDDD 格式的 4 个数字表示，其中，Y 是年的最后一个有效数字，DDD 是一年里天数的顺序号，其范围 001—366。

字段 11：周期长度。用于表示所有借记交易累积金额不能超过授权金额（见字段 8）的时间期限。在周期长度所定义的期限内，持卡人可以任意交易，但交易总量不能超过授权金额。该字段内容定义如下：

00——表明卡的本周期余额只能减少，不能重置

01—86——定义周期长度

87—89——ISO 保留

90—99——可由独立发卡者使用，但不适用于国际交换

在会计上，评价一个企业的经济状况是在一个区间（称为会计年度）内进行的；同样的，衡量一个持卡人的交易情况也需要在一定时间范围内进行，这个时间范围就是交易周期。字段 10 和字段 11 合起来表明了一个交易周期。

字段 12：输入次数。记录输入卡个人识别号（PIN）允许不成功的次数。该字段在发卡时设置（在国际交换中一般设为 3），每次成功输入 PIN 后，该字段重设为原值；而每次 PIN 输入错误后，该字段减 1。如果该字段内容减到 0，则此磁卡不能再用于任何交换。例如，该字段内容等于 3，这说明，如果连续 3 次输入 PIN 错误，卡将自锁、报废，此时持卡人必须求助于发卡机构。

字段 13：个人识别号控制参数（PINPARM）。该字段用算法标识符和验证值的形式提供一个可选的安全性能。

格式代码=01 时，该字段为 AAVVVV 形式

AA 是算法标识符，00—09 值表示使用一特殊算法，10—19 表示使用 DEA-1 算法，20—99 由 ISO 保留

VVVV 是验证值，它同计算方法联合使用，用来表明个人识别号的有效性。

格式代码=02 时，该字段为 AKVVVV 形式

A 是算法标识符，0 值表示使用一特殊算法，1 值表示使用 DEA-1 算法，2—9 值由 ISO 保留

K 是密钥标识符，其值(0—9)由发卡者酌情处理

VVVV 是验证值。

当持卡人输入 PIN 后，读卡设备就利用 PINPARM 中所指示的算法对 PIN 进行计算，结果与 PINPARM 中的验证值对比，以确定 PIN 的有效性。如果不需要 PINPARM，该字段以 1 个 FS 字符代替。

字段 14：交换控制符。用于表明磁卡允许进行交换的类型。其值为：

0 表示无限制

1 表示不适用于国际交换

2—8 限制交换。即卡只能限制在一个地区、城市或国家使用

9 ISO 建议用作测试卡。

字段 15：PAN 的帐户类型(TA)和服务限制(SR)。第 1 个数字为 TA，定义字段 3 中主帐号所记录的帐户类型：

0 PAN 不在第 3 磁道编码

1 储蓄帐户

2 现金或支票帐户

3 信用卡帐户

4 一个帐户有多种类型，例如通用帐户

5 有息现金或支票帐户

6—8 ISO 保留

9 发卡者内部使用，不用于交换。

第 2 个数字是 SR，定义如下：

0 无限制

1 无现金服务

2 无销售点(POS)服务

3 无现金和销售点交易

4 要求授权

5—7 ISO 保留

8—9 发卡者限制使用范围。

字段 16：SAN-1 的帐户类型和服务限制。

字段 17：SAN-2 的帐户类型和服务限制。

字段 16 和字段 17 分别涉及 ASN-1 和 ASN-2(见字段 21 和 23)中包含的帐号,其格式、内容与字段 15 一致,只是 TA＝0 表明对应的字段(SAN-1 或 SAN-2)不在第 3 磁道编码。

字段 18:失效日期。其格式为 YYMM。YY 是失效日期的年度,MM 是失效日期的月份。如果没有失效日期,该字段以 1 个 FS 字符代替。

字段 19:卡顺序号。用于区别具有相同 PAN 的卡(这些卡同时或连续发出)。该字段在最初发卡或者在卡失效后换卡时赋值;每次增加卡或发新卡时,该字段值增加。而对于格式代码 02,该字段值可以为 1 个 FS,此时表明字段 27.3 中存在卡序列号。

字段 20:卡保密号。用于联系物理卡片和卡上磁条所含的数据。如果存在,其格式为 MCCCCCCCC,M 是保密方法标识符,CCCCCCCC 是由保密方法决定的代码。若不存在,该字段为 1 个 FS 字符。

字段 21:第 1 辅助帐号(SAN-1)。标明第一个可选用的辅助帐号。

字段 22:字段分隔符。1 个 FS 字符。

字段 23:第 2 辅助帐号(SAN-2)。

字段 21(SAN-1)和字段 23(SAN-2)的长度是可变的,但是要保证第 3 磁道的编码总长度不大于 107 个字符。

字段 24:字段分隔符。1 个 FS 字符。

字段 25:传送标记。提供使得银行计算中心间所交换的信息长度可以减少的功能。该字段表明,交换的信息是否要包含附加数据字段(字段 27)的内容。

字段 26:加密验证数(CCD)。提供一种用加密公式来验证第 3 磁道数据元的完整性的方法。如果不存在 CCD,该字段以 1 个 FS 字符代替。

字段 27:附加数据。包含一些对发卡者有意义的可选数据。对格式代码 01 来说,其内容由发卡者自行定义。而对格式代码 02 来说,如果没有附加数据,该字段以 1 个 FS 字符代替;如果有附加数据,依照下面的字段(字段 27.1—字段 27.5)定义。

字段 27.1:交易日期。用 YDDD 4 个数字表示最近支出现金的日期。每笔现金支出之后,该字段被当前日期更新。如果不需要记录交易日期,该字段以 1 个 FS 字符代替。

字段 27.2:附加验证值。用于 PIN 的验证,提供一个不同密钥(key)值的 PIN 验证过程的联系。其内容为 8 个数字,可以作为 2 个 4 位数字的验证值,可以作为 1 个 8 位数字的验证值,也可以同字段 13 的后 4 位数字(验证值)一道作为 2 个 6 位数字的验证值。如果不需要附加验证值,该字段以 1 个 FS 字符代替。

字段 27.3:备用卡顺序号。其格式为"nnn"。该字段含义同字段 19,用于区别具有相同 PAN 的卡。注意:此字段若存在,字段 19 应为 FS 字符。

字段 27.4:国际网络标识符。用 3 个数字表示可提供接收服务的发卡者国际组织。当 ISO 7812 预先定义的发卡者标识符(IIN,见第 2.5 节)没有使用时,用该

字段的内容标识该组织。如果不需要，该字段以 1 个 FS 代替。

字段 27.5：随意数据。包括任意对发卡者有意义的数据。

字段 28：结束标记(结束字符)。表明第 3 磁道有意义数据的结束，值为 BCD 码的 15(见表 2.3)。

字段 29：纵向冗余校验字符(LRC)。

2.5 主帐号格式

主帐号(PAN)是标识持卡人的号码，它等同于 ISO 7812 中所定义的标识号码(ISO 4909 对 PAN 的有关内容作了补充规定)。标识号码(或称 PAN)由图 2.5 所示的三部分组成。

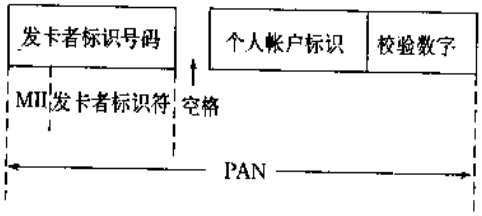


图 2.5 PAN(标识号码)的组成

1. 发卡者标识号码

它是标识主要行业和发卡者的号码。该号码由两部分组成：主要行业标识符(MII)和发卡者标识符(见表 2.8)。

表 2.8 发卡者标识号码的格式

MII	发卡者标识符	行 业
0		保留将来分配
1	×××	航空业
2	×××	航空业保留将来分配
	×××××	其它
3	×××××	旅游和娱乐业
4	×××××	银行/金融业
5	0××××	银行/金融业
	1×	
	2××	
	3×××	
	4××××	
	5×××××	
	6××××××	
	7×××××××	
	8××××××××	
	9 特殊处理	

续表

MII	发卡者标识符	行　业
6	×××××××	商业和银行业
7	×××××××	石油业
8		保留将来分配
9	CCC(国家代码,参见 ISO 3166)+发卡者标识符	

注：① 一个"×"代表 1 个数字。

② MII=9 时,由 CCC 指定的国家标准部门分配发卡者标识符。

MII 用于标识发卡者所属行业,用 1 个数字表示。发卡者标识符用于标识各行业内不同发卡者,其长度由 MII 预先确定。当 MII=5 时,根据发卡者标识符的第 1 个数字确定其长度;而当 MII=5 后紧跟数字 9 时,发卡者标识符由金融机构分配,而并非像其他情况一样由 ISO 注册授权机构发布。此时可将"59"整个看作是 MII,标识金融行业。金融机构发布的发卡者标识符最多由 8 个数字组成,并用一个字段分隔符(空格)终止。

2. 个人帐户标识

它是由发卡部门分配给独立单位或个人的号码,用于标识一个独立的帐户。

3. 校验数字

个人帐户标识之后紧跟一数字,用以使 PAN 有效。它是根据 PAN 前面所有数字(从 MII 开始)计算得到的(字段分隔符计算时以 0 代替)。其计算方法是采用计算模 10"隔位倍加"校验数的 Luhn 公式,步骤如下:

步骤 1:从右边第 1 数字开始(低序)每隔 1 位乘以 2。

步骤 2:把步骤 1 中获得的乘积的各位数字与原号码中未乘 2 的各位数字相加。

步骤 3:求这个总和的个位数字的"10 的补数",这个补数就是校验数字。如果步骤 2 得到的总和是以 0 结尾的数(如 30、40 等),则校验数字为 0。

例如:无校验数字的帐号　499273 9871

步骤	4	9	9	2	7	3	9	8	7	1
1			×2		×2		×2		×2	
			18		4		6		16	2

2　4+1+8+9+4+7+6+9+1+6+7+2=64

3　4 的补数=6

结果：　带有校验数字的帐号为

499273 98716

4. PAN 的长度

在第 1 磁道和第 2 磁道上,PAN 最多为 19 个数字;而在第 3 磁道上,PAN 的最大长度依赖于发卡者标识号码。对于银行/金融业,其最大长度定义如下:

(1) MII=4 或 6:　1 个数字

发卡者标识符:　5 个数字

个人帐户标识:　最多 12 个数字

校验数字：　　1 个数字

故 PAN 最大长度：19 个数字

(2) MII＝5：　　1 个数字

发卡者标识符：　2—5 个数字

个人帐户标识：　最多 15 个数字

校验数字：　　1 个数字

故 PAN 最大长度还是限制为 19 个数字。

(3) MII＝59：　　2 个数字

发卡者标识符：　最多 8 个数字

字段分隔符：　　1 个数字

个人帐户标识符：最多 23 个数字

校验数字：　　1 个数字

此时规定 PAN 最大长度为 28 个数字。

2.6　金融交易内容

前面几节讲述了各磁道的格式及内容，但用户持有卡以后，如何使用、接受卡的一方和发卡方的关系怎样、如何协调呢？一般来说，因磁条保密性较差，易伪造、修改，所以大多数情况下磁卡都是作为静态数据输入使用。虽然第 3 磁道可读写，并且有金额字段，也只是用于小金额的应用领域。例如用作电话卡。

在金融行业，作为金融交易卡(FTC)的磁卡，一般配合强大、可靠的计算机网络系统使用。用户的各方面信息，诸如金额、交易记录等等，均保存在金融机构计算机的数据库中，用户所持的卡片只是提供用户的主帐号(PAN)等索引信息，便于在数据库中迅速找到用户数据。一个典型的网络系统见图 2.6。

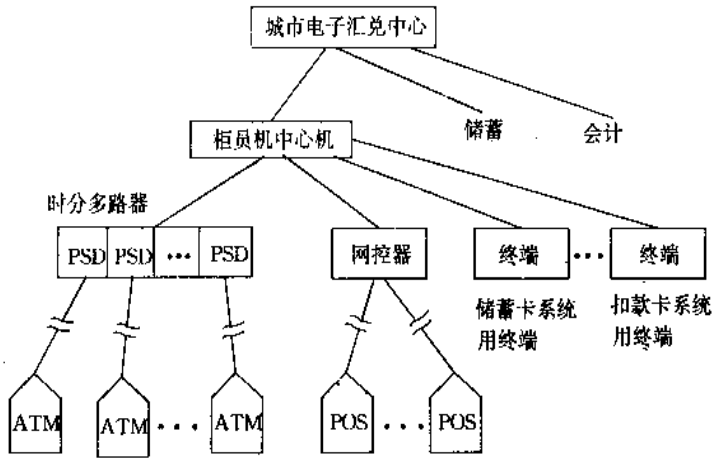


图 2.6　城市金融电子网络示意图

ATM、POS(详见第 8 章)或其它卡用终端等读卡设备接受 FTC 卡信息后，向上传输

直到城市电子汇兑中心(有可能还要向上传输至省金融机构的中心机),在中心计算机上处理后再逆向(向下)传输至读卡设备,完成授权或拒付等操作。

在整个 FTC 卡的发卡、用卡系统中,涉及到多个对象,它们的关系可以用一个简单的示意图(图 2.7)表示出来。

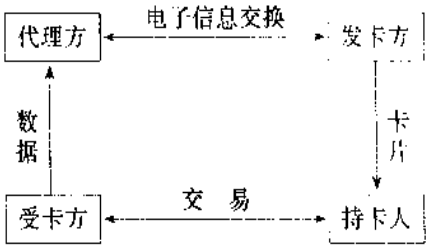


图2.7 FTC卡各方关系示意图

发卡方(发放识别卡给持卡人的机构或其代理)将卡片发给持卡人(要求同受卡方进行交易并且与特定的主帐号相联系的客户),持卡人就可以凭着卡片同受卡方(接受卡并把交易数据传输给代理方的机构)进行交易。受卡方将交易的内容、数据传输给代理方(从受卡方获取有关交易数据并把数据引入交换系统的金融机构或其代理),代理方再通过交换系统同发卡方进行信息交换,取得对持卡人交易的控制。

举个例子。某银行(发卡方)核对了你(持卡人)的帐目后,发给你一张消费卡,上面有你的帐号,你最多一次可使用的金额等等。你持这张卡到某商店(受卡方)去购物。商店将你的帐号、所购物金额数记录下来,某一天通知商店的开户银行(代理方),告诉它你今天在这儿花了多少钱(如果你购物的金额过大,超过了授权额,商店也许还要先向其开户银行申请授权,请银行担保你能使用这笔费用),随后商店的开户行就会通过信息交换系统同发卡的银行联系,以修正你在该银行中的帐目或请求获得消费担保,整个过程就结束了。

目前在大多数情况下,发卡方和代理方实际上是一家,这实际上构成了一个专用系统。随着技术的发展,发卡方和代理方的独立性越趋明显,这就使得用户真的能"一卡在手、走遍天下"了,而不管发给我卡的是哪家银行,我消费的地方又属于哪家银行了。

代理方和发卡方可能采用不同的应用规范,这两方的信息交换就需要有一个标准。国际标准化组织针对采用不同应用规范的专用系统,制定了一个信息交换规范。所有信息的格式、内容、交换协议都应遵循这个规范(参见 ISO 8583:1987)。

ISO 8583:1987 规定,所有在系统间传输的信息都包括三部分:信息类别识别符、一个或多个比特图、一个按比特图表示的顺序排列的数据元序列(见图 2.8)。

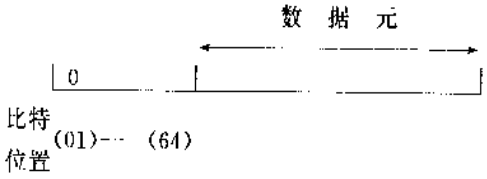
信息类别识别符	比特图	数据元序列

图 2.8 金融交易的信息结构图

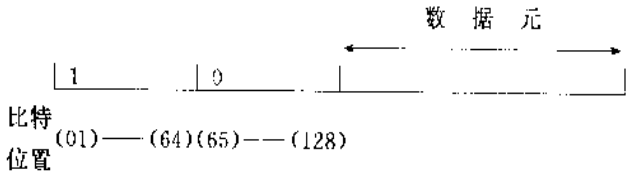
- 信息类型识别符是一个 4 位数字的数字型字段,目前 ISO 已定义的信息类别有七类:授权信息、金融交易信息、文件更新信息、撤消信息、对帐控制信息、管理信道

和网络管理信息。

- 比特图由 64 个位构成，每 1 位用“1”或“0”表示与该特定位对应的数据元信息存在与否。如果比特图左边第 1 位为“1”，表明其后紧跟有一个辅助的比特图(见图 2.9)。



(a) 只有基本的比特图



(b) 基本的和扩展的比特图

图 2.9 比特图

- 数据元序列是利用比特图作为索引，对信息按顺序进行重组构成的。ISO 8583：1987 以表的形式给出了各数据元在比特图中的位置，并且根据信息类型识别符，对这些数据元的存在作了规定。例如，主帐号(PAN)位于比特图的第 2 位。如果比特图第 2 位为“1”，那么信息的第 3 部分的第 1 个数据元就是 PAN。

ISO 8583:1987 不仅定义了不同系统间交换信息的格式，还规定了交换双方的信息流向，即交换协议。以请求授权为例，图 2.10 示出了这个过程。

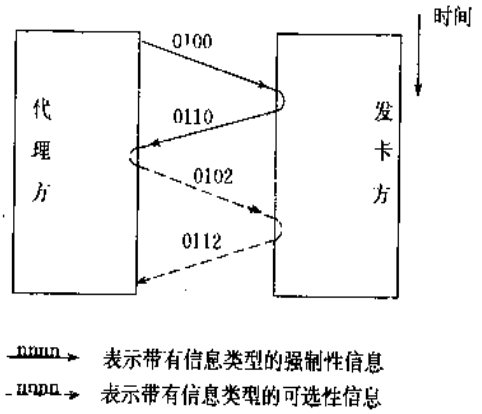


图 2.10 授权请求过程

代理方向发卡方发出类型为 0100(授权请求)的信息，请求发卡方进行授权(发卡方给代理方或受卡方的认可或担保)。发卡方返回 0110(授权请求响应)信息进行应答。授权过程这时已基本完成。为了保险，代理方可以(也可不进行)发出 0102(授权完成确认)信

息询问发卡方授权是否完成，发卡方以 0112(授权完成响应)进行回答表示授权已经完成。整个授权过程就结束了。

2.7 磁卡存在的问题

磁卡因其简单、价廉广泛应用于金融、邮电、航空等领域，世界范围内磁卡的发行量已超过数十亿张。但磁卡的应用存在一些问题，这是由磁卡本身的特性所决定的，主要表现在卡的保密性和卡的应用方式上。

1. 磁卡保密性较差

磁条容易读出和伪造。因此，自 FTC 卡发行以来，各式各样的作弊、诈骗行为日益增加，给银行及其代理带来了损失。诸如售货商作弊、偷窃、伪造、冒领、诈骗等等。为了防备更严重的诈骗行为，各行业采取了其他一些方法对磁卡的使用加以限制，如要求授权、限制一天内交易次数及交易金额等，这从某种程度上减轻了损失。

2. 磁卡的应用方式比较单一、受限制

磁卡的方便应用往往需要其它方面的条件，例如强大可靠的计算机网络系统、中央数据库等等，其应用方式是集中式的，这就给用户带来了很大不便。例如，一个持有北京市某银行发行的磁卡的人，如在外地消费。目前需由商户在当地用电话与北京进行联系，请求北京的银行对此持卡人进行授权，用户往往得等半个小时以上，还不如现金方便。即使有了网络通道，又存在网络速度、网络吞吐率等问题了。所有这些问题都是因为磁卡中磁条本身信息量少、保密性差引起的。

近年来随集成电路发展而兴起的 IC 卡(集成电路卡)，其保密性好、容量大。在上面的例子中，可以在 IC 卡中记录持卡人的帐目信息(包括金额)，这样持卡人消费时，受卡方只需查看一下卡中信息就可处理交易了。过一段时间(如晚上)受卡方再同异地银行打交道，进行清算(所谓清算是指为最终记帐，对前期完成的一笔或多笔交易进行的资金转帐)。这样大大方便了用户，缩短了交易时间。

IC 卡的使用相当于将持卡人从集中式数据管理方式下解脱出来。每张卡相当于一个流动的小数据库，这些数据库非实时地与中央数据库打交道、交换数据。也就是说，将集中式数据处理方式转化为分布式数据处理。这将大大方便用户，是很有发展前途的一个方向。

2.8 与磁卡有关的国际标准

国际标准化组织(ISO)制定了一系列标准来描述识别卡和磁卡。磁卡应遵循的国际标准大致有：

ISO 7810：1987，定义了识别卡的物理特性。

ISO 7811/1：1985，描述识别卡的凸印技术。

ISO 7811/2：1985，描述识别卡的磁条特性。

ISO 7811/3：1985，描述 ID-1 卡上凸印字符的位置。

ISO 7811/4:1985,描述磁卡上第1磁道和第2磁道的位置。

ISO 7811/5:1985,描述磁卡上第3磁道的位置。

ISO 7812:1987,描述发卡者标识符编号体系与注册程序,包括PAN(主帐号)的格式等内容。

ISO 7813:1987,描述作为金融交易卡的磁卡的第1磁道和第2磁道的格式及内容。

ISO 4909:1987,描述磁条第3磁道的格式及内容。

ISO 7580:1987和ISO 8583:1987,描述了银行卡交换信息规范,即定义了金融交易的内容。

思 考 题

1. 什么是识别卡?磁卡有哪些物理特性?
2. 磁条采取何种编码技术?简述其方法。
3. 磁卡有几条标准磁道?各磁道在卡上位置如何排列?
4. 磁道1采用的编码字符集是什么?磁道2和磁道3采用什么字符集进行编码?
5. 磁道编码时采用什么错误检测技术?
6. 试述LRC字符的计算方法。
7. 简述FTC卡第1磁道的格式及内容。
8. 简述磁道1上姓名字段的格式。
9. 简述FTC卡第2磁道的格式及内容。
10. 三条磁道信息的最大长度各是多少?
11. FTC卡第3磁道上都有哪些内容?
12. 何为主帐号?主帐号是如何构成的?其长度多少?
13. 主帐号的校验数字如何计算?
14. 在整个FTC卡系统中,涉及到哪几个对象?其关系如何?
15. 金融交易的信息包括哪几部分?各部分内容是什么?
16. 以授权请求为例简述金融交易双方进行信息交换的交换协议。

第3章　IC卡国际标准(一)

ISO(国际标准化组织)和IEC(国际电子技术委员会)一起组成了国际化工作的专门委员会,作为ISO或IEC成员的国家团体通过技术委员会参与国际标准的制定。ISO与IEC的技术委员会在彼此有兴趣的领域互相合作,其他与ISO和IEC有联系的国际组织,无论是官方的或非官方的,也参与了该项工作。

在信息技术领域,ISO和IEC共同建立了一个技术委员会,即ISO/IEC JTC 1,被该委员会所采纳的国际标准草案由各国家团体投票,被发布作为国际标准至少需要得到75%参加投票的国家团体的赞成。

已发布的国际标准,在今后仍可能被修改,因此,在使用国际标准时,要注意应用国际标准的最新版本。

IC卡国际标准的总名称为:识别卡　　接触型集成电路卡;国际标准为ISO/IEC 7816。包括以下部分:

第一部分:ISO 7816-1,物理特性。

第二部分:ISO 7816-2,触点尺寸和位置。

第三部分:ISO/IEC 7816-3,电信号和传输协议。

第四部分:ISO/IEC 7816-4,行业间交换用命令。

第五部分:ISO/IEC 7816-5,应用标识符的编号系统和注册过程。

上述第四部分,到目前为止仍为草案,其余几部分已正式被通过为国际标准。在本章内,将较详细介绍第一、二、三部分,第四、五部分在下一章中作专门介绍,与原文相比,已进行了精简,如读者对全文感兴趣,请查阅相应的国际标准。

3.1　ISO 7816-1,接触型集成电路卡的物理特性

本标准制定的物理特性适合于ID-1型的识别卡,其尺寸为85.6×53.98×0.76mm(参见第2章)。

ISO 7810中为各种识别卡定义的物理特性适用于IC卡,ISO 7813中对金融交易卡定义的阻燃性和外形尺寸也适用于IC卡。此外还提出了以下附加特性:①防护紫外线的能力;②X光照射的剂量;③触点的表面轮廓;④卡和触点的机械强度;⑤触点电阻;⑥磁条与集成电路之间的电磁干扰;⑦指定强度磁场的影响;⑧静电影响;⑨热耗等。

标准规定了上述各项测试的具体指标,并要求经测试后的集成电路不应损坏或丧失功能。

使用时卡的表面温度不应超过50℃。

3.2 ISO 7816-2，接触型集成电路卡的触点尺寸和位置

ISO 7816-2 规定了 ID-1 型集成电路卡各触点的尺寸、位置和功能。规定每个触点都应有一个不小于 2.0×1.7mm² 的矩形表面区域，各触点间应互相隔离，但未规定触点的形状和最大尺寸。

IC 卡有 8 个触点，从 C1 到 C8，触点可安排在卡的正面或反面。触点的位置如图 3.1 所示(以卡的接触面的左边和上边为基准线)，每个触点的功能见表 3.1。

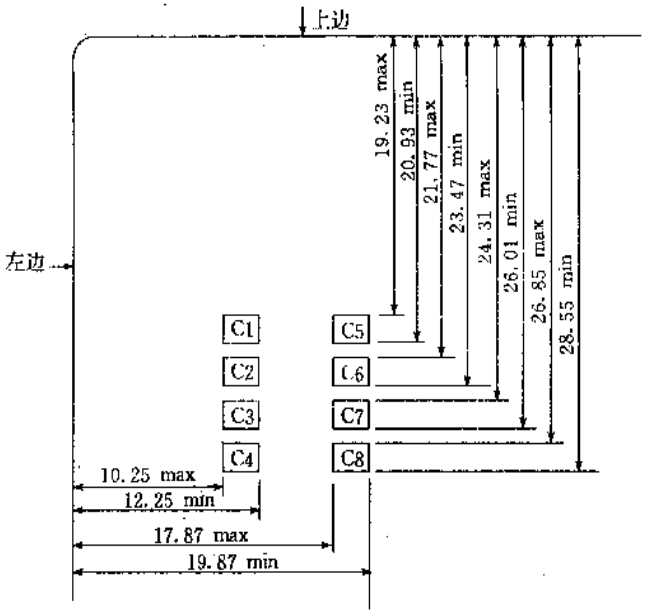


图 3.1 触点的位置

表 3.1 触点功能

触点编号	功能	触点编号	功能
C1	V_{cc}(电源电压)	C5	GND(地)
C2	RST(复位信号)	C6	V_{pp}(编程电压)
C3	CLK(时钟)	C7	I/O(数据)
C4	ISO/IEC JTC1/SC17 保留于将来使用	C8	ISO/IEC JTC1/SC17 保留于将来使用

3.3 ISO/IEC 7816-3，接触型集成电路卡的电信号和传输协议

本协议由两部分合并而成，它们是：ISO/IEC 7816-3；ISO/IEC 7816-3 AMEND-

MENT 1(在本书中简化为 ISO/IEC 7816-3 A.1)。

前一部分包括同步传输协议和异步传输协议(T=0)的内容,在本节中描述。

后一部分包括异步传输协议(T=1)的内容,在 3.4 节中描述。

ISO/IEC 7816-3 中规定了电源及信号的结构,以及 IC 卡和接口设备之间的信息交换,包括信号频率、电压电平、电流值、奇偶校验协定、操作过程、传送机制以及接口设备与 IC 卡之间的通信协定等。在这里不包括信息和指令的内容,如发行者和用户的身份识别,服务与限制、安全(密码体制)特点和指令定义等均不在此说明。

根据以上所述,可将 ISO/IEC 7816-3 中定义的传输协议归纳如下:

1. 同步传输协议。

2. 异步传输协议(T=0;T=1)。

同步传输协议规定 I/O 上的信息由 CLK 进行同步,从目前情况来看,适用于逻辑加密卡。

异步传输协议规定 I/O 上的信息用帧方式传送(在本章 3.4.4 中介绍),我们在分析国外产品后,可以肯定该协议适用于内含微处理器的智能卡。

3.3.1 触点的电特性

在 ISO 7816-2 中已对 IC 卡的 8 个触点作出规定,它们是:

I/O:IC 卡的串行数据的输入和输出端。

V_{CC}:电源电压输入端(由卡选用)。

GND:地(参考电压)。

V_{PP}:编程电压输入端(由卡选用)。

CLK:时钟或定时信号输入端(由卡选用)。

RST:复位信号(总清信号),可由接口设备提供复位信号给 RST 触点;或由 IC 卡内部的复位控制电路在加电时产生内部复位信号。如果实现内部复位,必须提供电压到 V_{CC} 端。

剩下的两个触点的用途将在相应的应用标准中规定。

在讨论每个触点的电特性之前,先将所用符号的意义叙述如下:

V_{IH}:高电平输入电压。

V_{IL}:低电平输入电压。

V_{OH}:高电平输出电压。

V_{OL}:低电平输出电压。

t_R:信号幅度 10%—90%之间的上升时间。

t_F:信号幅度 90%—10%之间的下降时间。

C_{IN}:输入电容。

C_{OUT}:输出电容。

I_{IH}:高电平输入电流。

I_{IL}:低电平输入电流。

I_{OH}：高电平输出电流。

I_{OL}：低电平输出电流。

I_{CC}：V_{CC}端电源电流。

I_{PP}：V_{PP}端编程电流。

下面将对每个触点逐一进行说明。

1. I/O

I/O 触点用于数据交换的输入(接收状态)或输出(发送方式)。I/O 触点有两种可能的状态：

(1) 传号或高状态(Z 状态)，当卡和接收设备均处在接收方式时，I/O 处于 Z 状态，也可被发送方规定为 Z 状态。

(2) 空号或低状态(A 状态)，可被发送方规定为 A 状态。

如卡与接口设备均处于接收方式时，I/O 端处于 Z 状态。当卡与接口设备处于不匹配的传输方式时，I/O 端的逻辑状态可能是不确定的。在操作期间，卡与接口设备不能同时处于发送状态。表 3.2 为正常操作状态下 I/O 的电特性。

表 3.2 正常操作状态下的 I/O 电特性

符号	条件		最小值	最大值	单位
V_{IH}	Either or[1]	$I_{IH\,max}=\pm 500\mu A$	2	V_{CC}	V
		$I_{IH\,max}=20\mu A$	$0.7\times V_{CC}$	V_{CC}[3]	V
V_{IL}	$I_{IL\,max}=-1mA$		0[3]	0.8	V
V_{OH}[2]	Either or	$I_{OH\,max}=-100\mu A$	2.4	V_{CC}	V
		$I_{OH\,max}=-20\mu A$	3.8	V_{CC}	V
V_{OL}	$I_{OL\,max}=1mA$		0	0.4	V
t_R t_F	$C_{IN}=30pF$；$C_{OUT}=30pF$			1	μs

1) 对接口设备，考虑两种状态。

2) 假设在接口设备中用了上拉电阻(建议 20kΩ)。

3) I/O 上的电压保持在 -0.3V—V_{CC}+0.3V 之间。

2. V_{CC}

本触点用于提供电源电压 V_{CC}。在正常操作状态下，V_{CC}=4.75V—5.25V，I_{CC}的最大电流为 200mA。

3. V_{PP}

卡内非易失性存储器 EEPROM 编程或擦除时从 V_{PP}端提供电源。V_{PP}有两种状态：空闲状态和激活状态。除编程和擦除外，均处于空闲状态。正常操作状态下 V_{PP}的电特性如表 3.3 所示。

表 3.3 正常操作状态下 V_{PP} 的电特性

符号	条件	最小值	最大值	单位
V_{PP}	空闲状态 (编程未激活)	$0.95\times V_{CC}$	$1.05\times V_{CC}$ 20	V mA
V_{PP} I_{PP}	激活状态 (对卡编程)	$0.975\times P$	$1.025\times P$ I	V mA
卡向接口设备提供 P 和 I 值(默认值：P=5,I=50)见 3.3.4 节。				

电压上升或下降时间：200μs(最大值)，V_{PP} 变化速率不超过 2V/μs。

最大功率 $V_{PP}\times I_{PP}$：在任意一秒时间内的平均值不超过 1.5W。

4. CLK

正常操作状态下的 CLK 电特性如表 3.4 所示。

表 3.4 正常操作状态下的 CLK 的电特性

符号	条件		最小值	最大值	单位
V_{IH}	Either or[1] or[1]	$I_{IH\ max}=\pm 200\mu A$	2.4	V_{CC}[2]	V
		$I_{IH\ max}=\pm 20\mu A$	$0.7\times V_{CC}$	V_{CC}[2]	V
		$I_{IH\ max}=\pm 10\mu A$	$V_{CC}-0.7$	V_{CC}[2]	V
V_{IL}	$I_{IL\ max}=\pm 200\mu A$		0[2]	0.5	V
t_R t_F	$C_{IN}=30pF$			9%of period with a maximum of 0.5μs	

1) 对接口设备，考虑三种状态。

2) CLK 上的电压保持在 −0.3V V_{CC}+0.3V 之间。

5. RST

正常操作状态下 RST 的电特性如表 3.5 所示。

表 3.5 正常操作状态下的 RST 的电特性

符号	条件		最小值	最大值	单位
V_{IH}	Either or[1]	$I_{IH\ max}=\pm 200\mu A$	4	V_{CC}[2]	V
		$I_{IH\ max}=\pm 10\mu A$	$V_{CC}-0.7$	V_{CC}[2]	V
V_{IL}	$I_{IL\ max}=\pm 200\mu A$		0[2]	0.6	V

1) 对接口设备，考虑两种状态。

2) RST 电压保持在 −0.3V—V_{CC}+0.3V 之间。

3.3.2 IC卡的操作过程

接口设备和卡之间的对话通过以下操作顺序实现。

——连接接口设备和"激活"触点；

——卡的复位(Reset)；

——卡对复位的应答(Answer To Reset)；

——在卡与接口设备之间连续进行信息交换；

——接口设备"释放"触点。

下面对"激活"触点和"释放"触点作一解释。

接口设备"激活"触点由以下操作顺序实现：

——RST 处于 L 状态；

——V_{CC}供电；

——接口设备的 I/O 处于接收方式；

——V_{PP}上升为空闲状态；

——RST 处于 H 状态(同步传输)；

——提供稳定的 CLK。

当信息交换结束或异常终止(卡未响应或检测到卡已拔掉)时，接口设备"释放"触点。

接口设备"释放"触点由以下操作顺序实现。

——RST 为状态 L(低电平)；

——CLK 为状态 L(低电平)；

——V_{PP}不起作用；

——I/O 为状态 A(空号)；

——V_{CC}不起作用。

3.3.3 卡的复位

1. 异步应答卡

异步应答卡的复位情况如图 3.2 所示。

激活触点结束后，在 T_0 时刻，时钟信号加到 CLK 端，在其后的 200 个时钟周期内(T_0 以后的 t_2 时间内)，I/O 线将被置于 Z 状态。

对于内部复位卡，在几个时钟信号周期后被复位，在 I/O 上的复位应答将在时钟信号加到 CLK 端之后的 400 −40000 个时钟周期(T_0 后的 t_1 时钟)之间开始。

使用低电平复位(active low reset)的卡，是依靠 RST 维持在状态 L 来进行复位的，RST 处于状态 L 至少 40000 个时钟周期(T_0 后的 t_3 时间)，在 T_1 时 RST 上升到状态 H，在 RST 上升沿之后的 400—40000 个时钟周期之间(T_1 后的 t_1 时间)，I/O 上的复位应答将开始。

如果 RST 处于状态 H(T_1 后的 t_3 时间)40000 个时钟周期内复位应答还没有开始，RST 将返回到状态 L(在 T_2 时)，同时接口设备将释放触点。

2. 同步应答卡

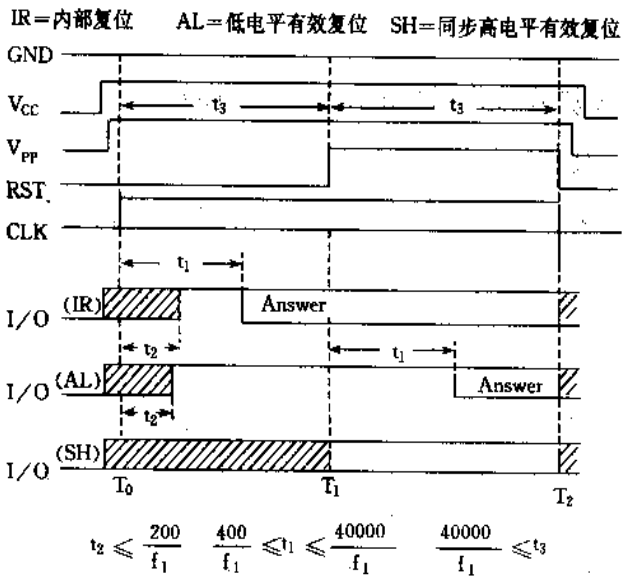


图 3.2 卡的复位(异步应答)

注意：阴影部分表示 I/O 状态不定

同步应答卡的复位情况如图 3.3 所示。

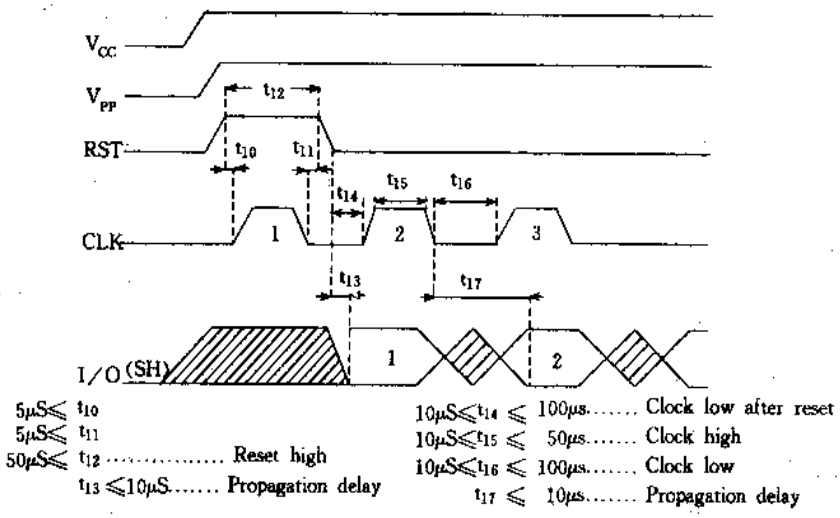


图 3.3 同步应答时卡的复位

复位操作时，接口设备首先把所有连线置于状态 L，然后 V_{CC} 供电，V_{PP} 置于空闲状态，接口设备的 I/O 处于接收方式，RST 信号上升，要求 RST 维持在状态 H 至少 50μs (t_{12})。

在 RST 上升沿之后的 t_{10} 时间之后加上时钟脉冲 CLK，CLK 处于状态 H 的时间可在 10μs 到 50μs(t_{12})之间，当 RST 处于状态 H 时，不允许加上 1 个以上的时钟脉冲。CLK 与 RST 下降沿之间的时间间隔是 t_{11}。

在 RST 下降沿之后的 t_{13}时间内，CLK 处于状态 L 且有效，在 I/O 线上将得到应答的第 1 个数据位。

3.3.4 异步传输的复位应答(Answer To Reset)

1. 复位应答的构成

复位应答信号以字符为单位(称为字符帧)进行传送。下面先介绍字符帧，然后描述复位应答信号。

(1) 字符帧(图 3.4)

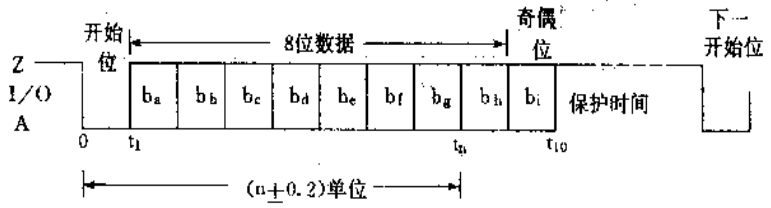


图 3.4 字符帧

在传送字符前，I/O 处于状态 Z。

每个字符由 10 位组成：起始位(1 位)为状态 A，8 位数据 b_a—b_h，第 10 位 b_i 为偶校验位(从 b_a 到 b_i，"1"的个数为偶数是正确的)。每一位在 I/O 线的持续的时间定义为基本时间单元。

一个数据字节由 b_1—b_8 组成，b_1 为最低位，b_8 是最高位，b_a—b_h 对应于 b_1—b_8。

两个连续字符之间的延时(两起始位上升沿之间)至少为 12 个基本时间单元，包括字符宽度 10 个单元和一段保护时间，在保护时间内，接口设备和卡都处于接收状态，因此 I/O线处于状态 Z。

在复位应答期间，卡发出的两个连续字符的起始位上升沿之间的延时不得超过 9600 单元，这个最大值称为初始等待时间。

当奇偶校验不正确时，从起始位上升沿之后的 10.5 单元开始，收方发送状态 A 作为出错信号，该信号宽度为 1 个单元或 2 个单元。发方检验 I/O 是在起始位上升沿之后的 11 单元处，如 I/O 处于状态 Z，则认为接收是正确的；如 I/O 处于状态 A，则认为有错，收方期望发方重发有错的字符(对使用 T＝0 异步传输协议的卡必须重发，对接口设备和其他的卡则是可选择的)。

(2) 复位应答信息的内容

卡产生的复位应答信息按以下顺序传送(最多 32 个字符)：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)以及校验字符 TCK。其中 TS 和 T0 是一定有的，接口字符和校验字符是可选择的。图 3.5 示出复位应答的一般构成。

① 初始字符 TS：I/O 开始处于状态 Z，然后是起始位 A，接着有两种表示方法如图 3.6 所示：当首先传送的是字符的最高有效位时，TS 为(Z)AZZAAAAAAZ，其中 A 为逻

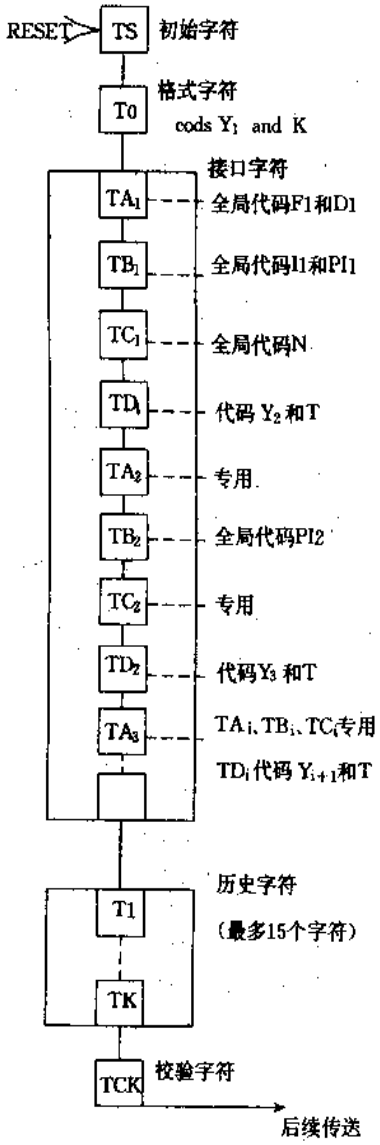


图 3.5　复位应答的一般构成

辑电平“1”,解码后的字符值为 3F,称之为反向约定;当首先传送的是字符的最低有效位时,TS 为(Z)AZZAZZZAAZ,其中 Z 为逻辑电平“1”,解码后的字符值为 3B,称之为正向约定。

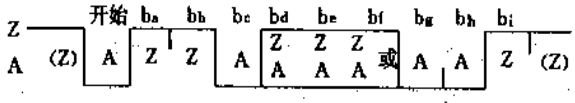
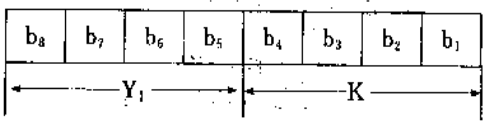


图 3.6　初始字符 TS

② 格式字符 T0:字符的高半字节有效位(b_5 b_6 b_7 b_8)命名为 Y_i,当相应位为 1 时,分别表示后续接口字符 TA_1 TB_1 TC_1 TD_1 存在;字符的低半字节有效位 b_4 到 b_1 命名为 K,

用它指出历史字符的个数 0—15，见图 3.7。



Y_1——接口字符存在的指示符

$b_5=1$，发送 TA_1

$b_6=1$，发送 TB_1

$b_7=1$，发送 TC_1

$b_8=1$，发送 TD_1

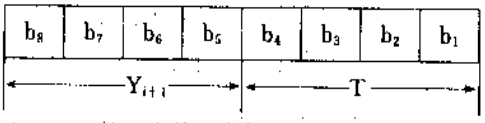
K——历史字符数(0—15)

图 3.7 T0 提供的信息

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

TA_i TB_i TC_i($i=1,2,3\cdots$)指示协议参数。

TD_i 指明协议类型 T 和是否存在后续接口字符，见图 3.8。TDi 包括 Y_{i+1}与 T 两部分，其中 Y_{i+1}由 b_5 到 b_8 组成，分别表示后续接口字符 TA_{i+1} TB_{i+1} TC_{i+1} TD_{i+1}是否存在，T 由 b_1 到 b_4 组成，表示后续发送的协议类型：



Y_{i+1}——接口字符存在的指示符

$b_5=1$，发送 TA_{i+1}

$b_6=1$，发送 TB_{i+1}

$b_7=1$，发送 TC_{i+1}

$b_8=1$，发送 TD_{i+1}

T—— 后续发送的协议形式

图 3.8 TD_i 提供的信息

T=0 异步半双工字符传输协议。

T=1 异步半双工分组传输协议。

T=2 和 T=3 保留，用于今后的全双工传输协议。

T=4 增强型异步半双工字符传输协议。

T=5 到 T=13 保留，今后使用。

T=14 用于 ISO 非标准协议。

T=15 保留，今后扩展使用。

TA_1 TB_1 TC_1 和 TB_2 是全局性接口字符，为了能处理任一种传输协议，将在后面解释这些全局性接口字符。其余的 TA_i TB_i TC_i 是专用接口字符，对它们的解释由协议类型 TD_{i-1}中的 T 决定。

如有一种以上协议类型被选用，且 T=0 是其中的一种，则首先指示 T=0。

④ 历史字符 T1，T2…TK：由 T0 的低 4 位 K 指出历史字符的个数，最多不超过 15 个。

⑤ 校验字符 TCK

TCK 的值应这样选择：使 T0 到 TCK 的所有字符的异或操作结果为零。

如仅用 T=0 协议，将不发送 TCK，而在所有其他情况下，都发送 TCK。

2. 全局接口字节 TA_1 TB_1 TC_1 TB_2

全局接口字节给出接口设备用来计算的一些参数(F、D、I、P、N)。

(1) 参数 F、D、I、P、N：在复位应答期间的初始时钟周期将被其后传送信息的工作时钟周期所代替，F 是时钟频率转换因子，D 是位速率调整因子，用来决定工作时钟周期。

对于内部时钟卡：初始时钟周期$=\frac{1}{9600}$s；工作时钟周期$=\frac{1}{D}\times\frac{1}{9600}$s。

对于外部时钟卡(设 f_1 为复位应答期间接口设备提供给 CLK 触点的实际频率，其后，由 f_1 切换到 f_s)：初始时钟周期$=\frac{372}{f_1}$s；工作时钟周期$=\frac{1}{D}\times\frac{F}{f_s}$s。

f_s 的最小值为 1MHz，F 以及 f_s 的最大值由表 3.6 给出，D 由表 3.7 给出。

表 3.6 时钟频率变换因子 F

F1	0000	0001	0010	0011	0100	0101	0110	0111
F	内部时钟	372	558	744	1116	1488	2232	RFU
f_s(最大)		5	6	8	12	16	20	—
F1	1000	1001	1010	1011	1100	1101	1110	1111
F	RFU	512	768	1024	1536	2048	RFU	RFU
f_s(最大)	—	5	7.5	10	15	20	—	

RFU 保留将来使用。

f_s 的单位为 MHz。

表 3.7 比特率调整因子 D

D1	0000	0001	0010	0011	0100	0101	0110	0111
D	RFU	1	2	4	8	16	RFU	RFU
D1	1000	1001	1010	1011	1100	1101	1110	1111
D	RFU	RFU	1/2	1/4	1/8	1/6	1/32	1/64

RFU 保留将来使用。

表中的 F1 和 D1 分别由 TA_1 的 b_8—b_5 和 b_4—b_1 给出。

最大编程电流因子 I 和编程电压因子 P 定义了 V_{PP} 的工作状态，I 的值由表 3.8 给出。

最大编程电流：I_{PP}=I mA

最大编程电压：V_{PP}=PV

表 3.8 最大编程电流因子 I

I1	00	01	10	11
I	25	50	100	RFU

表中的 I1 由 TB_1 的 b_7 和 b_6 给出。PI1 由 TB_1 的 b_5—b_1 给出，TB_1 的 $b_8=0$。

PI1 的值的范围为 5—25，由它给出电压 P(单位为伏)，即相应的编程电压为 5V—25V。PI1=0 表示 V_{PP} 不连接到卡，而从 V_{CC} 直接生成内部编程电压，PI1 的其他值保留给今后使用。

PI2 由 TB_2 的 b_8—b_1 给出，当存在 PI2 时，PI1 被忽略，PI2 的值的范围为 50—250，由它给出电压 P(单位为 0.1V)，PI2 的其他值保留给将来使用。

(2) 额外保护时间 N：N 指出额外保护时间 0—254 周期，两个字符上升沿之间的间隔=(12+N)周期，当 N=255 时，表示两个相邻字符的上升沿之间的间隔为 11 个时钟周期，减至最小。N 由 TC_1 的 b_8—b_1 给出。

这些参数的默认值：F=372，D=1，I=50，P=5，N=0。

3.3.5 同步传输的复位应答(Answer To Reset)

1. 时钟频率和 I/O 线上的比特率

I/O 线上的比特率和接口设备提供的 CLK 时钟频率有线性关系。复位过程的时钟频率可在 7KHz 至 50KHz 之间任意选取。时钟频率 7KHz 相当于波特率 7Kbit/s。

2. 复位应答标头结构

复位操作将得到卡的应答，此应答包含一个从卡发送到接口设备的标头，标头的长度固定为 32 位，并由两个 8 位字段 H_1 和 H_2 开始。

信息比特率的传输时间顺序对应于 b_1—b_{32}，且最低有效位(b_1)先传送。

3. 标头的时序

复位过程之后(见 3.3.3 节和图 3.3)，时钟脉冲控制输出信息，在 RST 下降沿后的 10μs 至 100μs(t_{14})产生第一个时钟脉冲，从卡中读取数据位，时钟脉冲的 H 状态在 10μs—50μs(t_{15})之间，时钟脉冲的 L 状态可在 10μs—100μs(t_{16})之间。

当时钟处于低电平且在 RST 下降沿之后至少 10μs(t_{13})内有效，在 I/O 线上得到第一个数据位。以后的数据位至少在 CLK 下降沿之后 10μs(t_1)内有效，每个数据位在下一个时钟脉冲下降沿之前均有效，因此数据位可在时钟脉冲的上升沿被采样。

4. 标头的数据内容

应答标头能迅速确定卡与接口设备是否兼容，如不兼容，触点被释放。

第 1 字段 H_1 指出协议类型，当编码值在'01'—'FE'范围内时，每个值表示一种协议类型(其值由 ISO/IEC JTC1/SC17 分配)。'00'和'FF'不用。

第 2 字段 H_2 是 H_1 给出的协议类型的参数，其值也由 ISO/IEC JTC1/SC17 分配，其余字段的说明不在 ISO/IEC 7816-3 范围之内，其作用应与前述的历史字符作用类似。

3.3.6 协议类型选择 PTS(Protocol Type Selection)

在复位应答之后，允许接口设备向卡发送命令，该命令头由标以 CLA、INS、P1、P2、P3 的 5 个连续字节组成。其中 CLA 为指令类别，当 CLA='FF'时，表示接口设备提出 PTS 请求，其作用是为以后的数据传送选择协议类型。当 CLA 为其他值时将在 3.3.7 节

和第 4 章中描述。

只有接口设备允许发出 PTS 请求，其过程如下：

——接口设备向卡发送 PTS 请求。

——若卡收到正确的 PTS 请求，则发出 PTS 确认信号来应答，否则将超出初始等待时间。

——若成功地交换 PTS 请求和 PTS 应答，这就选择好了新的协议类型和(或)传送参数，然后按规定将数据从接口设备送到卡中。

——若卡收到错误的 PTS 请求，则不发回 PTS 确认信号。

——若初始等待时间超时，接口设备将卡复位或予以拒绝。

——若接口设备收到错误的 PTS 确认信号，将卡复位或予以拒绝。

PTS 请求和 PTS 确认信号的组成：

PTS 请求和 PTS 确认信号都是由初始字符 PTSS(代码为 FF)、格式字符 PTS0，后跟三个任选字符 PTS1、PTS2、PTS3 以及最后一个校验字符 PCK 组成。

PTS0 的作用与 TD 相似，其中 b_5 b_6 b_7 分别表示任送字符 PTS1、PTS2 和 PTS3 是否存在。b_1—b_4 选择协议类型，b_8 留作今后使用。PTS1 给出 F1 和 D 的参数值，PTS2 给出 N 值，PTS3 的使用正在制定。

PTK 的值是使从 PTSS 到 PCK 的所有字符的异或结果为零的值。

3.3.7 异步半双工字符传输协议(T=0)

下面讨论由接口设备向卡发送的命令结构及其处理过程。

本协议所用的参数都是在复位应答时所指定的，除非被协议类型选择(PTS)所修改，此时由 PTS 指定参数。

在复位应答信号中，接口字符 TC_2(b_8—b_1)表示出整数值 W1。由卡发送的字符的起始位上升沿与前一个字符的起始位上升沿(由卡发送或接口设备发送)之间的时间间隔不超过 960×D×W1 个工作时间单元，这个最大值称为工作等待时间。W1 的默认值为 10。

命令总是由接口设备发出的，在一个 5 字节头中告诉卡要做些什么。

在卡和接口设备发送期间，字符的检错和重发如图 3.9 所示。

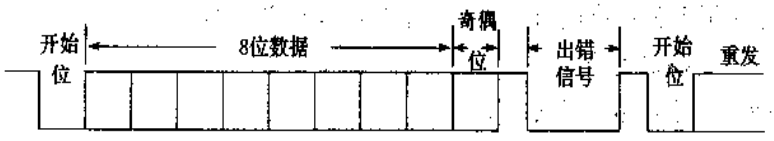


图 3.9 字节传送(出错重发)

1. 接口设备发送的命令头

由 CLA、INS、P1、P2、P3 5 个连续字节组成。

——CLA 是指令类别，其值为'FF'时被指定为 PTS(协议类型选择)。

——INS 是指令码，当其最低有效位为 0，且有效的高半字节不是'6'或'9'时，指令码才有效。

——P1,P2 为参数。

——P3 编码数据字节(D_1…D_n)的数量 n,在命令执行期间传送这些数据字节,数据的传送方向包含在指令码中(由指令的功能决定)。在输出数据传送指令中,P3=0,从卡输出 256 个字节,在输入数据传送指令中,P3=0,不传送数据。

在这 5 个字节传送后,接口设备等待卡的应答。

2. 由卡发送的应答字节

有三种应答,分别指出接口设备完成的不同操作,见表 3.9。

表 3.9 三种应答字节

字节	值	结 果
ACK	INS	V_{PP}空闲。所有其余的数据字节相继被传送。
	INS+1	V_{PP}激活。所有其余的数据字节相继被传送。
	$\overline{INS}$	V_{PP}空闲。下一个数据字节随后被传送。
	$\overline{INS+1}$	V_{PP}激活。下一个数据字节随后被传送。
NULL	'60'	V_{PP}上没有进一步激活。接口设备等待程序字节。
SW1	SW1	V_{PP}空闲。接口设备等待 SW2 字节。

——确认字节 ACK(ACKnowledge byte),用于控制 V_{PP}状态和数据传送。

当 ACK 字节中 7 位高有效位全部等于或互补于 INS 字节中的相应位(除了"6×"和"9×"外)时,允许数据传送。当 ACK 字节和 INS 字节的异或值为 00 或 FF 时,接口设备使 V_{PP}处于空闲状态,当 ACK 字节和 INS 字节的异或值为"01"或"FE"时,接口设备使 V_{PP}处于激活(工作)状态。

——NULL 字节(60) 用于重置工作等待时间,接口设备等待卡发出下一个应答信号。

——状态字节 SW1—SW2(SW1="6×"或"9×",除"60";SW2=任意值),用于表示命令结束。

正常结束时,SW1—SW2="90"-"00"。

当发生与应用无关的错误时,SW1 的高有效半字节为 6:

'6E' 卡不支持这类指令。

'6D' 指令码不被编码或无效。

'6B' 参数是错误的。

'67' 长度不正确。

'6F' 未给出正确的诊断。

其他值 ISO/IEC JTC1/SC17 保留于将来使用。

当 SW1 不是'6E',也不是'6D'时,卡支持该指令。

ISO/IEC 7816-3 中没有解释内容为'9×'的 SW1 字节,也没有解释 SW2 字节,这些字节的含意与应用有关。

3.4 ISO/IEC 7816-3 AMENDENT1 异步半双工分组传输协议(T=1)

在复位应答 TD_1 字节中定义了 T=1,或在 PTS 中定义了 T=1 之后,将按 ISO/IEC 7816-3 A.1 实现协议。在本节中定义了传输控制命令的结构和处理以及对 IC 卡的控制。

分组传输协议的主要特点:

1. 分组是最小的数据单元,它可以在 IC 卡(ICC)与接口设备(IFD)之间传送。

分组的应用数据对传输协议是透明的,传输控制数据中包含了传输错误处理信息。

2. 为了整个分组数据的正确接收,在数据传送之前,可对分组结构的定义进行检查。

3. 分组的标识(组的起始与结束的认可)在数据链路层的字符中处理。

4. 无论在复位应答或协议类型选择 PTS(见 3.3.5 节)之后,都由接口设备 IFD 送出第一组数据来启动协议,以后可交替传送数据块。

本协议使用复位应答时定义的字符帧以及全局接口字节(见 3.3.4 节)定义的物理参数。若以后被 PTS 所修改,则采用 PTS 定义的参数。

本协议是根据 OSI(开放系统互连)参考模型分层原则设计的,分三个层次:

(1) 物理层:数据位的交换参见 3.3.4 节。

(2) 数据链路层:数据交换由字符部分(参见 3.3.4 节字符帧)和分组部分(参见 3.4.1)定义,两相邻字符之间的最小时间间隔为 11 个时间单元。

(3) 应用层:处理命令,每次交换数据至少一个分组或若干个分组。

3.4.1 分组基本组成——分组帧(Block frame)

分组包括三个字段(见图 3.10):开始字段(Prologure field),信息字段(Information field)和结尾字段(Epilogue field)。其中开始字段与结尾字段是必须有的,信息字段则是可选的。

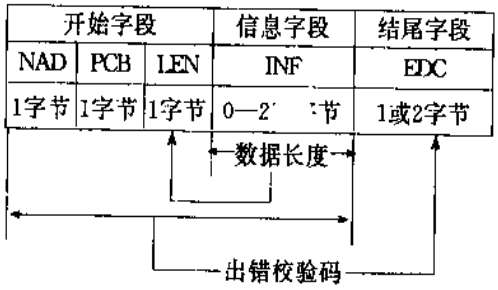


图 3.10 分组结构

1. 开始字段

(1) 结点地址(NAD)(Node ADdress)

b_1—b_3 是源结点地址(SAD),b_5—b_7 是目的结点地址(DAD),b_4 和 b_8 用于 V_{PP} 状态控制。当地址无用时,将 SAD 和 DAD 置"0"。

(2) 协议控制字节 PCB(Protocol Control Byte)

协议定义三种基本分组类型：

① 信息分组(I-block)，用于应用层传送信息。

② 接收准备分组(R-block)，用于传送正向或反向应答，它的信息字段不存在。

③ 管理分组(S-block)，在 IFD 和 ICC 之间交换控制信息，它的信息字段是否存在取决于控制功能。

(3) 长度 LEN (LENgth)：LEN 指出被传送的信息字段的字节数，其代码从“00”到“FE”(0 到 254 字节)。

2. 信息字段 INF(INformation Field)

INF 字段是可选的，当它存在时，可以是应用数据(I-block)或控制和状态信息(S-block)，被传送的字节数据由 LEN 指出。

3. 结尾字段

包含被传送分组的错误校验码 EDC (Error Detection Code)，可以采用纵向冗余校验 LRC(1 字节)或循环冗余校验 CRC(2 字节)。

3.4.2 专用接口参数

1. 信息字段长度

卡和接口设备允许传送的最大信息长度(分别用 IFSC 和 IFSD 表示)由专用接口字符 $TA_i(i>2)$给出，其值在 1 到 254 范围内，默认值为 32。

2. 字符等待时间 CWT

在同一分组内两相邻字符上升沿之间的最大时间称为字符等待时间，由 $TB_i(i>2)$的 b_4 到 b_1 给出字符等待时间整数 CWI，经计算得 CWT：

$$CWT=(2^{CWI}+11)\text{工作单元}$$

所以 CWT 的最小值为 12 工作单元，默认值是 13。

3. 分组等待时间(BWT)

发送到卡的最后一个字符的上升沿与从卡发出的第一个字符之间的最大时间称为分组等待时间。由 $TB_i(i>2)$的 b_8 到 b_5 给出分组等待时间整数 BWI，经计算得 BWT，计算公式如下：

$$BWT=2^{BWT}\times 960\times 372/fs\ s+11\ \text{工作时间单元}$$

(对外部时钟卡)

$$BWT=2^{BWT}/10\ s+11\ \text{工作时间单元}$$

(对内部时钟卡)

在此处，$0\leqslant BWI\leqslant 9$，而 $BWI>9$ 保留于将来使用。BWI 的默认值为 4。

分组等待时间用来检测不作出应答的卡。

4. 检验码的选择

用 $TC_i(i>2)$的 b_1 来选择检验码：

$b_1=1$ 用于 CRC。

$b_1=0$ 用于 LRC(默认值)。

b_2—b_8 置 0，保留于将来使用。

3.4.3 协议操作

1. 数据链路层——字符部分

V_{PP}控制：V_{PP}的状态由卡发送的 NAD 的 b_8 位和 b_4 位控制。

$b_8=0, b_4=0$ V_{PP}处于空闲状态。

$b_8=1, b_4=0$ V_{PP}激活(工作)在接收 PCB 之后回到空闲状态。

$b_8=0, b_4=1$ V_{PP}激活(工作)一直到接口设备接收到另一个 NAD 字节。

$b_8=1, b_4=1$ 禁用

如超时或 NAD 奇偶错，V_{PP}应回到或保持在空闲状态。

2. 数据链路层——分组部分

(1) 操作过程

在复位应答或协议类型选择(PTS)之后的第一个分组是由接口设备 IFD 传送到 IC 卡的，可以是信息分组(I-block)或管理分组(S-block)。

在传送一个分组(I-，R-或 S-block)之后，在下一个分组传送之前，发方应该接收到应答。

信息分组内有一个发送序列号 N(S)，N(S)是一个二进制位(bit)，它的起始值为 0，在传送一个信息分组之后加 1。

接收准备分组(R-block)内有一个 N(R)，它的值等于下一个要传送的 I-block 中的 N(S)。R-block 用于链接。

管理分组(S-block)有请求分组 S(…request)-block 和应答分组 S(…response)-block 两种，在接收到请求分组后发出一个应答分组。

(2) 链接

分组传输协议具有链接功能，允许接口设备 IFD 或 IC 卡(ICC)传送信息的长度大于 IFSD 或 IFSC(见 3.4.2 节)规定的长度。

分组的链接情况受 I-block 中的协议控制字节 PCB 中的 M 位控制。M 位指出 I-block 的两种状态：

M=0，表示当前的 I-block 是链的最后一个分组；

M=1，表示链还跟有后面的分组。

现将 PCB 编码情况介绍如下：

① I-block 的 PCB 字节

由 b_8—b_1 组成。

b_8 位恒为 0，表示是 I-block。

b_7 为发送序列号 N(S)。

b_6 为 M 位，指示后面是否还有分组。

b_5—b_1 保留于将来使用。

② R-block 的 PCB 字节

b_8b_7 为 10，表示是 R-block。

b_5 为 N(R)。

b_6=0，且 b_4—b_1 为 0000　表示正确。

b_6=0，且 b_4—b_1 为 0001　表示奇偶错。

b_6=0，且 b_4—b_1 为 0010　为其他错误

所有其他值保留于将来使用。

③ S-block 的 PCB 字节

b_8 b_7 为 11，表示是 S-block。

b_6 为应答位。若 b_6=0，表示请求(request)；若 b_6=1，表示应答(response)。b_5—b_1 提出是何种请求或何种应答。叙述如下：

- b_5—b_1 为 00000。若 b_6=0，则为“重新同步请求 S(RESYNCH request)”，此请求仅由接口设备 IFD 发送，将分组传输协议的参数复原到初始值；若 b_6=1，则为“重新同步应答 S(RESYNCH response)”，是 IC 卡接收到重新同步请求后发出的应答。
- b_5—b_1 为 00001。若 b_6=0，则为“信息字段长度请求 S(IFS request)”；若 b_6=1，则为“信息字段长度应答 S(IFS response)”。IC 卡发出 S(IFS request)，表示出它能支持的新 IFSC(卡允许的最大信息长度)，接口设备 IFD 发出 S(IFS request)表示出它能支持的新 IFSD(设备允许的最大信息长度)。对方接收到 S(IFS request)后应发出 S(IFS response)作为应答。
- b_5—b_1 为 00010。若 b_6=0，则为“中止请求 S(ABORT request)”；若 b_6=1，则为“中止应答 S(ABORT response)”。
- b_5—b_1 为 0011。若 b_6=0，则为“等待时间扩充请求”；b_6=1，则为“等待时间扩充应答”。IC 卡发此请求表示它需要超过 BWT 时间去处理前面接收到的 I-block。BWT 为分组等待时间，参考 3.4.2 节。

图 3.11 举例说明链接功能。

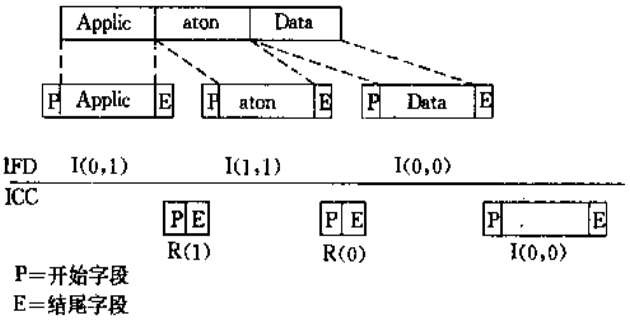


图 3.11　链接功能举例

应用数据 Application Data 由接口设备 IFD 传送到 IC 卡，假设分成三个信息分组，分别为：Applic、ation 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 表示后面是否还有分组需要传送。所以当发送第一个分组时，PCB 给出 I(0,1)，即 PCB 字节的 b_7=N(S)=0，b_6=M=1。IC 卡接收后，给出 R-block，其中包

括 R(N(R)),N(R)为下一个要接收的分组序列号,所以 N(R)=1,即 R(N(R))=R(1)。……。当发送完第三分组时,IC 卡发回信息长度为零的 I-block ,I(0,0)表示传送结束。其操作过程如图 3.12 所示。

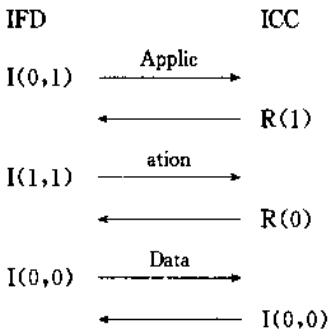


图 3.12 接口设备发送链接 I-block 举例

小 结

根据 7816-3 和 7816-3A.1 IC 卡异步传输协议(T=0 和 T=1)和第 4 章的 7816-4 标准,可得出智能卡的工作流程如图 3.13 所示,从卡插入接口设备开始工作,首先由接口

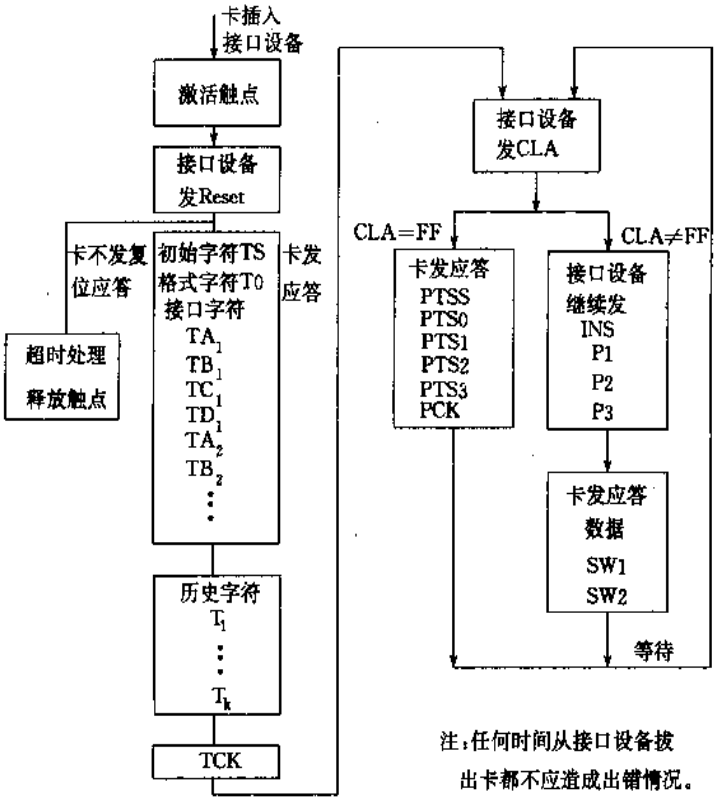


图 3.13 智能卡工作流程

设备向卡发 Reset 信号，然后由卡向设备发应答(称为复位应答)信号：说明卡所使用的传输协议(T=0，T=1 或其他)和一些工作参数，其中历史字节将在 ISO 7816-4 中说明。在复位应答后，首先由接口设备发命令，在 7816-3 协议中规定命令头由 CLA、INS、P1、P2 和 P3 五个字节组成。当 CLA=FF 时，可重新选择协议类型，在其后接口设备所发的命令均按新协议处理；当 CLA≠FF 时，由 INS 字节给出指令(如读指令、写指令、……)。有关内容也在 ISO 7816-4 中定义。另外在 7816-4 中规定命令头 CLA、INS、P1 和 P2 4 个字节是必须有的，而 P3 则由一个数据体构成，某些命令不存在数据体。

卡接收命令后，发应答信号，命令和应答总是成对出现的，称为“命令应答对”。

采用异步传输协议的智能卡芯片一般由 CPU(中央处理单元)、ROM(只读存储器)、RAM(随机存储器)、E^2PROM(电可擦除的只读存储器)等组成。ROM 中存放片内操作系统 COS(Chip Operating System)，接收到接口设备送来的命令后，在操作系统 COS 控制下进行处理，然后将处理结果(即“应答”)送回接口设备，智能卡芯片结构和 COS 将在第六章中论述。

在以后各章将 ISO/IEC 7816-3 和 ISO/IEC 7816-3 A.1 统称为 ISO/IEC 7816-3。

最后还要说明一下，标准本身可能会修改，在第 4 章中讨论的标准在个别地方与本章中讨论的标准有一些矛盾。另外标准制定有一个时间过程，实际应用的卡可能不全部遵守标准的规定，也有的卡是在标准制定之前发行的。因此发生上述情况的可能性是存在的。

思 考 题

1. IC 卡的尺寸与磁卡相同否，IC 卡为何保留磁条？
2. IC 卡上保留有多少个触点？存储器卡、逻辑加密卡与智能卡的触点数据相同否？你知道每个触点的功能吗？
3. 有哪些国际标准是直接对 IC 卡作出规定的？为什么要制定国际标准？
4. 同步卡开始工作时，为什么需要由接口设备送来 Reset 信号？同步卡接收到 Reset 信号后作出什么反应？如此时接口设备不送 Reset 信号，是否还可以采取其他办法？
5. 复位应答信号(Answer To Reset)包含哪些内容？是在哪个国际标准中给出定义的？
6. 目前 IC 卡中常用的异步传输协议是什么？IC 卡加电后首先是由 IC 卡还是接口设备通知对方采用什么传输协议？
7. 复位应答后，接着是由 IC 卡还是接口设备发命令？每个命令后的应答信号是由哪一个发出的？应答信号包括哪些内容？其中什么内容是必须有的？
8. 在异步传输协议中，T=0 协议与 T=1 协议的主要差别是什么？
9. 请说出字符帧的结构，当传送有错时如何表示？
10. 请说出协议传输选择 PTS 的作用。
11. 接口设备发出的命令是否正确，怎样在卡发回的应答信号中反映出来？
12. 在 T=1 的分组传输协议中，每一个分组包括哪些字段？其中哪些是必须有的？哪些是可选的？

第4章　IC卡国际标准(二)

本章描述IC卡国际标准ISO/IEC 7816-4(草案)：1994和ISO/IEC 7816-5：1994。其中ISO/IEC 7816-4描述了行业间交换用命令，将在本章4.1～4.7中介绍；ISO/IEC 7816-5描述了应用标识符的编号系统和注册过程，将在本章4.8中介绍。

4.1　ISO/IEC 7816-4(行业间交换用命令)规定的范围

1. 在接口设备与卡之间传送的命令和应答信息内容。
2. 在复位应答期间由卡发送的历史字节内容。
3. 当处理交换用行业间命令时，在接口见到的文件结构和数据。
4. 在卡中的文件和数据的访问方法。
5. 定义在卡中的文件和数据访问权限的安全结构。
6. 关于安全信息。
7. 对由卡处理的算法的访问方法，但不描述这些算法。

4.2　数据结构

本节包含信息：在接口处见到的数据的逻辑结构。

4.2.1　文件组织

三种文件：主文件MF(Master File)，专用文件DF(Dedicated File)，基本文件EF(Elementary File)。

图4.1示出了这三种文件的关系，MF(第一级)为根文件，是必须有的，DF(第2，3，……级)是可选的。

定义了两种基本文件：

1. 内部基本文件：存放的数据由卡进行解释，即为了达到管理和控制的目的，由卡来分析和使用这些数据。

2. 工作基本文件：卡不能对文件中的数据进行解释，而是由外界来使用这些数据。

基本文件的结构：图4.2示出4种基本文件结构。

(1) 透明结构：从接口看到的文件是一个数据单元序列。

(2) 具有固定长度记录的线性文件。

(3) 具有可变长度记录的线性文件。

(4) 具有固定长度记录的环形文件。

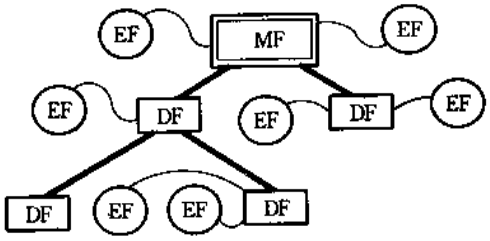


图 4.1 逻辑文件组织

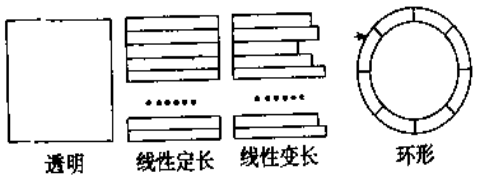


图 4.2 基本文件结构

4.2.2 数据访问(存取)方式

1. 文件访问方式

当一个文件不能被默认(隐式)选择时,至少可采用下述方法之一进行选择:

(1) 利用文件标识符(identifier)进行访问:每一文件中有两字节长的标识符,MF 的标识符=3F00,允许不同文件具有相同的标识符,但为了避免选择文件时可能出现的二义性,要求直接处于给定 DF 下的所有 EF 和 DF 应具有不同的文件标识符。

(2) 依靠路径进行访问:路径 Path(文件标识符的链接)从 MF 或者当前的 DF 的标识符开始,而以被选文件的标识符结束,在这两个标识符之间可能有一串 DF(如有的话)标识符,其方向由"父"指向"子"。如果不知道当前 DF 的标识符,可以用"3FFF"数值作为路径的开始。

(3) 利用短 EF 标识符进行访问:短 EF 标识符有 5 位代码(其值在 1—30 之间),短 EF 标识符不能用在路径中或作为文件标识符,例如不能用在选择文件命令(Select File Command)中。

(4) 用 DF 名字进行访问:DF 名字的长度为 1 到 16 字节,为避免选择的二义性,在一张卡中的每一个 DF 名字应是唯一的。

2. 数据访问方式

数据可以作为记录、数据单元或数据对象(data object)访问。在记录结构的 EF 中,数据可考虑为存储在一顺序记录串中,在透明结构的 EF 中,数据可考虑为一顺序数据单元串。

数据访问方式、记录编号方法和数据单元长度可以在 ATR(复位应答)、ATR 文件和任一文件控制信息中给出指示。对一个给定的 EF 文件而言,如在多处给出指示,那么,从 MF 到这一 EF 的路径中,最靠近它的文件中给出的信息是有效的。

(1) 访问记录:在记录结构的 EF 中,可以用记录标识符或记录编号来访问,记录标识符和记录编号是一个无符号的 8 位整数,其可用值从 01 到 FE,00 保留于专用,FF 保留于将来使用。

记录标识符是由应用提供的,假如在信息的数据字段中,记录是一个"Simple-TLV 数据对象"(Simple-TLV data object),那么数据对象的第一个字节即为记录标识符。

在一个 EF 中,每一个记录的记录编号是唯一的,且是顺序安排的。

(2) 访问"数据对象":按数据对象的头(即标志 Tag)进行访问。

在 ISO/IEC 7816-4 协议中支持两种数据对象，它们是：

① BER-TLV 数据对象

BER 是 Basic Encoding Rules 的缩写。TLV 是 Tag(标志)、Length(长度)和 Value(值)三个字的第一个字母。在这里介绍的 BER-TLV 对象是 ASN.1 的基本编码规则在本协议中的应用。ANS.1 对象在 ISO/IEC8824 中定义，其编码在 ISO/IEC8825 中描述。

BER-TLV 数据对象包括 2 个或 3 个字段，其中 T 字段由 1 个或几个字节组成，L 字段由 1 个或几个字节组成，假如 L 字段不空，则 V 字段的长度为 L 个字节，若 L 字段为空，则无 V 字段。

下面分别介绍各个字段：

· T 字段

T 字段的第一个字节是数据对象标志的级别(class)、类型(type)和编号(number)。

其中 b_8-b_7 表示标志级别，如果：

$b_8-b_7=00$，为通用级；

$b_8-b_7=01$，为应用级；

$b_8-b_7=10$，为上下文一特定级；

$b_8-b_7=11$，为私用级。

b_6 表示标志类型，如果：

$b_6=0$，为原型数据对象；

$b_6=1$，为结构数据对象。

b_5-b_1 的意义与标志的长度有关，如长度为 1 个字节，b_5-b_1 为标志的编号，且不能为全"1"；如长度大于 1 个字节，则 b_5-b_1 为全"1"，下一字节的 b_8 位为 1(如再下一字节仍为编号)，b_7-b_1 为编号，而最后一个编号字节的 b_8 位为 0。

· L 字段

当 L 字段为单字节时，$b_8=0$，b_7-b_1 的数据是 V 字段的字节数。当 L 字段为多字节时，$b_8=1$，b_7-b_1 的数值表示本字段后跟的字节数，在这些字节中的数值才表示 V 字段的字节数。

· V 字段

某些原型 BER-TLV 数据对象的 V 字段由 0 个，1 个或多个 simple-TLV 数据对象组成。其余的由 0 个、1 个或多个数据项组成。

结构数据对象的 V 字段由 0 个、1 个或多个 BER-TLV 数据对象组成。

② Simple-TLV 数据对象：由 2 个或 3 个字段组成。

T 字段为单字节，其值从 1 到 254，例如用作记录标识符。

L 字段由 1 个字节或 3 个字节组成。如 L 字段的第 1 个字节的内容从 00 到 FE，则表示 L 字段由 1 个字节组成；如为 FF，则表示第 2，3 两个字节示出 L 的值，即 L 字段由 3 个字节组成。

如 L 字段为空，则不存在 V 字段。

(3) 访问数据单元

在透明结构的 EF 文件中，每一个数据单元的位置由命令(command)的偏移值给出，

其下一个数据单元的位置由偏移值加1后产生。如IC卡没有给出数据单元长度，则默认其长度为1个字节。

4.2.3 文件控制信息(FCI)

文件控制信息(FCI)为数据字节串，在选择文件命令(Select File Command)的应答信息中有用。任一文件都可含有文件控制信息。

当按BER-TLV数据对象编码时，文件控制信息有三种传送模式如表4.1所示。

表4.1 文件控制信息三种模式

标志T	数值V
62	文件控制参数(FCP)
64	文件管理数据(FMD)
6F	文件控制信息(FCI)

FCP(File Control Parameter)模式：传送文件控制参数，也就是在表4.2中定义的任一BER-TLV数据对象。

表4.2 文件控制参数FCP

标志T	长度L	数值V	适用于
80	2	文件中数据字节数，包括结构信息	透明EF文件
81	2	文件中数据字节数，包括结构信息(如有)	任意文件
82	1	文件描述字节(表4.3)	任意文件
	2	文件描述字节，后接数据编码字节(表4.75)	任意文件
	3或4	文件描述字节，后接数据编码字节和最大记录长度	记录结构的EF文件
83	2	文件标识符	任意文件
84	1 16	DF文件名	DF文件
85	可变	专有信息	任意文件
86	可变	安全属性(不属于ISO/IEC 7816-4范围)	任意文件
87	2	包含FCI扩展部分的EF文件的标识符	任意文件
88到9E		保留于将来使用	
9FXY		保留于将来使用	

FMD(File Management Data)模式：传送文件管理数据，也就是在本协议、ISO/IEC 7816-5或ISO/IEC 7816-6中指定的BER-TLV数据对象。

FCI(File Control Information)模式：传送FCP和FMD。以上三种模式可根据Select File Command中的选择任选项而得到(表4.45)。

表4.2中涉及的文件描述字节的含意参见表4.3。

表 4.3 文件描述字节

b_8	b_7	b_6	b_5	b_4	b_3	b_2	b_1	意 义
0	×	—	—	—	—	—	—	文件访问能力
0	0	—	—	—	—		—	—非共享*文件
0	1	—	—	—	—	—	—	—共享文件
0	—	×	×	×	—	—		文件类型
0	—	0	0	0	—		—	—工作 EF
0	—	0	0	1	—			—内部 EF
0	—	0	1	0	—	—	—	保留
0	—	0	1	1	—	—	—	用于
0	—	1	0	0	—	—	—	专有的
0	—	1	0	1	—	—	—	EF
0	—	1	1	0	—	—	—	类型
0	—	1	1	1	—	—	—	—DF
0	—	—	—	—	×	×	×	EF 文件结构
0	—			—	0	0	0	不给出信息
0	—		—	—	0	0	0	透明
0	—		—	—	0	1	0	线性固定，无其他信息
0	—	—		—	0	1	1	—线性固定，Simple-TLV
0	—	—		—	1	0	0	线性可变，无其他信息
0	—	—	—	—	1	0	1	线性可变，Simple-TLV
0	—	—	—	—	1	1	0	—环形，无其他信息
0	—	—		—	1	1	1	环形，Simple-TLV
1	×	×	×	×	×	×	×	保留于将来使用

*共享是指该文件至少支持不同逻辑通道的并发访问

4.3 卡的安全结构

本节描述以下特点：安全状态，安全属性，安全机制。

在执行命令和/或访问文件时，安全状态要与安全属性进行比较。

4.3.1 安全状态

安全状态表明完成下列操作后的当前状态：

(1) 复位应答(ATR)或协议类型选择(PTS)。

(2) 完成认证过程的一条命令或一串命令。

安全状态也可以是由于安全过程的完成而得到的结果，该过程涉及到实体的识别。例如：

(3) 通过通行字 password 认证(例如使用检验命令 Verify Command)。

(4) 通过密钥认证(例如使用一条取口令命令 Get Challenge Command，后跟一条外部鉴别命令 External Authenticate Command)。

(5) 通过安全信息 Secure messaging(例如信息鉴别)。

考虑了三种安全状态:

① 全局安全状态:可以在完成与 MF 有关的认证过程时进行修改(例如通过属于 MF 的通行字或密钥的实体鉴别)

② 特定文件安全状态:可以在完成与专用文件 DF 有关的鉴别过程时进行修改。

③ 特定命令安全状态:仅当执行一条使用安全信息并涉及鉴别的命令时才存在。

4.3.2 安全属性

安全属性定义了允许执行的操作,以及完成这些操作的过程。

每一文件有与其相联系的安全属性,应满足一定的安全条件,才允许对文件进行操作。文件的安全属性依赖于:

①文件的种类(DF 或 EF);

②在文件中和/或它们父文件中的控制信息的可选参数。

4.3.3 安全机制

本协议部分提供以下安全机制:

1. 通行字鉴别:外部输入通行字,与卡内的秘密数据进行比较,这一机制用以保护用户利益。

2. 密钥鉴别:例如使用 Get Challenge Command 后跟 External Authenticate Command。

3. 数据鉴别:卡使用秘密的或公开的内部数据,检查从外界接收的冗余数据。或者卡使用内部的秘密数据计算出一项信息(密码检验和/或数字签名),并将它插入数据中送到外界。这一机制可用来保护"提供者"权利。有关"数字签名"请参考本书第五章。有关"提供者"请参考 ISO/IEC 7816-5。

4. 数据加密:卡使用秘密的内部数据,对接收在数据段中的密码解密。或者,使用秘密的或公开的内部数据,计算出一个密码,有可能还有其他数据,插入数据段中。这一机制提供保密服务,可减少消息泄漏。

鉴别的结果可根据应用的要求登录在内部基本文件(EF)中。

4.4 应用协议数据单元(APDU)的信息结构

应用协议中的操作步包括以下操作:发送一个命令(command),在接收此命令的实体中进行处理,并送回一个应答(response)。因此一个特定的命令有一个特定的应答,视为"命令—应答对"。

命令信息或应答信息,分别从接口设备送到卡或从卡传送到接口设备。

命令信息和应答信息可以包含数据,也可以不包含数据,因此有 4 种情况如下:

情况 1:无命令数据,无应答数据。

情况 2:无命令数据,有应答数据。

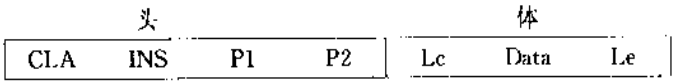
情况 3：有命令数据，无应答数据。

情况 4：有命令数据，有应答数据。

4.4.1 命令 APDU

1. 命令 APDU

命令 APDU 包括一个必备的 4 字节头和一个可选的可变长度的体如下：



头为命令的编码，Lc 为体内数据(data)长度，Data 为发送的数据。Le 是期望中的应答 APDU 数据字段的最大字节数。当 Le＝0 时，表示请求送回最大应答数据字节数，如 Le 为 1 字节长度，则最大数据字节数为 256。图 4.3 示出命令 APDU 的 4 种结构。

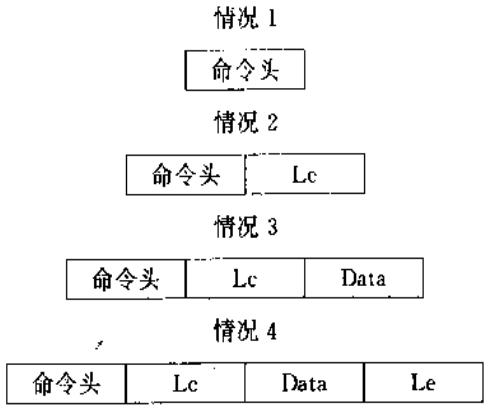


图 4.3 命令 APDU 的 4 种结构

情况 1 表示 Lc、Data 和 Le 均为空。

情况 2 表示 Lc 和 Data 为空，Le 不为空，体内仅有 Le 字段。

情况 3 表示 Lc 和 Data 不为空，Le 为空，因此体内有 Lc 和 Data 字段。

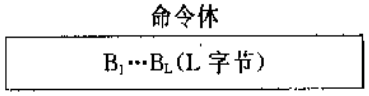
情况 4 表示 Lc、Data 和 Le 均存在，体内 Lc 后跟着 Data 和 Le。

其中 Lc 和 Le 有短型(S)和扩展型(E)两种情况，其长度分别为 1 个字节和 3 个字节。

2. 命令体的编码

上述情况 1，命令体为空。

情况 2、3 和 4，命令 APDU 的体包括 B_1 到 B_L 共 L 字节如下所示：



在表 4.4 中列出命令 APDU 的体长度 L。

表 4.4 命令 APDU 的体长度

情况	长度	条件
1	L=0	
短 2(2S)	L=1	
短 3(3S)	L=1+(B_1)	(B_1)≠0
短 4(4S)	L=2+(B_1)	(B_1)≠0
扩展 2(2E)	L=3	(B_1)=0
扩展 3(3E)	L=3+(B_2 ‖ B_3)	(B_1)=0;(B_2 ‖ B_3)≠0
扩展 4(4E)	L=5+(B_2 ‖ B_3)	(B_1)=0;(B_2 ‖ B_3)≠0

表中(B_1)表示 B_1 字节的内容,B_2 ‖ B_3 表示将 B_2B_3 拼接起来,所以(B_1)表示的字节长度为 1—256,(B_2 ‖ B_3)表示的字节长度为 1—65536。

4.4.2 应答 APDU

应答 APDU 由可变长度的体(可选的)和 2 字节尾部(必备的)组成如下:

体	尾
数据 Data	SW1 SW2

其中体的字节数由命令 APDU 的 Le 指出。Data 是接收设备(如 IC 卡)接收命令 APDU 并进行处理后送回发送设备(如接口设备)的数据。尾部 SW1 和 SW2 为状态代码。如命令夭折,则由 SW1 和 SW2 指明错误情况。

4.4.3 命令头部、数据字段和应答尾部的代码约定

表 4.5 给出命令 APDU 的内容。

表 4.5 命令 APDU 内容

代码	名字	长度	说明
CLA	类别	1	指令类别
INS	指令	1	指令代码
P1	参数 1	1	指令参数 1
P2	参数 2	1	指令参数 2
Lc	长度	1 或 3	在命令的数据字段中存在的字节数
Data	数据	可变长度=Lc	发送的字节串
Le	长度	1 或 3	期望应答送回的最大字节数

1. 类别字节 CLA(CLAss byte)

表 4.6 给出 CLA 的编码与意义,表 4.7 补充说明安全信息的格式和逻辑通道编号。

表 4.6 CLA 的编码和意义

代码	意　　义
0×	命令与应答的结构与编码，由本协议给定，×的编码见表 4.7
10　7F	保留于将来使用
8×，9×	命令与应答的结构，由本协议给定，命令与应答的编码和意义是专有的，×的编码见表 4.7
A×	除了由应用上下文指定的以外，命令与应答的结构与编码由本协议给定，×的编码见表 4.7
B0—CF	命令与应答的结构由本协议给定
D0　FE	命令与应答有专有结构与编码
FF	保留给 PTS

表 4.7 当 CLA＝0×、8×、9×或 A×时，×的编码与意义

b_4	b_3	b_2	b_1	意　义
×	×	—	—	安全信息 SM(Secure messaging)格式
0	×	—	—	无 SM 或专有的 SM 格式
0	0	—	—	无 SM
0	1	—	—	专有 SM 格式
1	×	—	—	安全信息按本协议解释
1	0	—	—	命令头不鉴别
1	1	—	—	命令头鉴别
—	—	×	×	逻辑通道编号

表 4.7 中的安全信息 SM 和逻辑通道编号的解释如下：

• 安全信息 SM(Secure messaging)

设置安全信息的目的是保护出入卡中部分信息的安全，它采用了两种安全措施：数据鉴别和数据保密。

安全信息依靠一种或多种安全机制达到上述目的。每一个安全机制涉及算法、密钥、论证，经常还包括初始化数据。

本处定义了 3 种与 SM 有关的数据对象(data object)类型：

(1) Plain value 数据对象

表 4.8 给出 Plain value 数据对象。

表 4.8 Plain value 数据对象

标志 Tag	数值(Plain value 组成)
B0，B1	BER-TLV，包括有关 SM 的数据对象
B2，B3	BER-TLV，不是有关 SM 的数据对象
80，81	不是 BER-TLV 编码数据

表中 BER 为遵循 ASN.1 的基本编码规则(Basic Encoding Rule),见本章 4.2 节。

(2) 安全机制数据对象:指的是该对象携带安全机制的计算结果。

(3) 辅助的安全数据对象:指的是该对象携带控制参数和应答描述符。

在数据字段中,当前的 SM 格式可用两种方法选择:

(1) 隐含的或固有的:例如由其前面的命令确定,即在发本命令前已确定。

(2) 显式的:即由本条命令的类别字节 CLA(见表 4.7)确定。

下面简单列出几种用于鉴别的数据对象:

(1) 密码检验和(checksum)数据对象。

(2) 数字签名数据对象。

(3) 用于保密的数据对象。

(4) 辅助的安全数据对象。

· 逻辑通道编号

在接口处见到的逻辑通道,其工作如同连到 DF 文件的逻辑链路。

各逻辑通道的动作是互相独立的,但可共享与应用有关的安全状态,因此与安全有关的命令可跨越逻辑通道(例如通道字验证)。

指定给某一逻辑通道的命令可通过 CLA 字节中的逻辑通道编号实现(见表 4.6 和表 4.7)。逻辑通道的编号从 0 到 3。卡支持的有效的逻辑通道最大编号在卡的历史字节中给出(见本章 4.6 节)。

接收一个命令以及发回相应的应答只能在一个逻辑通道内进行,当一个逻辑通道被打开时,它将一直保持打开,直到有一条管理通道命令(Manage Channel Command)将它关闭为止。

1 个以上逻辑通道可以被同一个 DF 文件所打开。1 个以上逻辑通道可以选择同一个 EF 文件。在任一逻辑通道上的选择文件命令(Select File Command)可以打开一个当前的 DF 文件,还可能打开一个当前的 EF 文件,因此每一个逻辑通道有一个当前 DF 文件,还可能有一个当前的 EF 文件。

基本逻辑通道的编号为 0,它总是有效的。

2. 指令字节 INS

表 4.9 列出在 ISO/IEC 7816-4 中定义的指令编码。

表 4.9 ISO/IEC 7816-4 中定义的指令

INS 编码	命令名	
0E	擦除二进制	Erase Binary
20	验证	Verify
70	管理通道	Manage Channel
82	外部鉴别	External Authenticate
84	取口令	Get Challence
88	内部鉴别	Internal Authenticate
A4	选择文件	Select File
B0	读二进制	Read Binary

续表

INS 编码	命令名	
B2	读记录	Read Record
C0	取应答	Get Response
C2	信封	Envelope
CA	取数据	Get Data
D0	写二进制	Write Binary
D2	写记录	Write Record
D6	修改二进制	Update Binary
DA	存数据	Put Data
DC	修改记录	Update Record
E2	增加记录	Append Record

从表中可见指令码均为偶数。在 ISO/IEC 7816-3 中指出，指令码为 6×或 9×的指令是无效的。

3. 参数字节 P1、P2

P1、P2 可为任意值，如不用该参数则将它置成“00”。

4. 数据字段字节

前已作说明，不再重复。

5. 应答状态字节 SW1－SW2

SW1－SW2 是在卡接收到命令并经过处理后送出的应答信号，指出卡的处理状况如图 4.4 所示。

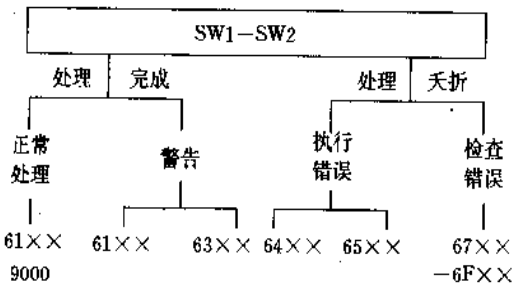


图 4.4 状态字节的结构图

当 SW1＝63 或 65 时，表示非易失性存储器的状态已变；当 SW1＝6×但不是 63 或 65 时，表示非易失性存储器的状态没变。

表 4.10 列出 SW1—SW2 的编码，在以后介绍各条指令时，将提供更详细的情况。

表 4.10 SW1－SW2 的编码

SW1-SW2	意　义
	正常处理
9000	正常
61××	SW2 指出仍可得到的应答字节数
	警告
62××	非易失性存储器状态未变(SW2 的意义见表 4.11)
63××	非易失性存储器状态改变(SW2 的意义见表 4.12)
	执行错误
64××	非易失性存储器状态未变(SW2＝00，其他值保留)
65××	非易失性存储器状态改变(SW2 的意义见表 4.13)
66××	保留给发布与安全有关的问题，待定义

续表

SW1-SW2	意　义
	检验错误
6700	长度错误
68××	不支持 CLA 的功能(SW2 的意义见表 4.14)
69××	不允许的命令(SW2 的决义见表 4.15)
6A××	P1、P2 参数错误(SW2 的意义见表 4.16)
6B00	P1、P2 参数错误
6C××	Lc 长度错误(SW2 指出适当的长度)
6D00	指令码错误
6E00	类型(class)不支持
6F00	诊断不精确

表 4.11～4.16 分别说明当 SW1 为 62、63、65、68、69 和 6A 时 SW2 的编码及其意义。

表 4.11　SW1=62 时,SW2 的编码

SW2	意　义
00	不给出信息
81	部分返回数据可能是错的
82	在达到 Le 字节之前,文件/记录已结束
83	选择文件无效
84	FCI(文件控制信息)格式不遵循本标准

表 4.12　SW1=63 时,SW2 的编码

SW2	意　义
00	不给出信息
81	上次写入时,文件已充满
C×	×提供计数值(0—15)

表 4.13　SW1=65 时,SW2 的编码

SW2	意　义
00	不给出信息
81	存储器失效

表 4.14　SW1=68 时,SW2 的编码

SW2	意　义
00	不给出信息
81	不支持的逻辑通道
82	不支持的安全信息

表 4.15　SW1=69 时,SW2 的编码

SW2	意　义
00	不给出信息
81	命令与文件组织不适配
82	安全状态不满足
83	鉴别方法封锁
84	参考数据无效
85	不满足使用条件
86	不允许的命令(无当前的 EF)
87	期望的 SM(安全信息)数据对象未得到
88	SM 数据对象不正确

表 4.16　SW1=6A 时,SW2 的编码

SW2	意　义
00	不给出信息
80	在数据字段中的不正确参数
81	功能不支持
82	没有找到文件
83	没有找到记录
84	文件中没有足够的空间
85	Lc 与 TLV 结构不一致
86	P1、P2 参数不正确
87	Lc 与 P1、P2 不一致
88	没有找到参照数据

4.5　基本行业间命令

这里所介绍的命令是在接口设备与 IC 卡之间传送的,IC 卡执行异步传输协议(T=0 或 T=1)。IC 卡接收到命令后,由片内的操作系统 COS(Chip Operating System)分析命令,并由卡内的中央处理部件 CPU 具体执行,所以这里所讲的命令与 CPU 的指令是有重大区别的。一个命令的功能由若干条指令完成。

在 ISO/IEC 7816-4 中描述的命令并不要求所有卡都必须采用。当进行国际交流时要用到的卡的系统服务和有关的命令将在 4.7 节中定义。

下面将分别介绍各条命令(参见表 4.9 和表 4.10)。

1. 读二进制命令(Read Binary Command)

功能:读出(部分)基本文件(EF)内容

使用条件与安全:当命令包含一个有效的短 EF 标识符时,则将此文件作为当前 EF。本命令对当前 EF 进行处理。仅当安全状态与此 EF 中定义的安全属性(读功能)相适合时才能执行本命令。如本命令对记录结构的 EF 进行操作,将被中止。

命令信息与应答信息如表 4.17 和表 4.18 所示。

表 4.17 读二进制(Read Binary)命令 APDU

CLA	见表 4.6 和 4.7
INS	B0
P1-P2	见文中解释
Lc	空
Data	空
Le	期望读出的字节数

表 4.18 读二进制(Read Binary)应答 APDU

数据字段	读出数据(Le 字节)
SW1-SW2	状态字节

在表 4.17 中，如 P1 的 $b_8=1$，则 b_7 和 b_6 置于 0，b_5—b_1 为一个短 EF 标识符，P2 是将要读出的第一个字节的偏移值(从文件开始处算起)。

在表 4.17 中，如 P1 的 $b_8=0$，则 P1—P2 是将要读出的第一个字节的偏移值(从文件开始处算起)。

如表 4.17 中的 Le=0，则最多读出 256 字节(短长度)或 65536 字节(扩展长度)。其状态字节如下：

警告条件：SW1=62，且 SW2=

- 81 部分返回数据可能是错的；
- 82 在读出 Le 字节之前，文件已结束。

出错条件：

(1) SW1=67，且 SW2=

- 00 长度错误(错误 Le 域)

(2) SW1=69，且 SW2=

- 81 命令与文件组织不适配；
- 82 安全状态不满足；
- 86 命令不允许(没有当前 EF)。

(3) SW1=6A，且 SW2=

- 81 功能不支持；
- 82 没有找到文件。

(4) SW1=6B，且 SW2=

- 00 参数错误(偏移值超出 EF)。

(5) SW1=6C，且 SW2=

- ×× 长度错误(Le 有错，××指示合适的长度)。

2. 写二进制命令(Write Binary Command)

功能：将二进制数据写入基本文件(EF)。

根据文件属性，本命令完成下述操作之一：

- 命令 APDU 中的数据与已存在于文件中的数据进行逻辑或 Logical OR(文件的位逻辑擦除状态为 0)。
- 命令 APDU 中的数据与已存在于文件中的数据进行逻辑乘 Logical AND(文件的

位逻辑擦除状态为 1)。

• 命令 APDU 中给出的数据一次性写入卡中。

当数据编码字节(见表 4.76)没有给出指示时,按逻辑或操作。

使用条件与安全:当命令包含一个有效的 EF 标识符时,则将此文件作为当前 EF。本命令对当前 EF 进行处理。仅当安全状态与 EF 中定义安全属性(写功能)相适合时才能执行本命令。

如果此命令对非透明 EF 进行操作,将被中止。

命令信息和应答信息如表 4.19 和表 4.20 所示。

表 4.19 写二进制(Write Binary)命令 APDU

CLA	见表 4.6 和 4.7
INS	D0
P1—P2	与"读二进制命令"类似
Lc	数据长度
Data	被写入的数据单元串
Le	空

表 4.20 写二进制(Write Binary)应答 APDU

数据字段	空
SW1-SW2	状态字节

对表 4.19 中的 P1—P2(与"读二进制命令"类似)解释如下:

"读二进制命令"中讲到的 P1—P2 内容,在这里都适用,但必须将其中的"读出"两字改为"写入"。在本节后面部分讲到的"与×××……类似"也表达同样的意见,不再一一说明。

表 4.20 中的状态字节描述如下:

警告条件:SW1=63 且 SW2=

• C× 计数器(写成功,但在执行内部重试程序之后。×≠0 表示重试次数;×=0 表示不提供计数器)。

出错条件:

(1) SW1=65,且 SW2=

• 81 存储器失效(写失败)。

(2) SW1=67,且 SW2=

• 00 错误长度(Lc 错)。

(3) SW1=69,且 SW2=

• 81 命令与文件组织不适配;

• 82 安全状态不满足;

• 86 命令不允许(没有当前 EF)。

(4) SW1=6A 且 SW2=

• 81 功能不支持;

• 82 没有找到文件。

(5) SW1=6B,且 SW2=

• 00 参数错误(偏移值超出 EF)。

3. 修改二进制命令(Update Binary Command)

功能：修改已存在于 EF 中的某些数据(位)，修改内容由命令 APDU 给出。

使用条件与安全：当命令包含一个有效的短 EF 标识符时，则将此文件当作为当前 EF。本命令对当前 EF 进行处理。仅当安全状态与 EF 中定义的安全属性(修改功能)相适合时才能执行本命令。如本命令对非透明结构的 EF 进行操作，将被中止。

命令信息与应答信息：如表 4.21 和表 4.22 所示。

表 4.21 修改二进制(Update Binary)命令 APDU

CLA	见表 4.6 和 4.7
INS	D6
P1—P2	与"读二进制命令"类似
Lc	数据字段长度
Data	用于修改的数据单元串
Le	空

表 4.22 修改二进制(Update Binary)应答 APDU

数据字段	空
SW1—SW2	状态字节

表 4.22 中的状态字节 SW1—SW2 描述如下：

警告条件：SW1＝63，且 SW2＝C×(同"写二进制命令")。

出错条件：与"写二进制命令"类似。

4. 擦除二进制命令(Erase Binary Command)

功能：EF(部分)内容置于逻辑擦除状态，从给定的偏移位置开始顺序执行。

使用条件和安全：当命令中包含一个有效的短 EF 标识符时，置此文件为当前 EF。此命令对当前 EF 进行操作，仅当安全状态与安全属性(擦除功能)相适合时才能执行本命令。如本命令对非透明 EF 进行操作，将被中止。

命令信息和应答信息如表 4.23 和表 4.24 所示。

假如表 4.23 中的 Data 字段存在，它指出文件中不被擦除的第一个数据单元的偏移位置，该偏移值应大于 P1—P2 中给出的值；如 Data 字段为空，擦除命令进行到文件结束处。

表 4.23 擦除二进制(Erase Binary)命令 APDU

CLA	见表 4.6 和 4.7
INS	0E
P1—P2	与"读二进制命令"类似
Lc	空或 02
Data	见文中解释
Le	空

表 4.24 擦除二进制(Erase Binary)应答 APDU

数据字段	空
SW1 SW2	状态字节

表 4.24 中的状态字节描述如下：

警告条件：SW1＝63 且 SW2＝C×，与"写二进制命令"类似。

出错条件：与"写二进制命令"类似。

5. 读记录命令(Read Record(s) Command)

功能：读记录命令的应答信息中给出 EF 中指定记录(或记录的开始部分)的内容。

使用条件和安全：仅当安全状态与 EF 读功能的安全属性相适合时才能执行该命令。如 EF 即是该命令发出时当前选择的文件，则不需要文件的鉴别即可处理该命令。

当命令包含一个有效的短 EF 标识符，它将该文件置为当前的 EF，并将当前的记录指针复位。

假如提供一个不是记录结构的 EF，该命令将被中止。

命令信息和应答信息：表 4.25 为命令 APDU，表 4.26 为 P2 的编码，表 4.27 为应答 APDU。

表 4.25 读记录(Read Record)命令 APDU

CLA	见表 4.6 和表 4.7
INS	B2
P1	读出的第一个记录的记录号或记录标识符(00 表示当前记录)
P2	访问控制(Reference Control)，见表 4.26
Lc	空
Data	空
Le	读出的字节数

表 4.26 访问控制 P2 的编码

b_8	b_7	b_6	b_5	b_4	b_3	b_2	b_1	意　义
0	0	0	0	0	—	—	—	当前选择的 EF
×	×	×	×	×	—	—	—	短 EF 标识符(b_8—b_4 非全"1"，非全"0")
1	1	1	1	1	—	—	—	保留于将来使用
—	—	—	—	—	1	×	×	P1 为记录号的用法
—	—	—	—	—	1	0	0	读记录 P1
—	—	—	—	—	1	0	1	读出所有记录(从 P1 到最后)
—	—	—	—	—	1	1	0	读出所有记录(从最后到 P1)
—	—	—	—	—	1	1	1	保留于将来使用
—	—	—	—	—	0	×	×	P_1 为记录标识符的用法
—	—	—	—	—	0	0	0	读第一个出现的
—	—	—	—	—	0	0	1	读最后出现的
—	—	—	—	—	0	1	0	读下一个出现的
—	—	—	—	—	0	1	1	读前一个出现的

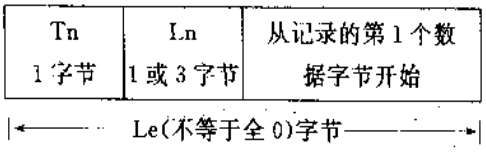
表 4.27 为应答 APDU。

表 4.27 读记录(Read Record)应答 APDU

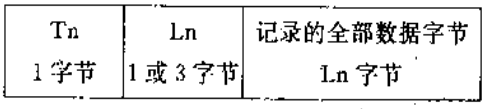
数据字段	Lr(可以等于 Le)字节,见图 4.5
SW1—SW2	状态字节

假如 Le 为全 0,最多有 256(短长度)或 65536(扩展长度)字节可读出。所有记录直到文件结束都应读出。

当记录为 Simple-TLV 数据对象时,应答信息的数据字段的格式如图 4.5 所示。

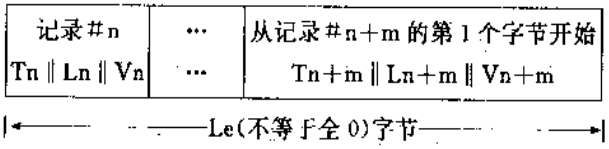


(a) 读 1 个记录的部分内容

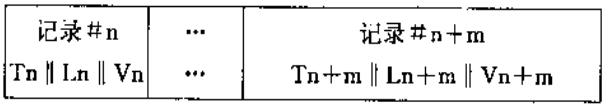


Le 等于全 0

(b) 读 1 个记录的全部内容



(c) 读记录序列的部分内容



Le 等于全 0

(d) 读多个记录直到文件结束

图 4.5 应答信息的数据字段格式

表 4.27 中的状态字节描述如下:

警告条件:SW1=62,且 SW2=

· 81 部分返回数据可能是错的;

· 82 在达到 Le 字节之前,记录已结束。

出错条件:

(1) SW1=67,且 SW2=

· 00 长度错误(Le 字段空)。

(2) SW1=69 且 SW2=

· 81 文件组织与命令不适配;

· 82 安全状态不满足。

(3) SW1=6A,且 SW2=

• 81　功能不支持；

• 82　没有找到文件；

• 83　没有找到记录。

(4) SW1=6C，且 SW2=

• ××　长度错误(Le 字段错，××指出适当的长度)。

6. 写记录命令(Write Record Command)

功能：完成以下写入操作中的一种：

(1) 一次写入一个记录。

(2) 按命令 APDU 中给出的记录数据字节与已存在此记录的数据记录字节的逻辑或(Logical OR)写入。

(3) 按命令 APDU 中给出的记录数据字节与已存在此记录的数据记录字节的逻辑乘(Logical AND)写入。

如数据编码字节(见表 4.76)没有给出指示，将按逻辑或处理。

使用条件和安全：如安全状态与 EF 的安全属性(写功能)相符合，才能执行此命令。已发出此命令时，如 EF 就是当前选择的文件，则不需要文件识别就能执行此命令。如命令中包含一个有效的短 EF 标识符，则将此 EF 置成当前 EF，并将当前记录指针复位。

如果此命令作用于透明结构 EF，此命令将被中止。

命令信息和应答信息：命令信息见表 4.28 和表 4.29，应答信息见表 4.30。

表 4.28　写记录(Write Record)命令 APDU

CLA	见表 4.6 和 4.7
INS	D2
P1	P1=00 指定当前记录
	P1≠00，P1 为指定记录编号
P2	见表 4.29
Lc	Data 长度
Data	写入的记录
Le	空

表 4.29　访问控制 P2 的编码

b_8	b_7	b_6	b_5	b_4	b_3	b_2	b_1	意　义
0	0	0	0	0	—	—	—	当前选择的 EF
×	×	×	×	×	—	—	—	短 EF 标识符
(不全部相等，即非全“1”，非全“0”)								
—	—	—	—	—	0	0	0	第一个记录
—	—	—	—	—	0	0	1	最后一个记录
—	—	—	—	—	0	1	0	下一个记录
—	—	—	—	—	0	1	1	前一个记录
—	—	—	—	—	1	0	0	P1 中给出记录号
其他值								保留于将来使用

如记录为 Simple-TLV 数据对象，则命令 APDU 的数据格式为：

Tn	Ln	记录的全部数据字节
1 字节	1 或 3 字节	Ln 字节

应答 APDU 见表 4.30。

表 4.30 写记录(Write Record)应答 APDU

数据字段	空
SW1—SW2	状态字节

状态字节 SW1—SW2 表示警告条件和出错条件如表 4.31 所示。

表 4.31 写记录(Write Record)应答的状态字节

警告条件	SW1=63	SW2=C×	同写二进制命令
出错条件	SW1=65	SW2=81	见表 4.13
	SW1=67	SW2=00	见表 4.10
	SW1=69	SW2=81 82 86	见表 4.15
	SW1=6A	SW2=81 82 83 84 85	见表 4.16

7. 增加记录命令(Append Record Command)

功能：在线性结构 EF 的末端增加一个记录或在环形结构 EF 写入编号为 1 的记录。

使用条件和安全：如安全状态与 EF 的安全属性相符合(增加记录)，才能执行本命令。在发出此命令时，如 EF 就是当前选择的文件，则不需要文件识别就能执行此命令。如命令中包含一个有效的短 EF 标识符，则将此 EF 置为当前 EF，并将当前记录指针复位。

假如此命令作用于透明结构 EF，它将被中止。

假如此命令作用于环形结构 EF，且该文件已充满记录，于是增加的记录将替代记录号最高的记录，并赋以记录号 1。

命令信息和应答信息：命令信息见表 4.32，应答信息见表 4.33。

表 4.32 增加记录命令 APDU

CLA	见表 6
INS	E2
P1	00
P2	当 P2=00000000 时，为当前选择的 EF 当 P2=××××××000，且××××××不全等时，为短 EF 标识符
Lc	Data 长度
Data	增加的记录
Lc	空

如记录为 Simple-TLV 数据对象，则命令 APDU 的数据格式为：

Tn	Ln	整个记录的数据字记
1 字节	1 或 3 字节	Ln 字节

应答 APDU 见表 4.33。

表 4.33 增加记录(Append Record)应答 APDU

数据字段	空
SW1—SW2	状态字节(见表 4.34)

表 4.34 增加记录(Append Record)应答 APDU 状态字节

警告条件	SW1=63	SW2=C×	同"写二进制命令"
出错条件	SW1=65	SW2=81	见表 4.13
	SW1=67	SW2=00	见表 4.10
	SW1=69	SW2=81	
		82	
		86	见表 4.15
	SW1=6A	SW2=81	
		82	
		84	见表 4.16
		85	

8. 修改记录命令(Update Record Command)

功能：利用命令 APDU 中给出的数据位修改指定的记录。

使用条件和安全：如安全状态与 EF 的安全属性相符合(修改记录)，才能执行本命令。在发出此命令时，如 EF 就是当前选择的文件，则不需要文件识别就能执行此命令。如命令中包含一个有效的短 EF 标识符，则将此 EF 置为当前 EF，并将当前记录指针复位。

假如此命令作用于透明结构 EF，它将被中止。

当此命令作用于线性固定长度结构 EF 或环形结构 EF，而且记录长度与存在的记录的长度不同，此命令将被中止。当此命令作用于线性可变结构 EF，即使记录长度与存在的记录的长度不同，此命令也能执行。

命令信息与应答信息：表 4.35 和表 4.36 分别为命令 APDU 和应答 APDU。

表 4.35 修改记录(Update Record)命令 APDU

CLA	见表 4.6 和表 4.7
INS	DC
P1	P1=00，修改当前记录
	P1≠00，修改指定记录
P2	见表 4.29
Lc	Data 长度

续表

Data	修改的记录
Le	空

如记录为 Simple-TLV 数据对象，则命令信息的数据字段格式为：

Tn	Ln	整个记录的数据字节
1 字节	1 或 3 字节	Ln 字节

表 4.36 修改记录(Update Record)应答 APDU

Data 字段	空
SW1—SW2	状态字节

表中 SW1—SW2 表示警告条件与出错条件，与写记录命令中的描述相同(见表 4.31)。

9. 取数据命令(Get Data Command)

功能：在当前的上下文中(例如特定应用环境)，检索 1 个或多个数据对象。

使用条件和安全：仅当安全状态满足应用在上下文中对功能定义的安全条件，才能执行本命令。

命令信息和应答信息：表 4.37 为命令 APDU，表 4.38 为应答 APDU。

下面对表 4.37 中的 P1--P2 作进一步解释。

当 P1--P2 在 0100—01FF 范围内时，P1—P2 的值为一标识符，用于卡的内部测试或专有服务(在给定的应用上下文中)。

当 P1—P2 为 00FF 时，取得上下文中所有可读的共用 BER-TLV 数据对象；当 P1—P2 为 02FF 时，取得上下文中所有可读的共用 Simple-TLV 数据对象；当 P1—P2 为 0200、4000 或 FFFF 时，保留于将来使用。

表 4.37 取数据(Get Data)命令 APDU

CLA	见表 4.6 和表 4.7
INS	CA
P1—P2	0000 Data 为 BER-TLV 标志
	0001—003F 保留于将来使用
	0040--00FF P2 中为 BER-TLV 标志(1 字节)
	0100—01FF 应用数据(专有编码)
	0200—02FF P2 中为 Simple-TLV 标志
	0300—03FF 保留于将来使用
	4000 FFFF P1—P2 中为 BER-TLV 标志(2 字节)
Lc	空或 Data 长度
Data	空或 BER-TLV 标志
Le	期望在应答中的字节数

表 4.38 取数据(Get Data)应答 APDU

Data 字段	Lr(可能等于 Le)字节
SW1—SW2	状态字节

如 Le 为 0,最多可达 256(短长度)字节或 65536(扩展长度)字节。所有需要的信息都应该返回。

表 4.39 取数据(Get Data)应答 APDU 状态字节

警告条件	SW1=62	SW2=81	见表 4.11
出错条件	SW1=67	SW2=00	见表 4.10
	SW1=69	SW2=82 85	见表 4.15
	SW1=6A	SW2=81 88	见表 4.16
	SW1=6C	SW2=××	见表 4.10

10. 存数据命令(Put Data Command)

功能:存储一个或多个数据对象(相同的操作)。存储功能(一次写和/或修改和/或增加)是由数据对象的定义或性质决定的。

此命令可用于修改 ATR(复位应答)文件或 DIR 文件等。

使用条件和安全:如安全状态满足应用在上下文中对功能定义的安全条件,才能执行本命令。

命令信息和应答信息:表 4.40 和表 4.41 分别为命令 APDU 和应答 APDU。

表 4.40 存储数据(Put Data)命令 APDU

CLA	见表 4.6 和 4.7
INS	DA
P1—P2	0000—003F 保留于将来使用
	0040—FFFF 同取数据命令 APDU,见表 4.37
Lc	Data 长度
Data	准备写入的参数和数据
Le	空

当表 4.40 中的 P1—P2 值为 00FF、02FF 或 4000 或 FFFF 时为保留值。

表 4.41 存储数据(Put Data)应答 APDU

Data 字段	空
SW1—SW2	状态字节(见表 4.42)

表 4.42 存储数据(Put Data)应答 APDU 的状态字节

警告条件	SW1=63	SW2=C×	见表 12
出错条件	SW1=65	SW2=81	见表 4.13
	SW1=67	SW2=00	见 4.10
	SW1=69	SW2=82 86	见 4.15
	SW1=6A	SW2=80 81 84 85	见表 4.16

11. 选择文件命令(Select File Command)

功能：在一个逻辑通道上设置一个当前文件，后续命令通过此逻辑通道提交给当前文件。

选择一个 DF(也可以是 MF)，置此文件为当前 DF，之后，通过这一逻辑通道可以引用一个默认的当前 EF。

选择一个 EF 时置一对当前文件：EF 和它的父文件。

在复位应答之后，除了在历史字节或初始数据串(见 4.7 节)中有不同说明以外，默认通过基本逻辑通道选择 MF。

使用条件与安全：

对一个打开的逻辑通道，可提供后面讲到的条件。

除非有其他说明，正确执行命令时将根据以下规则修改安全状态。

- 如当前 EF 改变时，或没有当前文件，那么以前的当前 EF 的安全状态(如有的话)将丢失。
- 如当前 DF 是以前的当前 DF 的一个子孙，或与以前的当前 DF 是同一个 DF，那么以前的当前 DF 的安全状态将保持不变。
- 如当前 DF 既不是以前的当前 DF 的子孙，也不和以前的当前 DF 是同一个 DF，那么以前的当前 DF 的安全状态将丢失。对以前的和新的当前 DF 的所有共同祖先的安全状态将保持不变。

命令信息和应答信息：表 4.43 为命令 APDU。

表 4.43 选择文件(Select File)命令 APDU

CLA	见 4.6 和表 4.7
INS	A4
P1	选择控制，见表 4.44
P2	见表 4.45
Lc	空或 Data 长度

续表

Data	根据 P1—P2 确定。如 Data 存在，可以是文件标识符、从 MF 开始的路径、从当前 DF 开始的路径或 DF 名
Le	空，或期望在应答 APDU 中的最大数据长度

表 4.44 选择控制 P1 的编码

b_8	b_7	b_6	b_5	b_4	b_3	b_2	b_1	意 义
0	0	0	0	0	0	×	×	用文件标识符选择
0	0	0	0	0	0	0	0	选 MF、DF 或 EF(Data=标识符或空)
0	0	0	0	0	0	0	1	选子 DF(Data=DF 标识符)
0	0	0	0	0	0	1	0	选当前 DF 下的 EF(Data=EF 标识符)
0	0	0	0	0	0	1	1	选当前 DF 的父 DF(Data 为空)
0	0	0	0	0	1	×	×	用 DF 名选择
0	0	0	0	0	1	0	0	用 DF 名直接选择(Data=DF 名)
0	0	0	0	0	1	0	1	保留于将来使用
0	0	0	0	0	1	1	0	保留于将来使用
0	0	0	0	0	1	1	1	保留于将来使用
0	0	0	0	1	0	×	×	用路径选择
0	0	0	0	1	0	0	0	从 MF 选择(Data=路径，无 MF 标识符)
0	0	0	0	1	0	0	1	从当前 DF 选择(Data=路径，无当前 DF 标识符)
0	0	0	0	1	0	1	0	保留于将来使用
0	0	0	0	1	0	1	1	保留于将来使用
其他值								保留于将来使用

如 P1—P2=0000，且 Data 空或等于 3F00，则选择 MF。

表 4.45 选择 P2 的编码

b_8	b_7	b_6	b_5	b_4	b_3	b_2	b_1	意义
0	0	0	0	—	—	0	0	首先或唯一出现
0	0	0	0	—	—	0	1	最后出现
0	0	0	0			1	0	下次出现
0	0	0	0	—	—	1	1	上次出现
0	0	0	0	×	×			文件控制信息选择(见 4.2.3)
0	0	0	0	0	0			返回 FCI 可选模板
0	0	0	0	0	1			返回 FCP 模板
0	0	0	0	1	0	—		返回 FMD 模板
0	0	0	0	1	1	—		不返回信息
其他值								保留于将来使用

表 4.46 选择文件(Select File)应答 APDU

数据字段	根据 P2 确定数据(最多 Le 字节)
SW1—SW2	状态字节(见表 4.47)

表 4.47 选择文件应答 APDU 的状态字节

警告条件	SW1=62	SW2=83	见表 4.11
		84	
出错条件	SW1=6A	SW2=81	见表 4.16
		82	
		86	
		87	

12. 检验命令(Verify Command)

功能：将来自接收设备的验证数据和存储在卡中的参照数据(例如通行字)进行比较，根据比较结果修改安全状态。

使用条件和安全：不成功的比较可记录在卡中(例如可限制今后继续使用参照数据的次数)。

命令信息和应答信息：表 4.48 和表 4.49 分别为命令 APDU 和应答 APDU。

表 4.48 检验(Verify)命令 APDU

CLA	见表 4.6 和 4.7
INS	20
P1	00
P2	当 $b_8=0$ 时为全局参照数据； 当 $b_8=1$ 时为特定参照数据(例如 DF 特定通行字)； (b_8—b_1 全为 0 时不给出信息；b_5—b_1 为参照数据号)
Lc	Data 长度
Data	空或检验数据
Le	空

表 4.49 中 Data 字段为空时，用来观察应答 APDU 的 SW1—SW2。

表 4.49 检验(Verify)应答 APDU

Data	空
SW1—SW2	状态字节(见表 4.50)

表 4.50 检验应答 APDU 的状态字节

警告条件	SW1=63	SW2=00	不给出信息(检验失败)
		C×	计数值(检验失败，×指示允许再重试次数)

续表

出错条件	SW1=69	SW2=83 84	见表 4.15
	SW1=6A	SW2=86 88	见表 4.16

13. 内部鉴别命令(Internal Authenticate Command)

功能：使用由接口设备送来的口令(challenge)和存储在卡中的有关秘密(例如密钥)进行鉴别数据的计算。

当有关的秘密属于 MF 时，此命令用于鉴别整个卡，当有关的秘密属于另一 DF 时，此命令用于鉴别该 DF。

使用条件和安全：本命令的成功执行取决于先前命令(如检验命令、选择文件命令)或选择(如有关秘密，……)的成功实现。当发送此命令时，如有一密钥或一算法是当前选择的，此命令默认使用此密钥与算法。

此命令的发送次数可以记录在卡中，用来限制以后试图使用有关秘密或算法的次数。

命令信息和应答信息：表 4.51 和表 4.52 分别为命令 APDU 和应答 APDU。

表 4.51 内部鉴别(Internal Authenticate)命令 APDU

CLA	见表 4.6 和表 4.7
INS	88
P1	卡中算法的引用，P1=00 表示不给出信息*
P2	秘密的引用，P2=00 不给出信息*
	b_8=0 为全局参考数据(如 MF 专有密钥)**
	b_8=1 为专有参考数据(如 DF 专有密钥)**
Lc	Data 长度
Data	与鉴别有关的数据(如口令 challenge)
Le	期望在应答中的最大字节数

* 在发出此命令前已知，或在 Data 字段中提供；

** b_5—b_1 为秘密号。

表 4.52 内部鉴别(Internal Authenticate)应答 APDU

数据字段	鉴别有关数据(如对口令的应答)
SW1—SW2	状态字节

应答信息可以包括用于以后应用安全功能的数据(例如随机数)。

表 4.53 内部鉴别应答 APDU 的状态字节

出错条件	SW1=69	SW2=84 85	见表 4.15
	SW1=6A	SW2=86 88	见表 4.16

14. 外部鉴别命令(External Authenticate Command)

功能：利用卡的计算结果(是或否)有条件地修改安全状态，该结果基于卡以前发出的口令(例如用 Get Challenged Command)、秘密存储在卡中的密钥和接口设备发送的鉴别数据。

使用条件和安全：要求从卡获得的最后的口令是有效的，才能成功地执行本命令。

不成功的比较可以记录在卡中(例如用于限制进一步使用算法和保密数据的次数)。

命令信息和应答信息：表 4.54 和表 4.55 分别为命令 APDU 和应答 APDU。

表 4.54 外部鉴别(External Authenticate)命令 APDU

CLA	见表 4.6 和表 4.7
INS	B2
P1	在卡中算法的引用
P2	保密的引用。当 b_8 为 0 时为全局参考数据(如 MF 专有密钥)，当 $b_8=1$ 时为专有参考数据(如 DF 专有密钥)，b_5-b_1 为秘密编号(如密钥编号或短 EF 标识符)
Lc	空或 Data 长度
Data	空或验证有关数据(如对口令的应答)
Le	空

表中 P1=00 或 P2=00 表示不给出信息，在发出此命令前已知，或在 Data 字段中提供。

如 Data 为空，此命令用于检索应答信息中的 SW1--SW2。

表 4.55 外部鉴别(External Authenticate)应答 APDU

Data	空
SW1—SW2	状态字节

表 4.56 外部鉴别应答 APDU 的状态字节

警告条件	SW1=63,	SW2=00 SW2=C×	不给出信息(验证失败) 计数值(验证失败) ×给出允许再重试的次数
出错条件	SW1=67	SW2=00	见表 4.10
	SW1=69	SW2=83 84 85	见表 4.15
	SW1=6A	SW2=86 88	见表 4.16

15. 取口令命令(Get Challenge Command)

功能：本命令需要得到一个口令(如随机数)，用于与安全有关的过程(如 External Authenticate Command)。

使用条件与安全：此口令至少对下一条命令有效，ISO/IEC 7816-4 未提出其他条件。

命令信息与应答信息：表 4.57 和表 4.58 分别为命令 APDU 和应答 APDU。

表 4.57 取口令(Get Challenge)命令 APDU

CAL	见表 4.6 和表 4.7
INS	84
P1—P2	0000
Lc	空
Data	空
Le	期望应答的最大长度

表 4.58 取口令(Get Challenge)应答 APDU

Data	口令
SW1—SW2	状态字节

表 4.59 取口令应答 APDU 的状态字节

出错条件：	SW1=6A	SW2=81 86	见表 4.16

16. 管理通道命令(Manage Channel Command)

功能：打开与关闭逻辑通道。

打开功能：打开新的逻辑通道，而且不是基本逻辑通道。可以指定一个逻辑通道号或

选择卡所支持的逻辑通道号。

关闭功能：明确地关闭一个逻辑通道，而且不是基本逻辑通道。在关闭成功以后，该逻辑通道可以被重新使用。

使用条件和安全：在基本逻辑通道成功地完成打开功能之后，MF 将被隐含地选作当前 DF，新逻辑通道的安全状态保持与复位应答(ATR)之后的基本逻辑通道的安全状态一致。新逻辑通道的安全状态应该与其他逻辑通道分开。

当从一个逻辑通道(非基本的逻辑通道)成功地完成打开功能之后，发出此命令的逻辑通道的当前 DF 被选作当前 DF，新逻辑通道的安全状态应与完成打开功能的逻辑通道的安全状态保持一致。

在成功完成关闭功能之后，与该逻辑通道通道有关的安全状态将不存在。

命令信息和应答信息：表 4.60 和表 4.61 分别为命令 APDU 和应答 APDU。

表 4.60 管理通道(Manage Channel)命令 APDU

CLA	见表 4.6 和表 4.7
INS	70
P1	00，打开一个逻辑通道
	80，关闭一个逻辑通道
P2	'00'，'01'，'02'，'03'(其它值保留于将来使用)
Lc	空
Data	空
Le	01(如 P1－P2＝'0000')，空(如 P1－P2≠'0000')

当 P1＝00，要求打开一个逻辑通道时，P2 的 b_1 和 b_2 为逻辑通道号。如 P_2 的 b_1、b_2 为空，卡将指定一个逻辑通道号，并在应答 APDU 的逻辑字段 b_2b_1 位返回此逻辑通道号；如 P2 的 b_1 和/或 b_2 不空，则为逻辑通道号(非基本逻辑通道)，于是卡将打开由外部指定的逻辑通道。

表 4.61 管理通道(Manage Channel)应答 APDU

数据字段	逻辑通道号(如 P1－P2＝0000) 空(如 P1－P2≠0000)
SW1－SW2	状态字节(警告条件；SW1－SW2＝6200，不给出信息)

17. 取应答命令(Get Response Command)

功能：卡向接口设备发送(部分)APDU(s)。

使用条件和安全：无条件。

命令信息和应答信息：表 4.62 和表 4.63 分别为命令 APDU 和应答 APDU。

表 4.62 取应答(Get Response)命令 APDU

CLA	见表 4.6 和 4.7
INS	C0
P1—P2	0000
Lc	空
Data	空
Le	期望在应答中的最大数据长度

如 Le 为全 0,最多有 256(短长度)或 65536(扩展长度)个字节返回。

表 4.63 取应答(Get Response)应答 APDU

数据字段	(部分)APDU,由 Le 决定
SW1—SW2	状态字节

表 4.64 应答 APDU 的状态字节

正常处理	SW1=61	SW2=××	表示可得到更多数据。 (××表示另有一定数量的数据在其后的 Get Response 命令中仍可得到)
警告条件	SW1=62	SW2=81	见表 4.11
出错条件	SW1=67	SW2=00	见表 4.10
	SW1=6A	SW2=86	见表 4.16

18. 信封命令(Envelope Command)

功能:用于发送 APDU(s),或部分 APDU,,或数据串。

使用条件和安全:无条件。

命令信息和应答信息:表 4.65 和表 4.66 分别为命令 APDU 和应答 APDU。

表 4.65 信封(Envelope)命令 APDU

CLA	见表 4.6 和表 4.7
INS	C2
P1—P2	0000
Lc	Data 长度
Data	(部分)APDU
Le	空或期望的数据长度

当 Envelope Command 用于发送数据串(T=0)时,一个空的 Envelope Command 表示字符串的结束。

表 4.66 信封(Envelope)应答 APDU

数据字段	空或(部分)APDU,由 Le 决定
SW1—SW2	状态字节

在 Envelope Command 的 Data 字段发出的命令状态字节有可能在信封应答的数据字段中找到。

出错条件：SW1＝67,SW2＝00 长度错误(Lc 字段不正确)。

4.6 历史字节

4.6.1 目的和一般结构

当根据 ISO/IEC 7816-3 确定传输协议后,历史字节告诉外部环境如何使用卡。

历史字节数(最多为 15 个字节)的说明和编码在 ISO/IEC 7816-3 中定义。

历史字节所携带的信息还可在 ATR 文件(默认 EF 指示符＝'2F01')中找到。

如果存在历史字节,它由三个字段组成：

——必有的类型指示符(1 字节)

——可选的 COMPACT-TLV 对象

——条件状态指示符(3 字节)

4.6.2 类型指示符(必有的)

第一个历史字节是类型指示符,如果它等于'00'、'10'或'8×',那么历史字符的格式将根据 ISO/IEC 7816 本部分决定。

表 4.67 类型指示符的编码

值	意 义
'00'	状态信息存在于历史字节的结尾(不在 TLV 中)
'10'	在 4.6.5 中说明
'80'	如存在状态信息,它将包含在一个可选的 COMPACT-TLV 数据对象中
'81—8F'	保留于将来使用
其他值	专用

4.6.3 可选的 COMPACT-TLV 对象

COMPACT-TLV 对象的编码是从 ASN.1 的基本编码规则引导而来,对带有标记'4X'和长度'0Y'的 BER-TLV 的对象可用'XY'及其后跟 Y 个数据来取代,在本节中,X 为标记号,Y 为长度。

除了在本节中定义的数据对象以外，历史字节还包含在 ISO/IEC 7816-5 中定义的数据对象，在这种情况下，数据对象的标志编码和字段长度将按上面所叙述的修改。

在本节中定义的 COMPACT-TLV 对象出现在 ATR 文件中时，它们将按 ASN.1 的基本编码规则进行编码(例如标志'4X'，长度='0Y')。

所有未在 ISO/IEC 7816 中定义的应用类标志均由 ISO 所保留。

1. 国家/发行者指示符

当存在这一数据对象时，由它指明国家或发行者。

此数据对象由 1Y 或 2Y 引出。

表 4.68 国家/发行者指示符

标志	长度	值
1	可变	国家代码和国家数据
2	可变	发行者标识号码

标志'1'后接长度(半字节)字段和用于指明国家的 3 个数字，如 ISO 3166 中所定义的。后接的数据(奇数个半字节)由有关的国家标准化团体选择。

标志'2'后接长度(半字节)字段和发行者标识号码，如 ISO 7812 所定义的。如果发行者标识号码由奇数个数字组成，则应在其右边填充半字节数值'F'。

2. 卡的服务数据

这一数据对象指出为支持在 4.7 中所描述的服务而在卡中可采用的方法。

这一数据对象由'31'引入。

当该数据对象不存在时，卡仅支持隐含的应用选择。

表 4.69 与应用无关的卡的服务

b_8	b_7	b_6	b_5	b_4	b_3	b_2	b_1	意义
1	—	—	—	—	—	—	—	用整个 DF 名的直接应用选择
—	1	—	—	—	—	—	—	用部分 DF 名的选择(见 4.7.3)
—	—	1	—	—	—	—	—	在 DIR 文件中可用的数据对象
—	—	—	1	—	—	—	—	在 ATR 文件中可用的数据对象
—	—	—	—	1	—	—	—	文件 I/O 服务(用读二进制命令)
—	—	—	—	0	—	—	—	文件 I/O 服务(用读记录命令)
—	—	—	—	—	×	×	×	000(其他值保留于将来使用)

3. 初始访问数据

这一可选的数据对象允许检索在 ISO/IEC 7816 中所定义的数据对象串，被这一数据对象所检索的数据串叫做初始数据串。

该数据对象由'41'、'42'或'45'引入。

在本节(4.6 节)中描述的任一命令 APDU 是在复位应答后发出的第一个命令。因此在此刻可得到的数据不一定能在后面检索到。

(1) 长度＝'1'

仅提供1个字节信息，它指示执行检索初始数据串的命令的长度。所执行的命令是一条读二进制命令，其结构如表4.70所示。

表4.70 当长度＝"1"时的命令编码

CLA	'00'(见表4.6和表4.7)
INS	'B0'
P1－P2	'0000'
Lc	空
Data	空
Le	初始访问数据的数值字段的第一个且是唯一的字节(指示将读出的字节数)

(2) 长度＝'2'

当提供两字节信息时，第一个字节指出文件结构(透明或记录)和将读出的基本文件的短标识符。第二个字节指示为了检索初始数据串而执行的读命令的长度。

表4.71 第一个字节的结构

b_8	＝1 记录文件
	＝1 透明文件
$b_7－b_6$	00 (其他值保留于将来使用)
$b_5－b_1$	短EF标识符

当b_8＝0时，执行的命令是一条读记录命令，其结构见表4.72。

表4.72 当b_8＝0时的命令编码

CLA	'00'(见表4.6和表4.7)
INS	'B2'
P1	'01'
P2	短EF标识符(取自初始访问数据的第一个字节)，后随b3－b2－b1＝110
Lc	空
Data	空
Le	初始访问数据的数值字段的第二个，即最后一个字节(指示将读出的字节数)

当b_8＝1时，执行的命令是一条读二进制命令，其结构如表4.73所示。

表 4.73 当 $b_8=1$ 时的命令编码

CLA	'00'(见表 4.6 和表 4.7)
INS	'B0'
P1	初始访问数据第一个字节的值
P2	'00'
Lc	空
Data	空
Le	初始访问数据的数值字段的第 2 个和最后一个字节(指示将读出的字节数)

(3) 长度='5'

在初始访问数据对象中找到的数值,由执行命令的 APDU 组成。当执行时,该命令在其应答数据字段中提供初始数据串。

4. 卡的发行者数据

该数据对象是可选的且长度可变。由卡发行者定义结构和编码。

该数据对象由 5Y 引入。

5. 发行前数据

该数据对象是可选的且长度可变,其结构和编码不在 ISO/IEC 本部分中定义,它用于指示:

——卡制造商

——集成电路类型

——集成电路制造商

——ROM 掩膜版本

——操作系统版本

该数据对象由 6Y 引入。

6. 卡的能力

该数据对象是可选的,且长度可变,其数值字段由第一个软件功能表,或开始两个软件功能表,或三个软件功能表组成。

该数据对象由'71'、'72'或'73'引入。

表 4.74 示出第一个软件功能表。

表 4.74 第一个软件功能表

b_8	b_7	b_6	b_5	b_4	b_3	b_2	b_1	意 义
								DF 选择
1	–	–	–	–	–	–	–	——用 DF 名
–	1	–	–	–	–	–	–	——用路径
–	–	1	–	–	–	–	–	——用文件标识符
–	–	–	1	–	–	–	–	——隐含
–	–	–	–	×	–	–	–	0(1 保留于将来使用)

续表

b_8	b_7	b_6	b_5	b_4	b_3	b_2	b_1	意　义
								EF 管理
—	—	—	—	—	1	—	—	支持短 EF 标识符
—	—	—	—	—	—	1	—	——支持记录号
—	—	—	—	—	—	—	1	——支持记录标识符

表 4.75 示出第二个软件功能表(数据编码字节),该数据编码字节也可存在于带标志'82'的文件控制参数中,作为第二个数据单元(见表 4.2)。

表 4.75　第二个软件功能表(数据编码字节)

b_8	b_7	b_6	b_5	b_4	b_3	b_2	b_1	意　义
—	×	×	—	—	—	—	—	写功能的行为
—	0	0	—	—	—	—	—	—— 一次写
—	0	1	—	—	—	—	—	——专用
—	1	0	—	—	—	—	—	写或(OR)
0	1	1	—	—	—	—	—	写与(AND)
—	—	—	—	—	×	×	×	数据单元大小(半字节)
								(权 2,如 001=2 个'半字节',缺省值=1 字节)
×	—	—	×	×	—	—	—	0…00(其他值保留于将来使用)

表 4.76 示出第三个软件功能表。

表 4.76　第三个软件功能表

b_8	b_7	b_6	b_5	b_4	b_3	b_2	b_1	意　义
×	—	—	—	—	—	—	—	0(1 保留于将来使用)
—	1	—	—	—	—	—	—	扩展 Lc 和 Le 的字段
—	—	×	—	—	—	—	—	0(1 保留于将来使用)
—	—	—	×	×	—	—	—	指定逻辑通道
—	—	—	1	—	—	—	—	由卡指定
—	—	—	—	1	—	—	—	——由接口设备指定
—	—	—	—	—	×	—	—	0(1 保留于将来使用)
—	—	—	—	—	—	X	Y	逻辑通道的最大数(=2X+Y+1)

4.6.4　状态信息

状态信息由三个字节组成:卡的生命状态(1 字节)和 SW1—SW2(2 个状态字节)。

卡的生命状态的值为'00'表示不提供卡的生命状态,值'80'到'FE'是专用的,所有其他值保留于将来使用。

SW1—SW2 为'9000'表示正常处理。

SW1—SW2 为'0000'表示不指示状态。

如类型指示符的值为'80',则状态信息可以存在于 COMPACT-TLV 数据对象中。在这种情况下,标志号为 8。当长度为 1 时,其值为卡生命状态,当长度为 2 时,其值为 SW1—SW2。当长度为 3 时,其值为卡生命状态,并后随 SW1—SW2。长度的其他值为 ISO 所保留。

4.6.5 DIR 数据访问

如果类别指示符为'10',其后随字节是 DIR 数据访问,该字节的编码及意义已超出 ISO/IEC 7816 本部分的范围。

4.7 与应用无关的卡服务

4.7.1 定义和范围

本节讨论与应用无关的卡服务,在下文中称为"卡服务",其目的是提供卡与终端之间的交换机制,而在此之前,它们彼此之间,除了皆遵照 ISO/IEC 7816 本部分协议之外,其他一无所知。

卡服务被下述任一组合所支持:历史字节;一个或多个保留的 EF 的内容;行业间命令的序列。

该命令使用 CLA = '00'(见表 4.6 和表 4.7),即不指出安全信息和基本逻辑通道。

当一种应用已在卡中识别和选择就不需要再遵循本条款。一种应用可以采用其他的与 ISO/IEC 7816-4 兼容的机制去达到类似的功能。但这样的解决可能不保证交换。

卡服务定义如下:

1. 卡鉴别服务:这一服务允许终端识别此卡,并知道如何处理它。

2. 应用选择服务:这一服务允许终端知道在卡中哪种应用在活动(如有的话)以及如何去选择和启动在该卡中的应用。

3. 数据对象检索服务:这一服务允许检索在 ISO/IEC 7816 某一部分中定义的数据对象。本节仅描述行业间数据对象的标准机制。

4. 文件选择服务:这一服务允许选择不知名的 DF 和 EF。

5. 文件 I/O 服务:这一服务允许访问存储在 EF 中的数据。

4.7.2 卡识别服务

本功能包括卡向外部提供有关其逻辑内容的信息以及所有应用均感兴趣的若干个通用数据(例如行业间数据对象)。称之为"卡识别数据"的信息可以由卡在历史字节中给出,也可能在复位应答后立即选择的隐含文件中给出。

在初始访问数据信息中指示访问该文件(见 4.6.3 节中的 3.)。

如果历史字节的初始访问数据不指示一条读命令,于是命令的应答包含卡识别数据。

4.7.3 应用选择服务

可以由卡隐含选择一项应用，或用它的名字显式选择一项应用。

1. 隐含应用选择

当卡隐含选择一项应用时，由 ISO/IEC 7816-5 定义的应用标识符应该在卡标识数据中指示出。如它不存在于卡标识数据中，则它应存在于 ATR 文件中。

2. 直接应用选择

在多应用环境中的卡，应该对选择文件命令实现的直接应用选择确实地作出应答，该命令指定应用标识符作为 DF 名。

在命令 APDU 中应完整地提供应用标识符。假如一种应用选择用部分 DF 名，下一个应用(与该名匹配)建议可能被选择，并在选择文件命令的应答消息中可得到 DF 全名，作为带标志'84'的文件控制参数(见表 4.2)。

执行命令的 APDU 如表 4.77 所示。

表 4.77 命令编码(直接应用选择)

CLA	'00'(见表 6)
INS	'A4'
P1—P2	0400
Lc	数据字段的字节长度
Data	DF 全名或 DF 部分名
Le	全 0

4.7.4 数据对象检索服务

用于与应用无关的国际交换的数据对象定义于 ISO/IEC 7816 各个部分中。

这些数据对象的检索依赖于下述一个或两个方法。

1. 数据对象存在于卡识别数据中。

2. 数据对象存在于 DIR 文件(路径='3F002F00')或 ATR 文件(路径='3F002F01')

检索数据对象所需要的信息通过间接方法定义在 ISO/IEC 7816-6 中。

4.7.5 文件选择服务

当已知到达一个 EF 的路径时，发出的选择文件命令的数量等于路径长度除以 2，减 1(此路径经常开始于当前 DF)。

如果路径长度大于 4 个字节，那么直到该路径的所有有效的 DF 标识符被使用到为止，一个或多个选择文件命令将被执行，这些命令带有的命令 APDU 见表 4.78。

表 4.78 利用文件标识符选择 DF 的命令编码

CLA	'00'(见表 4.6 和 4.7)
INS	'A4'
P1—P2	'0100'
Lc	'02'
Data	DF 标识符(取自路径字节 3 和 4)
Le	空

最后的且可能是唯一的选择是一个 EF 选择,见表 4.79 的命令 APDU。

表 4.79 选择一个 EF 的命令编码

CLA	'00'(见表 4.6 和 4.7)
INS	'A4'
P1—P2	'0200'
Lc	'02'
Data	EF 标识符(路径的最后两字节)
Le	空

4.7.6 文件 I/O 服务

当用于行业间交换的文件已被选择好,有关交换的内容将用下面的命令 APDU 中的一个返回。

1. 如第一个软件功能表缺,或不支持面向记录的命令,于是将执行表 4.80 中的命令。

表 4.80 读透明文件的命令编码

CLA	'00'(见表 4.6 和表 4.7)
INS	'B0'
P1—P2	'0000'
Lc	空
Data	空
Le	存在,内容为全'0'

2. 如果第一个软件功能表示支持面向记录的命令,于是将执行表 4.81 中的命令。

表 4.81 读面向记录文件的命令编码

CLA	'00'(见表 4.6 和表 4.7)
INS	B2
P1—P2	0005
Lc	空
Data	空
Le	存在,内容为全'0'

4.8 ISO/IEC 7816-5 应用标识符的编号系统和注册过程

ISO/IEC 7816-5 指明了应用标识符的编号系统以及对于应用提供者标识符的注册过程。

本标准中描述的编号系统提供了一种方法，由提供者所提供的应用和相关服务去验证给定的卡中是否含有该应用及相关服务所需的单元。

应用标识符(AID)用于确定卡中应用的地址。本标准规定了应用标识符的编码以及在卡中应用部分的寻址方法和机制。

4.8.1 定义和缩写

1. 应用标识符 AID

识别卡中应用的一个数据单元，应用标识符可以包括注册应用提供者标识符。

2. 应用提供者

是一个实体，它提供了用于实现不同应用的卡上的一个应用的组成部分。

3. 应用标签

一个用于人机接口的数据单元。

4. 应用模板

一个数据单元，可能存在于一个 DIR 文件中，包含一个或多个与应用相关的 ASN.1 对象。

5. ASN.1 对象

在本标准中包含一字节标志，后跟一字节体长信息，随后是至多 127 字节的一个体，该体的长度由体长给出。

6. 目录(DIR)文件

一个可选的基本文件，包含被卡所支持的应用列表，还包含定义于ISO/IEC 7816-5 中可选的相关数据单元。

7. 主文件(MF)、路径(Path)、复位应答(ATR)文件、数据单元(data element)

定义于 ISO/IEC 7816-4 中。

ATR 定义于 ISO/IEC 7816-3 中，ATR 文件定义于 ISO/IEC 7816-4 中。

4.8.2 数据单元

如果在此处定义的数据单元表示为 ASN.1 对象的体，则其编码如表 4.82 所示。

表中 P 表示原始 ASN.1 对象的体，包含一个数据单元。C 表示结构 ASN.1 对象的体，包括原始或结构 ASN.1 对象。

现将表 4.82 中的值 V(数据单元)分别描述在下面。

1. 应用标识符 AID

AID 使用十六进制编码，首字节最高的 4 位是注册类别(见表 4.83)，用以区别注册

标识符和专用应用标识符。

表 4.82 ASN.1 数据单元编码

标志 T(1 字节)	长度 L(1 字长)	值 V(数据单元)(L 字节)	类型
'4F'	'01'—'10'	应用标识符(AID)	P
'50'	'00'—'10'	应用标签	P
'51'	'00'—'7E'	路径	P
'52'	'04'—'7F'	可执行命令,见 7816-4	P
'53'	'00'—'7F'	任意数据	P
'73'	'00'—'7F'	任意 ASN.1 对象	C
'61'	'03'—'7F'	应用模板	C
类型 P=原始 ASN.1 对象 C=结构 ASN.1 对象			
其他应用类标志为 ISO 所保留			

表 4.83 注册类别

0—9	定义于 ISO 7812
A	国际注册
B	ISO 保留
C	ISO 保留
D	国内注册
E	ISO 保留
F	专用、非注册

现将注册类别分别说明如下:

(1) 注册类别='0'—'9'

应用标识符(AID)

IIN	'FF'	PIX

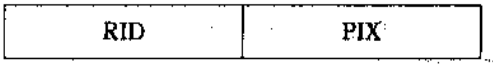
IIN 为发行者标识号,定义于 ISO 7812 中,IIN 的第一个数字为注册类别('0'—'9'),如 IIN 为奇数个数字,将在最低字节的 1 至 4 位填补'F'。

PIX 为专用应用标识扩展名,如它存在,将前置一编码为'FF'的字节。

IIN 的长度未定义,AID 的总长度为 2 到 16 个字节。

(2) 注册类别='A'

应用标识符



RID 为应用提供者标识符，由 4 位注册类别(1010)和 36 位(9 个数字)注册应用提供者编号组成，其长度为 5 个字节。

PIX 为专用应用标识扩展名，长度≤11 个字节。

(3) 注册类别＝'D'

应用标识符

RID 由 4 位注册类别(1101)，12 位注册当局国家代码(3 个数字)和 24 位国家当局指定的字段组成，共 5 个字节。

PIX 的长度≤11 字节。

(4) 注册类别＝'F'

应用标识符 AID 仅包含专用应用标识符一项。AID 的长度为 1 到 16 字节。

标识符不注册，不同应用提供者可能使用相同的 AID。

2. 应用标签

该应用单元可被应用提供者指定，用于人机接口，例如显示给客户的商标，长度为 0—16 个字节。

3. 路径

在 ISO/IEC 7816-5 中，所有路径开始于主文件。这个数据单元的字节数为偶数，长度为 0—126 字节。

4. 可执行命令

"可执行命令"数据单元是关于应用选择的命令 APDU(参见 ISO/IEC 7816-4)，长度为 4—127 字节。

5. 任意数据

应用提供者可将任何有关信息填入该数据单元，长度为 0—127 字节。

6. 任意 ASN.1 对象

长度为 0—127 字节。

7. 应用模板

应用模板包含 1 个或多个与应用有关的 ASN.1 对象，在其中，ASN.1 对象必须包含应用标识符，所有在 ISO/IEC 7816-5 中定义的其他 ASN.1 对象可任选，长度为 3—127 字节。

4.8.3 检索 ASN.1 对象

在 ISO/IEC 7816-5 中定义的 ASN.1 对象可被找到于：

——在 ATR 历史文字节中。

——在 DIR 文件中。

——在 ATR 文件中。

——在 ASN.1 被使用的任何命令或应答消息中，例如在一个文件的文件控制信息中，参见 ISO/IEC 7816-4。

DIR 文件仅包含一串应用标识符和/或应用模板。删除了的 ASN.1 对象可被一串'00'或'FF'取代。

包含 AID 的 ASN.1 对象的标志和长度，如存在于 ATR 的历史字节中，应该按 ISO/IEC 7816-4 编码。

4.8.4 数据单元的使用

1. 应用标识符

应用标识符使 IFD 能：

——确定可以在卡中初始化的应用；

——识别在卡中一个特定应用的访问方法。

2. 检索应用标识符

如果卡中提供了应用标识符检索，在 DIR 文件和/或 ATR 文件中，可以读到应用标识符，正如在 ISO/IEC 7816-4 中所定义的。

对于单一应用卡，AID 可在历史字节中找到。

3. 应用选择

卡支持下列应用选择方法：

(1) 使用 AID 直接应用选择

使用 Select File 命令来选择，指定 AID 为 DF 名(专用文件名)。

(2) 使用 DIR 文件或 ATR 文件选择

一个 DIR 文件包含一序列应用模板 ASN.1 对象或 AID ASN.1 对象，这样的序列可存在 ATR 文件中。

(3) 隐含应用选择

在 ATR 或 PTS 后，可以隐含选择一个应用，这是在历史字节中指示的。

建议多应用卡不要使用隐含应用选择。

4. '命令执行'ASN.1 对象的使用

该 ASN.1 对象包含有关应用程序选择的命令消息，如果几个这样的对象相关于一个应用，这些命令应按给出的顺序执行。

4.8.5 标识符的注册

1. 请求分配 RID

一个已命名和识别的应用提供者，可以使用表 4.8.4 的格式，向他的国家标准化团体提出分配 RID 的要求。在没有国家标准化团体的情况下，应向负责 ISO/IEC 7816-5 的 ISO 技术团体秘书处提要求，于是国家标准化团体(或负责 ISO/IEC 7816-5 的 ISO 技术团体的秘书处)作为该请求的主管当局。

2. 主管当局

(1) 请求分配

分配 RID 的请求可以通过以下团体提交给注册当局：任何 ISO 的成员团体；负责 ISO/IEC 7816-5 的 ISO 技术团体；任何被 ISO 进行了有关 RID 授权的组织。

(2) 主管当局的责任

① 从他们负责的国家或地区接收 RID 的注册表；

② 提交给注册当局请求 RID 的注册表，这些注册表遵循 ISO/IEC 7816-5 标准。

3. 注册当局

按照 ISO 指导的对注册当局的任命和操作规则，ISO 理事会指定：

KTAS

ISO/IEC 7816-5 Registration authority

Teglholmsgrade 1

DK-1790 Copenhagen V

作为注册当局。

注册当局的责任：

(1) 分配应用提供者号，注册 RID 并通知主管当局安排这些请求；

(2) 保持分配给应用提供者标识符的注册表；

(3) 每年向负责 ISO/IEC 7816-5 的 ISO 技术团体秘书处提交注册表拷贝；

(4) 国家标准化团体要求一份注册表拷贝的要求成为可能，该拷贝提供后不可散发到任何第三者。

5. 注册管理组(RMG)

其责任由负责 ISO/IEC 7816-5 的 ISO 技术团体决定。

表 4.84 请求注册应用提供者标识符的注册表

1. 由申请组织填写

组织名称	
注册地址	
主要联系组织	
电话号码	传真号码
通信/汇款地址	
日期	签名

2. 由国家标准化组织填写

请求接收者	
日期	签名

3. 由 ISO/IEC 7816-5 注册当局填写

注册应用提供者标识符	
日期	签名

思 考 题

1. 在 ISO/IEC 7816-4 中定义了哪几种文件？对每一种 IC 卡来讲是否都是必须有的？
2. 在 ISO/IEC 7816-4 中所讲的命令是否就是智能卡中的微处理器指令？如不同的话，请说明它们的主要差别。
3. 请说明 4 种基本文件结构的主要特征。
4. 请说明命令 APDU 的结构。其中哪些内容是必须有的？
5. 应答 APDU 包含哪些内容？当命令正确执行时返回什么样的状态字节？
6. 写二进制命令(Write Binary Command)可执行哪几种操作？
7. 读二进制命令和读记录命令各对什么 EF 结构起作用？如文件结构不满足要求，将发生什么情况？
8. 名词解释：安全状态、安全属性和安全机制。
9. 在复位应答之后，IC 卡与读写之间是怎样配合工作的？是否 IC 卡和接口设备都有可能发命令？
10. 在 ISO/IEC 7816-4 所推荐的命令中，有哪些命令主要是为了安全或相互认证而引入的？在实际应用时，为了满足符合国际标准的要求，所有公司所确定的命令是否应该完全一致？
11. IC 卡接收到接口设备发来的命令后，如何实现命令所规定的功能？
12. 历史字节中包含哪些内容？

第5章　智能卡的安全和鉴别

随着智能卡应用范围的不断扩大，针对智能卡的各种各样的攻击性的犯罪现象已经出现，而且有增长的趋势，因此智能卡的安全和保密性显得日益重要。本章将介绍智能卡目前采用的一些安全保证措施，诸如身份鉴别技术、报文鉴别技术和数字签名技术，采用这些安全技术可以保证智能卡的内部信息在存储及交易过程中的完整性、有效性和真实性，防止对智能卡进行非法的修改。不过，无论采取什么样的手段和方法，在设计智能卡的安全和鉴别体制时，我们都应遵循以下的基本原则，即简单、实用、易于操作、价格合理，这样的系统才有竞争力。

5.1　对智能卡安全的威胁

在智能卡的生命周期中，可能会受到各种各样的攻击，它们中间有些是无意识的行为，例如在交易过程中可能出现的一些误操作；有些则是蓄意的，例如使用非法卡作弊、截取并篡改交易过程中所交换的信息等行为。根据各种攻击所采用的手段和攻击的对象的不同，我们一般可以把它们归纳为以下三种方式：

1. 第一种行为是使用伪造的智能卡，以期进入某一系统。例如：像制造伪钞那样直接制造伪卡；对智能卡的个人化过程进行攻击；在交易过程中替换智能卡，等等。

所谓个人化进程是指IC卡发给个人时，由发行商向卡内写入发行商代码、用户密码以及金额等的过程。个人化后将卡交给持卡人使用。

2. 第二种行为是冒用他人遗失的，或是使用盗窃所得的智能卡，以图冒充别的合法用户进入系统，对系统进行实质上未经授权的访问。这类行为还包括私自拆卸、改装智能卡的读写设备。

3. 第三种行为则是一种主动攻击方式。它是直接对智能卡与外部通信时所交换的信息流（包括数 据和控制信息）进行截听、修改等非法攻击，以谋取非法利益或破坏系统。

对应于这三种形式的犯罪行为，我们将从相应的三个方面对智能卡的安全进行讨论。这三个方面是：智能卡的物理安全，个人身份鉴别以及智能卡的通信安全和保密。后两个方面本质上都属于智能卡的逻辑安全范畴。

5.2　物 理 安 全

智能卡的物理安全实际上包括两个方面的内容：一是智能卡本身物理特性上的安全保证；二是指能够防止对智能卡的外来的物理攻击，即制造时的安全性。

智能卡本身的物理特性必须做到能够保证智能卡的正常使用寿命。因此，在设计制造智能卡时，应该确保其物理封装的坚固耐用性，并且必须做到能够承受相应的应力作用而

不致损坏;能够承受一定的程度的化学、电气和静电损害。另外,智能卡的电触点也必须有保护措施,使之不受玷污的影响。一般而言,在这一方面的安全性要求与智能卡的具体设计方案和制造时的材料选择有关。

对智能卡的物理攻击则包括制造伪卡、直接分析智能卡存储器中的内容、截听智能卡中的数据以及非法进行智能卡的个人化等手段。为了保证智能卡在这一方面的安全,一般应该采取如下的一些措施:

1. 在智能卡的制造过程中使用特定的复杂而昂贵的生产设备,同时制造人员还需要具备各种专业知识或技能,以增加直接伪造的难度,甚至使之不能实现;

2. 对智能卡在制造和发行过程中所使用的一切参数都严格保密;

3. 增强智能卡在包装上的完整性。这主要包括给存储器加上若干保护层,把处理器和存储器做在智能卡内部的芯片上,选用一定的特殊材料(如对电子显微镜的电子束敏感的材料)。防止非法对存储器内容进行直接分析;

4. 在智能卡的内部安装监控程序,以防止对处理器/存储器数据总线及地址总线的截听,而且,设置监控程序也可以防止对智能卡进行非授权的个人化;

5. 对智能卡的制造和发行的整个工序加以分析,以确保没有人能够完整地掌握智能卡的制造和发行过程,从而在一定程度上防止可能发生的内部职员的犯罪。

5.3 逻辑安全

智能卡的逻辑安全主要是由下列途径来实现的。

5.3.1 用户鉴别

逻辑安全的首要问题是验证持卡人的身份,减少智能卡被冒用的可能性,这一过程被称为用户鉴别,也叫做个人身份鉴别。用户鉴别可以采用若干种方法来实现,目前在这一方面使用得最多的方法就是通过验证用户个人识别号(Personal Identification Number)来确认使用 IC 卡的用户是不是合法的持卡人。验证过程大致如下:

持卡人利用读写设备的键盘向 IC 卡输入 PIN,IC 卡把它和事先存储在卡内的 PIN 加以比较,比较结果在以后访问存储器和执行指令时作为参考,用来判断可否访问或执行。根据使用要求,如果在一定的连续次数以内(通常设定为 3 至 4 次)没有输入正确的 PIN,IC 卡就判定现在的用户不是合法的持卡人,并且将自己锁定,禁止以后的操作。这样可以防止非法持卡人对 PIN 进行多次猜测的情况,这一过程如图 5.1 所示。

在验证过程中,由于智能卡内含有处理器芯片,因此把 PIN 的比较过程放到智能卡的内部去完成,这样也就减少了内部 PIN 暴露的可能性。但是,从图中也可以看出,由于在终端机和卡片之间采用的是明码 PIN 传送,因此这种方式的抗攻击能力不强,持卡人输入的 PIN 容易被人窃取而暴露。为了克服这一缺点,针对具有密码计算能力的 CPU 卡,人们又提出了一种带密码运算的 PIN 验证方法 ,如图 5.2 所示(参见 5.5 节)。

采用上述方法明显增强了 PIN 验证的可靠性和准确性。

PIN 认证技术从一个方面解决了验证持卡人身份的问题,但是从它的本质上看,它能

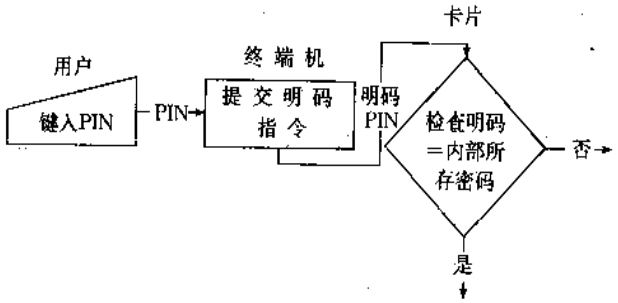


图 5.1 PIN 明码比较过程

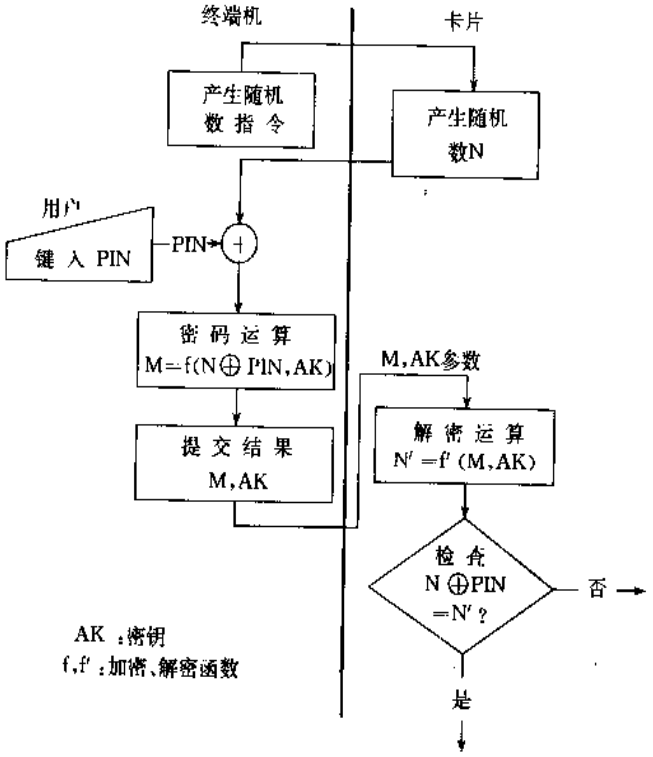


图 5.2 PIN 密码运算鉴别方法

证明的只是当前使用智能卡的用户知道这张卡片的 PIN 号，这与证明持卡人是该智能卡的真正合法授权人并不等同。因为常常有一些用户为了不忘记 PIN 号，就直接把它记在自己的智能卡上，这样一旦失窃，就会被非法分子所利用；而且一般用户往往还会不经意地泄露自己的 PIN 号，所以如果要保证智能卡达到较高的安全水平，仅仅使用 PIN 认证技术是不够的，必须使用一些新的安全防护方法。下面介绍两种常见的方法：利用人的生物特征的生物鉴别方法和利用人的下意识特征进行验证的鉴别技术。

人的生物特征具有很高的个体性，世界上没有两个人的生物特征是完全相同的，而且人的生物特征是无法伪造的，因而生物鉴别技术的安全性很高。实际上，人们使用生物鉴

别技术的历史已经很长了，例如人们很早就在侦破犯罪案件的过程中使用指纹、血液等生物特征来识别罪犯。生物鉴别技术包括指纹、血液、体形、手型、语音和视网膜鉴别技术，它在智能卡中的应用是基于生物统计学的规律。表 5.1 列出了一些常用的生物鉴别技术及其相应的一些重要参数。表中的“拒绝失败率”是指对不应该接受的特征没有拒绝的概率，“接受失败率”是指对应该接受的特征没有正确接受的概率，二者之间相对于不同安全要求的系统有不同的平衡关系，对安全要求高的系统拒绝失败率应低，反之则可以稍高一些。使用生物鉴别技术一般需要比较大的存储容量，相应的费用也高，所以目前这种技术在智能卡中还没有得到广泛的应用。但是随着存储器芯片集成度的不断提高，生物鉴别技术的应用正日益成为智能卡发展的趋势。

表 5.1 生物鉴别技术一览

	需要容量(bytes)	拒绝失败率(%)	接受失败率(%)
动态手写签名	40—60	1.0	0.5
手形	10—30	<1.0	1.5
指纹	300—800+	1.0	0.025
语音	100—500	3.0	<1.0
视网膜	40—80	<1.0	可忽略

类似于人的生物特征，人的下意识动作也具有一定的特征。这方面常见的例子是手写签名。手写签名作为一种身份鉴别方法也有较长的历史了，例如签订合同、签署协议时都需要有相应负责人的签字，因为每个人签名时书写所用力度、笔迹特点等都是不一样的，根据这些特征就能够识别出签名人。

总的来说，这些新的方法大多利用了生物统计学的规律，其技术复杂，需要的存储量大，还需要在实践中加以验证和改进。因此目前 PIN 验证方法仍然被广泛地使用。

5.3.2 存储区域保护

存储区域保护是指把智能卡的数据存储器划分成若干个区，对每个区都设定各自的访问条件；只有在符合设定条件的情况下，才允许对相应的数据存储区域进行访问，如表 5.2 所示(O 为允许，×不允许)。需要指出的是，表 5.2 中例举的存储区域，其访问条件的设定因用途不同而不同，因此表中的条件设定不具有普遍性，仅供参考。

表 5.2 存储区域保护示意

存储区域	确认发行密钥以后		确认 PIN 以后		确认 PIN 以前		数据例
	读	写	读	写	读	写	
条件 1 区	O	O	×	×	×	×	加密密钥
条件 2 区	×	×	O	O	×	×	交易数据
条件 3 区	O	O	O	×	×	×	户头名、存取权限
条件 4 区	O	O	O	×	O	×	用户姓名、住址

通过存储区域的划分，普通数据和重要数据被有效地分离，各自接受不同程度的条件保护，相应地提高了逻辑安全的强度。

5.3.3 智能卡的通信安全与保密

智能卡的通信安全与保密和个人身份鉴别一样，也属于智能卡的逻辑安全范畴。而且通信安全与保密也是智能卡的安全特性中最为重要的一个方面，因为无论一张卡使用的目的是什么，它都必须与别的设备(或者是读写设备，或者是银行主机……)进行通信。同时也由于智能卡自身已具备了存储及计算的能力，完全可以将它看作是一台袖珍型的计算机，因此它也在卡类系统中第一次提供了端到端的安全控制。

一般而言，在通信方面对信息的修改可以有许多不同的方法，主要的包括以下方式：

1. 对信息内容进行更改、删除、添加；
2. 改变信息的源点或目的点；
3. 改变信息组/项的顺序；
4. 再次利用曾经发送过的或者是存储过的信息；
5. 篡改回执。

从安全的角度考虑，就是要针对以上的这些攻击手段采取适当的技术防范措施，以求达到保证智能卡与外部设备进行信息交换的过程的有效性与合法性的目的。具体而言，即是要保证该交换过程的完整性(Integrity)、真实性(Authenticity)、有效性(Validity)和保密性(Privacy)。这里，完整性是指智能卡及系统必须能检测出在它们之间交换的信息是否已经被修改了，无论这种修改是无意的还是蓄意的；有效性是指卡和系统能把真正合法的信息与一个非法人员所发的欺骗信息(这种信息可能是他在以前所截听到的一些合法的交易信息)正确区分开，既能保证合法交易的进程，又能防止可能的诈骗行为；真实性是指智能卡和系统都必须有一种确证能力，能够确证它们各自所收到的信息都确实是真正由真实对方发出的信息，而且自己所发出的信息也确实是被真正的对方所接受到了；保密性则是指利用密码术对信息进行加密处理，从而防止非授权者窃取所交换的信息。满足这四种特性的要求是保证一个信息交换过程安全性的最基本条件，缺一不可。

首先是对完整性的保证。为了保证所交换的信息内容不被非法修改，对之进行鉴别是非常重要的，这种鉴别称为对报文内容的鉴别。一般方法是在所交换的信息报文内加入一个报头或报尾，称其为鉴别码。这个鉴别码是通过对报文进行的某种运算而得到的，它与报文的内容密切相关，报文的正确与否可以通过这个鉴别码来检验。鉴别码由报文发送方计算产生，并和报文一起经加密后提供给接收方，接收方在收到报文后，首先对之脱密，然后用约定的算法计算出脱密报文的鉴别码，再与收到报文中的鉴别码相比较，如果相等，则认为报文是正确的；否则就认为该报文在传输过程中已被修改过，接收方可以采取相应的措施，如拒绝接收或者报警等。在鉴别过程中，鉴别算法的设计是至关重要的，最简单的算法是计算累加和，即把所传输报文中的所有位全加起来作为该报文的鉴别码。比较理想的鉴别算法一般是与密码学相联系的。不过，与加密算法相比较，鉴别过程不需要脱密运算，所以鉴别算法在设计上比加密算法要简单。采用这种鉴别方式，则鉴别过程的安全性就取决于鉴别算法的密钥管理的安全性。采用密码鉴别的一个例子是 Sievi 在 1980 年向

OSI 提出的 DSA(Decimal Shift and Add)鉴别算法。该算法将要鉴别的信息看作是一个十进制数串，然后利用两个秘密的十位长的十进制数作为密码，对该数串进行相应的运算，产生出鉴别码。下面将介绍 DSA 算法的详细过程。

该算法在收发双方同时利用两个十位长的任选的十进制数 b_1 和 b_2，作为密钥。将要鉴别的信息看成是十进制数串，然后分组，十位为一组。每次运算取一组，两个运算流并行进行，直到所有信息组运算完为止。举例如下：

用 R(X)D 表示对 D 循环右移 X 位，如 D=1234567890，则 R(3)D=8901234567。

用 S(3)D 表示：$S(3)D=R(3)D+D \pmod{10^{10}}$。

在上例中，S(3)D 可由以下计算得出：

```
R(3)D= 8901234567
+   D= 1234567890
-----------------
S(3)D= 0135802457
```

假设信息 M=15834926375283586 9，鉴别码的计算过程如下：

首先将信息分成十位一组，最后一组不足十位时补零，所以 $m_1=1583492637$，$m_2=5283586900$。又任选密钥 b_1 和 b_2，设 $b_1=5236179902$，$b_2=4893524771$，两运算流同时进行。

运算流 1		运算流 2		
m_1	1583492637	m_1	1583492637	
+ b_1	5236179902	+ b_2	4893524771	
p	=6819672539	q	=6477017408	——第一个中间运算结果
+ R(4)p	=2539681967	+ R(5)q	=1740864770	—— p 的移位次数由 b_2 第一位决定
				—— q 的移位次数由 b_1 第一位决定
S(4)p	=9359354506	S(5)q	=8217882178	——第一次运算结果
+ m_2	=5283586900	+ m_2	=5283586900	
u	=4642941406	v	=3501469078	——第二个中间运算结果
+ R(8)u	=4294140646	+ R(2)v	=7835014690	—— u 的移位次数由 b_2 第二位决定
				—— v 的移位次数由 b_1 第二位决定
S(8)u	=8937082052	S(2)v	=1336483768	——第二次运算结果

至此，两组信息已运算完毕，得到两个十位长的十进制数，再组合一下，最简单的方法是将它们按模 10^{10} 加起来。

```
  S(8)u  8937082052
+ S(2)v  1336483768
-------------------
         0273565820
```

其结果即为鉴别码。

关于信息交换过程的有效性，主要是为了防止对曾经发送过的或存储过的信息的再利用。例如在某次交易过程中的一条真实信息(假设是某人从银行帐号内提取了一笔钱

款)，如果这一消息被一个非法截听者记录了下来，他就有可能一遍遍地重发该消息，如果不能进行报文有效性的验证，那么该人银行帐号内的存款将很快就被提光。由此可见，有效性本质上是对报文时间性的鉴别，即它必须能保证所传送的消息每一条都是唯一的，任何随后产生的重复消息都应当被认为是非法的。实现这种报文时间性鉴别的方法有很多种，常用的方法是每条消息在发送时都附加一个发送当时的日期和时间；或者可以在所发消息中加入一个记录消息个数的数；还可以在报文中加入一个随机数。总之，实现报文时间性鉴别的方法可以归为两大类，第一种方法是收发方预先约定一个时间变量，然后用它作为初始化向量对所发送的报文加密，第二种方法也是由收发双方预先约定一个时间变量，然后在发送的每份报文中插入该时间变量，从而来保证报文的唯一性。采用这些时间性鉴别的方法，显然还能防止在传送过程中可能发生的对信息组顺序的改变。

至于真实性，指的是对报文发送方和接收方的鉴别，即对话的双方彼此都要对对方的真实性进行验证，这种验证称为双向鉴别。智能卡和主机之间的相互鉴别是消息认证和电子签名的基础，在智能卡技术中占有很重要的地位。双向鉴别的具体内容将在第 5.5 节中，即在密码技术之后讨论。

在完成双向鉴别之后，为了保证传输过程中信息的安全性，对每条信息也应该进行报文源的鉴别，否则将无法确定一个具体报文的发送者。例如，某一非法截听者截收了一条由智能卡发往读写设备的报文，过后的某个时候，又把它插入到通信线路中，并改向传给智能卡。这样，智能卡就将无法正确判断出该报文是否真是由接收设备所发送。为了解决这样的问题，一是可以在报文中加上发送者的标识号，另外也可以直接通过报文加密实现。方法如下：在智能卡与接收设备的通信过程中采用两个不同的密钥，智能卡所发送的信息用一个密钥加密，并在接收端用同样的密钥脱密还原；而接收端则使用另一密钥加密它所发送的信息，然后再送给智能卡，由智能卡用相同的密钥还原信息。这样，只要双方都能正确还原出对应的信息就可以证明所接收报文的真实性。

然后是交换过程中的保密性问题。在这方面主要是利用密码技术对信息进行加密处理，以掩盖真实信息，使之成为不可读，达到保密的目的。由于加密、脱密是通信安全中最常用的技术，也是通信安全的基础之一，其地位极其重要，因此下文专门进行讨论。

5.4 密码技术

密码的出现最初即是以通信的秘密性为目的的，其基本思想就是伪装信息，使局外人不能理解信息的真正含义，而局内人却能理解伪装信息的本来意义。密码的实际应用可以追溯到远古时代。公元前 50 年，古罗马的凯撒在高卢战争中就用过一种密码技术来保证其军事命令在传输过程中的保密性。他把从 A 到 W 的每个英文字母均用字母表中它后面的第三个位置上的字母来代替表示，字母 X、Y、Z 分别用 A、B、C 表示。如果分别以数字 0、1、…、25 来对应字母 A、B、…、Z，则他的这种密码变换规则就可以表示成如下形式：

$$\Phi=\theta+3 \mod 26$$

我们把被伪装的信息称为明文，伪装后的信息称为密文，而加密时所采用的信息变换规则称为密码算法。在上式中，Φ 为密文字母，θ 为明文字母，3 就是这种密码算法的密钥。显

然，这种密码算法是十分简单的。而到了现代，随着计算机在密码学领域的广泛应用，同时也由于现代数学的发展，使现代密码学无论在原理、概念和工具上都有了巨大的创新与改进。然而另一方面，这些新的技术知识也给破译者提供了强有力的工具，从而又给现代密码学提出了新的任务。

加密，就是对机密信息加以伪装的一个过程。通常把一个加密系统所采用的基本工作方式称作密码体制。一个密码体制一般由两个基本要素构成：密码算法和密钥。这里，密码算法是一些公式、法则或者程序，一般与现代数学中的某些理论相联系；密钥则可以看作是密码算法中的可变参数。相对来说，密码算法在一个时期内是相对稳定的，变化的只是密钥。而从数学角度来看，改变密钥本质上是改变了明文与密文之间等价的数学函数关系。考虑到密码算法本身很难做到绝对地保密，因此现代密码学总是假定密码算法是公开的，真正需要保密的只是密钥，即一切秘密都蕴藏在密钥之中。所以现代密码学中，密钥管理是极为重要的一个方面。

与加密对应的是密码分析，也叫破译，是指非授权者通过各种方法窃取密文，并通过各种方法推导出加密算法和密钥，从而读懂密文的操作过程。而用以衡量一个加密系统的不可破译性的尺度称为保密强度。一般而言，一个加密系统的保密强度应该与这个系统的应用目的、保密时效要求及当前的破译水平相适应。能够达到理论上不可破译是最好的，否则也要求能达到实际的不可破译性，即原则上虽然能够破译，但为了由密文得到明文或密钥却必须付出十分巨大的计算，而不是能够在希望的时间内或实际可能的经济条件下就可以求出准确答案。

密码体制的分类很多。例如，可以按照密码算法对明文信息的加密方式，分为序列密码体制和分组密码体制；按照加密过程中是否注入了客观随机因素，分为确定型密码体制和概率密码体制；按照是否能进行可逆的加密变换，分为单向函数密码体制和双向函数密码体制。不过人们常用的是按照密码算法所使用的加密密钥和解密密钥是否相同，能不能由加密过程推导出解密过程（或者反之，由解密过程推导出加密过程）而将密码体制分为对称密码体制和非对称密码体制。

5.4.1 对称密码体制

对称密码体制又称为单钥密码体制、对称密钥密码体制、秘密密钥密码体制。在这种密码体制中，加密密钥和解密密钥是相同的，即使二者不同，也能够由其中的一个很容易地推导出另一个。在这种密码体制中，有加密能力就意味着必然有解密能力。一般而言，采用对称密码体制可以达到很高的保密强度，但由于它的加密密钥和解密密钥相同，因此它的密钥必须极为安全地传递和保护，从而使密钥管理成为影响系统安全的关键性因素。因而难以适应当今计算机系统的开放性要求。

传统的加密方法一般都属于对称密码体制。目前，在智能卡中应用较多的加密技术基本上也是对称密码体制。其中较典型的加密算法是 DES 算法。该算法是一种分组密码算法，分组密码算法的基本设计技巧是 Shannon 所建议的扩散（diffusion）和混乱（confusion）。所谓扩散，就是要将每一位明文的影响尽可能迅速地作用到较多的输出密文位中，以隐蔽明文的统计特性。扩散同时也是指把每一位密钥的影响尽可能地扩散到较

多的输出密文位中。扩散的目的是希望密文中的每一位都尽可能地与明文和密钥相关，以防止将密钥分解为若干孤立的小部分，给破译者以各个击破的可能性。所谓混乱是指密文和明文之间的统计特性的关系应该尽可能的复杂化，要避免出现很有规律的、线性的相关关系。在分组密码算法的设计中还要考虑的一个问题是如何保证明文与密文的一一对应关系。因为如果加密算法设计不当，就有可能会使多个明文状态对应同一密文状态，使解密出现困难。

在这种算法的设计上，比较成功的例子就是 DES 算法。DES 的全称是 Data Encryption Standard(数据加密标准)，它是 IBM 公司于 1975 年研究成功并公开发表的，这也开创了公开全部算法的先例。1977 年，美国国家标准局宣布 DES 用于非国家保密机关。此后，DES 算法得到了广泛应用，并出现了专门处理 DES 加密算法的硬件，下面简单介绍该算法。

DES 算法是把 64 位的明文输入块变换为 64 位的密文输出块，它所使用的密钥也是 64 位的，整个算法的流程如图 5.3 所示。要加密的一组数据先经过初始置换 IP 的处理，

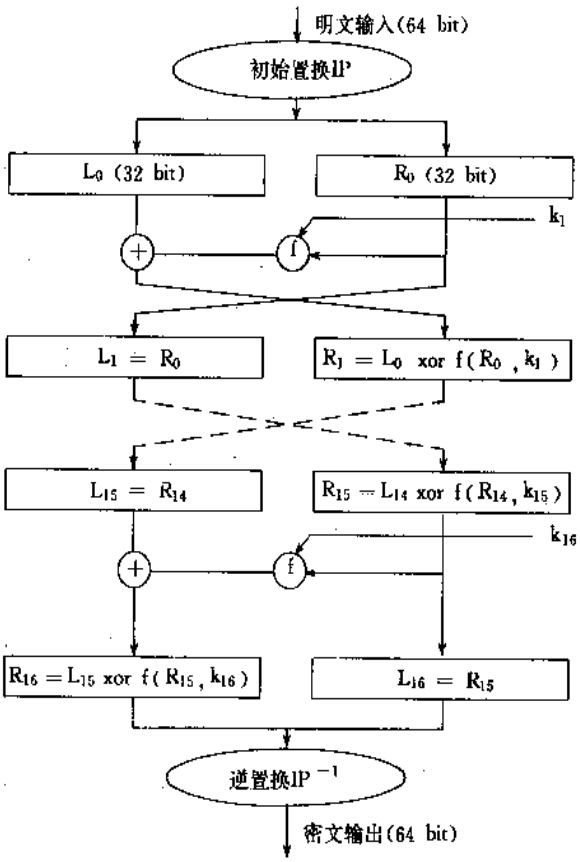


图 5.3 DES 算法

然后通过一系列迭代运算，最后经过 IP 的逆置换 IP^{-1} 给出加密的结果。图 5.3 中，k_i(i=1—16)是初始密钥 K 经分解、移位后产生的 48 位长的子密钥。由图中可见，与密钥有关的算法包括子密钥的生成和密码函数 f。

首先，我们讨论初始置换 IP，IP 的功能是将输入的 64 位数据块按位重新组合，并把

输出分为 L_0、R_0 两部分，每部分各长 32 位。重新组合的规则见表 5.3。

表 5.3　初始置换 IP

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

即将输入的第 58 位换至第 1 位，第 50 位换至第 2 位，依此类推，最后一位是原来的第 7 位。L_0 和 R_0 则是换位输出后划分的两部分，L_0 是输出结果的左边 32 位，对应地，R_0 就是右边的 32 位。即，如果令置换前的输入值为 $b_1b_2\cdots b_{64}$，则经过初始置换后的结果为：

$$L_0=b_{58}b_{50}\cdots b_8 \quad ; \quad R_0=b_{57}b_{49}\cdots b_7。$$

接下来就是迭代过程，将 R_0 与子密钥 k_1 经密码函数 f 的运算得到 $f(R_0,k_1)$，与 L_0 按位模 2 加得到 R_1，将 R_0 作为 L_1，就是完成了第一次迭代，依此类推，第 i 次的迭代可以表示为：

$$L_i=R_{i-1}$$

$$R_i=L_{i-1} \text{ xor } f(R_{i-1},k_i)$$

其中的 xor 表示按位作模 2 加。在迭代过程中，重要的部分是函数 f。f 的结构如图 5.4 所

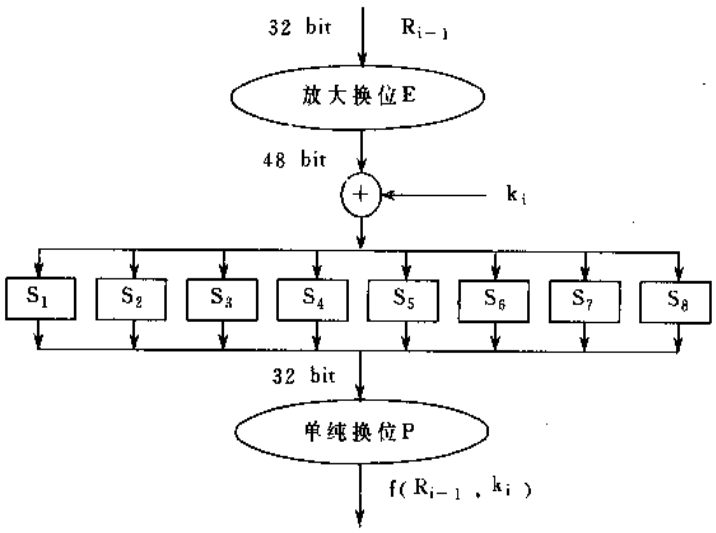


图 5.4　$f(R_{i-1}, k_i)$函数

示。它的功能是利用放大换位表 E(如表 5.4 所示)将 32 位的 R_{i-1} 扩展至 48 位，与子密钥 k_i 按位模 2 加后，把结果分为 8 个 6 位长的数据块，再分别经选择函数 S_1、S_2…S_8 的变

换，产生 8 个 4 位长的块，合为 32 位，最后经过单纯换位 P(见表 5.5)得到输出。

表 5.4　放大换位表 E

32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

表 5.5　单纯换位表 P

16	7	20	21
29	12	28	17
1	15	23	26
5	18	31	10
2	8	24	14
32	27	3	9
19	13	30	6
22	11	4	25

其中，S_i 的变换规则见表 5.6，其完成的功能都是把 6 bit 的输入转化为 4 bit 输出。

表 5.6　选择函数 S_i

R \ h	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7	
1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8	S_1
2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0	
3	15	12	8	2	4	*9	1	7	5	11	3	14	10	0	6	13	
0	15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10	
1	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5	S_2
2	0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15	
3	13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9	
0	10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8	
1	13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1	S_3
2	13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7	
3	1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12	
0	7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15	
1	13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9	S_4
2	10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4	
3	3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14	
0	2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9	
1	14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6	S_5
2	4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14	
3	11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3	
0	12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11	
1	10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8	S_6
2	9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6	
3	4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13	
0	4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1	
1	13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6	S_7
2	1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2	
3	6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12	
0	13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7	
1	1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2	S_8
2	7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8	
3	2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11	

以 S_1 为例说明其功能，例如，设输入为：

$$B=b_1b_2b_3b_4b_5b_6$$

由 $b_2b_3b_4b_5$ 代表 0—15 间的某一数，设为 h；由 b_1b_6 代表 0—3 之间的某一数，设为 R，即：

$$h=b_2b_3b_4b_5$$

$$R=b_1b_6$$

然后在 S_1 表的第 R 行第 h 列得一个数 S，以 4 位二进制表示之，即 $S=s_1s_2s_3s_4$，此即为输出。

经过 16 次迭代运算后，得到 $R_{16}L_{16}$，将之作为输入，进行逆置换 IP^{-1}，即得到密文。IP^{-1} 完成的功能正好是 IP 的逆过程，例如第 1 位经过 IP 置换处于第 40 位，而经过 IP^{-1} 换位，又将第 40 位换回第 1 位，其变换规则如表 5.7 所示。

表 5.7　逆置换 IP^{-1}

40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25

下面介绍子密钥的生成。子密钥 k_i 的生成过程如图 5.5 所示。

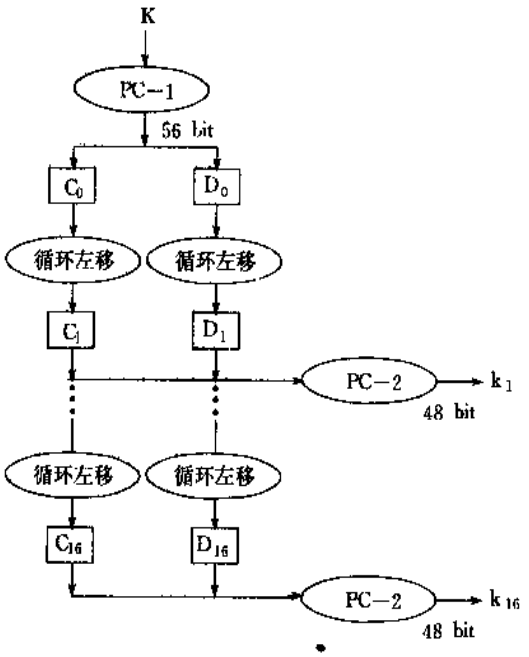


图 5.5　子密钥的生成

密钥 K 本身为 64 位，但其中第 8、16、24、…、64 位是奇偶校验位，所以 K 实质只有 56 位，将这 56 位的数据经过选择换位 PC－1(换位规则见表 5.8)后产生的结果分为两部分 C_0、D_0，分别是左、右各 28 位，然后分别经过循环左移位，得到 C_1、D_1，合并后，再经缩小换位 PC－2(见表 5.9)，即得到 48 位的子密钥 k_1。同样，将 C_1、D_1 经过循环左移，合并后，再经缩小换位 PC－2，得到子密钥 k_2，依此类推可以产生 k_3、…、k_{16}。不过，对应的循环左移位的次数(即位数)要按照表 5.10 的要求。

表 5.8　选择换位 PC－1

57	49	41	33	25	17	9
1	58	50	42	34	26	18
10	2	59	51	43	35	27
19	11	3	60	52	44	36
63	55	47	39	31	23	15
7	62	54	46	38	30	22
14	6	61	53	45	37	29
21	13	5	28	20	12	4

表 5.9　缩小选择换位 PC－2

14	17	11	24	1	5
3	28	15	6	21	10
23	19	12	4	26	8
16	7	27	20	13	2
41	52	31	37	47	55
30	40	51	45	33	48
44	49	39	56	34	53
46	42	50	36	29	32

表 5.10　循环移位次数

迭代次数	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
左移位数	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

以上介绍了 DES 的加密过程，DES 的脱密算法是一样的，只是在第一次迭代时使用 k_{16}，第二次使用 k_{15}…，最后一次用 k_1，算法本身没有任何变化。

DES 算法的安全性在于攻击者破译的方法除了穷举搜索外还没有更有效的手段，而 56 位长的密钥的穷举空间是 2^{56}，这意味着如果一台计算机的速度是一秒钟检测一百万个密钥，则它搜索完全部密钥就需要近 2000 年的时间，可见 DES 算法的保密强度还是比较高的。当然，随着科学技术的发展，更高速计算机及分布式计算机的出现，可能会使 DES 的密钥长度再增长一些，才能达到一定的保密强度。

对称密码体制的密钥使用了一段时间以后就需要更换，加密方需通过某种秘密渠道把新密钥传送给解密方。在传递过程中，密钥容易泄露。而对下面将要介绍的非对称密钥体制，由于加密密钥与解密密钥不同，且不能用加密密钥推出解密密钥，从而使加密密钥可以公开传递。

由于对称密码体制的加密密钥和解密密钥是相同的，在智能卡中采用 DES 算法，当信息的收发方对信息内容及发送源点产生争执时，DES 算法就显得无能为力了。典型的例子是发送方可能是不诚实的，由于他发送的信息可能对他不利，因此他就可以利用加密算法直接修改他所发送的信息在己方的记录内容，并谎称他发送了真实消息，而反称接收方伪造了该消息，而接收方又无从证明该消息确实是由发送方发过来的。在这一争执中，作为仲裁的第三方也无法区分哪一种情况是真实的。造成这种情况的原因在于双方都拥

有同样的加密算法和密钥，而使用非对称密码体制可以消除这种争执。

5.4.2 非对称密码体制

非对称密码体制又叫做双钥密码体制、公开密码密钥体制。在这种密码体制中，一个加密系统的加密和解密能力是分开的，加密和解密分别通过两个不同的密钥实现，并且由其中的一个密钥推导出另一个密钥是不可行的。采用非对称密码体制的每个用户都有一对选定的密钥，其中一个可以公开，称为公开密钥，简称为公钥，另一个由用户自己秘密保存，称为密钥。

非对称密码体制的思想是 W. Diffie 和 M. E. Hellman 于 1976 年在《密码学的新方向》一文中首先提出的，它的出现是现代密码学研究的一次重大突破。与传统的对称密码体制相比较，非对称密码体制具有如下的一些优点：

1. 密钥分发简单。由于加密和解密密钥不同，而且不能从加密密钥推导出解密密钥。因而加密密钥表可以象电话号码本一样分发；

2. 秘密保存的的密钥量减少。每张智能卡只需秘密保存自己的解密密钥。N 张智能卡和 M 个主机相互鉴别只需产生(N+M)对密钥；

3. 公钥的出现使得非对称密码体制可以适应开放性的使用环境；

4. 可以实现数字签名。所谓数字签名，主要是为了保证接收方能够对公正的第三方(仲裁方)证明其收到的报文的真实性和发送源的真实性而采取的一种安全措施。它的使用可以解决上一节最后提到的那种由于收发方的不诚实而产生的争执，即可以保证收发方不能根据自己的利益来否认或伪造报文。

但是，目前非对称密码体制也存在一些问题需要解决。这里最为重要的一点是它的保密强度目前还远远达不到对称密码体制的水平。迄今为止所发明的非对称密码体制大部分被破译，剩余的几种也不能证明完全不存在缺陷。而且，由于非对称密码体制不仅算法是公开的，而且公开了加密密钥，从而就提供了更多的信息可以对算法进行攻击，结果使这种算法的设计相对受到限制。此外，至今为止，所发明的非对称密码算法都是很容易用数学公式来描述的，因此它们的保密强度总是建立在对某一个特定数学问题求解的困难性上，然而，随着数学的发展，许多现在看起来难以解决的问题可能在不久的将来会得到解决；而诸如 DES 之类的对称密码算法甚至难以表示成一个确定的数学形式，其保密强度因此相应地要高，这也是非对称密码体制目前的一个不足之处。尽管如此，由于非对称密码体制的优点还是很明显的，而且在某些特殊的场合也不得不使用非对称密码体制，因此对非对称密码体制的研究一直在进行中，其中最为著名的一个例子就是 RSA 算法。

RSA 算法是由 Rivest、Shamir 和 Adleman 三个人提出来的，从提出到现在已经经历了十多个年头，经受了各种攻击的考验，被认为是目前最优秀的非对称密码方案之一，国外也已经研制出了多种的 RSA 专用芯片。下面对 RSA 算法本身加以简单介绍。

RSA 算法也是一种分组密码算法，它以数论为基础，其安全性是建立在大整数的素数因子分解的困难性上的，后者在数学上至今还没有一种有效的算法。要建立一个 RSA 密码系统，首先任意选取两个大素数 p、q，使

$$n = p \cdot q,$$

并得到 Euler 函数：

$$\phi(n) = (p-1)(q-1),$$

然后，任意选择一个与 $\phi(n)$ 互素的小整数 e 作为加密密钥，再根据 e 求出解密密钥 d，d 满足：

$$de \equiv 1 \bmod \phi(n)。$$

事实上，加密密钥 e 和解密密钥 d 在功能上是完全可以互换的，因此在生成 e、d 时，不论先假设哪一个，再由它去求另一个都是可以的。在这些参数(p、q、n、$\phi(n)$、e、d)中，p、q、$\phi(n)$、d 是保密的，n、e 则是公开的。有了这些参数，就能进行加密和脱密运算了。

加密之前，先将明文(以 m 表示)数字化，并把明文分成长度小于 log n 位的明文块，以确保每个明文块值不超过 n。对明文 m 加密的过程是：

$$c \equiv E(m) = m^e \bmod n,$$

式中，c 即为密文。而脱密过程则是：

$$m \equiv D(c) = c^d \bmod n。$$

利用 Euler 定理可以证明该加密/脱密过程的一致性，具体的证明过程在这里不加论述。

下面举例说明 RSA 加密算法。

(1) 设计密钥

设素数 $p=5$，$q=17$，公开密钥 $e=19$(实际应用时，应选大素数，以满足安全的需要)。

计算：　$n = p \cdot q = 5 \times 17 = 85$

$\phi(n) = (p-1)(q-1) = 4 \times 16 = 64$

其中 n 与 e 是公开的：$n=85$，$e=19$

(2) 计算解密密钥 d

采用转辗相除法：

首先令 $G(0)=\phi(n)$，$G(1)=e$，$V(0)=0$，$V(1)=1$，

然后进行下列运算

$$G(i+1) = G(i-1)-[G(i-1)/G(i)] \cdot G(i)$$

$$V(i+1) = V(i-1)+[G(i-1)/G(i)] \cdot V(i) \qquad i=1,2,\cdots,$$

式中除法运算的商取整数，$G(i+1)$实际上是 $G(i-1)/G(i)$的余数。

上面的运算一直进行到 $G(k)=1$ 为止，此时的 $V(k)$即为解密密钥 d。

根据上面提供的方法，进行具体计算如下：

$$G(0) = \phi(n) = 64$$

$$G(1) = e = 19$$

$$G(2) = G(0) - [G(0)/G(1)] \cdot G(1)$$

$$= 64 - [64/19] \cdot 19$$

$$= 7$$

$$V(2) = V(0) + [G(0)/G(1)] \cdot V(1)$$

$$= 0 + [64/19]$$

$$= 3$$

$$
\begin{aligned}
G(3) &= G(1) - [G(1)/G(2)] \cdot G(2) \\
&= 19 - [19/7] \cdot 7 \\
&= 5 \\
V(3) &= V(1) + [G(1)/G(2)] \cdot V(2) \\
&= 1 + [19/7] \cdot 3 \\
&= 7 \\
G(4) &= G(2) - [G(2)/G(3)] \cdot G(3) \\
&= 7 - [7/5] \cdot 5 \\
&= 2 \\
V(4) &= V(2) + [G(2)/G(3)] \cdot V(3) \\
&= 3 + [7/5] \cdot 7 \\
&= 10 \\
G(5) &= G(3) - [G(3)/G(4)] \cdot G(4) \\
&= 5 - [5/2] \cdot 2 \\
&= 1 \\
V(5) &= V(3) + [G(3)/G(4)] \cdot V(4) \\
&= 7 + [5/2] \cdot 10 \\
&= 27
\end{aligned}
$$

即秘密的解密密钥 d=27。

(3) 发送方用公开的加密密钥 e 将转换成等效数字的明文 m 加密成密文 c。

设明文为数字"2",则密文

$$c = m^e \pmod n = 2^{19} \pmod{85}$$

实际上 m 的数值很大时,m^e 是一个更大的数,给运算带来麻烦。由于 $C=A \cdot B \pmod n$ 的运算结果等效于 $C=C_1 \cdot C_2 \pmod n$,其中 $C_1=A \pmod n$,$C_2=B \pmod n$,因此可首先分别对各个数据进行模 n 运算,然后再相乘。当相乘数据个数增加时,上述关系仍成立,因此 c 的计算可按下述方法进行:

$$
\begin{aligned}
c &= 2^{19} \pmod{85} = (2^8)^2 \pmod{85} \times 2^3 \pmod{85} \\
&= 1 \times 8 \pmod{85} \\
&= 8 \pmod{85}
\end{aligned}
$$

(4) 接收方用加密密钥 d 将密文 c 转换成明文 m:

$$
\begin{aligned}
m &= c^d \bmod n = 8^{27} \pmod{85} \\
&= 2^{81} \pmod{85} \\
&= (2^8)^{10} \pmod{85} \times 2 \pmod{85} \\
&= 1 \times 2 \pmod{85} \\
&= 2 \pmod{85}
\end{aligned}
$$

下面介绍大指数模 n 运算的一种简单算法。对于软件来讲,这种算法不是最好的,但适于用硬件实现,其描述如下:

```
RSA(k、e、n、m、c)
  算法:c = m^e mod n
  k:指数 e 的二进制位数
  e(i):指数 e 的二进制数据 e(k-1),…,e(1),e(0)。e(0)是 e 的最高位。
  n:模数
  m:明文(底数)
  c:密文(运算结果)
begin
  c ← 1
  for i=k-1 to 0 step -1 do
  begin
    c←c^2 mod n
    if e(i)=1 then c←c * m mod n
  end
end
```

在 RSA 算法中,比较重要的是对素数的选择。为提高 RSA 的安全性,要求 p、q 应该是安全素数和强素数。所谓安全素数,是指 p、q 应满足:

$$p=2a+1,\ q=2b+1,$$

其中,a、b 均为奇素数。

所谓强素数,是指 p(或 q)应是一个位数足够长的随机选择的素数,而且 p+1 和 p-1 也都应该有一个大的素数因子。以外,如果条件允许,还应做到 p、q 长度相差不大,p-1、q-1 的公约数 gcd(p-1,q-1)应很小等。

至于 RSA 算法的安全性,由于无法从理论上直接把握它的保密性能,因此目前的结论仅仅是:攻破 RSA 算法不会比大数分解问题更难,因为在 RSA 算法中,n、e 是公开的,所以如果能将 n 分解为 p 和 q,则很快就可以求出 $\phi(n)$,再由 e 与 $\phi(n)$求出 d 从而攻破 RSA。但这个结论也不排除在不分解因子的条件下找到一个有效的破译方法的可能性。RSA 的成功刺激了大数分解技术的改进,使各种新技巧不断出现,今后是否会有突破性进展还难以预料,因此当准备采用 RSA 时,应当考虑上述情况。

RSA 算法的主要缺点是:密钥的产生过于麻烦,要受到素数生成技术的限制;其次,分组长度不够,而为了保证安全性,其密钥 n 要求在 500 位以上,从而使运算速度大为降低。尽管有这些缺点,采用 RSA 算法却可以很方便地解决数字签名的问题:由于发送方不知道接收方的解密密钥,从而使发送方伪造或修改已发送报文的可能性不复存在。下面就对 RSA 在数字签名上的应用作一些讨论。

假设用户 A 要传送一个签名信息 M 给用户 B,则 A 先对明文 M 作变换:

$$S \equiv M^{d_A} \bmod n_A,$$

其中,d_A 和 n_A 是用户 A 的解密密钥,只有用户 A 才掌握。然后 A 进一步利用用户 B 的加密密钥 e_B、n_B 作运算:

$$C \equiv S^{e_B} \bmod n_B,\qquad 0<C<n_B,\text{若 } n_A<n_B$$

而如果 $n_A > n_B$，则应该先将S分解为比 n_B 小的块，再进行以上运算。与此同时，A把明文M也用B的加密密钥进行加密，然后将这两个结果联合在一起送给B。对用户B，则首先用它的解密密钥恢复S和M，然后用A的加密密钥对S作运算，产生明文M′，如果M′与M相等，则用户B就可以确信信息确实是由A所发送，同时用户A也不能否认发送过这个信息，因为S的产生是通过仅有A才掌握的解密密钥 d_A、n_A 完成的，别人无法伪造，这同时也就保证了用户B无法伪造该签名，从而满足了对签名的要求。

不过目前看来，把RSA算法应用在智能卡技术中还有很多困难，由于受到卡片外形尺寸的限制，智能卡的计算能力还不强，如果使用RSA算法，将使智能卡的响应时间慢得无法忍受。当然，随着技术的进步，在智能卡技术中采用非对称密码体制是一种不可避免的趋势。

5.4.3 密钥管理

无论在智能卡中采用哪种密码体制，都要考虑一个重要的问题，就是密钥的管理。密钥是一个加密系统中的可变部分，在现代密码学公开加密算法的前提下，密钥成为了加密系统的关键。因此，密钥管理也就具有了极其重要的地位。

密钥管理是一门综合性的技术，它涉及到密钥的产生、检验、分配、传递、保管和使用、销毁的全部过程，并且与密钥的行政管理制度以及人员的素质密切相关。目前，国际标准化组织也已经开始开展密钥管理标准化的工作，并制定了密钥管理标准DIS-8732。不过总的来说，对应于具体的系统往往会有具体的实际要求，因此标准化工作事实上很难统一。对一个密钥管理系统的评价，一般可以参照以下的三点具体要求：

1. 密钥难以被非法窃取；
2. 在一定条件下，即使窃得密钥也毫无用处；
3. 密钥的分配及更换过程对用户透明。

针对以上的具体要求，现在的密钥管理系统一般采取层次结构，其基本思想是用密钥来保护密钥，即用第i层的密钥 K_i 来保护第(i+1)层的密钥 K_{i+1}，同时 K_i 本身也受到第i−1层的密钥 K_{i-1} 的保护。至于具体应该设计成几层，则由密钥管理系统的功能来确定。功能越简单，层次就可以越少，反之就可以适当增加层数。采用这种分层模式可以大大提高安全性。由于下层的密钥内容可以设计成按某种协议而不断变化，从而使整个密钥管理系统表现为一种动态的特征。

5.5 鉴别体制

相应于密码体制，智能卡的鉴别体制分为两类。

5.5.1 对称鉴别体制

目前，智能卡常用的鉴别方法是对称鉴别体制，采用如DES这样的密码算法。这种鉴别体制的特点是加密和解密采用的是一个共同的密钥。其鉴别过程如图5.6所示：在主机(或终端机)执行对智能卡的鉴别时，首先由主机产生一个随机数R，并发送给智能卡。智

能卡收到主机传来的数据 R，并结合卡内存储的密钥 K，进行加密运算 f，并产生出密文 X′。然后卡片将 X′回送给主机，主机从密钥库中检索出该卡片的密钥 K，利用 K 和 X′进行解密运算 f′，得到值 R′。如果 R′=R，则说明该智能卡是合法的。

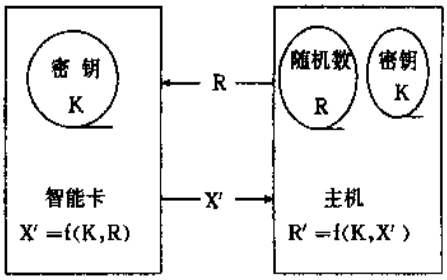


图 5.6　对称鉴别体制

同样，如果智能卡需要对主机(或终端机)进行鉴别时，也采用上述方法，只是数据流向相反，由智能卡产生随机数，并且在卡内判断主机的合法性(见图5.2)，图 5.2 同时验证了持卡人的身份。

采用对称鉴别体制的一个实际例子是法国的家庭金融系统，又称为远程支付系统(Telepayment System)，这是一种将家庭、公司的终端和金融部门的计算机用通信线路连接，实现交易、接受服务的系统。其工作规程如图 5.7 所示。

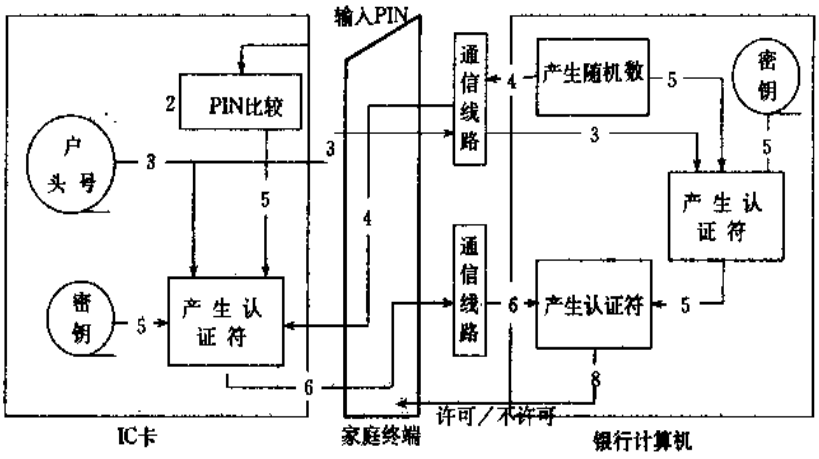


图 5.7　法国远程支付系统示意图

1. 用户输入 PIN；

2. IC 卡把输入的 PIN 和卡内的 PIN 进行比较；

3. 若比较相等，将用户的户头号送入银行计算机；

4. 银行计算机产生随机数，并送给 IC 卡；

5. 终端命令 IC 卡产生认证符。因为 PIN 比较结束，所以 IC 卡接受命令，并且采用密码算法，从加密密钥、户头号和随机数三者中产生认证符；同时银行计算机也采用同一算法产生出认证符；

6. 将 IC 卡计算出的认证符发送给银行计算机；

7. 银行计算机对两个认证符进行比较；

8. 若相等，则银行计算机确信通信的对方为送来户头号的顾客，从而允许后续交易。

对称鉴别体制的特点是加密和解密都采用同一个密钥(即使不相等，也很容易从其中

一个密钥推导出另一个密钥)。在这种体制中,加密、解密双方都必须保守密钥,不能泄露。它存在下列问题:

- 密钥使用了一段时间后就需要更换。而加密方启用新密钥后,就必须通过某种秘密途径把密钥传递给解密方。在传递过程中,密钥容易泄露;
- 如果N张卡片和M台主机进行验证,就需要NM个密钥。密钥量太大,不易管理;
- 难以解决对数据的签名和验证问题。

5.5.2 非对称鉴别体制

非对称鉴别体制又称为公开密钥鉴别体制。它把加密过程和解密过程设计成不同的途径,当算法公开时,在计算上不可能由加密密钥求解解密密钥,因而加密密钥可以公开,只需保存解密密钥。非对称鉴别体制通常以RSA算法为基础加以设计。RSA算法的具体内容在上节中已经讲述,在这里我们重点讲述其在IC卡中的应用。

总部设在巴黎的国际IC卡协会(INTAMIC)讨论了RSA密码体制在IC卡中的应用问题。图5.8表示了INTAMIC提出的,使用IC卡的POS(销售点终端)的规程方案,简介如下:

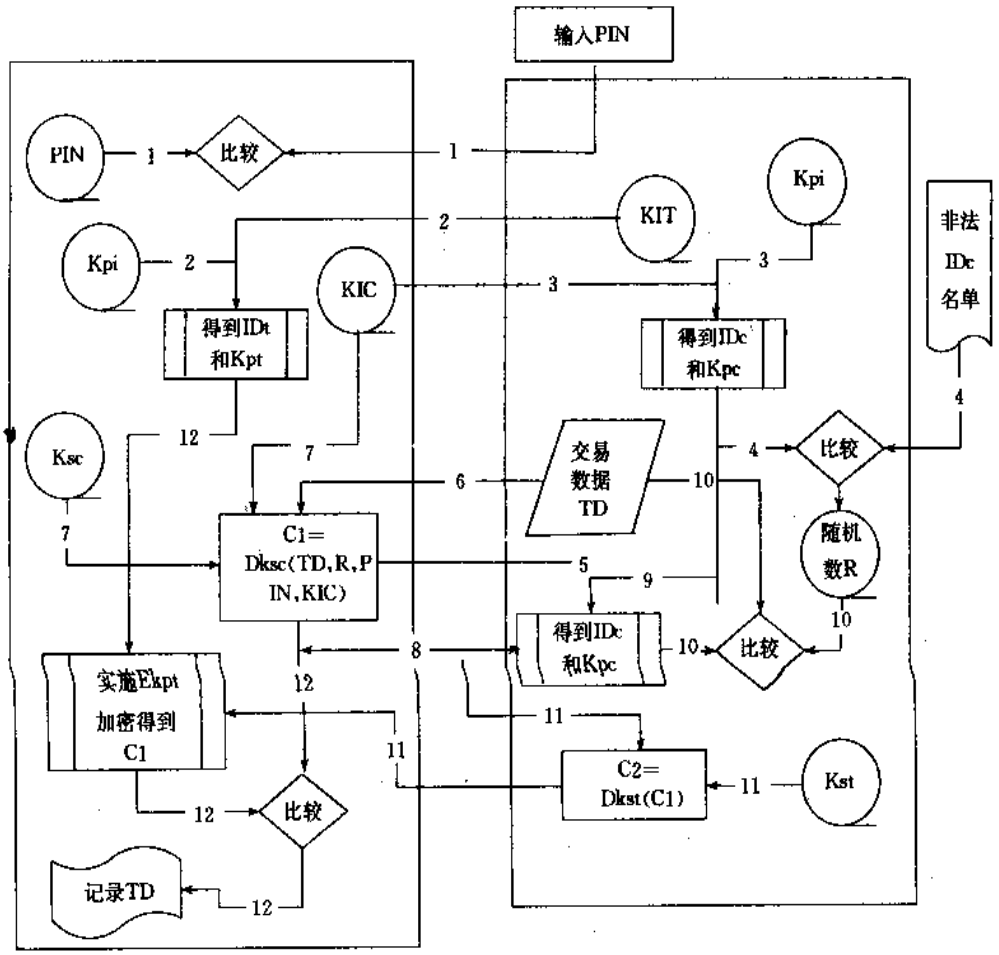


图5.8 使用IC卡的POS系统规程

图中，IDc＝智能卡 ID 号，IDt＝终端 ID 号

R＝随机数，TD＝交易数据

(Kpi,Ksi) ＝ 发行人的公开密钥和秘密密钥；

(Kpc,Ksc) ＝ 智能卡的公开密钥和秘密密钥；

(Kpt,Kst) ＝ 终端的公开密钥和秘密密钥；

KIC＝Dksi(IDc,Kpc) 用发行人的秘密密钥对智能卡的 ID 号和公开密钥进行数字签名；

KIT＝Dksi(IDt,Kpt) 用发行人的秘密密钥对终端的 ID 号和公开密钥进行数字签名。

规程的解释如下：

1. 用户输入 PIN，IC 卡进行核对；

2. 终端把 KIT 告诉 IC 卡。KIT 由发行人事先写入终端内的存储器中，IC 卡用发行人的公开密钥 Kpi 对 KIT 实施 Ekpi 加密，得到 IDt 和 Kpt；

3. IC 卡把 KIC 送入终端。KIC 由发行人事先写入 IC 卡内的存储器中，终端用发行人的公开密钥 Kpi 对 KIC 进行 Ekpi 加密，得到 IDc 和 Kpc；

4. 终端确认非法的 IC 卡名单中没有 IDc；

5. 终端产生随机数 R，并送给 IC 卡；

6. 终端把交易数据 TD 送入 IC 卡；

7. IC 卡用密钥 Ksc 做成签名文件 C1；

8. IC 卡向终端传送 C1；

9. 终端利用 3 中得到的 Kpc 对 C1 实施 Ekpc 加密；

10. 确认加密后的 TD、R 与原来的 TD、R 是否一致；

11. 终端用 Kst 对 C1 签名，并把结果 C2＝Dkst(C1)送入 IC 卡；

12. IC 卡利用 2 中得到的 Kpt 对 C2 进行 Ekpt 加密，并确认结果与原 C1 是一致的，IC 卡记录一次交易数据 TD。至此整个交换规程结束。

该系统使用 RSA 密码体制来确认 IC 卡和终端之间的正当性。例如：终端向 IC 卡送出电文 R、TD，IC 卡用自己的秘密密钥 Ksc 签名，然后终端再用 IC 卡的公开密钥 Kpc 对其加密，并确认得到的电文 R、TD，从而实现了 IC 卡的正当性鉴别。同样，IC 卡在确认终端的正当性时，也使用同样的方式。

此系统的特点在于其获得公开密钥 Kpc 和 Kpt 的方法。从 RSA 密码体制的基本形态来看，各终端应保存 IC 卡的公开密钥文件，但实际上给各终端设置公开文件，无论从存储器容量还是密钥管理方面来说，这种方式都不合适；而且在 IC 卡内部存储器中也不可能存储太多的终端公开密钥。因此，在系统构成上采用终端需要时从 IC 卡那里接受公开密钥 Kpc 的方式。然而，采用从 IC 卡获得公开密钥的 方法，会令人担心通过伪造秘密密钥 Ksc 和公开密钥 Kpc 而伪造 IC 卡，使正当性鉴别失去意义。为了防止这种情况发生，IC 卡内存储的并非原样 Kpc，而是用发行人的秘密密钥 Ksi 签过名的 KIC。因为除了发行人之外无人知道 Ksi，所以伪造者不可能通过改写使 Kpc 和 KIC 对应起来，从而保证系统的安全性。这样，各终端只需保有发行人的发行密钥 Kpi 即可。同样，终端的公开密

钥 Kpt 也用 Ksi 签名成 KIT 并发送给 IC 卡，IC 卡内也只需保存发行人的公开密钥 Kpi。

总的来说，具体采用何种鉴别体制、应用何种密码算法取决于两种情况：算法实现的可能性和密钥管理的要求。

当前，取决于芯片技术的发展，在智能卡系统中有三种途径实现加密算法：

(1) 简化算法，在智能卡的芯片上实现。这种方法通过降低算法强度，减少密钥量，使芯片存储量和所需计算能力降低，但却降低了安全等级。

(2) 用硬件实现密码算法并将其放在接口设备处，使之构成一个有物理保护的安全模块。这种方法弥补了集成度不高，无法在芯片内实现高保密度算法的不足。而且比第一种方法更抗攻击，也是在当前芯片水平上一种比较可行的方法。

(3) 在智能卡芯片中实现足够强度的加密算法。从安全的角度讲，这是最佳的解决方案。但是，鉴于当前的芯片水平，实现算法的强度要折中选择，不能一味强调提高安全等级，算法强度的设计只要能使破译该算法的总费用大大超过信息本身的价值就可以了。这是密码算法设计者、智能卡发行者和使用者都应该遵循的原则。

思 考 题

1. 对智能卡的安全造成威胁的有哪些行为？
2. 应采取什么措施来保证智能卡的物理安全？
3. 说出为验证持卡人是否是假冒的而经常采取的验证方法？
4. 如果持卡人多次输入 PIN，但都不正确，将发生什么情况？
5. 说明智能卡和读写设备之间相互认证的方法，即如何确定对方是真实的而不是伪造的。
6. DES 加密算法属于何种密码体制，它的主要特点是什么？加密与解密过程怎样？
7. RSA 加密算法属于何种密码体制，它的主要特点是什么？加密与解密过程怎样？
8. 在智能卡和读写设备之间相互认证时，通常采用发送随机数而不是固定数的方法，这是为什么？
9. 为了保证在系统中交换的信息报文不被篡改而在报尾增加鉴别码的作用及产生方法？
10. 说明 DSA(Decimal Shift and Add)算法产生鉴别码的方法。
11. 什么是数字签名？
12. 根据 DES 算法和 RSA 算法的具体实现，对卡内 CPU 硬件有何不同的要求？
13. 你认为应如何综合考虑智能卡安全、卡内芯片水平和接口设备三者之间的要求。
14. 当采用 RSA 密码体制时，为便于计算机硬件实现，对大指数模 n 运算可采取什么样的算法？

第6章　IC卡及其专用芯片

IC卡按其所装配的芯片不同而分成存储器卡、逻辑加密卡和智能卡三种类型。本章主要论述适合IC卡使用的存储器芯片、逻辑加密芯片和CPU(内含COS)芯片。

6.1　IC卡的存储器芯片

IC卡是从磁卡发展而来的，从使用角度出发，IC卡至少应存储如发行者标识、个人密码等相对固定的信息以及与消费金额等有关的可修改数据，而且用户随身携带的IC卡平时无法由外界供电，只有在与读卡设备接触时才能取得电源，这就决定了IC卡中的存储器不能是易失性的随机存储器RAM或不能改变内容的只读存储器ROM，而只能采用可电擦除的可编程的只读存储器EEPROM。与其它存储器比较，EEPROM写入时要求的电压较高、时间较长。另外根据ISO制定的国际标准，IC卡上的芯片总共只有8个引出端，其中一个为数据(输入/输出)端，因此芯片与外界传送信息(数据、地址)只能以串行方式进行。

下面以美国ATMEL公司生产的AT24C01A/02/04/08/16存储器芯片为例来进行说明。

1. 芯片特点

(1)低电压。选择以下一种电压：

5.0V(V_{CC}=4.5V—6.0V)

3.0V(V_{CC}=2.7V—6.0V)

2.5V(V_{CC}=2.5V--6.0V)

2.0V(V_{CC}=1.8V—6.0V)

(2) 内部组成：

AT24C01A的容量为1K位(128×8)，AT24C02的容量为2K位(256×8)，AT24C04的容量为4K位(512×8)，AT24C08的容量为8K位(1024×8)，AT24C16的容量为16K位(2048×8)；

(3) 双线串行接口(双线指的是：时钟SCL，串行数据SDA)；

(4) 支持ISO/IEC 7816－3同步协议；

(5) 高可靠性：

擦写次数：100,000周期

数据保存期：100年

(6) 可以以晶片、模块及标准封装形式提供。晶片、模块可提供给IC卡使用。标准封装有8引出端和16引出端两种形式，是通用2线串行CMOS EEPROM芯片。

2. 芯片的封装

这里仅介绍IC卡使用的模块，符合ISO/IEC 7816协议，其触点的安排见表6.1和图6.1。

表6.1 EEPROM模块功能

芯片的触点	引出端名	功　能
C_1	V_{CC}	工作电压
C_2	NC	未连接
C_3	SCL(CLK)	串行时钟
C_5	GND	地
C_6	NC	未连接
C_7	SDA(I/O)	串行数据(输入/输出)

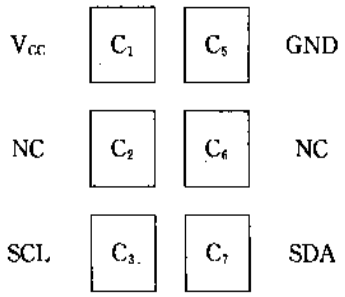


图6.1 EEPROM模块触点

3. 逻辑图

图6.2为EEPROM逻辑图。

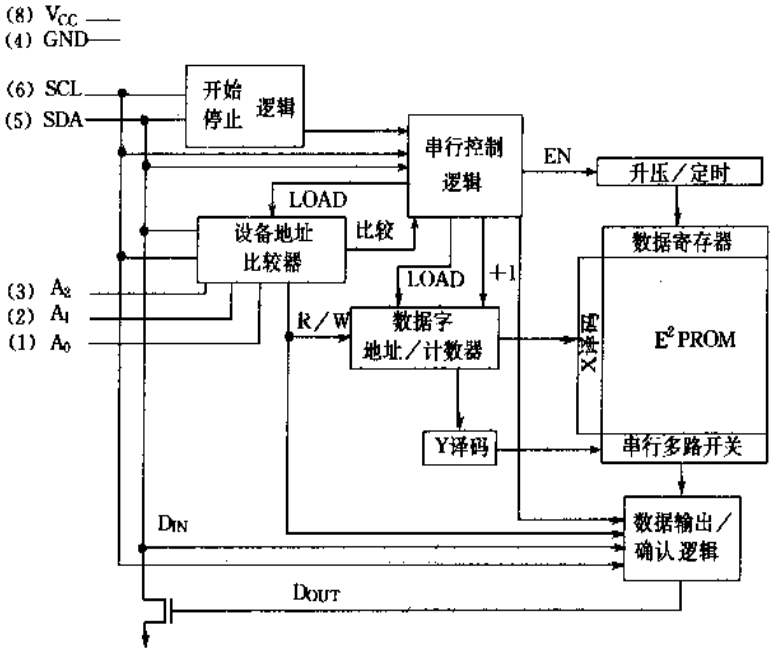


图6.2 EEPROM逻辑图

(1) 引出端说明

SCL(串行时钟)：SCL上升沿将数据输入到EEPROM芯片，下降沿将EEPROM中的数据输出。

SDA(串行数据)：双向串行数据传送端，该端采用漏极开路驱动，可以与其它漏极开路或集极开路器件进行“线或”。

A_2、A_1、A_0(器件/页地址)：器件地址输入端，应用于标准封装中，当在IC卡中使用时，不将A_2、A_1、A_0引到触点上，详细讨论见“器件寻址”。

(2) 逻辑图组成

启动停止逻辑：控制一次读/写操作的开始和终止。

串行控制逻辑：当该芯片应用于 IC 卡中时，与逻辑有关的信号线仅有 SCL 和 SDA 两根。SCL 为同步用的时钟，其它信息诸如地址、数据和读写控制命令均从 SDA 输入，串行控制逻辑需要区分这些信息，并将它们送到相应的部件。

地址/计数器：形成访问 EEPROM 存储单元的地址，分别送 X 译码器进行字选(字长 8 位)、送 Y 译码器进行位选。

升压/定时线路：EEPROM 的写入操作需要高电压，为此，在片内有升压线路，将标准电压升高到写入数据所需的电压(一般在 12V—20V 范围内)。

数据输入/应答逻辑：控制数据的输入/输出和确认应答信号。

4. 器件操作

时钟和数据传送：SCL 和 SDA 通常各自通过一个电阻上拉到高电平。SDA 上的数据仅在 SCL 为高电平时有效，在低电平时允许数据变化如图 6.3 所示。当 SCL 高电平时，如数据发生变化，则将形成“开始”或“停止”两种状态如下：

“开始”状态：SCL 处于高电平时，SDA 从高电平转向低电平表示一种操作的开始，因此开始状态应在操作命令之前建立；

“停止”状态：SCL 处于高电平时，SDA 由低电平转向高电平表示一种操作的结束，其后将终止所有通信。在读时序之后，停止命令置 EEPROM 于后备电源方式。

“开始”状态和“停止”状态的定义如图 6.4 所示。

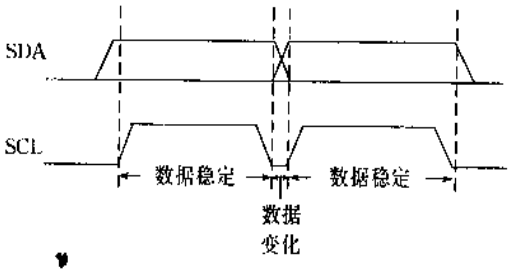


图 6.3 数据的有效性

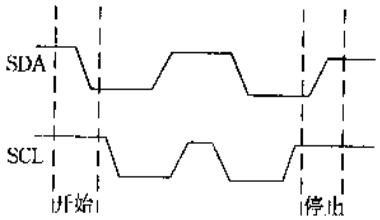


图 6.4 “开始”和“停止”的定义

确认(ACK)：所有地址和数据字以 8 位码串行输入/输出 EEPROM，任何接收数据的设备在成功地收到了每一个字以后发生应答，将 SDA 置于低电平，这发生在一个字传送完毕之后，即在第 9 个时钟周期内。EEPROM 在收到每个地址码或数字码之后，也以置 SDA 于低电平的方式予以确认。其波形图如图 6.5 所示。

图 6.6 给出 SCL 与 SDA 上的输入/输出数据的时间关系。图中各符号的意义见表 6.3(交流特性)

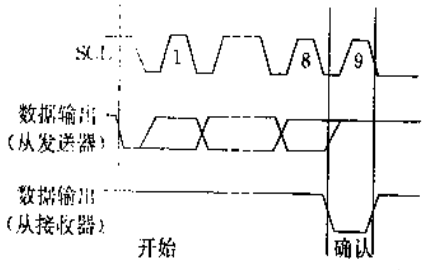


图 6.5 数据传送与确认

5. 器件寻址

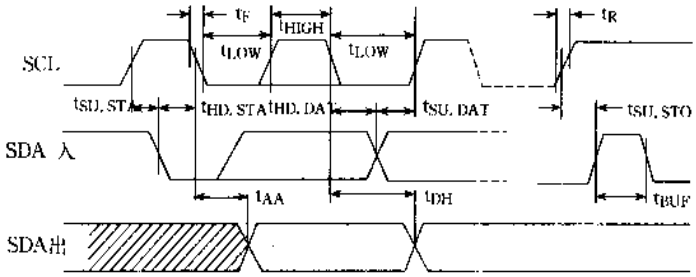


图 6.6 总线时序(SCL 与 SDA 的时间关系)

1K、2K、4K、8K 和 16K EEPROM 在开始状态之后紧跟着 8 位器件地址，使芯片能执行读/写操作(参见图 6.7)。

1K/2K	1	0	1	0	A_2	A_1	A_0	R/W
	MSB							LSB
4K	1	0	1	0	A_2	A_1	P0	R/W
8K	1	0	1	0	A_2	P1	P0	R/W
16K	1	0	1	0	P2	P1	P0	R/W

MSB:最高位 LSB:最低位

图 6.7

器件地址码的高 4 位为 1010，对这里讨论的所有器件都适用。

对标准封装器件来说，接下来的 3 位将因芯片容量的不同而有不同的定义。叙述如下：

1K/2K EEPROM:接下来的 3 位为器件地址位 A_2、A_1 和 A_0，这 3 位必须与它们的相应硬布线输入端(pin)相比较；

4K EEPROM:A_2、A_1 为地址位，另一位为页面地址位 P0。A_2、A_1 必须与它们的相应硬布线输入端(pin)相比较，A_0 引出端不连接；

8K EEPROM:A_2 为地址位，另 2 位为页面地址位 P1、P0。A_2 必须与它的相应硬布线输入端(pin)相比较，A_1 与 A_0 引出端不连接。

16K EEPROM:不用地址位，3 位均用于页面地址，它们是 P2、P1、P0。A_2、A_1 和 A_0 引出端不连接。页面地址位应被视为随后的数据字地址的最高位。

典型的系统总线结构如图 6.8 所示。因 SDA 和 SCL 为漏极开路电路，所以允许将多个器件直接连接起来。

现在仍讨论开始状态后紧跟的器件地址，它的第 8 位是读/写操作选择位，该位处于高电平时为读，低电平时为写。

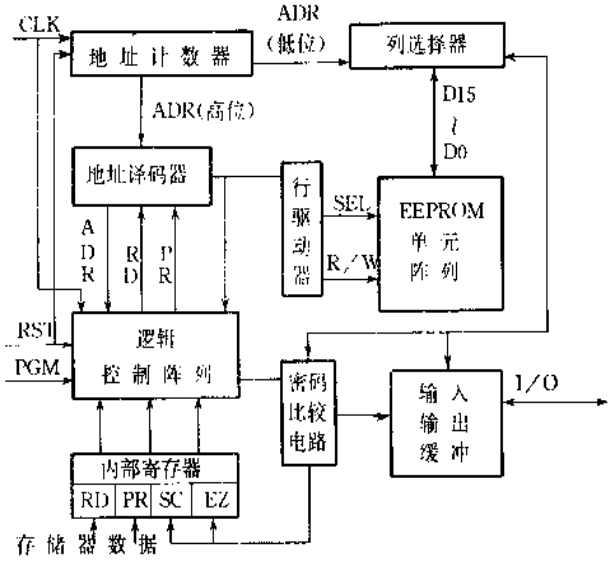


图 6.15　逻辑加密卡芯片的功能框图

地址计数器只有计数功能，不能从外界接收地址，当加电或者 RST 信号来时清零，所以对 EEPROM 只能按照地址顺序访问。

6.2.3　芯片内部存储区域分配

逻辑加密卡一般具有如下的存储分区：

1. 制造代号区 (Fabrication Zone)

由制造厂商在出厂时写入，用于记录卡片的制造信息，以便于以后验证卡的出处。对这一区的写入和擦除只有在熔丝 1 未断时进行，制造厂商可对同一批芯片写入一特定的标识代号，随后将熔丝 1 熔断，使制造代号不能再更改。

2. 发行代号区 (Issuer Zone)

由发行商在发行给个人的时候写入，用于记录卡片的发行信息。对这一区的写入和擦除只有在熔丝 2 未断时进行，当熔丝 2 被熔断后即不可更改。制造代号和发行代号在应用时可以自由读出，以便验证卡的出处。

3. 用户密码区 (Security Code)

当卡片个人化完成后，由该密码保护卡内的应用区域。使用时由用户输入用户密码，只有密码比较正确后，才允许对应用区进行读写操作和修改密码操作。

4. 密码比较计数区 (Security Code Attemps Count)

出于安全保护的目的，防止人为的对密码进行猜测，需要限制密码比较次数。用该区来累计不正确的密码比较次数。经过连续四次不正确的比较后，卡将自锁，以后拒绝用户的任何操作。密码比较计数区遵循如下的写操作条件：写入操作是任意的，不受保护，而对它的擦除则受到用户密码的保护，只有在用户密码比较正确的条件下，才能进行擦除操作。

在实现时操作过程如下：

(1) 密码比较计数区只用到前四位，个人化后其值为 1111。第一次密码比较后，必须在第一个'1'的位置上写入'0'，即为 0111，而后由密码比较结果控制对该区的擦除操作。比较正确则可擦除为 1111，否则擦除操作不成功，其值保持为 0111，表示用户已有一次错误的密码输入，还剩下三次机会。

(2) 第二次密码比较后，也必须在第一个'1'的位置上写入'0'，密码比较计数为 0011。若这次密码比较正确，则可恢复为 1111，否则擦除不能进行，其值为 0011，用户还剩两次比较机会。

(3) 当用户输入四次均为错误密码后，密码比较计数区变为 0000。这时，在前四位再也没有合适的'1'供写'0'使用，卡将自锁，以后拒绝用户的任何操作。

5. 用户个人区 (Code Protected Zone)

记载用户的个人身份标识。写入和擦除受密码保护，但可以自由读出，以核实用户身份。

6. 应用区 (Application Zone)

该区的头两位标识该应用区的读写属性，并和用户密码一起控制对应用区的读出和写入，擦除操作则由擦除密码来控制进行，并且受到删除计数的限制。当删除计数区中没有可用的位'1'时，擦除操作也不能进行。

7. 擦除密码 (Erase Key)

该区用以记录应用区的保护密码。这个密码是个人化的时候，由发行商写入芯片内并供发行商使用的。发行商输入密码后，与片内的删除密码进行比较，如果相等，且删除计数区不是全'0'，则可以对整个应用区进行擦除，相当于再次写入用户的预付款额，以达到一卡重复使用多次的目的。

在卡未发行时(即熔丝 2 熔断以前)，在核实用户密码以后，该区可以自由地读出、写入和擦除，当卡发行后，对擦除密码的读出、写入、擦除的操作都不能进行。

8. 擦除计数 (Erase Counter)

该区中的每一个'1'表示可以对应用区进行一次擦除操作。当删除计数区全为'0'时，不能再对应用区进行擦除操作。

对该区的擦除只能在卡发行之前进行，当卡发行后，对它只能作读出和写入操作。

虽然国际标准中并没有规定逻辑加密卡的存储器分区结构，但是事实上几乎所有的逻辑加密卡都遵循以上的存储区域分配，而只是在各分区的长度上存在着差异，这样的存储器分区结构已经成为事实上的设计标准。在以下对 AT88SC102 和 SLE4404 的分析中，我们不难发现这一现象。

6.2.4 AT88SC102 分析

AT88SC102 是由美国 ATMEL 公司设计的具有密码比较逻辑的 1K 位 EEPROM 芯片，是一种典型的逻辑加密卡芯片。它支持 ISO 7816-3 同步协议，在制造中使用了低功耗 CMOS 技术，提供给用户 2 个 512 位的可用存储分区；芯片内部的存储区域分配合理，能满足大部分应用领域的要求。除此之外，它还具有内部的自升压电路，使芯片只需要+5V 电压支持，而不需要外部提供进行 EEPROM 单元擦除所需的较高电压；其 EEPROM

单元的允许擦除次数在10万次以上，数据保存年限为100年。

1. 卡片的触点

图6.16为芯片模块触点，表6.4为触点的功能说明。

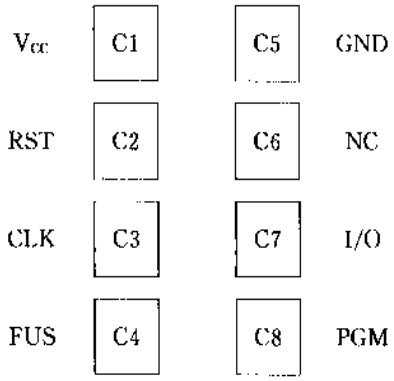


图6.16 AT88SC102芯片的触点结构

表6.4 AT88SC102芯片的触点结构

ISO触点	触点号	触点名	说　明
C1	8	Vcc	电源(Operating Voltage)
C2	7	RST	复位信号(Reset)
C3	6	CLK	时钟信号(Clock and Address Control)
C4	5	FUS	熔丝信号(Identification Fuses)
C5	1	GND	地(Ground)
C6	2	NC	未使用(Not Connect)
C7	3	I/O	双向数据线(Bi-direction Data Port)
C8	4	PGM	编程信号(Programming Control)

以上信号遵从ISO/IEC 7816-3同步协议。其中Vcc、RST、CLK、GND、I/O信号在协议中有详细规定。而PGM信号与FUS信号为自定义信号，作用如下：

(1) FUS熔断信号，用以进行熔断操作。

(2) PGM编程信号，用以通知芯片进行写入和擦除操作，可参看时序图4。由于芯片内部有升压电路，因此不需要读写设备提供高压VPP信号，而采用PGM信号作编程通知。

2. 芯片的存储区域分配

AT88SC102的地址计数器有11位，即计数范围可为0—2047。但是实际使用的地址区间是0—1567，当地址计数器计至1567后，在下一个时钟周期到来时，地址翻转为0。而留给用户使用的地址是0—1423，共1424位，如表6.5所示。

表 6.5 AT88SC102 芯片的存储区域分配

区域名	字段	地址	位数	说明
Fabrication Zone (FZ)	0	0—15	16	制造代号
Issuer zone (IZ)	1—4	16—79	64	发行代号
Security Code(SC)	5	80 95	16	用户密码
Security Code Attemp Counter (SCAC)	6	96 111	16	用户密码比较计数
Personal Zone (CPZ)	7—10	112—175	64	用户个人区
Application Zone1 (APP1)	11—42	176—687	512	应用区 1
Erase Key 1 (EZ1)	43 45	688 735	48	擦除密码 1
Application Zone2 (APP2)	46 77	736 1247	512	应用区 2
Erase Key2 (EZ2)	78 79	1248 1279	32	擦除密码 2
Erase Counter (EC)	80 87	1280 1407	128	擦除计数
Test Zone (MTZ)	88	1408 1423	16	存储器测试区

注释：存储器测试区不受保护，可以进行任何操作，它用以测试 EEPROM 单元阵列的各项性能。除此之外，芯片内还有：

- 三个供内部使用的 EEPROM 单元：FUSE1、FUSE2 和 EZ1 的控制位；
- 两个供特殊控制用的地址，当访问到其中一个指定地址时，可取得物理熔丝的状态（熔断或者未熔断）；访问到另一些地址时，可对全片进行擦除。

现分别介绍如下：

(1) FUSE1

FUSE1 是留给制造商使用的。在 FUSE1 未熔断时，EEPROM 的所有单元均可自由地读出、写入和擦除。

FUSE1 单元本身可以自由写入（写 0）；它的擦除（写 1）则受物理熔丝控制，当物理熔丝熔断后，就不能被擦除。

(2) FUSE2

FUSE2 是留给发行商使用的，卡从制造商到发行商手中时，FUSE1 已熔断，FUSE2 未熔断，此时发行商可以对除了 FZ 区之外的任意单元作写入和擦除操作，为用户进行个人化的操作。个人化完成后，发行商熔断 FUSE2，则卡的 IZ、EZ1、EZ2、EC 区将不能被擦除，其中 EZ1、EZ2 也不能写入和读出，卡成为最终用户手中的卡。

与 FUSE1 一样，FUSE2 的擦除受物理熔丝控制，当物理熔丝熔断后，就不能被擦除。

(3) EZ1 的控制位

当这一位为‘0’时表示卡内不设置 EZ1 区，此时 EZ1 地址被跳过，即从地址 687 直接跳到地址 736 。当 EZ 为‘1’时对 APP1 的擦除需要核对 EZ1 密码，且要求 SC 比较正确。

对该位的写入只有在 FUSE1 未熔断前进行，即由制造商根据实际应用情况决定是否设置 EZ1 区 。该位不能擦除，也不能读出。

(4) 对全片擦除的控制

该控制功能留给制造商和发行商用。在卡片未出厂前，FUSE1 未熔断，当对某些预先

指定的地址(>1424)进行写入和擦除操作时,实际上是打开了 EEPROM 单元阵列的所有行选线,即在该行写入和擦除操作实际上是对全片的写入和擦除。

当卡片出厂且未发行时,也即 FUSE1 已熔断而 FUSE2 未熔断时,只要用户密码 SC 比较成功,对上述指定地址的写入和擦除,则是对除了 FZ 区外的所有 EEPROM 单元进行写入和擦除。

3. 访问控制

对各存储区域的访问(制造商测试)是由 FUS 触点上的电压和内部的两个熔丝(FUSE1 和 FUSE2)的状态共同控制的,如表 6.6 所示,详细的控制条件如表 6.7 和表 6.8 所示。

表 6.6 AT88SC102 存储区的访问控制

FUS 触点上的电压	熔丝 1	熔丝 2	访问控制
0 V	任意	任意	见表 6.8
5 V	熔断	未熔断	见表 6.7
5 V	未熔断	熔断	见表 6.8

表 6.7 个人化时(FUSE2 未熔断)的访问控制条件

区域名	SC	1PR	1RD	2PR	2RD	EZ1	EZ2	EC	读	擦除	写入	比较
FZ	×	×	×	×	×	×	×	×	可以	不可	不可	不可
IZ	0	×	×	×	×	×	×	×	可以	不可	不可	不可
	1	×	×	×	×	×	×	×	可以	可以	可以	不可
SC	0	×	×	×	×	×	×	×	不可	不可	不可	可以
	1	×	×	×	×	×	×	×	可以	可以	可以	不可
SCAC	0	×	×	×	×	×	×	×	可以	不可	可以	不可
	1	×	×	×	×	×	×	×	可以	可以	可以	不可
CPZ	0	×	×	×	×	×	×	×	可以	不可	不可	不可
	1	×	×	×	×	×	×	×	可以	可以	可以	不可
APP1	0	×	0	×	×	×	×	×	不可	不可	不可	不可
	0	×	1	×	×	×	×	×	可以	不可	不可	不可
	1	×	×	×	×	×	×	×	可以	可以	可以	不可
EZ1	0	×	×	×	×	×	×	×	不可	不可	不可	不可
	1	×	×	×	×	×	×	×	可以	可以	可以	不可
APP2	0	×	×	×	0	×	×	×	不可	不可	不可	不可
	0	×	×	×	1	×	×	×	可以	不可	不可	不可
	1	×	×	×	×	×	×	×	可以	可以	可以	不可
EZ2	0	×	×	×	×	×	×	×	不可	不可	不可	不可
	1	×	×	×	×	×	×	×	可以	可以	可以	不可

续表

区域名	SC	1PR	1RD	2PR	2RD	EZ1	EZ2	EC	读	擦除	写入	比较
EC	0	×	×	×	×	×	×	×	可以	不可	可以	不可
	1	×	×	×	×	×	×	×	可以	可以	可以	不可
MTZ	×	×	×	×	×	×	×	×	可以	可以	可以	不可

注：SC=1 表示 SC 比较正确；

1PR=APP1 区的第一位(176 位)，1RD=APP1 区的第二位(177 位)；

2PR=APP2 区的第一位(736 位)，2RD=APP2 区的第二位(737 位)；

EZ1=1 表示 EZ1 比较正确；

EZ2=1 表示 EZ2 比较正确；

EC=1 表示 EC 区还有有效的位'1'。

表 6.8　个人化后用户使用时的访问控制条件

区域名	SC	1PR	1RD	2PR	2RD	EZ1	EZ2	EC	读	擦除	写入	比较
FZ	×	×	×	×	×	×	×	×	可以	不可	不可	不可
IZ	×	×	×	×	×	×	×	×	可以	不可	不可	不可
SC	0	×	×	×	×	×	×	×	不可	不可	不可	可以
	1	×	×	×	×	×	×	×	不可	可以	可以	不可
SCAC	0	×	×	×	×	×	×	×	可以	不可	可以	不可
	1	×	×	×	×	×	×	×	可以	可以	可以	不可
CPZ	0	×	×	×	×	×	×	×	可以	不可	不可	不可
	1	×	×	×	×	×	×	×	可以	可以	可以	不可
APP1	0	×	0	×	×	×	×	×	不可	不可	不可	不可
	0	×	1	×	×	×	×	×	可以	不可	不可	不可
	1	0	×	×	×	0	×	×	可以	不可	不可	不可
	1	0	×	×	×	1	×	×	可以	可以	不可	不可
	1	1	×	×	×	0	×	×	可以	不可	可以	不可
	1	1	×	×	×	1	×	×	可以	可以	可以	不可
EZ1	×	×	×	×	0	×	×	×	不可	不可	不可	可以
APP2	0	×	×	×	0	×	×	×	不可	不可	不可	不可
	0	×	×	×	1	×	×	×	可以	不可	不可	不可
	1	×	×	0	×	×	0	×	可以	不可	不可	不可
	1	×	×	0	×	×	×	0	可以	不可	不可	不可
	1	×	×	0	×	×	1	1	可以	可以	不可	不可
	1	×	×	1	×	×	0	×	可以	不可	可以	不可
	1	×	×	1	×	×	×	0	可以	不可	可以	不可
	1	×	×	1	×	×	1	1	可以	可以	可以	不可
EZ2	0	×	×	×	×	×	×	×	不可	不可	不可	可以
EC	×	×	×	×	×	×	×	×	可以	不可	可以	不可
MTZ	×	×	×	×	×	×	×	×	可以	可以	可以	不可

注：SC=1 表示 SC 比较正确；

1PR=APP1 区的第一位(176 位)，1RD=APP1 区的第二位(177 位)；

2PR=APP2 区的第一位(736 位)，2RD=APP2 区的第二位(737 位)；

EZ1=1 表示 EZ1 比较正确；

EZ2=1 表示 EZ2 比较正确；

EC=1 表示 EC 区还有有效的位'1'。

4. 操作模式

由 PGM、RST、CLK 信号和内部地址计数器决定了四种操作模式，如图 6.17 所示。在这四种操作模式中，输出的控制在卡内完成。如果读出的条件不满足，则在 I/O 线上出现的数据无效(Z 状态)；此外，CMP 操作和 INC 操作从外部控制来看是一样的(RST 和 PGM 俱为'0')，它们是通过内部地址计数器来区分的：CMP 操作只在 SC 和 EZ 地址区进行，其他地址区域均进行 INC 操作。芯片内部地址计数器的最大值为 1567，超过这个值，计数器将翻转为'0'。

命令名	PGM	RST	CLK	描　　述
RESET	X	⎺_	0	卡内地址计数器清零。当RST和CLK信号都为'0'时，存储器内的数据开始出现在I/O线上。(图6.17) 当RST为高时，禁止地址计数器计数；计数器在RST的下沿清零。
INC (INC/READ)	0	0	⎺_/⎺	卡内地址计数器加一，存储器内的数据输出在I/O线上。(图6.18) 以上操作在时钟下沿进行。
CMP(INC/CMP)	0	0	⎺_/⎺	外部输入数据与卡内密码进行比较。(图6.19) 当CLK为低时，输入数据在I/O线上必须稳定。地址计数器在时钟下沿加一。
WRITE	1	0	_/⎺	在时钟上升沿前，I/O数据必须准备好，然后CLK必须保持为高至少5ms时间，等待写入操作完成。(图6.20)
VERIFY	0	0	⎺_	随后，在时钟下降沿，刚写入的数据出现在I/O线上，以被验证。在这个时钟下沿，地址计数器不加一。

图 6.17　AT88SC102 的操作模式

图 6.17 中的复位(Reset)时序，对应于图 6.18；读(Read)时序，对应于图 6.19；比较(Compare)时序，对应于图 6.20；写(Program)时序，对应于图 6.21。

SC 和 EZ 的完整比较过程如图 6.22 所示。在整个过程中各阶段完成的功能如下：

A：SC 或 EZ 的比较时序。(见图 6.20)

B：找到 SCAC 或 EZAC 行中第一个逻辑'1'的位。

C：在这个位地址处进行写入(即写'0')操作。

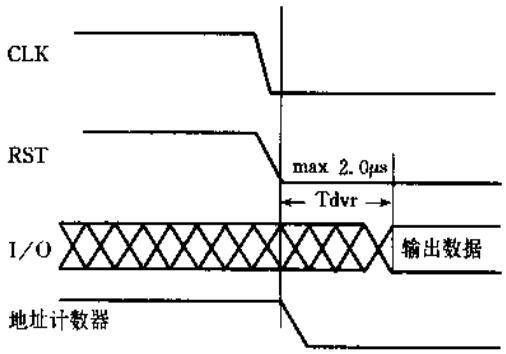
D：芯片输出该位的值。若写入操作成功进行，输出值为 0。如密码比较正确，SC 或 EZ 寄存器将被置为 1。

E：在同一个位地址处再进行擦除(即写'1')操作。

如果在 SCAC 行，将擦除 SCAC 行；如果在 EC 行，将擦除 EC 和 APP2 的所有行。

F：芯片输出当前位的值。如果擦除操作成功进行，输出值为 1。

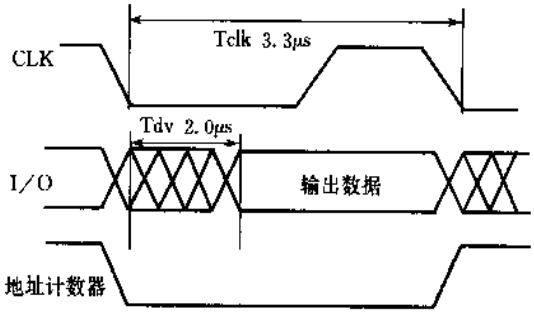
G：在 CLK 的下降沿，地址计数器加一，芯片输出下一位的值。



注：RST 为高时禁止计数。

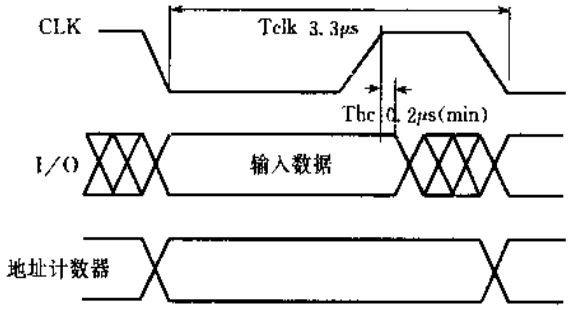
RST 的下降沿地址计数器清零；延时 Tdvr 后，I/O 线上输出数据

图 6.18 Reset 时序图



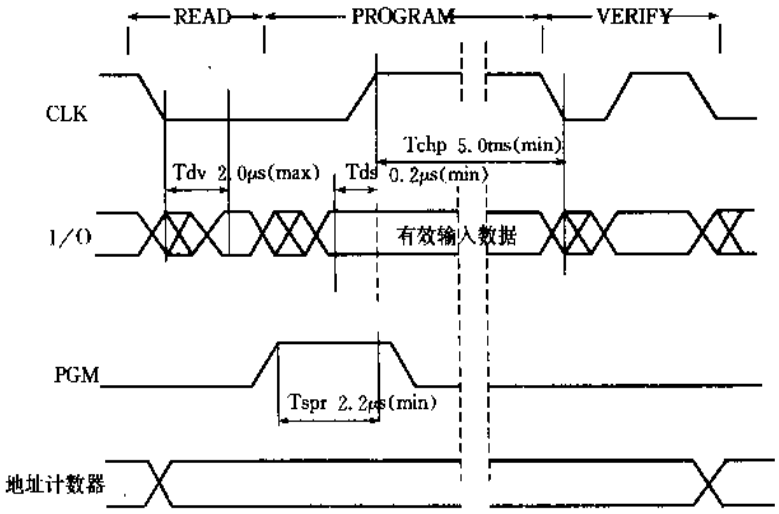
注：Tclk 为时钟周期。在 CLK 的下沿，计数器加一。存储器内的数据经过一段延时 Tdv 以后，读出在 I/O 线上。在这个时序中包含了地址加一(INC)和读出(READ)两种操作。

图 6.19 读(Read)时序



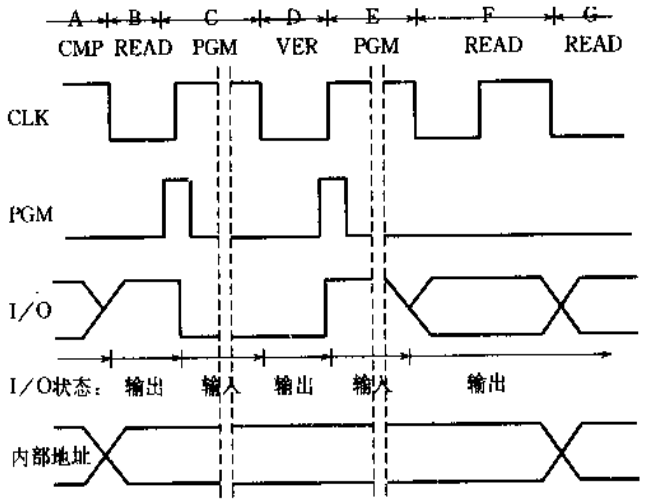
注：在 CLK 下降沿，地址计数器加一，这时外部开始输入待比较的数据；在 CLK 上升沿，I/O 上的数据被锁存，I/O 线上的数据在 CLK 上升沿后至少保持 Thc 时间。当下一个 CLK 下降沿来临时，执行这次比较操作，同时地址计数器加一。

图 6.20 比较(Compare)时序



注：在CLK上升沿到来之前(Tspr时间)，PGM应升为'1'，I/O上由外部给出写入数据(提前T ds时间)。当CLK为'1'时，开始执行写'0'或写'1'操作，这时CLK应至少保持5ms时间为'1'(Tchp)。在紧接着的CLK下沿，地址计数器不发生变化，I/O上出现存储器输出的数据，提供给外部验证上次写操作是否成功。

图 6.21　写(编程 Program)时序



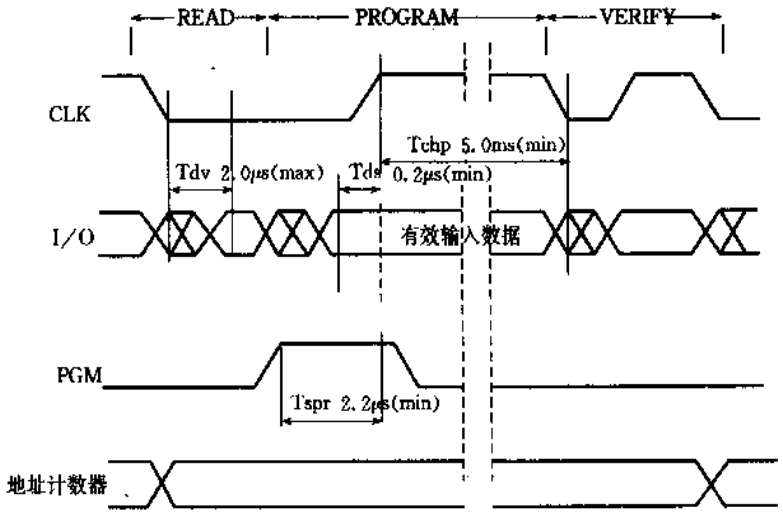
注：1. 从操作B一直进行到F，地址计数器不发生变化。密码比较的全过程是先比较，然后在比较计数行找到某一个不为0的位，在同一位进行先写入再擦除的操作。

2. 如果在EC区的任意一位，进行上述操作(先写入再擦除)。如果操作成功，将擦除APP2的所有行。

图 6.22　SC和EZ的比较过程

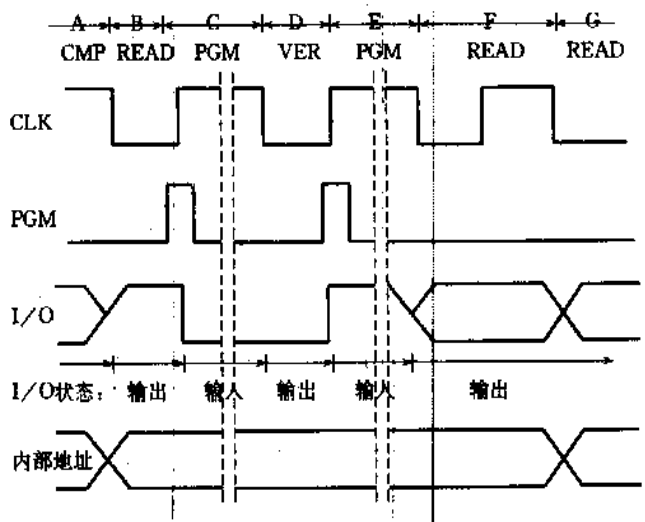
6.2.5　SLE4404分析

SLE4404是由德国SIEMENS公司设计的逻辑加密卡芯片。它支持ISO/IEC 7816-3同步协议，在制造中使用的是NMOS技术。它共含416位的EEPROM单元，其中提供给



注：在CLK上升沿到来之前(Tspr时间)，PGM应升为'1'，I/O上由外部给出写入数据(提前T ds时间)。当CLK为'1'时，开始执行写'0'或写'1'操作，这时CLK应至少保持5ms时间为'1'(Tchp)。在紧接着的CLK下沿，地址计数器不发生变化，I/O上出现存储器输出的数据，提供给外部验证上次写操作是否成功。

图 6.21　写(编程 Program)时序



注：1. 从操作B一直进行到F，地址计数器不发生变化。密码比较的全过程是先比较，然后在比较计数行找到某一个不为0的位，在同一位进行先写入再擦除的操作。

2. 如果在EC区的任意一位，进行上述操作(先写入再擦除)，如果操作成功，将擦除APP2的所有行。

图 6.22　SC和EZ的比较过程

6.2.5　SLE4404分析

SLE4404是由德国SIEMENS公司设计的逻辑加密卡芯片。它支持ISO/IEC 7816-3同步协议，在制造中使用的是NMOS技术。它共含416位的EEPROM单元，其中提供给

表 6.10 SLE4404 芯片的存储区域分配

区域名	字段	地址	位数	说　明
Fabrication Zone (FZ)	0	0—15	16	制造代号
Issuer zone (IZ)	1—3	16--63	48	发行代号
Security Code (SC)	4	64—80	16	用户密码
Security Code Attemp Counter (SCAC)	5	80--96	16	用户密码比较计数
Personal Zone (CPZ)	6	96--111	16	用户个人区
Application Zone (APP)	7　19	352--383	208	应用区
Erase Key (EZ)	20—21	320　351	32	删除密码
Erase Counter (EC)	22—25	352　415	61	删除密码比较计数

3. 操作模式

由 P、RST、CLK 信号和内部地址计数器决定了四种操作模式，如图 6.24 所示。

命令名	P	RST	CLK	描　述
RESET	×		0	卡内地址计数器清零。当RST和CLK信号都为'0'时，存储器内的数据开始出现在I/O线上。(时序图6.24) 当RST为高时，地址计数器清零。
INC (INC/READ)	0	0		卡内地址计数器加一，存储器内的数据输出在I/O线上。(时序图6.25) 地址加一操作在CLK上沿进行。数据输出操作在CLK下沿进行。
CMP(INC/CMP)	0	0		外部输入数据与卡内密码进行比较。(时序图6.26) 当CLK为低时，输入数据在I/O线上必须稳定。地址计数器在CLK上沿加一。
WRITE	1	0		在CLK上升沿前，I/O数据必须准备好，然后CLK必须保持为高至少5ms时间，等待写入操作完成。(时序图6.27)
VERIFY	0	0		随后，在CLK下降沿，刚写入的数据出现在I/O线上，以被验证。在这个CLK上沿，地址计数器不加一。

图 6.24　SLE4404 操作模式

在这四种操作模式中，输出的控制在卡内完成，如果读出的条件不满足，则在 I/O 线上出现的数据无效(H 状态)；CMP 操作和 INC 操作从外部控制来看是一样的(RST 和 P 俱为'0')，它们是通过内部地址计数器来区分的：CMP 操作只在 SC 和 EZ 地址区进行，其他地址区域均进行 INC 操作。此外，芯片内部地址计数器的最大值为 512，超过这个值计数器将翻转为 0。

图 6.24 中的复位(Reset)时序，对应于图 6.25；读(Read)时序对应于图 6.26；比较

(Compare)时序对应于图 6.27;写(Program)时序对应于图 6.28。

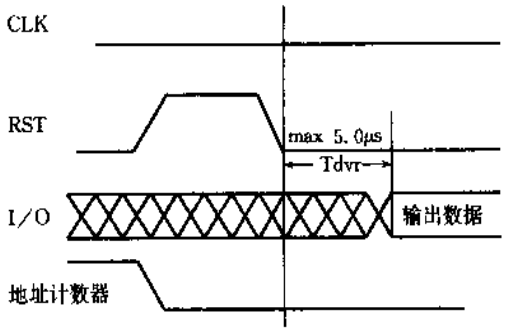


图 6.25 复位(Reset)时序

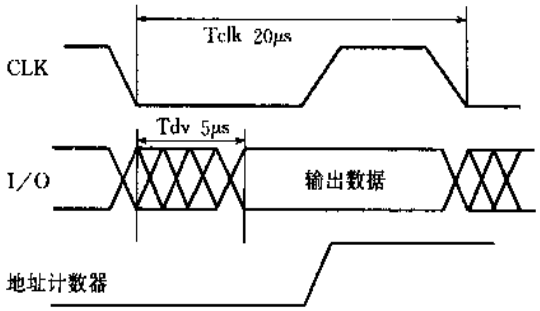


图 6.26 读(Read)时序

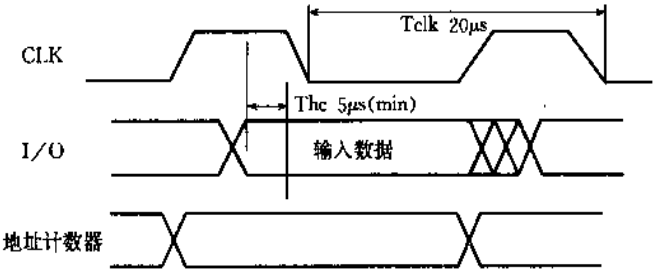


图 6.27 比较(Compare)时序

6.2.6 几种典型电路分析

1. 上电复位电路

上电复位电路的作用是当 IC 卡加电时产生一段"┘‾‾└"型脉冲,这发生在将卡插入接口设备时。该脉冲提供给芯片内的寄存器,使之复位,脉冲的宽度应该符合国际标准 ISO/IEC 7816-3 中的规定。上电复位信号不同于逻辑加密卡芯片的触点上外加的 RST 信号,RST 信号的作用只是复位地址计数器,而芯片内部的寄存器的复位则由上电复位信号来完成。

2. 密码比较电路

这部分电路的作用是验证持卡人和发行商的身份,所以是整个逻辑电路的核心,图

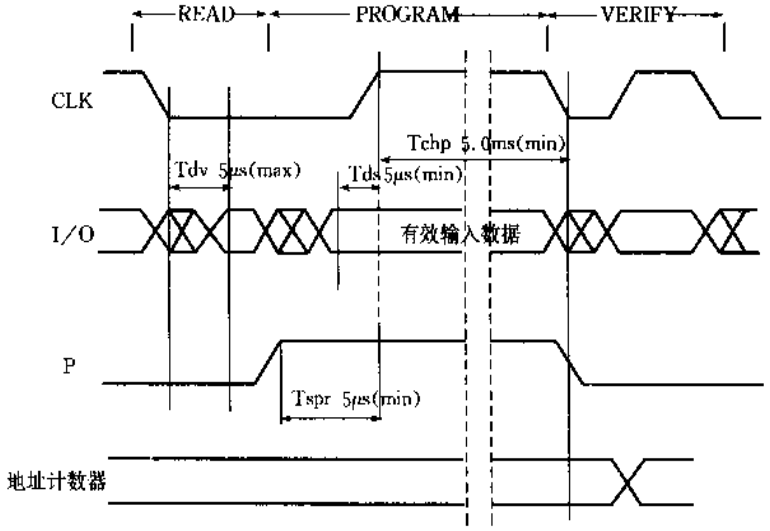


图 6.28 写(编程 Program)时序

6.15 和表 6.7 中列出的 SC 和 EZ(EZ1 或 EZ2)即是密码比较的结果。

(1) 删除密码比较电路

形成 EZ 的电路如图 6.29 所示,图中 COMP 为密码比较结果触发器,取 EZ=$\overline{COMP}$。当 EZ=1 时,表示密码比较正确。

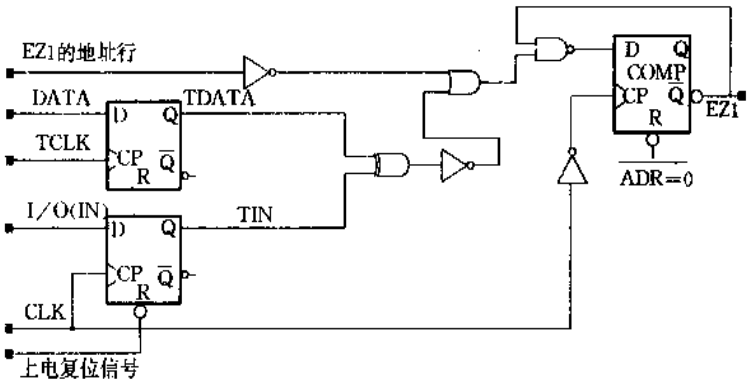


图 6.29 密码比较电路图

图 6.29 比较电路的设计原则是:EZ 的初始状态为'1',如密码比较相等,EZ 仍然为'1';如密码比较不正确,则 EZ=0,即 COMP=1,然后 COMP 保持为'1',EZ 保持为'0'。电路的工作原理如下:

当地址为'0'时,$\overline{ADR}$=0 有效,触发器被清零,COMP=0,EZ=1;

当地址未到密码区时,COMP 的 D 端为'0',因此 COMP 保持为 0,EZ 仍然为 1;

当地址在密码区时,由 EEPROM 读出的数据 DATA 经锁存为 TDATA;外部数据 I/O(IN) 输入触发器后为 TIN。二者经异或门进行比较:

若比较结果相等,则 D 端为'0',COMP 保持为 0,即 EZ 保持为 1;

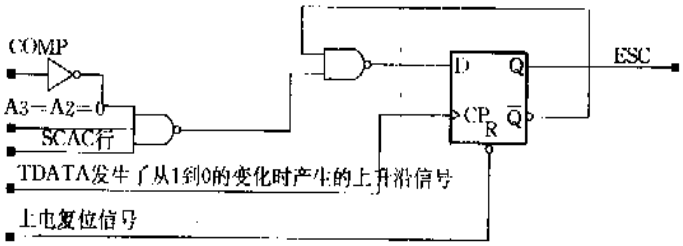
若比较结果不等,则 D 端为'1',COMP 跳变为'1',然后依靠 $\overline{Q}$ 输出到 D 端的连线,使它保持为'1',因此 EZ 保持为 0。

TIN 在 CLK 的上升沿时形成，TDATA 在 TCLK 为'1'时锁存，而比较结果在 CLK 的下降沿时形成。也就是说，在时钟的上升沿保存要比较的数据，在时钟的下降沿进行比较。

EZ 和地址译码结果相结合，就能产生正确的读写控制。

(2) 用户密码比较电路

对于 SC 来说，由于有比较次数的限制，因此即使比较结果正确，但如果超过了四次的限制，仍然是无效的。因此 SC 的比较结果要结合 SCAC 区的情况综合考虑，除了保留图 6.30 的密码比较 电路外，还需要增加图 6.30 所示的电路，当 ESC=1 时，才表示用户密码正确。



注：$A_3 \sim A_0$ 为选择某一位的地址，0000~0011为选择前4位的地址。

图 6.30 密码比较结果锁存电路图

当上电复位有效时，ESC 被清零，表示 SC 的比较结果处于无效态。而只有在 SCAC 区的前四位 (A3=A2=0)和 COMP 有效，且 TDATA 经历了从'1'到'0'的变化时，ESC 被置'1'，处于有效态，而且 ESC 一旦有效后，将保持有效直到下一个上电复位信号的到来。ESC 置'1'的条件代表了下列意义：

限制 SC 的比较次数在四次以内，由 SCAC 区的前四位条件来保证；

保证在 SCAC 的某一个'1'的位置上成功地写入了一个'0'。前面已经提到了 SCAC 密码比较计数的原理，每次比较时，必须找到 SCAC 区前四位中的第一个'1'，先写入'0'，然后等待密码比较正确后，才能将这四位擦除。这里 TDATA 经历了从'1'到'0'的变化，保证了 SCAC 写'0'的成功，限制了试图猜测用户密码的入侵者的输入次数。

3. 熔丝电路

熔丝的作用是控制某些特殊的读写操作，当熔丝熔断后，这些读写操作就无法进行，从而达到保密的目的。逻辑加密卡芯片内部设计有两个熔丝 FUSE1 和 FUSE2，其中 FUSE1 由生产厂家掌握，用于出厂前控制芯片的初始化工作，出厂时生产厂家将 FUSE1 熔断，芯片移交给发行商；FUSE2 由发行商掌握，用于进行芯片的个人化工作，在个人化完成后，发行商将 FUSE2 熔断，芯片就可以交付给用户使用。

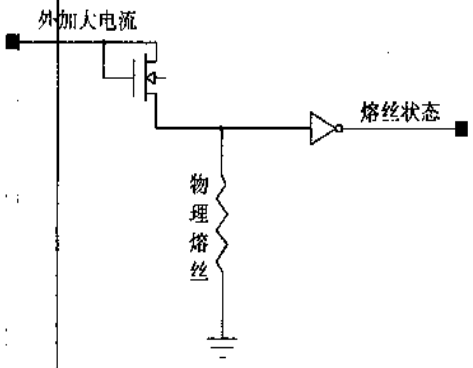


图 6.31 物理熔丝电路示意图

FUSE1 和 FUSE2 的实现有以下三种方式：

(1) 采用两个物理熔丝分别代表 FUSE1 和 FUSE2，都采用外加电流的方式熔断。在芯片内，物理熔丝是一段多晶硅电阻区，可用外加的大电流烧断。如图 6.31 所示。

由于物理熔丝所占的面积较大，这种方式会增加芯片的面积。

(2) 采用一个物理熔丝，而用两个 EEPROM 单元来代表 FUSE1 和 FUSE2，用这个物理熔丝来控制 FUSE1 和 FUSE2 的读写操作。当物理熔丝未熔断时，可对 FUSE1 和 FUSE2 单元进行擦除操作；而物理熔丝熔断后，由附加的逻辑电路控制，只能对 FUSE1 和 FUSE2 单元进行一次写入操 作，也就达到了熔断的目的。

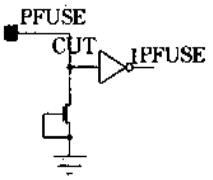


图 6.32 芯片划片示意图

(3) 利用芯片出厂的切片操作来替代熔断物理熔丝，如图6.32所示，出厂时厂家在图中 CUT 位置 进行切片，切断了部分逻辑电路，间接地从物理上达到了熔断的目的 。

6.3 智能卡的硬件环境

智能卡的硬件主要包括两部分：微处理器和存储器。逻辑结构大致如图 6.33 所示。在这两大硬部件之间通常还有一些连接及控制电路。一般而言，微处理器接收从接口设备发送来的命令，对之进行分析后，根据需要控制对存储器的访问；访问时，微处理器向存储器提供要访问的数据单元的地址(必要的话还有数据)，然后由存储器根据地址返回对应的数据给微处理器，由微处理器再对这些数据进行进一步的处理。此外，智能卡所需要的运算(例如加密运算)也是由微处理器完成的。在上述的这些过程中，如何控制及实现这些过程则是由智能卡的操作系统 COS 来完成的。

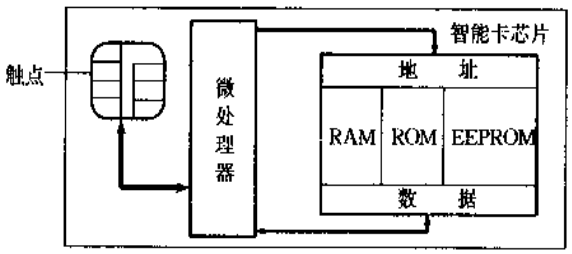


图 6.33 智能卡的硬件结构

智能卡内部的微处理器目前一般都采用 8 位字长的 CPU，例如由德国 GAO 和 GMD 开发的 STARCOS(Smart Card Chip Operating System)中所使用的微处理器就是 8 位字长的 Hitachi H8/3101。采用 8 位字长的 CPU 主要是由于受到了智能卡的外形尺寸的限制以及当前的集成电路技术的制约，使得微处理器的内部电路不能过于复杂；而另一个原因也是因为目前智能卡本身所需要的管理工作及所要实现的功能还都比较简单，使用 8 位的微处理器通常就能够达到要求了。至于将来，随着集成电路技术的发展和智能卡功能的增强，采用 16 位(甚至更高)微处理器也不是没有可能的。

智能卡通常采用 DES、RSA 等密码算法以提高安全度，当采用 RSA 算法时，由于要进行大指数模运算，对微处理器的运算速度要求较高，因此在芯片内还可以设置有专用的

协处理器。

与微处理器一样，智能卡内的存储器由于受到卡的外形尺寸的限制，容量一般都不是很大。智能卡的存储器通常由 ROM、RAM 和 EEPROM 组成。其中，RAM 通常不超过 256 个字节，仅提供给 COS 存放数据；COS 的代码部分（程序）则存储于 ROM 中。EEPROM 是智能卡的用户真正能够访问的存储区，这一部分存储了智能卡的各种信息、密码以及应用文件等，其容量通常在 2KB—32KB 之间。在这一部分采用 EEPROM 使得智能卡的成本相对较为昂贵，但却能够有效地提高可靠性，减少易失性，而且采用 EEPROM 也易于修改，容易保存数据，同时读写起来也十分方便，不需要附加设备。本节以后如果不特别说明，那么所说的存储器特指 EEPROM 部分。

由于存储器的容量不大，因此COS通常使用直接寻址方式，也就是直接使用物理地址访问存储单元。这样做的好处是可以使读写控制相对简单化，适应了智能卡简便的要求。

关于智能卡中存储器（EEPROM 部分）的布局情况，一般是随各自卡的不同而有各有的特点。但归纳起来，这些存储分区中通常应该至少包括如下几个部分：发行商区、保密字区、文件区。以法国 GEMPLUS 公司的产品 PCOS（Payment COS）为例，其存储器的布局如图 6.34 所示。从图中可见，其存储器划分为五个区：发行商区、ROM 代码控制区、保密字区、文件区和 FAT（File Allocation Table）区。其中，发行商区存储了智能卡及发行商的各种信息，例如卡的序列号、发行商的代码等等；ROM 代码控制区存储的是与操作系统相关的一些控制信息，例如用以标记智能卡使用阶段的锁定字、用以记录卡交易次数的交易计数器等等；保密字区存储了与文件操作的权限（例如读写权限）有关的各密码及其相应的描述信息；文件区用于存储智能卡的各种文件；FAT 区则用于存储与文件区中各个文件相对应的描述信息，其中包括文件在存储器中的起始地址、文件长度、文件权限，等等。总之，不同智能卡的存储器分区情况会有所不同，但大体上都至少包括了在前面提到的三个基本部分，尽管它们在分区中所对应的位置可能各不相同。

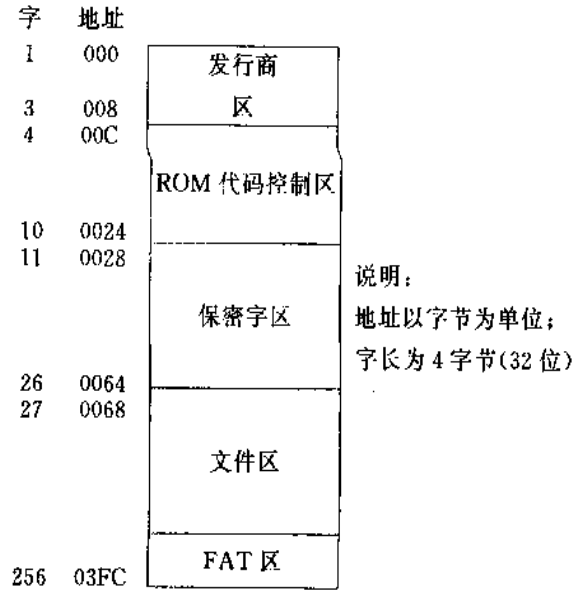


图 6.34 PCOS 的存储器组织

6.4 智能卡的操作系统——COS

随着IC卡从简单的同步卡发展到异步卡，从简单的EPROM卡发展到内带微处理器的智能卡(又称CPU卡)，对IC卡的各种要求越来越高。而卡本身所需要的各种管理工作也越来越复杂，因此就迫切地需要有一种工具来解决这一矛盾，而内部带有微处理器的智能卡的出现，使得这种工具的实现变成了现实。人们利用它内部的微处理器芯片，开发了应用于智能卡内部的各种各样的操作系统，也就是在本节将要论述的COS。COS的出现不仅大大地改善了智能卡的交互界面，使智能卡的管理变得容易；而且，更为重要的是使智能卡本身向着个人计算机化的方向迈出了一大步，为智能卡的发展开拓了极为广阔的前景。

6.4.1 COS概述

COS的全称是Chip Operating System(片内操作系统)，它一般是紧紧围绕着它所服务的智能卡的特点而开发的。由于不可避免地受到了智能卡内微处理器芯片的性能及内存容量的影响，因此，COS在很大程度上不同于我们通常所能见到的微机上的操作系统(例如DOS、UNIX等)。首先，COS是一个专用系统而不是通用系统。即：一种COS一般都只能应用于特定的某种(或者是某些)智能卡，不同卡内的COS一般是不相同的。因为COS一般都是根据某种智能卡的特点及其应用范围而特定设计开发的，尽管它们在所实际完成的功能上可能大部分都遵循着同一个国际标准。其次，与那些常见的微机上的操作系统相比较而言，COS在本质上更加接近于监控程序，而不是一个通常所谓的真正意义上的操作系统，这一点至少在目前看来仍是如此。因为在当前阶段，COS所需要解决的主要还是对外部的命令如何进行处理、响应的问题，这其中一般并不涉及到共享、并发的管理及处理，而且就智能卡在目前的应用情况而言，并发和共享的工作也确实是不需要的。

COS在设计时一般都是紧密结合智能卡内存储器分区的情况，按照国际标准(ISO/IEC 7816系列标准)中所规定的一些功能进行设计、开发。但是由于目前智能卡的发展速度很快，而国际标准的制定周期相对比较长一些，因而造成了当前的智能卡国际标准还不太完善的情况，据此，许多厂家又各自都对自己开发的COS作了一些扩充。就目前而言，还没有任何一家公司的COS产品能形成一种工业标准。因此本章将主要结合现有的(指1994年以前)国际标准，重点讲述COS的基本原理以及基本功能，在其中适当地列举它们在某些产品中的实现方式作为例子。

COS的主要功能是控制智能卡和外界的信息交换，管理智能卡内的存储器并在卡内部完成各种命令的处理。其中，与外界进行信息交换是COS最基本的要求。在交换过程中，COS所遵循的信息交换协议目前包括两类：异步字符传输的T=0协议以及异步分组传输的T=1协议。这两种信息交换协议的具体内容和实现机制在ISO/IEC 7816-3和ISO/IEC 7816-3 A1标准中作了规定；而COS所应完成的管理和控制的基本功能则是在ISO/IEC 7816-4标准中作出规定的。在该国际标准中，还对智能卡的数据结构以及COS的基本命令集作出了较为详细的说明。至于ISO/IEC 7816-1和2，则是对智能卡的物理

参数、外形尺寸作了规定，它们与 COS 的关系不是很密切。

6.4.2 COS 的体系结构

依赖于上一节中所描述的智能卡的硬件环境，可以设计出各种各样的 COS。但是，所有的 COS 都必须能够解决至少三个问题，即：文件操作、鉴别与核实、安全机制。事实上，鉴别与核实和安全机制都属于智能卡的安全体系的范畴之中，所以，智能卡的 COS 中最重要的两方面就是文件与安全。但再具体地分析一下，则我们实际上可以把从读写设备（即接口设备 IFD）发出命令到卡给出响应的一个完整过程划分为四个阶段，也可以说是四个功能模块：传送管理器（TM）、安全管理器（SM）、应用管理器（AM）和文件管理器（FM），如图 6.35 中所示。其中，传送管理器用于检查信息是否被正确地传送。这一部分主要和智能卡所采用的通信协议有关；安全管理器主要是对所传送的信息进行安全性的检查或处理，防止非法的窃听或侵入；应用管理器则用于判断所接收的命令执行的可能性；文件管理器通过核实命令的操作权限，最终完成对命令的处理。对于一个具体的 COS 命令而言，这四个阶段并不一定都是必须具备的，有些阶段可以省略，或者是并入另一阶段中；但一般来说，具备这四个阶段的 COS 是比较常见的。以下我们将按照这四个阶段对 COS 进行较为详细的论述。

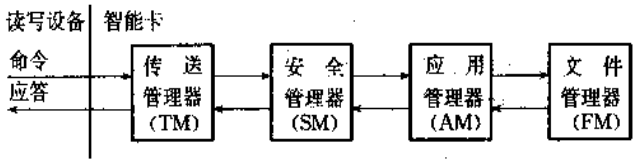


图 6.35 命令处理的过程

在这里需要提起注意的是，智能卡中的“文件”概念与我们通常所说的“文件”是有区别的。尽管智能卡中的文件内存储的也是数据单元或记录，但它们都是与智能卡的具体应用直接相关的。一般而言，一个具体的应用必然要对应于智能卡中的一个文件，因此，智能卡中的文件不存在通常所谓的文件共享的情况。而且，这种文件不仅在逻辑上必须是完整的，在物理组织上也都是连续的。此外，智能卡中的文件尽管也可以拥有文件名（File Name），但对文件的标识依靠的是与卡中文件一一对应的文件标识符（File Identifier），而不是文件名。因为智能卡中的文件名是允许重复的，它在本质上只是文件的一种助记符，并不能完全代表某个文件。

1. 传送管理（Transmission Manager）

传送管理主要是依据智能卡所使用的信息传输协议，对由读写设备发出的命令进行接收。同时，把对命令的响应按照传输协议的格式发送出去。由此可见，这一部分主要和智能卡具体使用的通信协议有关；而且，所采用的通信协议越复杂，这一部分实现起来也就越困难、越复杂。

我们在前面提到过目前智能卡采用的信息传输协议一般是 T=0 协议和 T=1 协议，如果说这两类协议的 COS 在实现功能上有什么不同的话，主要就是在传送管理器的实现上有不同。不过，无论是采用 T=0 协议还是 T=1 协议，智能卡在信息交换时使用的都是

异步通信模式；而且由于智能卡的数据端口只有一个，因此信息交换也只能采用半双工的方式，即在任一时刻，数据端口上最多只能有一方（智能卡或者读写设备）在发送数据。T=0、T=1 协议的不同之处在于它们数据传输的单位和格式不一样：T=0 协议以单字节的字符为基本单位，T=1 协议则以有一定长度的数据块为传输的基本单位。

传送管理器在对命令进行接收的同时，也要对命令接收的正确性作出判断。这种判断只是针对在传输过程中可能产生的错误而言的，并不涉及命令的具体内容，因此通常是利用诸如奇偶校验位、校验和等手段来实现。对分组传输协议，则还可以通过判断分组长度的正确与否来实现。当发现命令接收有错后，不同的信息交换协议可能会有不同的处理方法：有的协议是立刻向读写设备报告，并且请求重发原数据；有的则只是简单地在响应命令上作一标记，本身不进行处理，留待它后面的功能模块作出反应。这些都是由交换协议本身所规定的。

如果传送管理器认为对命令的接收是正确的，那么，它一般是只将接收到的命令的信息部分传到下一功能模块，即安全管理器，而滤掉诸如起始位、停止位之类的附加信息。相应地，当传送管理器在向读写设备发送应答的时候，则应该对每个传送单位加上信息交换协议中所规定的各种必要的附属信息。

2. 安全体系(Security Structure)

智能卡的安全体系是智能卡的 COS 中一个极为重要的部分，它涉及到卡的鉴别与核实方式的选择，包括 COS 在对卡中文件进行访问时的权限控制机制，还关系到卡中信息的保密机制。可以认为，智能卡之所以能够迅速地发展并且流行起来，其中的一个重要的原因就在于它能够通过 COS 的安全体系给用户提供一个较高的安全性保证。

安全体系在概念上包括三大部分：安全状态(Security Status)，安全属性(Security Attributes)以及安全机制(Security Machanisms)。其中，安全状态是指智能卡在当前所处的一种状态，这种状态是在智能卡进行完复位应答或者是在它处理完某命令之后得到的。事实上，我们完全可以认为智能卡在整个的工作过程中始终都是处在这样的、或是那样的一种状态之中。安全状态通常可以利用智能卡在当前已经满足的条件的集合来表示。安全属性实际上是定义了执行某个命令所需要的一些条件，只有智能卡满足了这些条件，该命令才是可以执行的。因此，如果将智能卡当前所处的安全状态与某个操作的安全属性相比较，那么根据比较的结果就可以很容易地判断出一个命令在当前状态下是否是允许执行的，从而达到了安全控制的目的。和安全状态与安全属性相联系的是安全机制。安全机制可以认为是安全状态实现转移所采用的转移方法和手段，通常包括：通行字鉴别，密码鉴别，数据鉴别及数据加密。一种安全状态经过上述的这些手段就可以转移到另一种状态，把这种状态与某个安全属性相比较，如果一致的话，就表明能够执行该属性对应的命令，这就是 COS 安全体系的基本工作原理。

从上面对 COS 安全体系的工作原理的叙述中，我们可以看到，相对于安全属性和安全状态而言，安全机制的实现是安全体系中极为重要的一个方面。没有安全机制，COS 就无法进行任何操作。而从上面对安全机制的介绍中，我们可以看到，COS 的安全机制所实现的就是如下三个功能：鉴别与核实，数据加密与解密，文件访问的安全控制。因此，我们将在下面对它们分别进行介绍。其中，关于文件访问的安全控制，由于它与文件管理器的

联系十分紧密，因此我们把它放到文件系统中加以讨论。

(1) 鉴别与核实：鉴别与核实其实是两个不同的概念，但是由于它们二者在所实现的功能上十分地相似，所以我们同时对它们进行讨论，这样也有利于在比较中掌握这两个概念。

通常所谓的鉴别(Authentication)指的是对智能卡(或者是读写设备)的合法性的验证，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；而核实(Verify)是指对智能卡的持有者的合法性的验证，也就是如何判定一个持卡人是经过了合法的授权的问题。由此可见，二者实质都是对合法性的一种验证，就其所完成的功能而言是十分类似的。但是，在具体的实现方式上，由于二者所要验证的对象的不同，所采用的手段也就不尽相同了。

具体而言，在实现原理上，核实是通过由用户向智能卡出示仅有他本人才知道的通行字，并由智能卡对该通行字的正确性进行判断来达到验证的目的的。在通行字的传送过程中，有时为了保证不被人窃听，还可以对要传送的信息进行加密/解密运算。这一过程通常也称为通行字鉴别，其具体流程可以参考图 6.36。

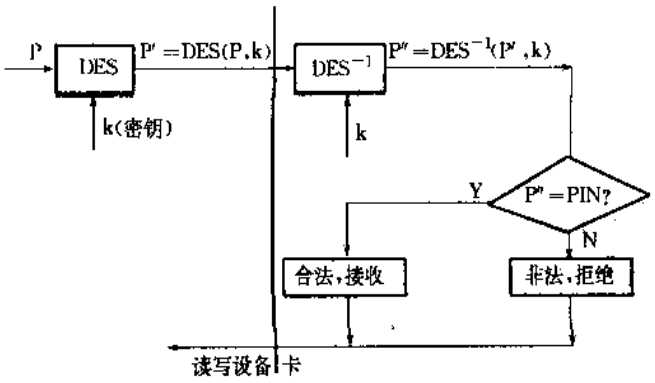


图 6.36 核实流程

鉴别则是通过智能卡和读写设备双方同时对任意一个相同的随机数进行某种相同的加密运算(目前常用 DES 算法)，然后判断双方运算结果的一致性来达到验证的目的的。根据所鉴别的对象的不同，COS 又把鉴别分为内部鉴别(Internal Authentication)和外部鉴别(External Authentication)两类。这里所说的“内部”、“外部”均以智能卡作为参照点，因此，内部鉴别就是读写设备对智能卡的合法性进行的验证；外部鉴别就是智能卡对读写设备的合法性进行的验证。至于它们的具体的实现方式，我们在第 5 章中已有详细论述，此处不再重复。

智能卡通过鉴别与核实的方法可以有效地防止伪卡的使用，防止非法用户的入侵，但还无法防止在信息交换过程中可能发生的窃听，因此，在卡与读写设备的通信过程中对重要的数据进行加密就作为反窃听的有效手段提了出来。关于数据加密的原理与方式可以参阅第 5 章。我们下面仅对加密中的一个重要部件——密码在 COS 中的管理及存储原理加以说明。

(2) 密码管理：目前智能卡中常用的数据加密算法是 DES 算法。采用 DES 算法的原因是因为该算法已被证明是一个十分成功的加密算法，而且算法的运算复杂度相对而言

也较小，比较适用于智能卡这样运算能力不是很强的情况。DES 算法的密码(或称密钥)长度是 64 位的。COS 把数据加密时要用到的密码组织在一起，以文件的形式储存起来，称为密码文件。最简单的密码文件就是长度为 8 个字节的记录的集合，其中的每个记录对应着一个 DES 密码；较为复杂的密码文件的记录中则可能还包含着该记录所对应的密码的各种属性和为了保证每个记录的完整性而附加的校验和信息，其结构如图 6.37 所示。其中的记录头部分存储的就是密码的属性信息，例如是可以应用于所有应用文件的密码还是只对应某一应用文件可用的密码；是可以修改的还是只能读取的密码等等。但是，不论是什么样的密码文件，作为一个文件本身，COS 都是通过对文件访问的安全控制机制来保证密码文件的安全性的。

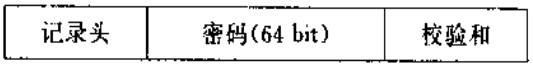


图 6.37　密码文件的记录结构

当需要进行数据加密运算时，COS 就从密码文件中选取密码加入运算。从密码文件中读出密码时，与读取应用数据一样，只要直接给出密码所在的地址就可以了。当然，最简单的产生密码的方法是直接从密码文件中随机读出一个密码作为加密用密码。但是这样的机制可能会多次选中同一密码，从而给窃听者提供破译的机会，安全性不太高。因此，比较好的办法是在随机抽取出一个密码后，再对密码本身作一些处理，尽量减少其重复出现的机会。例如 PCOS 产品中，采用的办法就是对从密码文件中选出的密码首先进行一次 DES 加密运算，然后将运算结果作为数据加密的密码使用。其计算公式如下：

$$Key = DES(CTC, K_s)$$

式中，K_s 是从密码文件中随机选取的一个密码；CTC 是一个记录智能卡的交易次数的计数器，该计数器每完成一次交易就增一；Key 就是最后要提供给数据加密运算使用的密码。使用这种方法可以提高智能卡的安全性，但却降低了执行的效率。因此，具体采用什么样的方法来产生密码应当根据智能卡的应用范围及安全性要求的高低而具体决定。

3. 应用管理器(Application Manager)

应用管理器的主要任务在于对智能卡接收的命令的可执行性进行判断。关于如何判断一条命令的可执行性，我们已经在安全体系一节中作了说明，所以我们可以认为，应用管理器的实现主要是智能卡中的应用软件的安全机制的实现问题。而因为智能卡的各个应用都以文件的形式存在，所以应用管理器的本质就是我们将要在下一节加以讨论的文件访问的安全控制问题。正是基于这一点，我们也可以把应用管理器看作是文件管理器的一个部分。

4. 文件管理器(File Manager)

与安全一样，文件也是 COS 中的一个极为重要的概念。所谓文件，是指关于数据单元或卡中记录的有组织的集合。COS 通过给每种应用建立一个对应文件的方法来实现它对各个应用的存储及管理。因此，COS 的应用文件中存储的都是与应用程序有关的各种数据或记录。此外，对某些智能卡的 COS，可能还包含有对应用文件进行控制的应用控制文件。在 COS 中，所有的文件都有一个唯一的文件标识符(File Identifier)，因此通过文件标

识符就可以直接查找所需的文件。此外，每个文件还可以有一个文件名作为助记符，它与文件标识符的不同之处在于它是可以重复的。COS 中的各文件在智能卡的个人化过程中由发行商(Issuer)根据卡的应用而创建，对卡的用户而言通常是不能对文件进行创建或删除的。但是用户可以根据情况对文件内容进行修改，可以对文件中的记录或数据单元进行增加、删除等操作。

(1) 文件系统：COS 的文件按照其所处的逻辑层次可以分为三类：主文件(Master File)，专用文件(Dedicated File)以及基本文件(Elementary File)。其中，主文件对任何 COS 都是必不可少的，它是包含有文件控制信息及可分配存储区的唯一文件，其作用相当于是 COS 文件系统的根文件，处于 COS 文件系统的最高层；基本文件也是必不可少的一个部分，它是实际用来存储各应用的数据单元或记录的文件，处于文件系统的最底层；而专用文件是可选的，它存储的主要是文件的控制信息、文件的位置、大小等数据信息。我们可以用图 6.38 的树状结构来形象地描述一个 COS 的文件系统的基本结构。

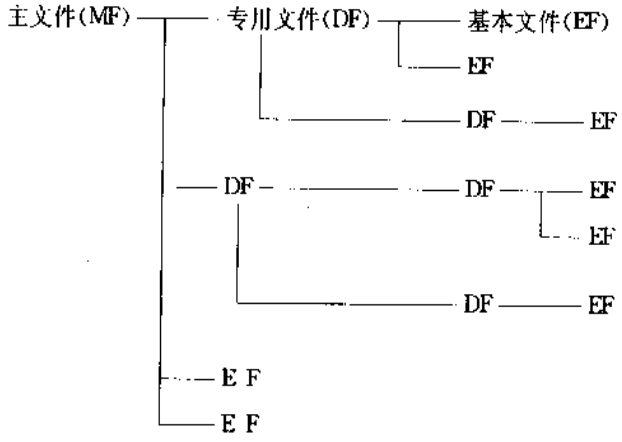


图 6.38 树状文件系统

当然，对于具体的某个 COS 产品，很可能由于应用的不同，对文件的实际分类标准会有所不同。但只要仔细地进行分析，都可以归结为上面的三个逻辑层次。例如前面提到过的 PCOS 产品。该产品的存储器分区情况在前面谈到图 6.34 的时候已经作了说明。它对文件的分类不是按照逻辑层次划分的，而是根据文件的用途进行的。它的文件分为三类：COS 文件(COS File)、密码文件(Key File)和钱夹文件(Purses File)。其中所谓的 COS 文件保存有基本的应用数据；密码文件存储的是进行数据加密时要用到的密码；钱夹文件的作用有些类似于我们日常生活中的钱包。由此可见，它的这三类文件本质上其实都属于基本文件(EF)类。在 PCOS 中，专用文件的概念不是很明显，但是事实上，如果大家留心的话，那么从以前的论述中，应该不难发现该产品存储器分区中 FAT 区内的文件描述器的作用就类似于专用文件；而整张 PCOS 卡本身的性质实际就是一个主文件。

COS 文件有四种逻辑结构：透明结构，线性定长结构，线性变长结构，定长循环结构。它们的定义及特点可以参阅 ISO/IEC 7816-4 协议中的有关部分，这里不再详述。不过，无论采取的是什么样的逻辑结构，COS 中的文件在智能卡的存储器中都是物理上连续存放的。卡中数据的存取方式、记录的编号方法、数据单元的大小等作为文件系统的特征，在智

能卡的复位应答过程中由卡给出。不过一般而言，在智能卡中最为重要的数据存取方式还是随机存取方式，也就是卡的用户在得到授权后，可以直接地任意访问文件中的某个数据单元或记录。至于COS具体对文件可以进行什么样的操作，我们将在COS的命令系统中进行讨论。

(2) 文件访问安全：对文件访问的安全性控制是COS系统中的一个十分重要的部分，由于目前的国际标准(ISO/IEC 7816-4)在这方面基本没有作出什么实质性的规定，因此，现有的文件访问的安全控制机制的具体实现方式多种多样。我们在这里准备介绍其中比较有代表性的两种实现方式：鉴别寄存器方式以及状态机方式。其中，采用鉴别寄存器方式的有PCOS、ME2000等产品；采用状态机方式的产品有STARCOS。

采用鉴别寄存器方式时，通常是在内存RAM中设置一个8位(或者是16位)长的区域作为鉴别用寄存器。这里的鉴别是指对安全控制密码的鉴别。鉴别用寄存器所反映的是智能卡在当前所处的安全状态。采用这种方式时，智能卡的每个文件的文件头(或者是文件描述器)中通常都存储有该文件能够被访问的条件，一般是包括读、写两个条件(分别用Cr、Cu表示)，这就构成了该文件的安全属性。而用户通过向智能卡输入安全密码，就可以改变卡的安全状态，这一过程我们通常称为出示，这就是鉴别寄存器方式的安全机制。把上面的三方面结合起来，就能够对卡中文件的读写权限加以控制了。具体的操作机制我们以PCOS为例加以描述。

首先，PCOS中的鉴别寄存器是8位字长的，这8位中的低7位分别与PCOS存储器中保密字区(参见图6.34)内的7个安全密码的序号一一对应。寄存器中每一位的初始值都被置为"0"。如果用户向智能卡出示了某一个安全密码，并且被卡判断为正确的话，系统就在鉴别寄存器的相应位上写入"1"。例如，如果处于保密字区中的第2个安全密码被用户正确出示的话，PCOS就在寄存器的第2位上写"1"。同时，文件描述器中的读、写条件Cr、Cu保存的都是在0和7之间的一个数，它的值对应了该文件进行读(或写)操作时所需要出示的密码在保密字区中的序号。在对某个文件进行读(或写)操作之前，系统首先判断在鉴别寄存器中对应的第Cr(或Cu)位是否已被置为"1"(如果Cr等于0，就表示该文件可以被用户随意读取；对于Cu也是一样)，只有当该位为"1"时，才表示读(或写)权限已经得到满足，才能对该文件进行读(或写)操作。这也就是说，如果用户想要对一个文件进行操作的话，就必须要首先出示对应于该文件的安全属性为正确的安全密码。系统据此就达到了对文件的访问进行安全控制的目的。

与鉴别寄存器方式完全不一样，状态机方式更加明显地表示出了安全状态、安全属性以及安全机制的概念以及它们之间的关系(关于状态机的知识不属于本书的范畴，有兴趣的读者请自行查阅有关资料)。以STARCOS为例，它采用的是一种确定状态机的机制，该机制通过系统内的应用控制文件(Application Control File，ACF)而得以实现。ACF文件的格式如图6.39所示，它是一个线性变长结构的文件，其中记录01包括了该ACF所控制的应用可以允许的所有命令的指令码(INS)；其余的记录分别与记录01中的指令码一一对应，其中存储的都是对应命令的变体(Varient)记录。所谓变体记录指的是这样的一些记录，记录中存储的是控制信息、初始状态、可能的下一状态以及某些附加的指令信息的组合，其结构可用图6.40表示。利用ACF中的这些变体记录就可以形成状态转移

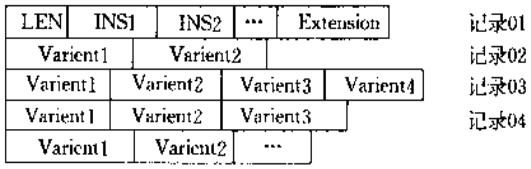


图 6.39　应用控制文件

图。在变体记录中，控制信息部分是必不可少的。不同的变体记录主要在两个方面有区别：一是命令所允许的状态不同；二是以 CLA 字节开始的指令信息部分不相同。这主要是由命令要操作的应用对象的不同而决定的。

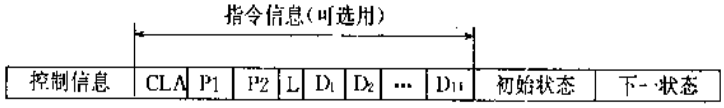


图 6.40　变体(Varient)记录结构

利用 ACF，COS 系统就可以实现对文件访问的安全控制了。当系统接收到一个应用进行操作的一条命令后，首先检验其指令码是否在相应的 ACF 文件的记录 01 中。如果不在其中，系统就认为该命令是错误的。在找到了对应的指令码后，系统把命令的其余部分与该命令对应的各变体记录中的指令信息按照该变体记录的控制信息的要求进行比较，如果比较结果一致，那么再查验变体记录中的初始状态信息。若所有这些检测都顺利通过，那么系统就进入对应变体记录中指明的下一状态；否则，继续查找下一个变体记录直到发现相应变体或是查完该命令对应的所有变体记录为止。如果没有找到相应的变体记录，说明该命令是非法的；否则就进入下一步对命令的处理，即由 COS 调用实际的处理过程执行对命令的处理。当且仅当处理过程正常结束的时候，系统才进入一个新的状态，并开始等待对下一条命令的接收。

6.4.3　COS 的命令系统

前面讲述了 COS 的体系结构，而在智能卡具体进行处理时，系统所采用的都是命令－应答对的方式，如图 6.41 所示。由读写设备发出命令，智能卡则接收命令，进行处理，处理完毕后送出相应的应答。所以要讨论智能卡的 COS，还有必要了解它的命令。

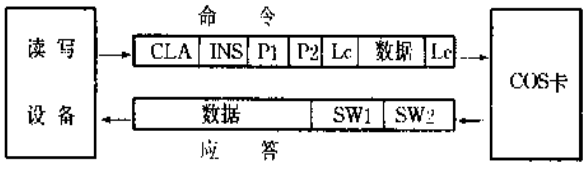


图 6.41　COS 的处理机制

COS 的基本命令集在 ISO/IEC 7816-4 国际标准中已有了规定，其中主要是有关文

件操作方面的命令，诸如记录的读写、数据单元的读写、数据流的存取等等，而数据的交换是通过逻辑信道进行的，因此命令集中还包括了信道管理命令；此外，还有鉴别与核实命令。从COS的命令集我们也可以看出智能卡的两个重要部分就是文件与安全。而对于一张具体的智能卡，往往因为它的应用的关系，使其命令集相对于国际标准中的基本命令集都要作一些不同程度的扩充，例如STARCOS的命令集共有28条命令，在其中属于ISO/IEC 7816-4标准命令集的则仅有9条(参见表6.11)。

表6.11 STARCOS的命令集

命　令	应用范围	符合ISO/IEC 7816-4
CLOSE FILE	文件管理	
CREATE FILE	文件管理	
CRYPT	加密运算	
DECREASE	计数器	
DELETE FILE	文件管理	
DELETE RECORD	文件管理	
EXCHANGE CHALLENGE	鉴别	
EXTERNAL AUTHENTICATE	鉴别	✓
GET CARD DATA	鉴别	
GET CHALLENGE	鉴别	
INCREASE	计数器	
INTERNAL AUTHENTICATE	鉴别	✓
KEY STATUS	密码管理	
LOCK FILE	文件管理	✓
LOCK KEY	密码管理	
MUTUAL AUTHENTICATE	鉴别	
READ BINARY	文件管理	✓
READ RECORD	文件管理	✓
REGISTER DF	文件管理	
SECURE DECREASE	计数器	
SECURE INCREASE	计数器	
SELECT FILE	文件管理	✓
SET KEY	信息安全	
VERIFY	鉴别	✓
VERIFY AND CHANGE	鉴别	
WRITE BINARY	文件管理	✓
WRITE KEY	密码管理	
WRITE RECORD	文件管理	✓

COS的命令格式在图6.41中已有表示。其中，CLA字节是类型字节，INS字节是指令码字节，P1、P2是命令参数字节，Le域是长度域，用以指明命令后面的数据区的长度，

Lc 域用以指明命令所希望的应答的长度。至于命令的具体细节，请参阅 ISO/IEC 7816-4 的相关部分。

智能卡接收命令后，对之进行处理，然后给出对命令的应答。应答的格式也在图 6.41 中作了表示。其中，数据域是应答数据，SW1、SW2 是命令处理完毕后的状态字，其具体细节也请参阅 ISO/IEC 7816-4 的相关部分。

为了加深对命令系统的理解，下面我们具体说明一条命令的实现过程。以命令 CREATE FILE 的实现为例。

CREATE FILE 命令不属于 ISO/IEC 7816-4 所定义的基本命令集，它是为了发行商的个人化进程而设计的。该命令的功能是从当前路径出发创建一个新的文件。

1. 命令格式及信息

命令格式如表 6.12 所示。

表 6.12 CREATE FILE 命令格式

CLA	INS	P1	P2	Lc	DATA					
"EX"	"E0"	IDH	IDL	"07"	FCI					
					DSC	LOCK	ACC	RLEN	BIG	MESSAGE

表 6.12 中各数据域的含义如下：

IDH：所要创建文件的标识符的高位字节；

IDL：所要创建文件的标识符的低位字节；

FCI：所要创建文件的信息，其中：

DSC：文件描述符，提供文件的类型、结构及可访问性的描述；具体内容参阅 ISO/IEC 7816-4。

LOCK：封锁标志字节，

BIT0 为读封锁标志，为"1"表示不可读；

BIT1 为写封锁标志，为"1"表示不可写；

ACC：文件读写权限标志；高四位表示文件的读权限，低四位表示文件的写权限；

RLEN：记录长度，表示线性定长结构文件的记录的长度；

BIG：所要创建的文件的长度；

MESSAGE：创建文件的一些信息，其内容和意义由具体文件具体决定。

2. 条件与限制

(1) 若当前文件只有 MF，则建立它的子文件；

若存在当前 DF，并且没有当前 EF 时，则建立该 DF 的 EF 子文件；

若存在当前 EF，则建立过程失败。

(2) 所创建文件的 ID 号不得与其它任何文件的 ID 号发生冲突；

(3) 创建文件必须出示发行商密码；

(4) 创建的文件为线性定长结构文件时，其记录长度不得为 0；

3. 应答格式及信息

本命令的响应APDU只包含状态字节SW1、SW2，数据域为空。SW1、SW2的具体含义见表6.13。

表6.13 CREATE FILE命令应答信息

SW1 SW2	意 义
"90－00"	文件创建成功
"6F－00"	命令APDU有错误
"6A 86"	命令参数P1不为0或者P2不为0
"67 00"	命令数据域长度Lc不等于7
"6A－81"	线性定长结构记录长度为0； DF的子文件仍然是DF；(1) 创建文件的长度过小；(2)
"69－86"	当前文件为EF
"69－82"	未出示发行商密码
"69－81"	文件标识符重复使用
"69－81"	没有足够空间创建文件

(1) 对于本命令所在的COS系统，由于只允许存在至多二层文件(MF－DF－EF)，所以DF之下不可能再有DF子文件；

(2) 对于本命令所在的COS系统，每个文件的长度都必须至少大于其文件头的长度，如果BIG的值小于文件头的长度，则系统认为创建失败。

4. 命令实现流程

对CREATE FILE命令的具体处理流程可以描述如下：

```
prodecure CREATE FILE
{
  if(APDU有错误)        exit(6F00);
  if(Lc不等于7)         exit(6700);
  if(创建文件的长度小于文件头长度)        exit(6A81);
  if(创建文件为线性定长结构而且记录长度为0)       exit(6A81);
  if(当前文件为EF文件)       exit(6986);
  if(未出示发行商密码)       exit(6982);
  if(创建文件ID号等于3F00或3FFF)       exit(6981);
  if(当前文件为DF文件)
  {
    if(创建文件ID号与该DF的兄弟文件相同)       exit(6981);
    if(创建文件为DF文件)       exit(6A81);
    if(创建文件ID号与该DF的子文件相同)       exit(6981);
    从当前DF查找可分配的存储区;
    if(没有找到可分配的存储区)       exit(6984);
```

```
        写入文件头;
        修改文件系统表;
        return(9000);
      }
      if(当前文件为 MF)
      {
        if(创建文件 ID 号与 MF 的子文件相同)        exit(6981);
        从 MF 查找可分配的存储区;
        if(没有找到可分配的存储区)        exit(6984);
        写入文件头;
        修改文件系统表;
        return(9000);
      }
    }
```

6.5 智能卡举例(MC68HC05SC 系列)

摩托罗拉(Motorola)公司推出的 MC68HC05SC 系列芯片专用于智能卡,该公司于1979 年推出的单芯片微控制器 MCU(Micro Controller Unit)用于法国银行,Motorola 公司在智能卡芯片技术领域内处于领先地位,该公司是将 HCMOS 和 EEPROM 技术应用于智能卡的第一个制造厂商,在过去 15 年中已运输出 4 千万个器件。Motorola 公司只生产芯片,不制造卡,即不进行将芯片模块嵌装入卡内的工作。世界上大多数智能卡制造厂包括 Bull、Citizen、Datacard、E. C. TEQ、Gemplus、GAO 和 Philips 等都使用 Motorola 公司的芯片。因此本节选择 Motorola 的 MC68HC05SC 系列芯片作为介绍智能卡的例子。下面首先简单介绍一下 Motorola 公司有关智能卡和安全问题的一些观点,然后介绍 MC68HC05SC 系列芯片。

1. 智能卡的优点

·提高数据安全性

智能卡可以采用多种方法提高安全性,因为它可以对存储在卡中的信息的存取作出限制,可以保护软件。

· 应用灵活性

智能卡可以同时用于几种不同的应用。卡与系统的互相操作是受存放在卡中和系统中的软件控制的。可以对卡中的部分软件进行修改,其方法是对卡中的非易失性存储器的一部分重新编程。

·应用与交易的合法性证实

当卡连到合法的系统以实现某项应用时,通过来自用户的数据(如生物特征或 PIN 数据)或系统的数据(如加密/解密密钥),可在任何时候对持卡人或系统进行验证。

· 价格通过有效性予以补偿

智能卡的价格比磁卡贵，但其原始价格可通过以下因素予以补偿：

(1) 发行后，智能卡的重构能力强；并具有同时存储几种不同应用的数据的能力。

(2) 减少发行收入的损失，即由欺诈性的使用和欺诈性的仿制造成的损失。

(3) 独立方式实现功能的能力强，因此可减少依赖于系统的花费。而且智能卡读卡器的价格也比基于投硬币的读卡器的价格便宜。

· 多应用能力

因为智能卡中有一个智能微处理器，因此可实现一种以上的应用，即一卡多用，从而可比使用多张卡节省费用。

· 脱机能力

因为智能卡可完成合法性检查、能存储交易的详细数据，因此不必为每一笔交易与中央计算机/数据库进行通信，提高了交易速度，降低了处理费用。

2. 安全问题

为了保证智能卡的安全应用，芯片制造商与卡的发行商要明确各自的职责。芯片制造商在设计芯片时要考虑安全问题，并注意制造安全；卡的发行商要保证应用安全。

从芯片设计到智能卡应用的全过程请参阅附录 F。

· 芯片安全的设计实现

MCU 包含有 CPU、RAM、ROM 和 EEPROM 等，ROM 中存放操作系统及固定数据；EEPROM 中存放密码和数据，有时还存放部分与应用有关的程序；RAM 中仅存放一些中间结果。外界对卡发布的命令需要通过操作系统才能对 CPU 起作用，而操作系统在 ROM 中，是不可能改变的，因此为安全应用提供了可靠的基础。

对 RAM、ROM 和 EEPROM 分成若干个存储区，根据安全需要可对各分区进行读保护，即在一定条件下，某些分区不允许读出，或虽允许从存储器中读出，但不能送到卡的触点上，以防不正当窃取。对 EEPROM 的各个分区还可分别进行写入/擦除保护。

对程序的失控采取预防性保护措施，设置多重“非正常运行状态”监视手段，以使该装置在非正常情况下停机（或采取其它保护措施），例如 MC68HC05SC27 和 MC68HC05SC28 设置“Watchdog”，监视程序是否“逃逸(runaway)”，并强迫它回到正确的程序流中。

在每个芯片的存储器中写入各不相同的序列号(跟踪数据)和密码；软件能对卡、持卡人、读写设备进行相互鉴别，使得任一方面都不能进行伪造，甚至包括每一笔交易数据在内。

此外 Motorola 公司还在不断探索新方法，以便为潜在的盗用者设置层出不穷的新障碍，例如在常规基础上通过巧妙地改变微处理器的某些细节，迫使未经授权的用户不得不一遍又一遍地进行解密，否则他们就不能非法进入该系统。

同样，出自安全考虑，制造厂对此不能介绍得很详细。

· 制造时的安全措施

封闭的制造环境和流程，不准无关人员进入制造地区，各个工序之间严格保持独立，对产品(每个模片)进行严格的跟踪管理；或者发运给客户，或者在内部安全地销毁。其目的是防止伪造和丢失。

限制接触载有客户的软件和保密规范的计算机系统和软件。每个装置可设置单独的密码。

将测试合格的芯片制成器件(模块或卡)后,可运送给发行商。为保证运输过程的安全,发行商可将他自己定义的密钥及算法告诉制造商,制造商按算法运算后,将结果作为"运输密钥"写入 EEPROM 中;发行商收到卡后,按照同一算法进行验证,通过后,才允许卡进一步工作,否则卡将自锁。

今将运输密钥介绍如下:

运输密钥 Transport Key=TK=f(TD,CP,MP)。

其中 TD 是跟踪数据,CP 是发行商 PIN,MP 是 Motorola 公司的 PIN。

运输密钥的生成与器件的激活过程:

在 Motorola 公司生成 TK,并将 TK、TD 写入 EEPROM,经过最后的测试后,断开熔丝,将器件运送给发行商,其过程如图 6.42 所示。

器件送到发行商处以后,在第一次加电时,从器件中读出 TD,送读卡器(Reader),根据同一算法,在读卡器中得到 TK,并将 TK 送到器件,在器件内将器件的 TK 和读卡器的 TK 进行比较,如相等,则表示通过,其过程如图 6.43 所示。仅当验证通过后,才允许对卡进一步操作。

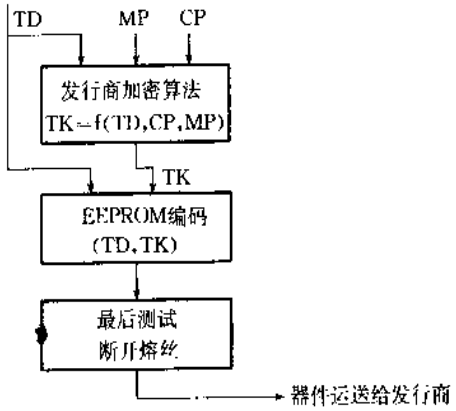


图 6.42 运输密钥的生成(在 Motorola 处)

·应用安全

Motorola 公司不仅自己认真对待保密事宜,而且教育和鼓励所有智能卡用户以同样的态度对待保密事宜,智能卡用户应对他们所控制的那部分系统(如固化在芯片上的软件以及系统的软件和硬件)采取适当的保密措施。

软件保密战略包括了从非常简单的到极为复杂的密码算法演算和鉴别过程,这些程序中有许多是个别用户的应用产品所独享和专用的,但也有一些简单的、普遍适用的、体现保密意识的软件开发手段:

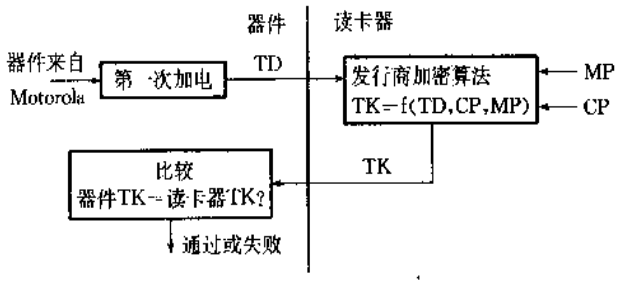


图 6.43 运输密钥验证(在发行商处)

(1) 考虑软件运行到关键部分时电源(意外和人为)中断后造成的后果。

(2) 在软件设计中加上计数功能，限制输入错误密码的次数。

(3) 在软件中加入一些程序，以保证在系统被重新设置后的特定时间里，某些特别敏感的事情(如向 EEPROM 写入新的数据或指令)不会不受限制地发生。

(4) 降低软件的可读性。

(5) 采用以时间为基准的子程序。

(6) 通过防止从 EEPROM 执行程序的方法，限制应用程序自我修改的能力。

(7) 在软件中加入"测试"命令，以便在无须输出任何软件内容的条件下对出现的问题进行调查。

(8) 控制在开发过程之中和之后了解软件和硬件的任何细节的途径。

3. MC68HC05SC 系列芯片

表 6.13 列出 MC68HC05SC 系列的型号、存储器容量和典型应用。与其它制造厂相比，Motorola 芯片的尺寸较小，这对芯片的可靠性有利。

表 6.13 MC68HC05SC 系列

型 号	ROM B	RAM B	EEPROM B	EPROM B	典型应用	芯片尺寸(mm²)
MC68HC05SC01	1800	36	无	1K	/	5.5×3.5
MC68HC05SC11	6K	128	无	8K	付费电视	3.5×5.6
MC68HC05SC21	6K	128	3K	无	GSM 移动电话，付费电视	2.9×5.1
MC68HC05SC24	3K	128	无	1K	银行	2.8×3.7
MC68HC05SC26	6K	224	1K	无	银行，预付费 GSM	3.8×3.8
MC68HC05SC27	16K	240	3K	无	银行，付费电视，GSM	4.2×5.0
MC68HC05SC28	12K	240	8K	无	GSM，多功能卡	4.9×5.3
MC68HC05SC29	13K	512	4K	无	秘密机器(武器)，健康，金融	4.8×6.2

(1) 芯片的组成及逻辑图

本系列各种型号的逻辑图基本相同。

图 6.44 为 MC68HC05SC21 的逻辑图。

图中 CPU 为中央处理单元，执行在 ROM 或 EEPROM 中的程序，图 6.45 示出寄存器的组成。

累加器 A(8 位)用于保持操作数或运算结果。

变址寄存器 X(8 位)用于变址寻址方式，也可用作暂存寄存器。

堆栈指针 SP(13 位)的高 7 位为 0000011，堆栈用于保存子程序调用时的返回地址和中断处理时的机器状态，其访存地址范围为 00FF—00C0，在 RAM 中。

程序计数器(13 位)指出下一条将执行的指令地址。

条件码寄存器 CC(5 位)指出刚执行的指令的结果，对其各位说明如下：

半进位位(H)　执行 ADD 或 AD 指令时，从第 3 位到第 4 位的进位。

中断屏蔽位(I)　当 I 位为 1 时，所有中断均被禁止。

负(N)　当 N 为 1 时，指出最后一次算术运算、逻辑运算或数据处理的结果为负(或

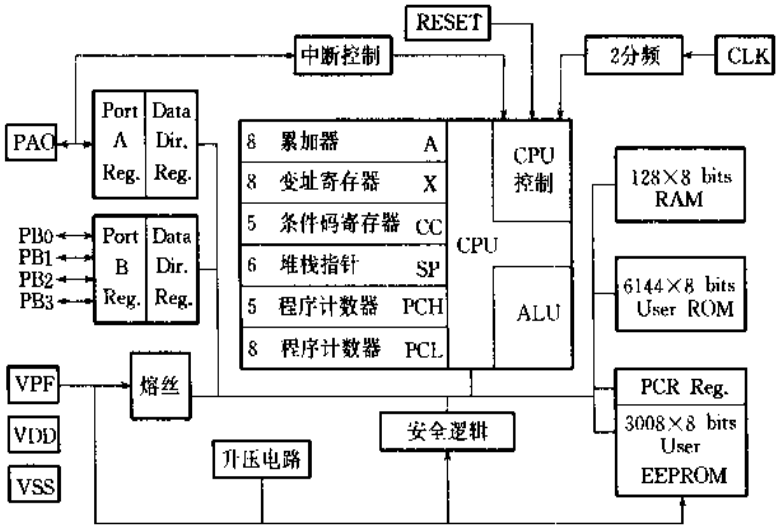


图 6.44　MC68HC05SC21 的逻辑图

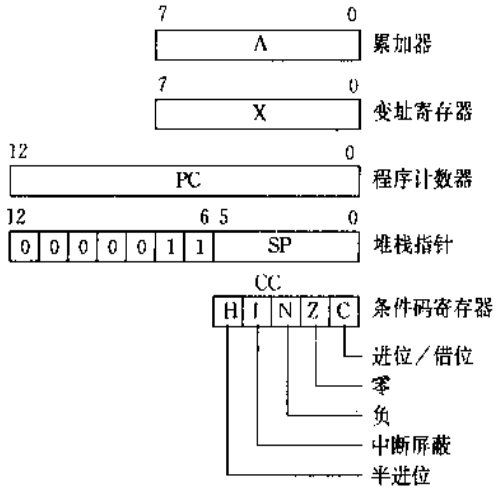


图 6.45　CPU 的寄存器

第 7 位为逻辑 1)。

零(Z)　当 Z 为 1 时,表示最后一次算术运算、逻辑运算或数据处理的结果为零。

进位/借位(C)　当 C=1 时,表示最后一次算术运算产生进位或借位。

图 6.46 示出芯片的压焊块。用于智能卡时有 6 个引出端,符合标准的规定。其中 VPF 用于烧断熔丝,PA0 为 I/O 端,其它 4 个引出端不再解释。

图 6.46 中还有 4 个压焊块 PB0、PB1、PB2 和 PB3。与 PA0 一起共为 5 个输入/输出线(见图 6.45),每根线可通过编程分别设定为输入线或输出线,但用于智能卡时,PB0—PB3 不起作用。图 6.44 中的 Port A Reg. 为 1 位数据寄存器,Data Dir. Reg. 为 1 位数据方向寄存器,指出数据的传送方向(输入或输出)。Port B Reg. 和 Data Dir. Reg. 的意义相似,但各有 4 位。

图 6.47 是存储器和寄存器的地址分配图。

存储器地址有 13 位，从 0000 到 1FFF。访问 ROM—0 页还是 ROM—1 页由 ROMPG 位来控制，当 ROMPG=1 时，访问 ROM—1 页。但 ROM—1 页仅有 2304B，其余仍按 ROM—0 页处理。执行擦除 EEPROM 操作后，被擦除的 EEPROM 的内容为“0”；写操作只允许写“1”。在 EEPROM 中有 n 个字节被称为安全字节，允许在测试方式对它进行编程，而在用户方式只能读出，芯片有两种工作方式：测试方式和工作方式。

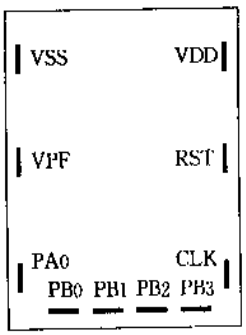


图 6.46 MC68HC05SC 的压焊块

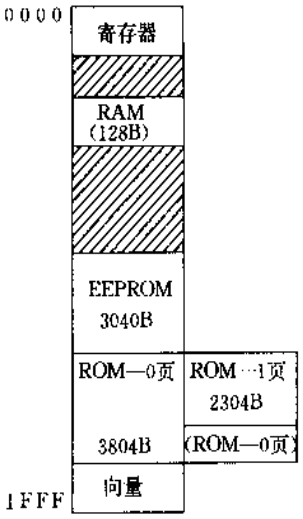


图 6.47 存储器和寄存器的地址分配

芯片出厂前处于测试方式，对它进行测试、编程和分析都比较容易。器件出厂时，被置于用户方式，由于外界访问 MCU 受到限制，因此当器件出问题时，要对它的运行情况进行测试和分析特别困难，需要运用软件知识以及依靠制造厂和用户之间的紧密合作才可能进行分析。而且一旦设置成用户方式后就不能再回到测试方式。

(2) MC68HC05SC21 芯片的布局和照片。

图 6.48 为芯片的布局图，图 6.49 为照片。

MC68HC05SC21 的芯片面积为 3.5×5.6mm²。今后，如果增加芯片逻辑的复杂性和增加存储器容量，紧凑的布图设计可能会成为关键问题。

不同类型存储单元，其面积不相同，若将 1 位 ROM 所占的面积定为 1，则有下列关系存在：

芯片类型	ROM	EPROM	EEPROM	DRAM	SRAM
面积：	1	3	7	15	30

(3) 其他特点

本系列中的某些型号芯片，在其内部有安全逻辑电路，并能经受冲击；有加电检测能力；有不工作时可处于省电的 STOP 和 WAIT 工作方式。另外芯片内部的 EEPROM 的允许擦写次数与温度、电压有关，如表 6.14 所示。

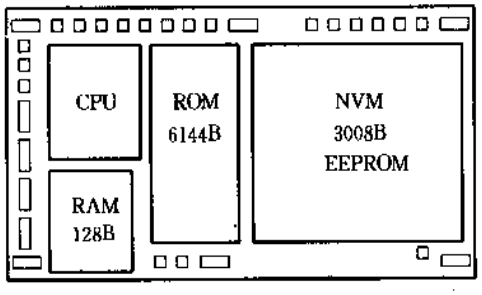


图 6.48 芯片的布局示意图

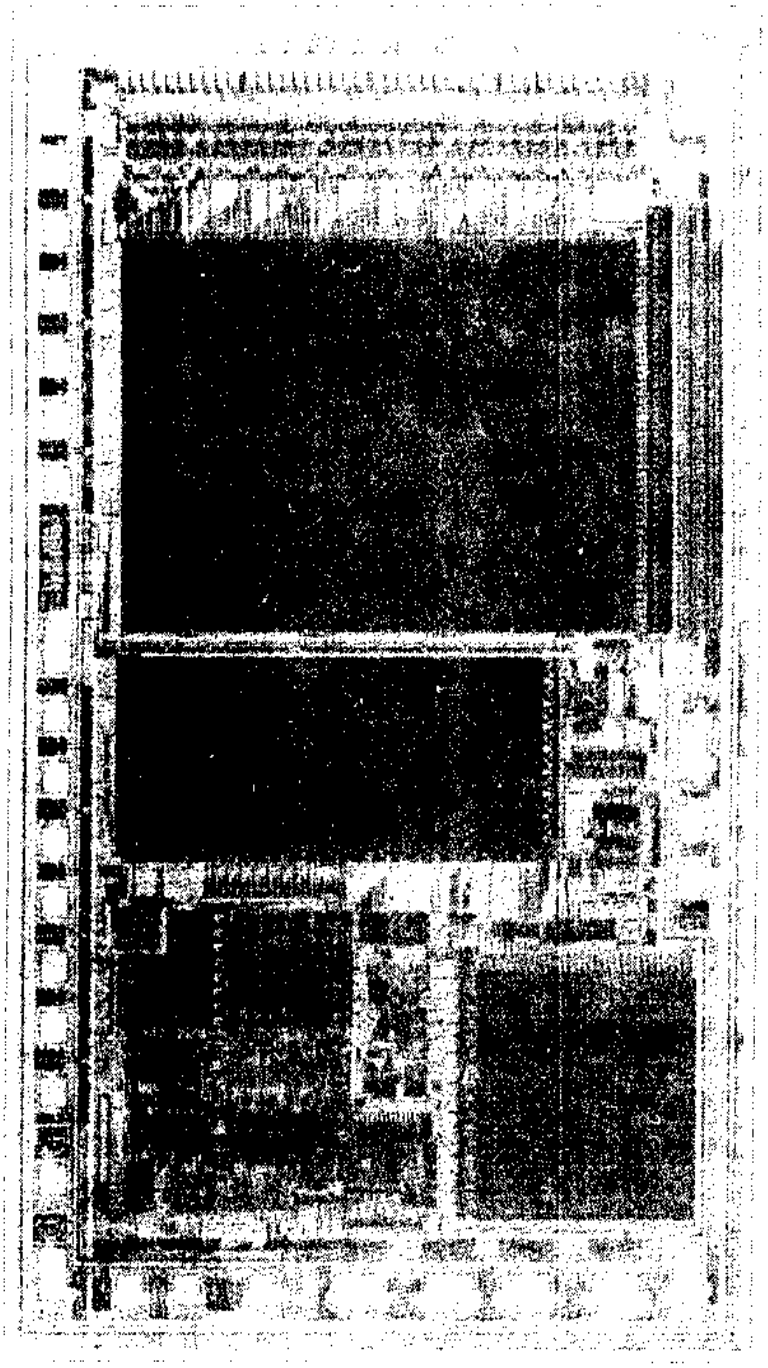


图 6.49　MC68HC05SC21 芯片的照片

表 6.14　擦/写次数与温度、电压的关系

擦/写次数	工作温度	工作电压	擦/写次数	工作温度	工作电压
10K 次	85℃	5V	100K 次	25℃	5V
20K 次	60℃	5V	200K 次	25℃	3V
35K 次	50℃	5V			

数据保持时间也与环境温度有关，在85℃环境下可保持10年，环境温度降低可延长数据保持时间。

4. MC68HC05SC的指令系统

与MC68HC05的指令系统相同，其CPU共有59条指令，6种寻址方式，指令字长度可变(1～3字节)，数据字长度为8位。

(1) 寻址方式

·固有的(或隐含的)寻址方式

一字节指令，操作数地址隐含在指令码中，如TAX指令，其功能是将变址寄存器(X)内容传送到累加器(A)，指令码为97。

·立即数寻址方式

二字节指令，第一字节为操作码，第二字节为8位立即数，如LDA #$B5指令，其功能是将立即数B5送到累加器中，其中#表示立即数，$表示其随后的数用16进制表示，这条指令的指令码为A6B5，即A6为操作码，B5为立即数，这两个字节在存储器中是相邻存放的。

·直接寻址方式

二字节指令，第一字节为操作码，第二字节为存储器地址，因地址只有8位，所以寻址的地址范围限于00—FF。这两个字节在存储器中是相邻存放的。

·扩展寻址方式

三字节指令，第一字节为操作码，第二字节和第三字节为地址码，因有16位地址，所以可对整个存储器进行寻址。这三个字节在存储器中是相邻存放的。

·变址寻址方式

一字节或三字节指令(指令中分别包含一字节或二字节偏移值)，访问存储器的地址=变址寄存器的内容(X)+偏移值。

·相对寻址方式

二字节指令，通常应用于转移指令中，转移地址=(PC)+偏移值。

(2) 指令系统

MC68HC05的指令及其功能列于表6.15中。

表6.15 MC68HC05指令集

类型	符号	功　能
传送指令	LD	从存储器装入A或从存储器装入X
	ST	将A的内容存入存储器或将X的内容存入存储器
	TAX	A的内容传送到X
	TXA	X的内容传送到A
算术运算指令	ADD	A+(M)→A　(M)表示存储器内容，下同
	ADC	A+(M)+C→A　C为进位，在CCR寄存器中，下同
	SUB	A−(M)→A
	SBC	A−(M)−C→A

续表

类型	符号	功　能
算术运算指令	CLR	0→A，或 0→X，或 0→M
	INC	A+1→A，或 X+1→X，或(M)+1→M
	DEC	A−1→A，或 X−1→X，或(M)−1→M
	COM	$\overline{A}$→A，或 $\overline{X}$→X，或($\overline{M}$)→M，取反码
	NEG	00−A→A，或 00　X→X，或 00−(M)→M
	MUL	A * X→X ‖ A
移位指令	ASL	算术左移
	ASR	算术右移
	LSL	逻辑左移
	LSR	逻辑右移
	ROL	循环左移
	ROR	循环右移
测试指令	TST	执行 A−00 或 X−00 或(M)−00，根据结果置 CCR 寄存器中的 N 和 Z
	BIT	用(M)作为屏蔽位选择 A 的相应位，并根据选择结果置 N 和 Z
	CMP	A−(M)，置条件码
	CPX	X−(M)，置条件码
CCR 指令	SEC	进位位置 1，1→C
	CLC	进位位清除，0→C
	SEI	中断屏蔽位置 1，1→I
	CLI	中断屏蔽位清除，0→I
逻辑指令	EOR	A⊕(M)→A
	OR	A ∨ (M)→A
	AND	A ∧ (M)→A
转移指令	BHI	如(C ∨ Z)=0，转移(大于转移)
	BHS	如 C=0，转移(大于等于转移)
	BPL	如 N=0，转移(正转移)
	BMI	如 N=1，转移(负转移)
	BEQ	如 Z=1，转移(相等转移)
	BNE	如 Z=0，转移(不等转移)
	BLS	如(C ∨ Z)=1，转移(小于等于转移)
	BLO	如 C=1，转移(小于转移)
	BCS	如 C=1，转移(进位位为 1，转移)
	BCC	如 C=0，转移(进位位为 0，转移)
	BRA	必转移(PC+d→PC)
	BRN	不转移(PC+2→PC)
	BM	I=0 转移或 I=1 转移(BMC 或 BMS)，I 为中断屏蔽位
	BI	IRQ=1 转移或 IRQ=0 转移，IRQ 为中断请求线
	BHC	H=0 转移或 H=1 转移，根据 CCR 中的 H 位转移
	BSET	根据 A，置存储器相应位，1→(M_n)
	BCLR	根据 A，清存储器相应位，0→(M_n)

续表

类型	符号	功　能
转移指令	BRCLR	如存储器中的某指定位为0,转移
	BRSET	如存储器中的某指定位为1,转移
	JMP	转移
	JSR	转子程序,PC→堆栈,SP－2→SP,转移地址→PC
	BSR	转子程序,PC→堆栈,SP－2→SP,PC＋d→PC
	RTS	从子程序返回,返回地址从堆栈送PC,SP＋2→SP
控制指令	RTI	从中断返回
	SWI	软中断
	WAIT	停止处理,并等待超时或中断
	STOP	下电,等待Reset或外中断
	NOP	不操作
	RSP	置堆栈指针

小　结

本章主要介绍了存储器卡、逻辑加密卡与智能卡,由于智能卡中有CPU,因此可以通过编程来适应各种应用场合,其可靠性、安全性和灵活性都居于首位,但价格也最贵。

除此以外,还有几种类型的卡,其价格、性能之间的比较如表6.16所示。

表6.16　卡的类型及比较

卡的类型	价格	容量	通用性	安全性	卡的类型	价格	容量	通用性	安全性
凸印塑料	低	无	无	无	带MCU	高	中	高	高
全息照相	低	无	无	低	带多芯片	高	中	高	高
带磁条	低	低	低	低	带光存储	中	高	中	中
带EEPROM	中	中	低	低	带机械存储	低	低	无	无
带逻辑加密电路	中	中	低	中					

注:· 当前有些卡是凸印塑料、磁条和芯片的组合。

· 多芯片在这里指的是带有MCU的无接触卡,依靠发射和接收电磁波来传送信息。

智能卡的CPU核心部分可采用一般通用的微处理器,实际上目前在智能卡中使用的CPU也就是通常在单片机中使用的微处理器,如MC68HC05,i8051等的核心部分。其差别是I/O接口比较简单,且I/O触点是串行入/出端,无外部中断等,很多特殊功能(如鉴别、安全等)都是依靠COS来实现的。因此COS的设计是很重要的。

对COS既希望它有良好的通用性和灵活性,又希望它不容易被攻破,这两个要求是互相矛盾的,但是又必须互相协调解决好,这就是COS设计的难点所在。

当采用某些加密/解密算法时,可能经常要重复进行某些复杂运算,如依靠通用的微处理器来完成这些运算,用户使用时所需等待的时间较长,此时可能要专门设计适用于某一算法的协处理器,但是由于IC卡对芯片尺寸的限制,较复杂的运算还是希望能够设法

在外部实现。在附录E中，将对RSA算法的实现进行介绍。

思 考 题

1. IC卡的卡内芯片有哪三种类型？各类芯片内部的组成情况如何？
2. EEPROM的擦除、写入是怎样定义的？它的读出和写入时间与RAM相比有什么特殊处？
3. 逻辑加密卡的存储器一般分成哪几个区，各区如何定义？
4. 在验证逻辑加密卡持卡人身份时，是否允许将PIN从卡中读出并送到读写设备中去进行比较？简述其原因。
5. 当用户输入错误的PIN，且输入次数已达到卡所允许的最大次数，为安全起见应采取什么措施？该措施需由用户设定还是由卡自动完成？如卡中还保存有余额，应该作废还是应该设法让用户不受损失或少受损失？
6. 逻辑加密卡的擦除密码的作用何在？
7. 逻辑加密卡卡内熔丝的作用何在？一般应设置多少个熔丝？采用什么手段实现熔丝的功能？
8. 智能卡芯片内包含哪些内容？各起什么作用？
9. 智能卡芯片中有三种存储器类型(ROM、RAM和EEPROM)，是否可减少？请说明原因？
10. 是否可将片内操作系统(COS)的功能移到读写设备中去实现？请说明原因？
11. COS中包括哪些内容？
12. 在本章中介绍的逻辑加密卡和智能卡各采取什么传输协议(同步传输协议或异步传输协议)？
13. 请总结执行异步传输协议时，对卡进行一次操作(即使用一次)的流程，从RESET开始，直到一次应用结束。
14. 如果IC卡芯片设计得好，可以保证绝对安全，即可杜绝一切作弊和非法行为，这种说法对吗？
15. 在什么情况下希望在芯片内部设有协处理器，主要完成什么功能？

第7章　IC卡接口设备技术

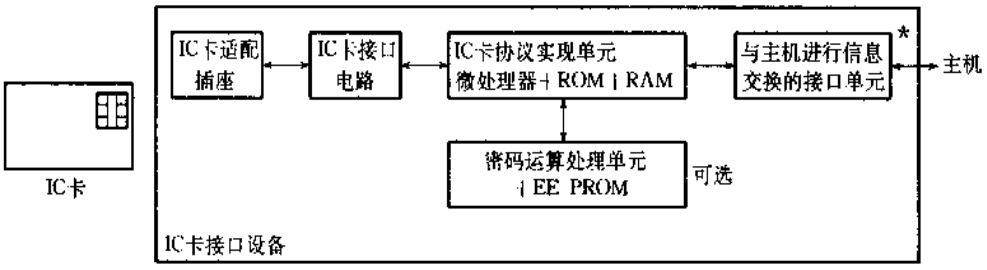
IC卡接口设备(又称读写设备/读写机具)是连接IC卡与应用系统间的桥梁,是IC卡应用中至关重要的一个环节。IC卡接口设备的种类很多,功能上由于不同的应用需要,差异亦很大,但就其对卡的操作功能来说,都应具备以下几个基本功能。

1. IC卡的插入/退出的识别与控制。
2. 向IC卡提供其所需的稳定的电源与时钟信号。
3. 实现与卡的数据交换,并提供相应的控制信号。
4. 对于加密数据系统,应提供相应的加密解密处理及密钥管理机制。
5. 提供相应的外部控制信息及与其它设备的信息交换。

7.1　IC卡接口设备的组成

IC卡接口设备可以是一个独立面向应用的应用机具或者以从设备方式(或称:外部设备)与主设备(一般为微机)一起构成一个IC卡应用机具。前者一般以简单专用设备方式出现,如水、电、煤气等的IC卡计费设备,IC卡自动售票机,IC卡付费电话,IC卡自动售货机等,这些机具的使用方式与功能均在出厂前由厂家制备好,使用仅能根据不同的情况进行小范围设定;后一类设备在功能上仅完成面向IC卡的操作,但以丰富而又灵活的应用接口给应用开发者提供了良好的支持,是系统应用中的一个非常合适的选择。

IC卡接口设备的组成如图7.1所示,它由IC卡适配插座(简称:IC卡座),IC卡电气接口电路、用于IC卡时序生成与数据交换的微处理器,以及与其它主设备(如果需要)的连接接口等部分组成。



*注:如为独立应用机具,无此部件

图7.1　IC卡接口高备总体结构框图

7.2 IC卡适配插座(IC卡座)

IC卡适配插座是构成IC卡与IC卡接口设备间的物理连接的部件。由于涉及到插入时的手感及插拔寿命要求较高的要求,IC卡座在设计和制造中比普通接插件的要求高,难度亦较大。

7.2.1 IC卡适配插座的结构形式

各厂家为迎合各类不同的使用需要,推出了多种多样的IC卡适配插座供选用。这些适配插座在结构上有较大不同,主要可在以下几个方面进行区分:

1. 触点的接触方式

根据IC卡在插入或退出时,按触点压触和脱离的方式区分主要有二种,一种是滑触式结构(Sliding),这种方式,触点处于固定位置,IC卡在插入或退出时,滑过与之不相关的位置,并滑接在固定的位置上,它的特点是结构简单,价格低。缺点是对卡的触点位置磨损较大,寿命仅在5万—10万次之间。另一类是着陆式结构(Landing),这种结构下,IC卡在插入过程中,触点与IC卡同步运动,逐步下压,并稳定于最终位置。由于在触点对卡的着力过程中卡与触头间没有相对位移,因而对卡表面的磨损小,触点寿命长,可达30万—100万次插拔,其价格较滑触式高出很多。

2. 卡的进退形式

卡的进退(插入和退出)过程,也是人机的交互过程,根据不同的使用需要,对卡的进退形式要求亦有较大不同,现行市场IC卡插座主要有如下几种形式:

(1) 推入-拉出结构

(2) 推入-推入弹出结构

(3) 压入-弹出结构

(4) 压入-电磁弹出结构

(5) 电动式入出卡控制结构

其中,推入-拉出结构是最常见的一种结构形式。而电动式入出卡结构,是一种全自动的运作方式,走卡平稳而可靠,但结构复杂,价格昂贵。为防止人为的不正当操作,有些IC卡座还设计了防拔卡装置。

3. 外形尺寸

有些应用对IC卡的外结构尺寸也有着严格的要求,因而部分卡座被设计成超薄的结构形式,高度在5mm左右的IC卡座现已问世。

4. 适用于特殊场合的IC卡插座

在户外或振动强度大的场合,普通的IC卡座不能满足使用要求,此时,防水型或抗振动形式的IC卡插座便是一种好的选择,这些卡座采取了密封防水设计及机械加固等方法,使得在环境较恶劣的条件下,使用IC卡成为可能。

7.2.2 选择 IC 卡适配插座时的几个重要的指标

在选用 IC 卡适配插座时，以下几个重要的指标是不容忽视的：

1. 触点的电气性能
2. IC 卡座的插拔寿命
3. 对卡的磨损程度
4. 卡的接触好到识别有效的位置差
5. 价格因素

其中，对卡的磨损，不单要看对卡的电气接触面的磨损，还要考查一下对卡的其它位置的磨损。此外，使用场合要求也是我们选择的一个重要指标。

7.3 IC 卡的接口电路和读写控制

7.3.1 IC 卡的接口电路

IC 卡的接口电路是连接 IC 卡与读写机具的通路，由它实现对 IC 卡的供电，并满足不带电插拔的要求。

一般来说，逻辑电路的'1'和'0'只是反映电压大小的关系，都处于带电状态。若带电插拔 IC 卡，有可能会给 IC 卡带来损伤，甚至损坏 IC 卡。因此在插拔前应先断开向 IC 卡供电的电源，并切断其逻辑连接，实现对 IC 卡的保护。

IC 卡的逻辑接口电路一般采用集电极开路(OC)输出及非箝位保护式输入结构，如图 7.2 所示。上拉电阻 R 源端与 IC 卡的供电电源相连接。当 IC 卡处于供电状态时，整个接口电路接通，接口设备与 IC 卡间构成逻辑通路；而当 IC 卡处于下电状态时(V_{cc} = OFF)，上拉电阻 R 的源端失去了供电，整个与卡接口的电路均处于不带电状态。这种电路的优点电路结构简单，可以与 CMOS、TTL 接口相兼容，上升沿阻尼较大，不易产出边沿振荡，它的缺点是当接口端子的分布电容较大时，上升沿过缓。在作为 CPU 卡的时钟驱动时(通常为 3.57MHz)，就有可能产生丢失脉冲等现象。解决这一问题的办法有两种，第一种是通过减小时钟驱动端的上拉电阻，减小上升时间来解决；另一种是采用互补驱动方式来进行时钟驱动，这种方式结构上略复杂些，但可以实现更高的时钟频率，如图7.3 所示。电路中 R 是一个去耦电阻，可有效地抑制上升及下降沿的抖动现象。

所有的 IC 卡的接口部分都加入了箝位保护二级管，这些箝位二级管可以使各引脚上的电压严格地限定在 $-V_D$—Vcc+V_D 之间，(V_D 是箝位二级管的正向压降，通常为 0.6V 左右)。这样可以抑制由于线路干扰和逻辑电平变化的边沿产生抖动所带来的瞬态过压，为 IC 卡提供了进一步的保护措施。

IC 卡接口设备中的 IC 卡供电电路也应是一个相对独立于其它回路，并提供完善的过流保护措施的稳压电路。这是由于 IC 卡接口设备是一个独立于 IC 卡的设备，当有卡插入时，接口设备便开始向 IC 卡提供其所需的电力。如果插入的是一张电源与地击穿的坏卡，或是一个金属片之类的物质，就会造成供电回路的短路现象，若 IC 卡接口设备中无过流保护措施，就会造成设备的损坏；即便有保护措施，若与 IC 卡接口设备的其它部分共

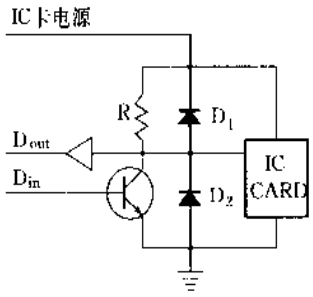


图 7.2 IC 卡的数据接口电路

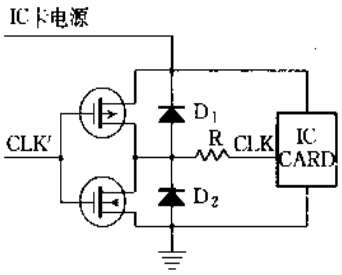


图 7.3 高频时钟的驱动电路

同使用一个保护回路，就会干扰整个设备的正常工作。图 7.4 所示的是一个两部分独立供电的供电电路。

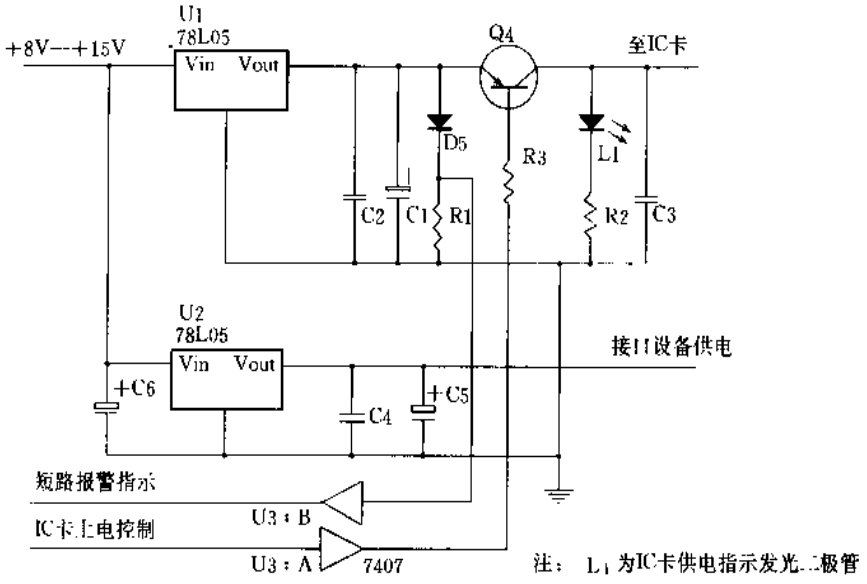


图 7.4 IC 卡接口设备的供电回路

该电路利用了带输出短路保护特性的 78 系列三端稳压集成电路。78L05 的最大输出电流可达 100mA，短路保护电流起点在 150mA～200mA 左右，符合 ISO/IEC 7816-3 所规定范围。当插入的卡是一个电源对地的短路负载时，U_1 会因输出过载而形成短路保护，由于 IC 卡接口设备的供电是在 U_2 提供的稳压回路上，因而不会干扰接口设备的工作，这一短路保护信息会在"输出短路"反馈信号线上形成一个低电平输出，IC 卡接口设备的微处理器则通过感知这一信号而切断对 IC 卡接口的供电，直到该卡退出为止，U_1 的输出也会随之而转入正常的电压输出范围，以便为后续插入的 IC 卡提供正常的供电服务。

当前市场上的 IC 卡，基本上都已采用 CMOS 工艺，功耗最大的亦不过十几毫安，在实际 IC 接口设备中，从 IC 卡接口设备的总体的最大功耗这一角度考虑，将向 IC 卡供电的过流保护点设置在 50～70mA 是比较适宜的。

7.3.2 IC卡的控制与读写技术

IC卡的控制与读写是IC卡接口设备中的核心操作部分，在图7.1中称之为IC卡协议实现单元。由于各种IC卡的实际操作有较大的不同，(ISO-7816标准只定义了一个最小操作，因而符合ISO-7816标准的卡亦不能保证其操作的一致性)，我们只有选取其中较具共性的部分作一介绍。本章的程序部分，将以MCS-51汇编程序方式给出。

1. IC卡的插入/退出识别与上电/下电控制技术

IC卡的插入与退出的识别是通过IC卡适配插座上的感应开关来识别的，对于复杂结构的IC卡适配插座，如电动式IC卡适配插座等，其识别与控制过程也相当复杂，且针对不同的卡座，其控制也各不相同。这里，我们仅针对那些手动插拔的IC卡适配插座来讨论，这种识别过程非常简单，仅有一个开关，表示卡是否已插入。如果卡已插入到正确位置，IC卡适配插座就会给出一个开关接通(或断开)的信号，而一旦卡离开这个位置，该信号就会立即发生反转。对于手动式IC卡适配插座来说，这一信号已经足够了。为了确保IC卡已准确地插到位置，插入的识别过程必须加入消颤处理。其程序如下。

```
Recog: JNB IC_SW, Recog   ; 若无卡插入，等待
       LCALL Delay-5ms    ; 延迟5ms
       JNB IC_SW, Recog   ;再次判断，若无卡输入等待
       RET
```

IC卡的供电控制是一个直接涉及是否能安全可靠地操作IC卡的过程。它必须严格地遵循ISO 7816-3所规定的操作顺序，否则，就有可能对IC卡带来永久性的损坏，ISO 7816-3标准规定的操作顺序如下：

(1) IC卡的激活(上电过程)：

——RST处于L状态

Vcc供电

——接口设备处于接收方式

Vpp上升为空闲状态

——CLK由相应稳定的时钟提供

(2) IC卡的去激活过程(下电过程)：

—— RST为状态L

CLK为状态L

——Vpp不起作用

——I/O为状态A

—— Vcc关闭

由于IC卡技术的进步，现有的IC卡事实上都已使用卡内自带升压电路的E^2PROM，因此，Vpp的控制，这一项既耗费电路投资、又很容易发生问题的过程(如果一个编程电压为12.5V的卡片，由于未能被编入识别序列而错误地加上了21V的编程电压，这张卡就会彻底地损坏)，已逐渐失去其具体的含义。

IC卡的时钟加载过程因同步卡和异步卡的不同而有着明确的区别，同步型IC卡的

时钟是与读写过程相同步的，无需提前加载，而异步卡的时钟则必须在 RST 信号无效前产生作用。如果一个 IC 卡接口设备需对这两类不同的卡都进行处理，那么只能依靠程序来进行识别，以确定是何种类型的卡。

图 7.5 是一个同步型 IC 卡接口的电路原理图，图中 P_1 是 IC 卡适配插座，其中 SW1，SW2 是 IC 卡插入识别的感应开关，其余为 ISO7816 中所定义的 8 个引脚(端口)，根据这一电路，我们可以描述其上电和下电过程分别为：

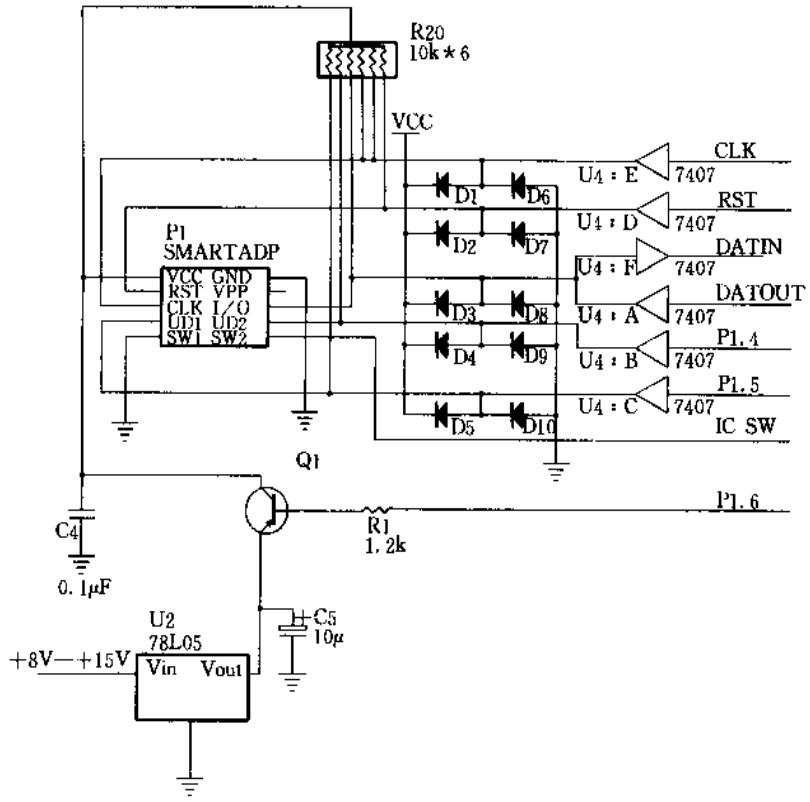


图 7.5　同步型 IC 卡的接口电路

① 上电过程：

```
PWRON1: LCALL Recog          ;识别是否有卡插入
        CLR RST              ;使 RST=L
        CLR CLK              ;使 CLK=L
        LCALL Delay-0.5ms    ;延迟 0.5ms，使端口逻辑信号稳定
        CLR PWR              ;给卡供电
        CLR DATOUT           ;使 I/O 端口=L
        RET                  ;返回
```

② 下电过程：

```
PWROFF1: CLR RST             ;使 RST=L
         CLR CLK             ;使 CLK=L
```

```
CLR DATOUT              ;使 I/O=L
LCALL Delay_0.5ms       ;延迟 0.5ms,使端口逻辑信号稳定
SETB PWR                ;给卡下电
RET                     ;返回
```

图 7.6 是一个异步型 IC 卡的接口电路,它与同步型 IC 卡接口电路主要差别是时钟的驱动,它提供给 IC 卡的是一个 3.57MHz 的稳定时钟,而不是一个软件时钟,此外,IC 卡的数据接口是连通在微处理器的异步通信口上(我们将在后续的部分讨论),其上、下电过程可描述为:

① 上电过程:

```
PWRON2: LCALL Recog             ;识别是否有卡插入
        CLR RST                 ;清除 RST
        CLR P1.0                ;禁止时钟,且 CLK=L
        LCALL Delay_0.5ms       ;延迟,使端口稳定
        CLR PWR                 ;给卡稳定供电
        CLR TXD                 ;使 I/O 为低电平状态
        SETB P1.0               ;允许时钟
        RET
```

② 下电过程:

```
PWROFF2: CLR RST;               ;清除 RST
         CLR P1.0               ;禁止时钟,且常置低
         CLR TXD                ;使 I/O 为低电平状态
         LCALL Delay_0.5ms      ;使端口稳定
         SETB PWR               ;给卡下电
         RET                    ;返回
```

2. IC 卡的读写技术

不同类型的 IC 卡其读写方式或数据协议方式是不同的,ISO-7816 标准的第三、第四部分对异步型 IC 卡的读写协议作了较充分的定义,而对于同步型 IC 卡,则只定义了其复位响应过程(ATR)的协议标准,这使得各厂家设计的同步型 IC 卡的读写方式不尽相同,而且由于同步型 IC 卡主要是不带微处理器的 IC 卡,接口协议是面向操作而进行的,因此,其操作协议方式也各不相同,好在许多厂家生产的 IC 卡都以 ISO 7816 同步复位响应协议作为 IC 卡的数据读协议方式,使我们能在这里进行一下简要的介绍。

(1) ISO 同步型 IC 卡读操作的实现

大多数符合 ISO-7816 标准的同步型 IC 卡的地址计数器是与时钟紧密相关的,当卡复位时,地址计数器置'0',以后,每向卡发一个节拍的时钟,都将使 IC 卡的地址计数器加"1",这一时钟频率上限一般在 50—300kHz 之间。

在复位之后的头 16—32 个时钟周期内,是卡的复位响应过程,该过程中,厂家的产品编码以位编码方式逐一在数据线上送出,以后的字段则根据厂家及用户所定义的含义不同而各不相同。若某字段定义为可读的,则可将时钟运行到该字段上,然后再逐时钟读出。

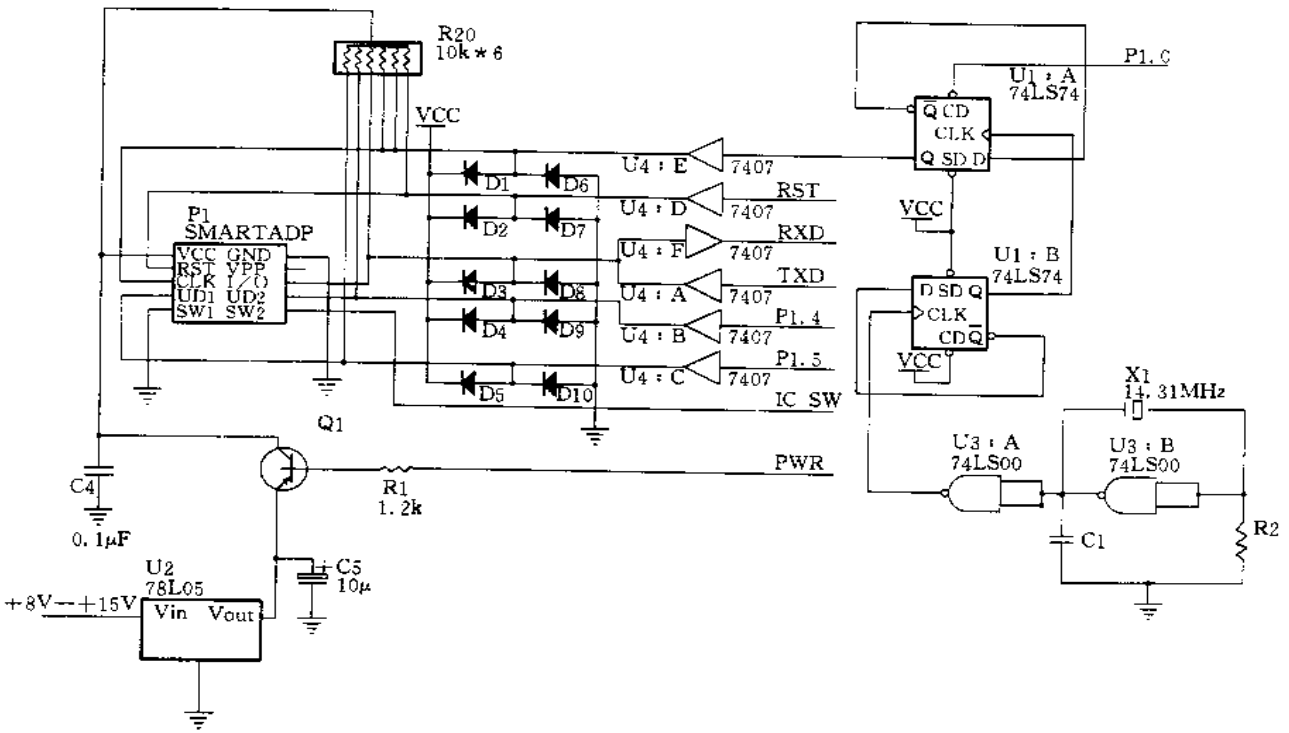


图 7.6　异步型 IC 卡接口电路

数据的读出过程可分为三个基本过程，即：复位，数据字段的定位和数据的读出。

① 复位过程：对符合 ISO-7816 同步协议标准的 IC 卡来说，其复位方式也与 ISO-7816 标准是相容的，因而该部分程序可描述为：

```
SYNRST: SETB DATOUT;        ;使能数据线
        SETB RST            ;复位使能
        LCALL Delay_10μs    ;延迟 10μs
        SETB CLK            ;置同步复位时钟 H
        LCALL Delay_10μs    ;延迟 10μs
        CLR CLK             ;时钟为 L
        Lcall Delay_10μs    ;延迟 10μs
        CLE RST             ;复位结束
        RET
```

② 数据字段的定位：前面已提到，数据字段的定位是以复位后的时钟数目来定标的，这里，我们设定：R_2，R_3 表示所定位的位地址数，R_2 为高位字节。则定位子程序如下：

```
SYNPOS: LCALL SYNRST        ;IC 卡复位
   SP1: CJNE R3, #00H,SP3   ;判低位
        CJNE R2, #00H, SP2  ;判高位
        RET                 ;返回
   SP2: DEC R2              ;高位减 1
   SP3: DEC R3              ;低位减 1
        SETB CLK            ;开始建立一个时钟脉冲
        LCALL Delay_10μs
        CLR CLK
        LCALL Delay_10μs    ;时钟脉冲结束
        SJMP SP1            ;继续下一次
```

③ 数据的读出过程：根据前二个过程，我们不难实现对卡的读操作。这里，我们实现一个从 R_2，R_3 所指定位置起读 R_4 个字节的数据，并保存在 R_0 为始址的，递增的若干个单元中。

R_2，R_3 ——起始读位置(位)

R_4 ——所要读的字节数；$R_4 \geqslant 1$

R_0 ——数据存放位置的起始地址

R_5，A ——暂存器

```
SYNREAD: LCALL SYNPOS       ;定位至起始地址
         SETB DATAIN        ;智能数据输入线
SR1:     MOV R5, #08H       ;置移位次数为 8 次(一个字节)
SR2:     SETB CLK           ;CLK=H
         MOV C,DATIN        ;将数据线上的内容输入到 C(进位)触发器中
         RLC A              ;A 寄存器循环左移，C 的内容进入 A 最低位
```

```
LCALL Delay_10μs      ;延迟 10μs
CLR CLK               ;CLK=L
LCALL Delay_10μs      ;延迟 10μs
DJNZ R5, SR2          ;判断是否接收完一字节,若是继续,否则转至
                       SR2,继续接收下一位
MOV @R0,A             ;将字节内容送(R0)单元
INC R0                ;数据存放地址加 1
DJNZ R4, SR1          ;判断是否接收完 R4 个字节,若是继续,否则
                       转至 SR1,继续接收
RET                   ;返回
```

(2) 异步型 IC 卡的协议实现

与同步型 IC 卡的操作相比,异步型 IC 卡读写设备的操作相对简单得多。异步型 IC 卡大多是带有微处理器的卡片,对卡的操作只有 ATR 过程和 COS 命令的传递与应答过程,其通信的协议方式严格符合 ISO-7816 第三部分的标准。

由于 ISO-7816 标准中的异步通信标准的格式与我们计算机的异步通信格式基本相同,而标准上所规定的卡在 3.57MHz 时钟频率下的初始速率为 9600bps(周期 104μs),这实际上已成为各厂家所共同遵从的数据交换速率规范,这一速率也完全符合我们现行的异步通信速率标准,为方便读写,我们将 IC 卡的数据端口与 IC 卡接口设备的异步通信接口构成相应的半双工异步通信逻辑通路(见图7.7所示),利用该数据协议通路,并配合其它相关的控制,可实现与 IC 卡间的信息交换。

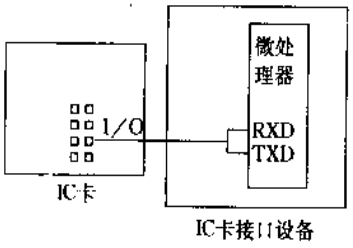


图 7.7 IC 卡与 IC 卡接口设备间半双工异步通信通路

异步通信接口的初始化设置为:

通信速率初始设置为 9600bps。

一个起始位

八个数据位

一个奇偶校验位

二个停止位

此外,这一接口还需要实现 ISO-7816 第三部分所规定的接收方的接收错误指示和发送方的指示监视功能,这一功能不属于标准的异步通信范畴。在 MCS-51 系列或 MC68 系列微处理器中,都设置了异步通信与 I/O 的复用功能,利用它们的这一特点,并配合相应的程序过程,可完整地实现 IC 卡的接口数据协议过程。

根据以上的描述,我们可以对数据的接收与发送进行流程描述,这里,我们仅以 T=0 协议为例(参阅 3.3.4 节)。

- 发送一个字节数据(图 7.8)。
- 接收一个字节数据(图 7.9)。

为了便于理解,以上过程采用了直观且易于理解的流程方式进行描述。在实际的程序编制中,根据具体环境的不同,相应有所变化。

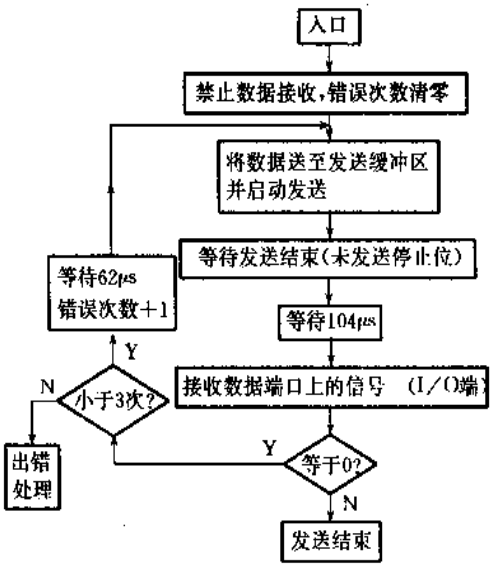


图 7.8 发送一字节数据流程图

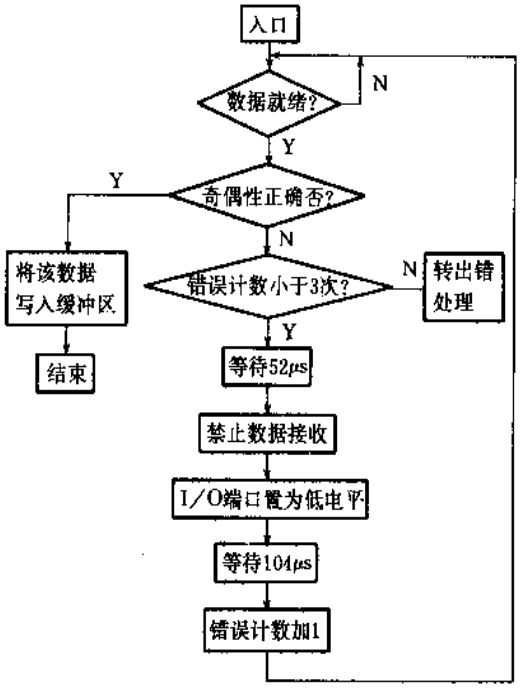


图 7.9 接收一字节数据流程图

① 异步型 IC 卡的复位应答过程(ATR):对于异步型 IC 卡来说(带有 MCU 的异步型 IC 卡),复位应答过程是由接口设备对卡撤离复位状态后,IC 卡所产生并传送给接口设备的一系列数据信息。ISO-7816 标准的第三部分对于这部分信息作了详细的定义。(参见第 3 章)。它主要包含如下同部分内容:

- 数据字节格式，分正向传送格式和逆向传送格式二种。
- 控制信息要求，包括编程电压、电流需求和最大等待应答时间等。
- 协议规程及波特率的再设定因子。
- 历史字符，主要用于应用识别。

这些规程字节被接口设备读入，并形成相应的控制与识别信息，以便于后续的操作。

IC卡的通信字节格式是IC卡接口设备能够准确与IC卡进行数据交换的基础，接口设备必须在初始读入复位应答时(即读入TS字节时)，便进入正确的状态判断。由于ISO 7816标准的第三部分中没有对从复位应答过程的开始(TS字节从IC卡中送出)到应答过程终止(TCK字节送出)的最大时间进行限制，且存在着长度无法准确指示等问题，(例如：按标准规定，TCK字节在T=0协议时有可能不被发送)。因而在设计构造复位应答程序时，采用简单的超时接收和协议分析接收方式，都无法准确地形成有效的响应时间控制，过长的超时时间会影响系统的操作性能。许多厂商，包括一些著名的国外厂商的接口设备产品，在这方面都不尽如人意。笔者通过对多种IC卡的应答数据流进行分析时发现，一旦IC卡开始进行复位响应，其字节流都是连续的，即使出现中断情况，时间也不超过2ms(在3.57MHz的时钟频下)，因此，可以通过字节间的超时判断来形成是否应答结束的判断。这一方式虽不能说是完备的，但至少对现在市场上的流通的IC卡来说，具有较好的通配性。这里我们给出IC卡接口设备的复位应答流程图(图7.10)，首先测试是否是低电位Reset有效，将RST置为'低'，等待ATR，若超时，说明不是低电位Reset有效；然后将RST置为'高'，若也超时，说明也非高电位Reset有效，此时表示卡可能存在问题。允许重复测试3次，若都超时，说明卡无效。若卡有效，再确定是正向协议还是反向协议，然后接收ATR并进行分析。

② COS的命令接口协议的实现：COS的命令接口是异步型智能卡的操作实现部分，卡接口设备按ISO协议向卡发送一组具有一定含义的数据块，IC卡接收到这组协议数据后，通过解释这组数据的具体含义，形成操作指示，进一步转换为读、写、比较、认证及其它控制操作，然后将操作的结果返回给接口设备，这样便完成了一次IC卡的操作过程。我们称接口设备向卡发送的具有特定操作含义的数据块为IC卡的操作命令；从IC卡返回接口设备的状态及数据信息称为应答。

ISO 7816第三部分对T=0协议的命令结构与应答进行了详细的定义(同样也适用于T=1协议，但ISO 7816-3与ISO 7816-4有相冲突的部分)。接口设备发送的命令头由CLA，INS，P1，P2和P3五个字节组成。在ISO 7816-4中，P3字节被更确切地定义为Lc、数据和Le字段，同时增补了Lc和Le字段同时存在的协议部分。

根据ISO 7816-3标准规定，一条IC卡操作命令可描述为由指令头，响应字节，发送的数据字段，回应的数据字段和状态字五部分组成。指令头是一个由CLA、INS、P1、P2、P3五个字节组成表明一定操作含义及控制参数的数据包，它指示IC卡进行何种操作，所需的控制参数及后续需发送的数据长度和回应的数据长度等信息；响应字节是IC卡在接收到一条有效的指令后，对接口设备的响应，同时也对接口设备的后续操作提供指示，响应字节的响应指示可以分为四种情形，即：INS，$\overline{\text{INS}}$，INS+1和$\overline{\text{INS}+1}$；这四种情形分别指示了IC卡的后续操作的资源需求(详见ISO-7816标准第三部分)，接口设备则根据

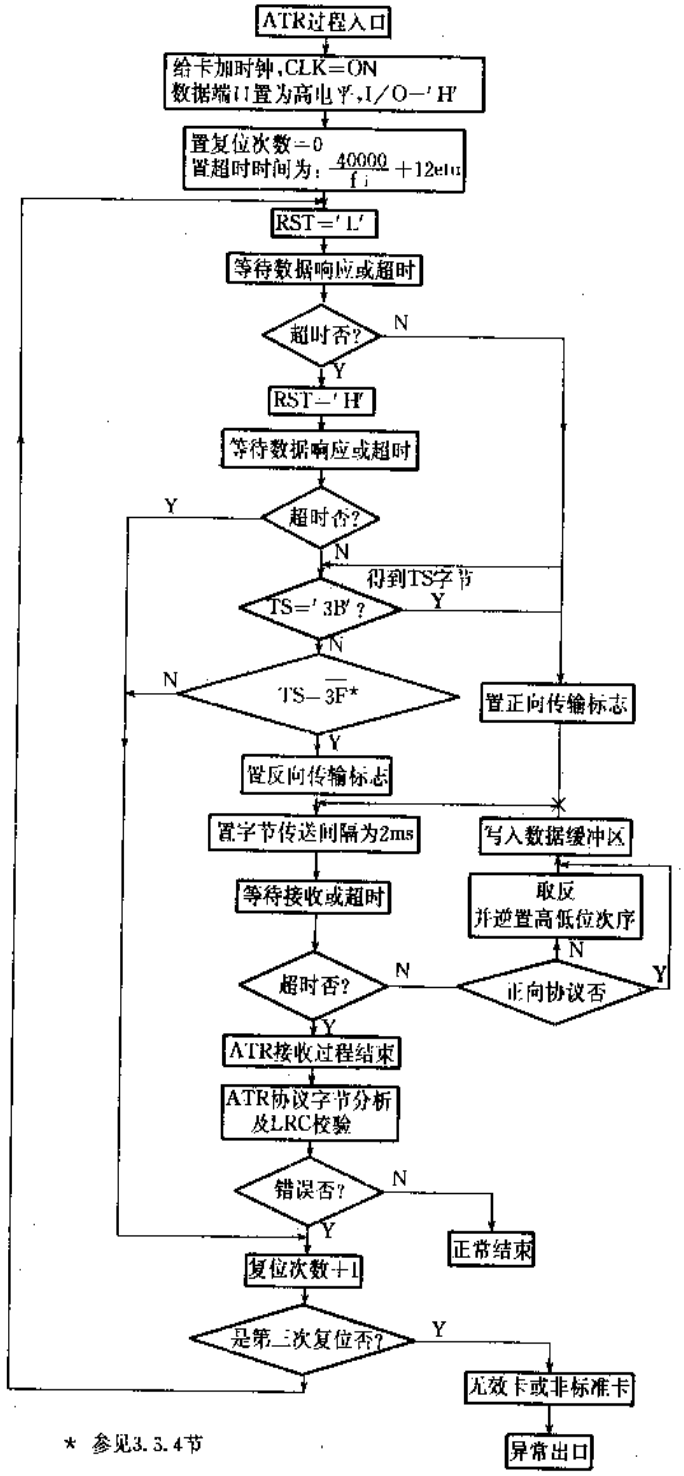
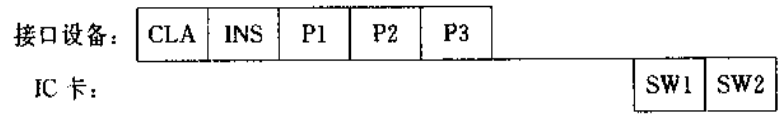


图 7.10 IC 卡接口设备复位应答流程图

这一响应字节进行下一步的操作；发送及回送的数据字段是由指令的操作性质决定的，是双方信息交换的目的字段，其长度一般由 P3 或其它方式所指定；在上述的操作执行

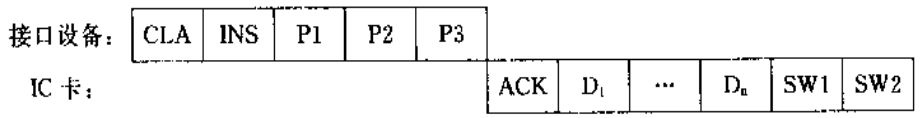
后，或操作中出现错误情况，IC 卡将向接口设备回送二个字节的状态信息，接口设备则依据此来判断一条命令是否正确完成。实际使用的三种命令结构分别是：

· 无数据命令结构，其操作过程为：



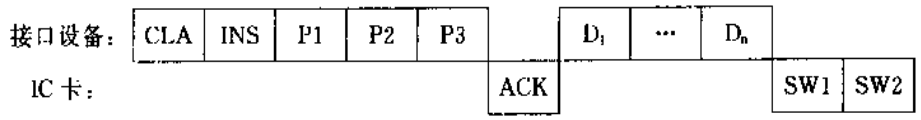
该结构的指令主要出现在无数据控制指令和一条错误的指令执行的时候。

· 获取数据命令结构(Outgoing)，其操作过程为：



该指令结构中，所需获取的数据长度一般由 P3 来指示，即：P3=Le

· 下载数据命令结构，其操作过程为：



该结构的指令中，数据字段的长度一般由 P3 字段给出，即 P3=Lc。

根据上述指令结构及信息交互方式的分析，可以构造出异步型 IC 卡的指令实现流程。由于现行 COS 卡大都为自带升压电路的 E^2PROM 卡，故其响应字节一般仅为 INS。为此而简化的流程如图 7.11 所示。

在实际构造程序时，每一部分还应加入超时判断和长度完整性判断等校验环节，以防止意外的误操作发生。

有关 ISO 7816-4 中规定的命令及应答情况请参阅第 4 章。

7.4 IC 卡的应用设备

IC 卡的使用离不开相关的 IC 卡应用设备，IC 卡的应用设备主要完成二个方面的工作：一个是面向应用需求，实现应用所需的功能操作部分；另一个则是完成与 IC 卡的数换交换。这两个方面的结合，使 IC 卡的流通与使用成为可能，并随着各种应用设备的不断发展与普及，而使我们能够在更广泛的领域中使用上 IC 卡。

IC 卡的应用设备种类很多，应用性质亦各不相同。现行的 IC 卡应用设备中，主要有 IC 卡水、电、煤气表，IC 卡公用电话，IC 卡自动售货机，IC 卡 POS，IC 卡 EFT，以及面向多领域应用的 IC 卡读写器等。这中间，可将 IC 卡应用设备大体分为两大类，一类是应用的 IC 卡数据结构明确，用户只需建立 IC 卡发行管理体系，即可发行使用的 IC 卡专用设备，另一类则属于用户在购买 IC 卡设备后，还必须进行二次开发才能投入使用的设备。这二类设备，构成了我们在复杂的应用场合使用的基础。

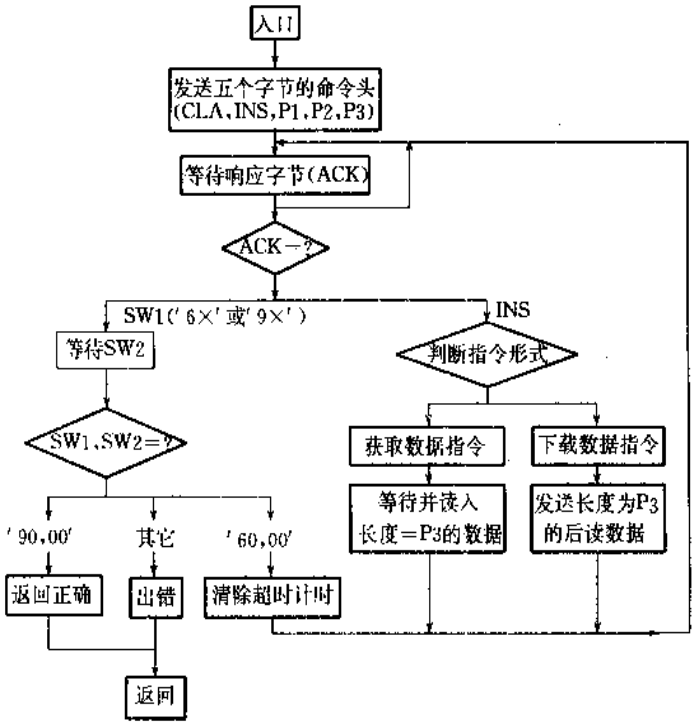


图 7.11　异步型 IC 卡指令实现的流程图

7.4.1　专用的 IC 卡应用设备

图 7.12 是一个 IC 卡电能表的电路结构原理图，它是 IC 卡专用设备中较具典型的实例。这台 IC 卡电能表是以我们传统的转盘式电度表为表体的，电能的计量来自于转盘的旋转圈数，转盘每旋转一圈，都会被 O1 和 O2 两个光电耦合式传感器所感知，并送到微处理器中进行处理。微处器对每一个校正后的脉冲信号进行累加，当累计达到一个计量单位时，便形成一次 IC 卡写过程，使 IC 卡中所存放的允许用户使用电量减一。当允许用户使用电量减至零时，电表将以显示或蜂鸣器等方式提醒用户，应到发行部门领取新卡或重新更新卡中数据以便再次使用，如用户不进行卡的更新过程，微处理器将通过 O3 驱动一个电力继电器以切断用户的电源供应。电能表中，U2 是一个串行的 E^2PROM，它允许发行商将 IC 卡的识别字，发行密钥和电能计量的校正数据存放在这个 E^2PROM 中，以作为电能表的识别与计量依据。该电能表中，计量部分采用了双光耦方式，是为了消除因转盘停止在光耦识别的边缘而产生振荡所造成的过量计量而设计的。两个光电耦合器所采集的信号在微处理中所进行的处理实际上等效于一个双预置的消颤电路，如图 7.13 所示。

电能表是以千瓦·时(kW·h)来计量的，我们设定 IC 卡中也是以 1kW·h 为一个计量单位，而电能表的校正参数则以 kW·h，转盘转动的圈数来设置的。假定一个电能表的校正参数是 2000，则转盘每转过 2000 圈，即微处理器每采集 2000 个有效的脉冲，便形成 1kW·h 的计量，并将该计量传递至 IC 卡中。

通过以上功能描述，我们可将其功能归纳如下：

1. IC 卡采用以 1kW·h 为基本计量单位

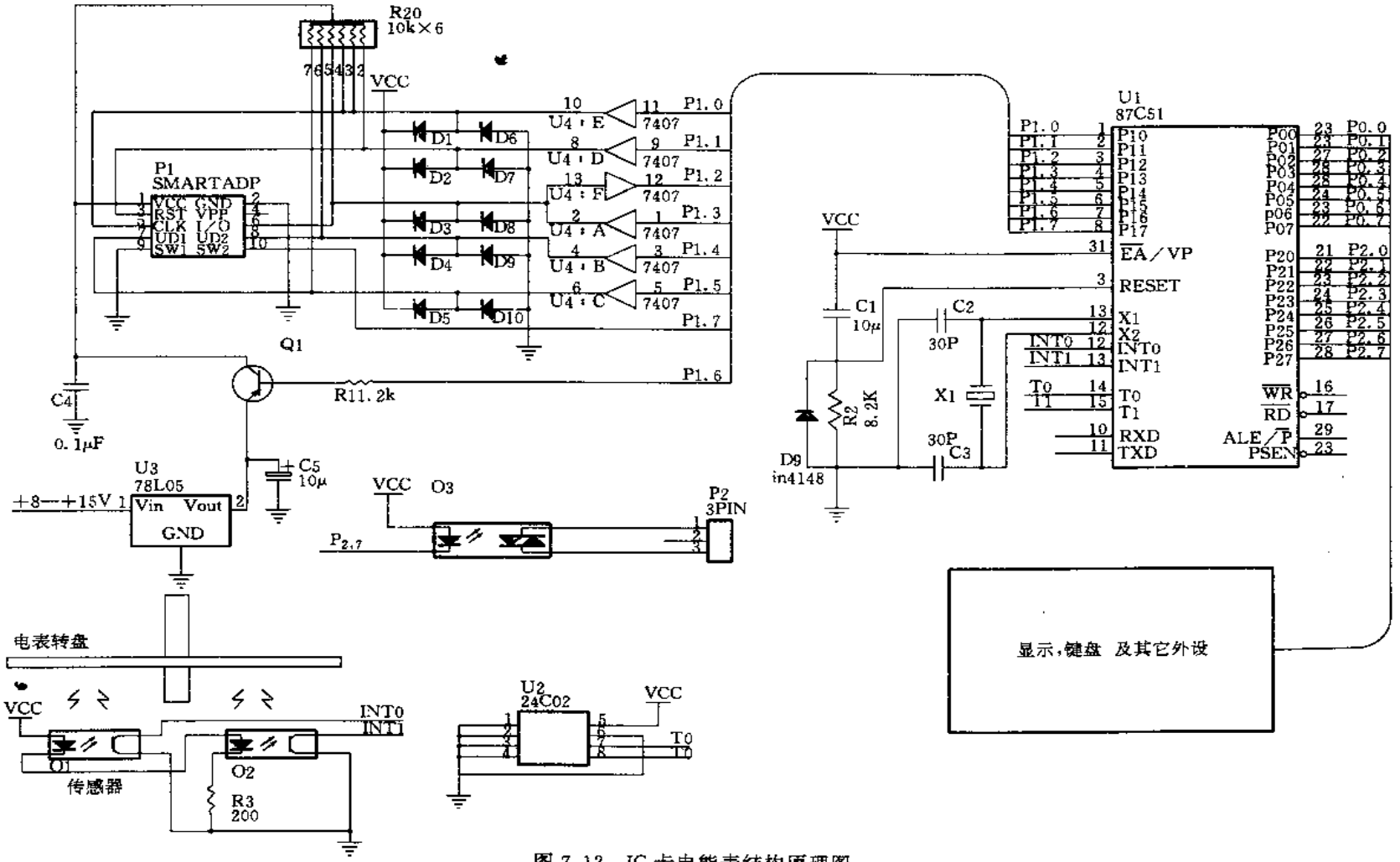


图 7.12 IC 卡电能表结构原理图

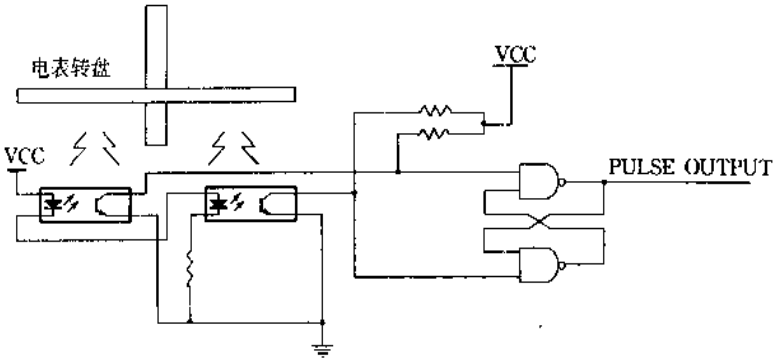


图 7.13　电度表数据采集消颤的等效电路

2. 电能表应具备用尽前的提前示警功能

3. 当 IC 卡预存的电量用尽后应切断供电

4. 电能表应具备对 IC 卡的识别及密码产生和核对的能力

⑤ 应以校正参数为基础，提供较精确的计量

在设定好电能表的基本功能后，便应选定一种适合应用需要的 IC 卡，由于作为预付电费使用的 IC 卡是一种储值卡，因而有必要选用那些防伪造、防复制的 IC 卡。而且，由于一次储值较小，因而应选用价格相对较低且能够重复使用的 IC 卡。根据以上需求，我们可以将 IC 卡的选用范围限定在小容量的带保密逻辑的 IC 卡上。这里，我们以西门子公司的 SLE4404 卡为例，来说明该种类 IC 卡是如何在 IC 卡电能表中使用的。

SLE4404 是一种专门为小额储值而设计的 IC 卡，它共有 416 bit(位)的存储容量，可进行 64 次以内的重复使用。该卡的各个区域的设置在生产中便已设定，使用时无法变更。在用作预储电量的使用时，我们可按表 6.10(参见第 6 章)来进行划分使用。

按照表 6.10 的使用分配，IC 卡电能表中实际所涉及的区域及完成的功能有：

① 制造商和发行商的识别号码，IC 卡电能表应对该卡是否是该发卡商所发行的卡进行初始识别，如不是，应示警并拒绝以后的操作。

② 密码，通过利用密钥与卡发行号的加密运算产生一个核对用的密码，并与卡内密码进行核对(核对过程在卡内实现)，以防止出现伪卡，如出现核对错误，电能表应示警并拒绝以后的操作。

③ 应用数据区(计费区)，每使用一度电时，都将产生一个寻找一个不为‘0’的位，并将其改写为‘0’，将 IC 卡的应用数据区的 208 bit 计费区域中不再有‘1’时，IC 卡电能表应产生提示，以提醒用户更换新卡或到发行商处进行更新。

④ 根据第③项用法，结合应用实际情况，宜采用预计费的方法使用，即，每有一度电将要使用时，预先在 IC 卡减掉一度电的计费。

IC 卡电能表的计费及控制程序流程图如图 7.14 所示。

7.4.2　通用型 IC 卡应用设备

通用型 IC 卡应用设备与专用型 IC 卡应用设备相比较，有如下不同：

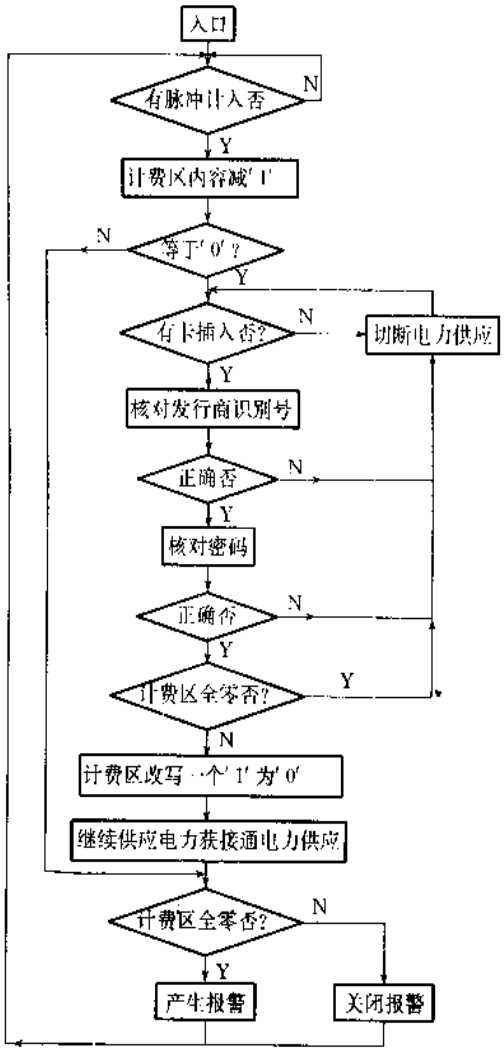


图 7.14 IC 卡电能表的控制流程图

1. 专用 IC 卡设备可以直接安装使用，并可内装其它设备与其它设备直接配接，而通用型 IC 卡应用设备一般只具备读写的功能，与其它设备的连接则以标准数据接口方式提供。

2. 通用型 IC 卡应用设备支持卡的种类较多可达数十种，而专用型 IC 卡应用设备一般只针对该系统应用需要，支持一种或几种 IC 卡。

3. 通用型 IC 卡应用设备一般都有辅助开发应用的开发平台提供给应用开发人员使用。偏重于二次开发使用，而专用设备一般不提供类似工具，偏重于用户直接使用。

现有的通用型 IC 卡应用设备多以标准计算机外设的 IC 卡读写器形式出现。它们采用符合计算机工业标准的 RS-232C 或 AT-Bus 数据接口方式与计算机联连，并可提供基于 IC 卡操作的二次开发平台，这种二次应用开发平台多以 C 函数接口，数据库函数接口或转换为磁盘文件等方式提供，是对计算机系统中丰富的应用开发软件的功能补充。

总之，利用通用IC卡应用设备构成IC卡应用系统是一个代价较高的方案，但它提供了一个多场合应用的手段，系统组织也更加灵活方便，对于小应用系统，无疑是一种较佳的选择方案。

思 考 题

1. 从功能上划分，接口设备可分成哪两种类型。叙述各种类型的主要组成部分。
2. 常用的读写设备的IC卡座有哪两种？
3. IC卡的电源是由哪个设备提供的？在IC卡插拔过程中，在什么时候加上电压比较安全。与电源有关的保护措施有哪些？
4. 加电(上电)和断电(下电)过程应遵循的国际标准是什么？接口设备又是如何实现此标准的？
5. 同步传输协议和异步传输协议对接口设备的要求相同否？
6. 接口设备中的微处理器起什么作用？它通过什么途径向IC卡发命令？
7. 设某电表计费卡的发行商，需要保存用户每月用电量及付费情况的记录，以便查询。你认为应选择何种类型的接口设备比较合适？
8. 试画出电话预收费卡接口设备的工作流程。
9. 当采用异步传输协议时，应遵循的国际标准是什么？
10. 在持卡人的一次消费过程中，IC卡与接口设备是如何配合工作的(分同步传输协议和异步传输协议两种情况讨论)？

第 8 章　自动柜员机 ATM 和销售点终端 POS

ATM 和 POS 是金卡工程建设必不可少的配套设备。

近两年来，我国发展电子化银行的步伐逐渐加快，各家银行都把银行的服务延伸到商业、服务业、旅游业等领域，越来越多的特约商户接受信用卡，开展无现金交易。电子转帐已逐渐被社会公众所接受。典型的电子资金转帐系统是由许多主机利用网络相互连接，并有众多的 POS 和 ATM 直接或通过网络连到主机。主机、网络、ATM 和 POS 共同组成一完整的系统，实现信用卡业务电子化。

8.1　ATM 的功能和结构

ATM (Automatic Teller Machine 的简写)即自动柜员机，也有称自动取款机的。它是银行设立的、面向持卡用户的金融设备，为用户提供自动金融服务功能。信用卡持有人可以通过 ATM 自动进行存款、取款、转帐、查帐、结算等业务，而不需银行业务人员的参预。这样既减轻了银行工作人员的负担，又大大方便了用户，使得用户进行金融活动时更加方便、更加快捷。因为目前实际应用的 ATM 更多的是提供取款业务，即持卡用户自动提取现金，所以很多人又称之为自动取款机。

从外形上看，一台 ATM 大致分成四个部分(图 8.1 所示)：底座，保险柜，电子柜和用户界面。底座(或称基座)是用来支撑整台 ATM 的，它可以是一个坚固的平台，也可以是几个坚固的撑脚或滑轮(图 8.1 所示 ATM 就是这样)。底座形态可以多种多样，其目的都是一样的：起支撑作用。保险柜是 ATM 最坚固的部分，备有多种防护措施。它里面有钱箱和点钞系统。保险柜一般位于 ATM 的下半部分。在保险柜的上面是电子柜，内装 ATM 的电子系统，控制 ATM 的行为，它是 ATM 的核心。电子柜的前面是用户界面，是用户直接面对的、和 ATM 打交道的部分，包括显示器、用户键盘、插卡口、出钞口等。这四个部分只是 ATM 的一般构成，并不是所有的 ATM 都是这样。现在许多 ATM 将保险柜和电子柜合在一起，从外形上看只是一个柜子。ATM 根据用途和安装方式不同，可分为大堂式(直接放于大厅内)和穿墙式(只有用户界面露出墙外，其它部分在墙内，用户只能见到用户界面部分)等多种类型。不同类型的 ATM 外形可能不一样，但不管外形如何，ATM 内部结构、功能和原理基本上是一致的。

我们将 ATM 分作三大部分：ATM 的硬件部分，软件部分及机械结构。以下各节分别从这三方面来介绍 ATM 的内部结构和原理，力图给读者一全面、深入的认识。

8.1.1　ATM 的硬件构成

ATM 的硬件部分包括图 8.2 所示的几个模块或系统。

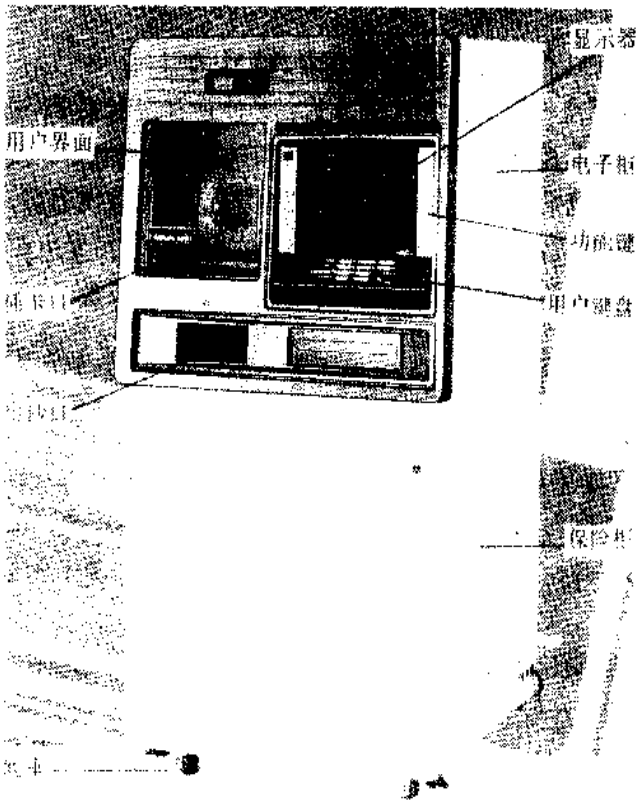


图 8.1　ATM 的外形

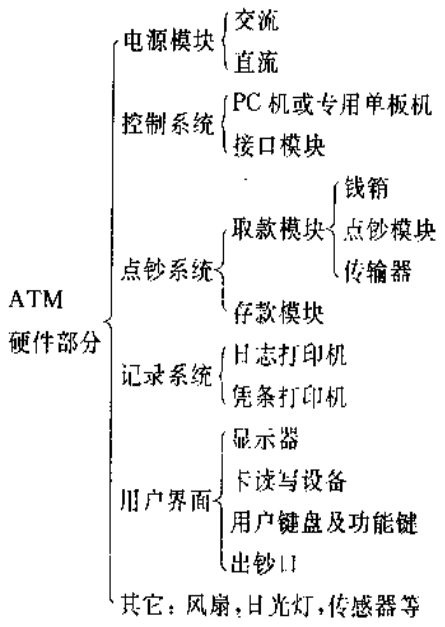


图 8.2　ATM 硬件部件构成

1. 电源模块

该模块将外部输入的三相交流电转化为 ATM 内部使用的交流和直流电，提供整个

ATM 的电源。电源的稳定是整个 ATM 正常工作的基本保障。

2. 控制系统

控制系统是 ATM 的核心部件，它控制着 ATM 的行为。

ATM 的控制系统一般有两种构成方式：一种是直接利用 PC 机；另一种是专门为 ATM 设计专用控制单板机。相应的，控制系统和外围设备的接口，如驱动点钞系统工作、和银行主机通信等，也采用两种构成方式：对采用 PC 机的系统而言，可直接将各种设备卡或通信卡插入计算机的插槽中，驱动其它模块工作；对采用专用控制板的控制系统而言，控制系统与外围设备的接口也要专门设计，设计专用接口板，达到控制其它模块的目的。

直接利用计算机系统减轻了开发设计负担，增强了系统的通用性。目前这种控制构成方式广泛地被国内外厂家所采用。例如，Bull 公司的多功能 ATM Questar 3410 就采用 80386 PC 机、DOS 操作系统构成 ATM 的控制系统。Bull Questar 1410 采用的是 486 PC 机（带一台 3.5 吋软驱和一台 80MB 的硬盘），也用 DOS 操作系统。NCR 的第四代自服务型 ATM，如 5663、5674、5675 等，都采用 386 PC 机，和 OS/2 操作系统构成其控制系统。

3. 点钞系统

ATM 的点钞系统位于保险柜中，是 ATM 重点保护的关键部件。它由钱箱、点钞模块、传输器构成。钱箱一般有多个，按币值分类安放纸币。点钞模块要求有高精度、高速度和高效率，如 Bull Questar 3410 一秒种可发钞 15 张。目前世界范围内只有几家公司可以生产点钞模块，其它厂家的 ATM 也都是利用这几家的。传输器用来传输钱币给用户。实际运作时，点钞模块根据用户的要求，按控制系统发出的指令，从钱箱中取出一定数量的现金，清点后通过传输器送到出钞口，交给用户。

上面介绍的点钞系统指的是取款模块，如果 ATM 有存款功能（这个功能在很多 ATM 上是可选的），点钞系统还应包括存款模块。

存款模块自成一小系统，它由信封分解器、存款信封打印机和存款箱构成。用户将钱封在专用信封里投入 ATM，ATM 就能帮助用户进行自动存款。信封分解器可将用户的信封根据类别进行分类，而存款信封打印机在信封上打印出用户帐号，备银行工作人员复核。存款箱用来装存款信封。因更多的用户更愿意将钱交给人（银行工作人员）而不是机器，再加上各国财务制度，存款方式不尽相同，以致 ATM 的存款功能不够完善。大多数厂家生产的 ATM 都只提供取款、查转帐等功能，而不涉及存款，只是将存款模块作为一可选部件。

4. 记录系统

ATM 的记录系统包括各类打印机。日志打印机用于打印操作过程、交易内容等信息以备查询，即用来打印交易流水帐，所以又称为流水帐打印机。凭条打印机打印用户凭条，作为用户进行金融交易的凭证。这些打印机既可采用通用的文字打印机也可利用专门的票证打印机，ATM 生产厂商根据实际需要进行确定。例如 Bull Questar 1410 中有两台打印机，流水帐打印机每一次换装后可打印 10,000 行文、数字；收据打印机（即凭条打印机）每一次换装可打印 2,100 张收据。富士通 7000 系列 ATM 内部也设有流水帐打印机和凭条打印机，其中凭条打印机是采用 24 针点阵式票据打印机，每行可打印 40 个字符，

每秒钟可打印3行。

5. 用户界面

当持卡用户面向ATM，不论ATM是大堂式的还是穿墙式的，用户所能见到的部分就是ATM的用户界面。持卡用户通过用户界面跟ATM进行交易，ATM将交易结果也通过用户界面交给用户。用户界面包括显示器、用户键盘和功能键、卡读写设备、出钞口等部分。

显示器向用户提供可视信息，提示并指导用户进行操作，显示交易结果。ATM的显示器可以是单色的，也可是彩色的；尺寸也不一样，9英寸、10英寸、12英寸、14英寸的都有。ATM生产厂家根据实际需要，衡量性能及成本来配置相应的显示器。NCR 5663采用的是10英寸彩色CRT，可具有640×480点阵16色或者320×200点阵256色图形显示。富士通7000系列配置的基本单元显示器是9英寸高亮度单色VGA显示器，用户可以根据需要选用10英寸高亮度的彩色VGA显示器。

用户键盘和功能键是ATM的输入设备。它提供人机对话，将用户输入的信息传送给ATM。功能键提供快速切入功能的手段。用户只要按一功能键就能进入相应的功能，而不必像在通用的PC机上需要敲一系列命令才能进入功能，方便了用户。用户键盘主要用来输入用户密码。有的ATM用触摸屏来代替用户键盘和功能键，使得用户操作起来更加方便、直观。

用户界面的另一个重要部分是卡的读写设备。该设备是专为接受信用卡准备的。目前信用卡多为磁卡，故ATM中卡的读写设备多为磁卡读写器。磁卡读写器接收用户从插卡口插入的磁卡，从卡中读出用户的信息，如帐号、姓名等传送给控制系统，控制系统处理后一方面将此信息与银行主机打交道，一方面将结果返回磁卡。用户实际上是通过信用卡和ATM打交道的。现在有的ATM安装IC卡读写设备作为选择，用于接收IC卡类的信用卡。例如NCR的第四代自服务(self-service)型ATM配备标准的磁卡阅读机，并把IC卡读写装置作为一选件进行装配。总之，不管是何种形式的卡读写设备，它都是ATM不可缺少的，非常重要的一个设备。

6. 其它

ATM还包括许多辅助设施。如帮助散热的风扇、提供夜间服务而用来照明的日光灯、用作安全保护的传感器等等。有的ATM还有摄像系统、远程监控系统，还有的ATM把多媒体技术集成在ATM内，可以说话、发声等等。所有这些措施都是出于两个方面的考虑：一是强化ATM的安全性能，增强其保固特性，使之更加可靠、耐用；另一方面是力图使ATM方便、实用，让用户使用起来更加直观、更加简便。

从ATM的硬件结构可以看出，ATM实质上是一独立、可靠的计算机系统。PC机(或其它专用机)对通过用户键盘和卡读写设备输入的用户信息(帐号等)和用户想要进行的操作进行处理；必要时通过通信接口(RS-232，485，modem或网络)与银行主机联系，共同对用户的操作进行响应；道过PC机内的设备卡(或专用接口板)驱动点钞机、打印机输出处理结果。此系统的核心就是作为控制系统的PC机，简单示意如图8.3。

值得注意的是，ATM虽然从原理上是一计算机系统，并不是说ATM就等于PC机＋读卡设备＋专用键盘＋钱箱＋……。其实，ATM是针对金融交易专门设计并融入计算

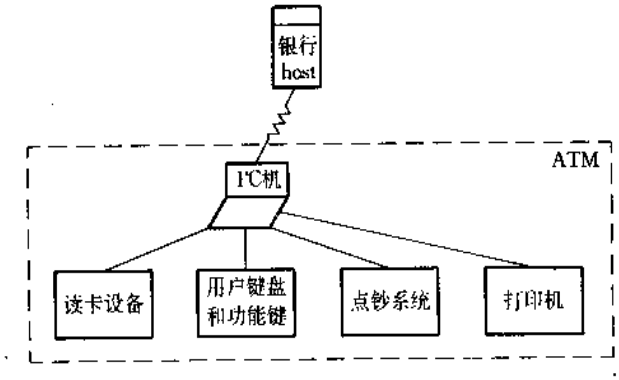


图 8.3　ATM 原理结构示意图

机核心技术的专用设备。ATM 所具有的许多特性是通用 PC 机绝不可能具有的，如为增强保固性而设计的符合 VL291 标准(美国国家安全局制定)的保险柜、多重密码钥匙锁、电子柜防盗锁、感应器、报警器等等。这些设计使得 ATM 的成本和价格比一般 PC 机要高得多。目前一台 ATM 售价要二、三十万元人民币，这是一般 PC 机所无法比拟的。同时，ATM 中的软件也是专用的，更多的考虑到安全和方便，考虑到金融交易的实际需要，具有很强的针对性。

8.1.2　ATM 的软件

软件是 ATM 的灵魂，赋予了 ATM 实际运作的能力。ATM 的软件是针对各电子部件、根据业务需要编制的。整个系统软件包含二个层次：直接建立在控制系统基本硬件基础上的、保障控制系统正常运作的操作系统(OS)；作为操作系统补充的、各电子部件的驱动程序，以及控制 ATM 进行交易、管理、通信的控制程序，如图 8.4 所示。

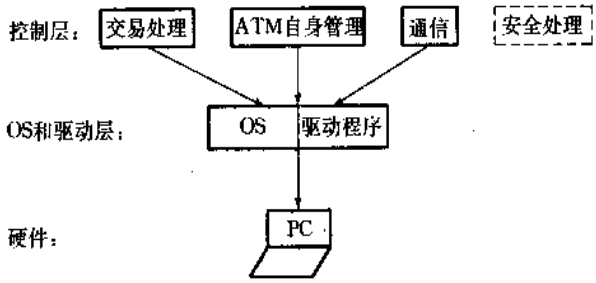


图 8.4　ATM 软件层次结构

正如多数 ATM 利用通用计算机(如 PC 机)构筑控制系统一样，ATM 的 OS 层也大多采用目前流行的操作系统。如 Bull Questar 1410、3410 都采用 MS-DOS，NCR 的第四代 ATM 广泛采用 OS/2 操作系统。利用现成的操作系统，可充分发挥硬件的功能，获得更大的利益和支持，缩短系统设计开发周期。

ATM 的驱动层程序用来驱动各电子部件、各个具体的模块。比如，ATM 中需要有驱

动点钞系统的部件、需要驱动卡读写设备、驱动通信设备(如网卡)。这些电子部件相对于控制系统来说相当于外围设备,要想这些设备高效地工作,需要设计得很好的驱动程序对它们进行管理和控制。

ATM 软件的主体是其控制层的程序。控制程序是根据银行业务的需求,以及 ATM 所能提供的服务等方面编制的。从内容上看,控制程序包括三部分:ATM 交换处理、ATM 自身管理以及与银行主机联网的通信处理。

ATM 提示用户插入磁卡(或 IC 卡),接收磁卡(或 IC 卡)的信息,根据用户发出的指令作出响应,驱动各部件作相应动作。这个流程就是交易处理。交易处理部分详尽地描述了 ATM 所提供的服务过程,是对 ATM 所承担的业务的反映。该部分规定了用户如何与 ATM 交易,ATM 如何处理用户指令以及如何将交易结果(如现金、收据等)交给用户。它是控制层的主要流程。

ATM 的自身管理包括错误处理、操作员管理等等。ATM 采取一些冗余措施来保证软件的可靠,可靠性是 ATM 一项重要的指标。各功能部件的检测都属于这个部分。作为控制系统的 PC 机一般带有系统键盘。这个键盘不同于我们前面所提到的用户键盘和功能键,它隐藏于 ATM 电子柜内部,用户看不见。它是用来提供操作员(银行工作人员)管理系统使用的,故可称为系统键盘。ATM 应提供操作员通过系统键盘进行管理的接口或方式,方便操作员进行内部管理。这也属 ATM 自身管理的范畴。

ATM 一般与银行主机或金融网络相联,联机使用。如何与银行主机(或网络)联网是 ATM 软件中必不可少的,也是比较重要的一部分。通信模块就是起这个联网作用的。目前 ATM 一般支持多种通信协议,以适应应用环境的不同。例如,Bull Questar 1410 支持 VIP7700、BSC3270、X.25、SNA/SDLC 和局域网等多种协议;富士通公司的 7000 系列 ATM 支持 SNA/SDLC、BSC3270、TD800 同步协议、TC500、2260 异步协议和 X.25 等等。通过通信模块,一方面 ATM 可以充分利用主机丰富的资源,查询用户的帐目信息;另一方面银行主机可以对 ATM 很好地控制和管理,监视 ATM 的正常运行。

值得一提的,除了上面所述的三部分内容外,ATM 软件还包括一重要部分,那就是安全性处理。从内容上看安全处理不是一独立的内容,但它贯穿在上面三个部分之中,是控制层不可缺少的模块。安全处理包括如下几个内容:卡(磁卡/IC 卡)的验证,非法卡的处理;用户密码的处理;以及通信数据的加密/解密等。ATM 接受卡以后,首先要判断用户插入的卡的合法性,然后提示用户通过用户键盘输入用户密码,核对无误后用户才能操作 ATM。如果 ATM 发现有误,要作出相应的处理,这些都是安全处理的范畴。ATM 通信数据的加密是个很重要的问题,否则交易的内容就暴露在外,容易受到侵犯。目前 ATM 广泛采用 DES 算法(详见第 5 章)对通信数据进行加、解密。另外,安全处理模块还包括接收各种感应装置的信号、驱动报警器等,增强 ATM 的保固性。

8.1.3 ATM 的机械结构

ATM 的机械结构指的是 ATM 的尺寸大小、外形、内部布局等非电气结构。设计 ATM 的机械结构,一定要考虑到 ATM 的用途、用户使用的方便程度、牢固程度等方面。总的来说,电子柜和保险柜分开,便于 ATM 内部布局合理化,电子部件维护、操作起来比

较方便，还可以采取多种措施保证保险柜的牢不可破。先进的ATM在许多方面设法保护保险柜。保险柜的壁用多层坚硬的钢板(或其它更坚固的材料)组成，夹层内填充有耐火、耐腐蚀材料，如水泥、混凝土等，防止非法者企图火烧或气割。ATM保险柜的锁是专门设计的，采用多道保险技术，一般有多道锁，有的锁还有多道密码。保险柜内钱箱也有密码锁进行防护。如果ATM是放在外面，无人监守，昼夜使用，一般设计成穿墙式，用户只能见到用户界面，其余部分均在墙内，起到保护ATM的作用。国际上已有多个标准化组织制定了ATM的安全性能指标，如UL291、RAL、RM/RT30……。各厂家的ATM在保固性能上都必须符合至少一种这类标准。

很多ATM内部设计有一些导轨和滑车，使得内部布局灵活、合理，电子部件移动容易、操作员(或管理员)对ATM的维护和管理也比较方便。ATM在机械上还有许多这样那样的设计，以致ATM的机械结构多种多样，但都是基于方便和牢固这两个原则的。

8.1.4 ATM应用流程

ATM作为银行设立的一种自动金融服务设备，一般要与信用卡配合使用。图8.5所示的是在ATM上使用信用卡的典型的业务流程。

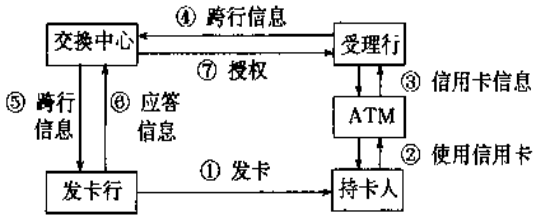


图8.5 在ATM上使用信用卡业务流程

发卡银行对信用卡个人化后，发给持卡人(过程①)。持卡人就可在任一受理行的ATM上使用信用卡(过程②)，产生ATM业务，信用卡信息通过ATM传给受理行(过程③)。此时，受理行可通过该行的信息网络向交换中心发出信息，由交换中心转发发卡行(过程④和⑤)。发卡行根据持卡人帐户情况决定交易能否进行。这是一个授权过程。如果用户帐户允许，发卡行通过交换中心回应授权信息给受理行(过程⑥和⑦)，授权受理行通过ATM和持卡人进行交易。

受理行每天对当天所进行的业务进行整理，通过计算机日结，并与交换中心核对确认后，同发卡行进行资金清算，保证帐目的平衡。

上面描述的流程是建立在强大、可靠的计算机网络基础上的。如果缺乏这样的网络，或网络系统不够完善，不够快，势必造成网络的拥挤或堵塞，给用户带来不便。这种情况下，ATM往往采取一种变通的应用方式：并不是每笔交易都需经过发卡行授权。发卡行在发卡给个人时，可规定他的信用额度，即限制用户一次交易的金额量以及交易的次数。持卡人在ATM上进行小于这个限额的交易不需要授权，可以马上完成(例如，提取小额现金)，ATM每天再成批地与银行主机进行资金清算。这种方式可能会给银行带来一定数量的损失，但限额的存在使这个损失不会很大，又大大方便了用户，目前大多数银行的

ATM 广泛采取这种应用方式。

8.1.5 ATM 应用现状与前景

ATM 是一种集电子、机械、保密等高新技术为一体的高可靠性金融设备，国际上只有十几家厂家能够生产。其中 NCR 公司的产品市场占有率达一半左右，其它如 Bull、Olivetti、Toshiba、Fujitu、IBM、Philips、Omron 等大公司也有部分产品。国内 ATM 的研制、生产近二年才开展，北京有线电厂已研制出了可称是我国第一台自行设计的 ATM，其性能虽然与国外同类产品相比有一定差距，但它更贴近国情、更符合我国的具体情况。

目前我国金融电子化发展存在一定程度的"死锁"，体现在 ATM 的发展上，ATM 的年装机量全国不足一千台，这有多方面的原因。首先，ATM 产品本身不能完全满足我国银行业务的要求。另一方面，我国金融网的不足也影响了 ATM 的发展。目前国内还没有完善的跨行交换中心，各专业银行拥有自己的网络和 ATM，跨行不能交易，甚至同一行内交易也要受地域限制，大额交易的授权往往要等很大时间，这样使持卡人使用起来反而不方便，用户较少。银行投入较大资金却吸引不了多少用户，投资难以收回，因而造成可使用 ATM 的网点较少，更限制了 ATM 的推广应用。

随着"金卡工程"的实施，国家金融网的建设，以及发卡量的增多，ATM 装机量将大量增加。到那时，ATM 将和 POS 一起充分发挥金融电子设备的优势，为广大用户持卡交易提供方便。

8.2 POS 和 POS 系统

POS(Point Of Sales)是另一种重要的金融设备。它安放在商店、旅社、餐厅等消费场所，使消费者只要持有信用卡就可在一定额度内自由消费，大大简化了消费者、店主和银行的关系，是电子资金转帐系统的另一支撑设备。

8.2.1 POS 结构和功能

POS，指的是销售点终端。它是由银行设置在商业网点或特约商户的信用卡授权终端机。无论从外形或内部结构上看，POS 很像一台小小的计算机，但与计算机相比，在组成部件上又略有不同。

POS 终端设备一般由主控机、凭证打印机和客户密码键盘三部分构成。如图 8.6 所示(注意，图中所示 POS 没有客户密码键盘)。

主控机就是一台微型计算机，包括有显示器、键盘、卡读写设备、网络接口等。卡读写设备接受用户的信用卡，读取用户信息。网络接口用于和银行的主机或网络相联，传输信息。

凭证打印机将交易的内容，如购物名称，消费金额、帐号等打印出一个凭证，交与用户作为收费完成的依据。

多数 POS 终端为保护信用卡所有者，一般都设置 PIN(Personal Identification Number)识别方式来鉴别卡持有人是否为原合法的所有者以防止窃取盗用。银行发卡时会让

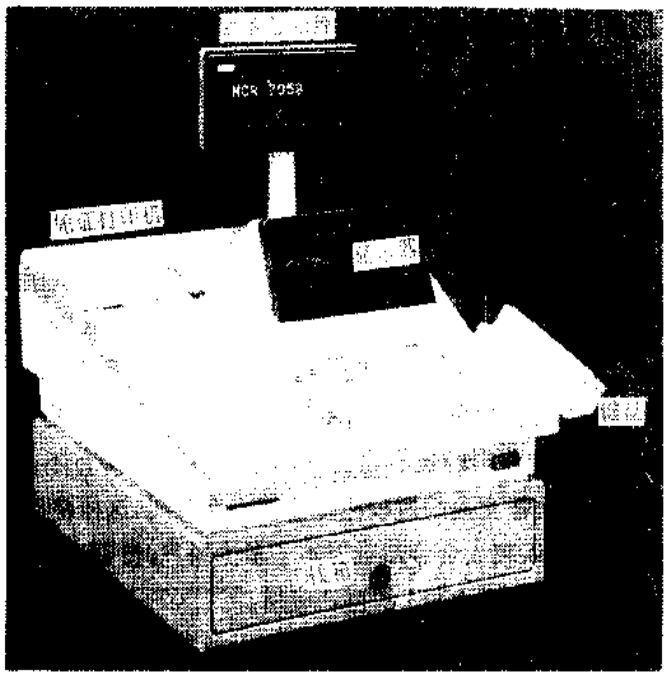


图 8.6　POS 终端设备

用户输入并记录一个号码作为用户密码，这个密码就是 PIN。持卡人在 POS 消费时必须先敲入这个 PIN，POS 通过银行网络将 PIN 和信用卡帐号核对无误后才允许用户进行消费。这个输入 PIN 的设备就是客户密码键盘。

除了以上几部分外，许多 POS 终端还配有条形码阅读器、钱箱等部件。现在许多商店的商品靠条形码来识别、分辨，既准确又可靠。这样条码阅读器就必不可少。有的 POS 除接受信用卡外，还可以让普通用户直接用现金付款，因而这种 POS 配备有钱箱。另外，有的 POS 还配有顾客显示牌(图 8.6 中立着的那个显示屏)，供顾客观看交易结果。总之，不同的厂家、不同的用途，各种各样的 POS 外形和组成上差别较大，但其核心是一致的，都用来收款。

POS 终端的软件主要是根据用户持信用卡购物消费、或用现金支付这个业务过程编写的。先进的 POS 融入了商店自动化的内容，在 POS 软件中加入了库存管理、进货管理和销售管理等内容，把 POS 终端从单一的收款机变成融收款和管理于一体的高性能系统。POS 终端软件和 ATM 一样，一般也建立在当前流行的操作系统(如 DOS 或 OS/2)上。

POS 终端根据装入的软件的不同，可提供多种功能，如读卡、显示、接受交易金额和密码、与银行计算机联网、存储交易信息、打印，以及商店自动化管理，等等。就用户而言，持卡人可以购物消费、查询和转帐。对特约商户而言，POS 可简化商户与银行之间资金清算的手续，加快速度、提高效率。

8.2.2 POS 终端的三种类型

POS 终端分三种类型：简易授权型专用终端、转帐终端和收银式 POS。

简易授权型专用终端包括读卡器、键盘、显示器和内置 Modem(调制解调器)，起沟通银行主机和持卡人的作用。这种终端操作简单，能有效防止人工输入错误，自动查黑名单。通过自动拨号即可将磁卡上的资料及键盘输入的金额送往银行主机，银行主机处理后授权 POS 进行交易，通过联机方式提高系统的可靠性和保密性。实际上，用户(持卡人和特约商户)是通过这种类型的终端直接跟银行主机进行交易。POS 主要起到信息传输作用，所以这种终端重点在其网络部分。

转帐终端除用作信用卡授权以外，还具有查询余额、转帐、冲正、清算等 20 多种功能。转帐终端一般带有密码键盘和收据打印机，比起授权终端，保密性和灵活性提高了许多，目前转帐终端正逐渐代替授权终端。

收银式 POS 是最高档的 POS，它本身是一台 286 或 386 微机，带钱箱、读卡器、收据打印机及流水帐打印机。它可以将现金帐和信用卡帐同时汇总，在完成每一笔交易的同时，将库存、销售、会计等项目同时更新，给商户带来更大的方便。这种 PC-Base 型 POS 终端，综合了计算机技术、通讯技术和机械技术，使收款机从早期单纯的信息采集工具进化为多功能的信息处理工具。因而对 POS 本身，对商户的自动化水平也提了比较高的要求。

目前这种收银式 POS 正逐渐占领市场，性能也越来越好。例如，IPC POS 采用 386 SX33 处理器、16MB 内存，以及 9 英寸 VGA 显示器，带有软驱、磁卡阅读器、条形码阅读器、顾客显示牌、钱箱等部件，还有一系列扩展接口，外形上更像一台 386 台式微机。富士通 TeamPOS 更是采用 25MHz 的 486 芯片和 DOS 操作系统，可以说是直接用 486 微机构成系统。前面图示(图 8.6)的 NCR POS 705B 也是 PC-Base 型的，采用 286 处理器和 DOS 操作系统。

以上三种类型的 POS 终端，从简单授权型到收银式，结构越来越复杂，功能也越来越齐全，反映了 POS 发展的一个趋势。同时，随着 POS 终端提供的功能越来越多，持卡用户或普通现金、支票用户到商户购物消费的方式也更加趋于方便。

8.2.3 POS 系统的构成与应用

根据商户自动化水平、银行金融网的发展状况以及用途的不同，POS 系统的构成方式多种多样。典型的有独立型和联机型方式。

独立型(stand alone)POS 系统简单地由 POS 终端和外围设备构成。这种 POS 系统用在商户自动化程度低的场合，只是起到电子收款机的作用。用户将现金或支票交给收款人，收款人通过 POS 打印一个收款凭据交给用户作为收费完成的标志。用户也可以持信用卡进行小额(一定限额内)消费。每天 POS 终端把当天交易的流水帐打印出来报告给商户，和银行对帐，进行清算。这种 POS 系统的功能是很有限的，不能充分发挥 POS 的作用。严格地说，这种构成方式甚至不能称为系统。

联机型(on-line 型)POS 系统是一种销售点电子资金转帐服务系统(Electronic Fund Transfer Point Of Sales System，缩写为 EFT-POS 或 E-POS)，它是指利用由银行设置在

商业网点或特约商户的信用卡授权机，由银行计算机联机地通过公用数据交换网构成的电子转帐服务系统。其功能是使持卡人在指定销售点购物或消费后，通过电子转帐系统直接扣款或信用记帐。我们来具体看看这种电子资金转帐系统(EFT System)的结构。

EFT 系统一般包括三部分：银行主机、通信网络和金融终端。典型的 POS 系统的结构是，多台主机利用网络相互连接，众多的 POS 终端直接或通过网络连到主机(如图 8.7)。主机放在银行内，存放用户和商户的帐目。用户通过设在商户中的 POS 终端进行交易。主机接到通过 POS 传来的信息后，首先检查磁卡(或 IC 卡)帐号的合法性，是否超过有效期，是否为止付卡(停止支付的卡)、要求的授权额是否超过可授权限额等等。如发现问题，主机发送相应错误信息到 POS 终端；如检查通过，主机修改顾客帐户文件的授权限额(或顾客帐户余额)，将回答码回送至 POS 终端。这个过程不论授权成功与否，主机自动记录授权、交易情况，以备查询。

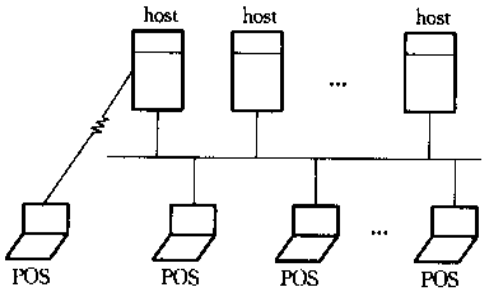


图 8.7　联机 POS 系统示意图

从计算机应用的角度来看，这种 POS 授权系统是一实时信息交换系统；而从银行业务的角度看，POS 授权系统是电子化的支付系统。

有的大型商户构成系统时，POS 终端并不直接与银行主机或金融网相连，而是先在商户内部自成一网络系统，再与银行金融网相接，如图 8.8 所示。

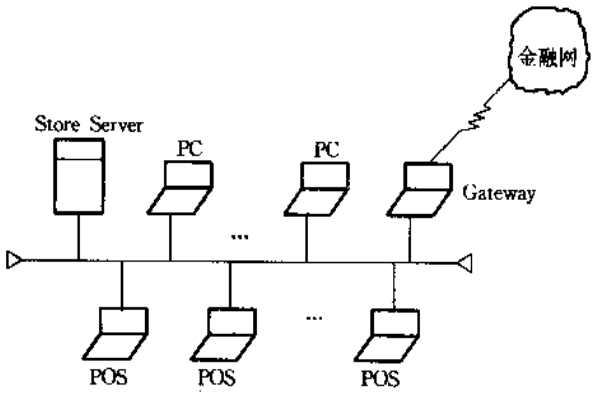


图 8.8　大型商户网络系统构成

这样构成的系统，融电子资金转帐与商店管理于一体，既可通过金融网对持卡用户授权，又可收集用户信息，进行进货、销售、库存、财务等方面的管理，供决策使用，大大提高

了商户自动化水平，提高了效率，增强了竞争力。同时，商户可以通过自身的网络对交易预作处理，等金融网空闲时再成批地与银行主机进行资金清算（批处理），这样既提高了交易效率，又缓解了金融网因拥挤而造成的压力。在这种系统中，POS 终端就不仅仅充当信用授权的角色，还具有了数据处理能力，真正发挥了 POS 的潜力。

联机型 POS 系统是建立在计算机网络基础上的。目前很多商业网点中的 POS 并没有并入银行金融网，只是单独使用（独立型 POS 系统）。用户的购物消费还大多用现金支付，如果用户持信用卡支付，那更加麻烦，大额消费需由收款人员通过与银行联系进行人工授权，时间往往较长，给用户带来不便。可见，网络在 POS 系统中起着非常大的作用。要想构筑一个高效的 POS 系统，必须先建立一个高速、可靠的金融网络。

图 8.9 所示的是一理想的在 POS 上持卡消费、使用信用卡的流程。

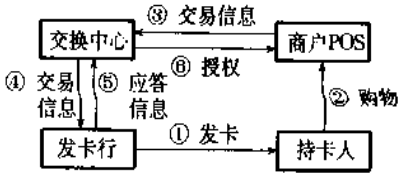


图 8.9 在 POS 上使用信用卡流程

发卡银行将信用卡发给持卡人后，持卡人就可在商户的 POS 上付款消费。当用户将信用卡插入 POS 的读卡设备，信用卡的信息以及交易消费信息就经过 POS 送至交换中心（过程③），经判别后信息转发至发卡行（过程④）。发卡行将处理结果经交换中心转回 POS，对商户和持卡人授权，（过程⑤、⑥），实现交易（或拒绝交易）。完成联机授权过程。

每天商户将所有 POS 上交易的信息交给银行（收单行，与发卡行可以不是一家银行）。收单行将收单信息发至交换中心，经汇总后向发卡行发出清算信息，由发卡行向收单行划出清算资金，进行清算。

随着国家金融网的建设和计算机技术的进步，这种理想系统的实现不是不可能的，到那时，“一卡在手，走遍中国”也许不再是一句口号，人们将真正感受到科学进步给人类带来的极大便利。

思 考 题

1. 什么是 ATM？它有哪些功能？
2. ATM 外形上包括哪几部分？各部分有什么作用？
3. ATM 硬件上包括哪些子系统或模块？各部分作用如何？
4. 简述 ATM 软件结构及功能。
5. ATM 采取哪些措施保证其牢固、可靠？
6. 简述在 ATM 上使用信用卡的业务流程。
7. 什么是 POS？POS 包括哪些部分？
8. 什么是 PIN？其用途是什么？

9. POS 终端有几种类型？各类 POS 功能如何？
10. POS 系统的构成方式有几种？
11. 简述 EFT 系统的一般构成？
12. 简述在 POS 上使用信用卡的业务流程。

第9章　IC卡应用技术

IC卡比磁卡的存储容量大，可靠性和安全性高，在应用上除了覆盖磁卡的全部应用范围以外，还提供了许多磁卡所不具备的应用特性。正是这些特性，使IC卡在脱机业务处理和联网数据一致性等方面表现出前所未有的优势。

IC卡虽具有很强的功能，但仅当IC卡加入到应用系统中，构成发行商、应用系统和持卡人之间的数据传输媒介时，才可能有效地发挥其优势。一个好的IC卡应用系统，除了应具备良好的应用特性和性能价格比以外，其安全特征也是一个绝不应忽视的问题。如何构造一个基于IC卡的应用系统，这一系统又以何种方式去运作，怎样发挥IC卡自身的优势，使系统具有较好的性能，目前又有哪些应用系统在运行，本章将对上述问题进行讨论。

9.1　IC卡的应用概况与技术优势

IC卡最初是为了解决金融交易中的安全性问题而设计的，它带来全新的交易概念与前所未有的优势。很快，这一优势也为其它应用部门所看中，使之广泛应用于电话、医疗保健、路禁控制和门锁控制等系统中。随着时间的推移，应用范围还在不断扩大，使用IC卡的数量亦呈几何级数增长。同时，为满足不同应用场合的需求，IC卡制造商们仍在不断地向市场推出新的IC卡，IC卡的价格将随着使用量的增加而逐年下降，所有这些，无疑又会大大推进IC卡在各个领域的普及。

IC卡在应用中的技术优势在于良好的机器读写能力、共同认可的安全防范技术和相对较大的数据存储能力。

1. 良好的机器读写性能便于人-机 卡之间的会话

IC卡是一种电路卡，它在机器读写性能上远优于磁卡和光卡，无需往复的机械动作即可完成人-机-卡之间的多次会话过程，使卡在应用时更容易进行操作与相互验证，给卡的应用开发者和使用者都带来了极大的便利。

2. 良好的安全防范技术使卡能够脱离网络使用

IC卡采用了为国际上各开发者与使用者所共同认可的半导体密码存放与软件加密技术，它可以有效地阻止卡的非法复制与数据的篡改。应用设备可以在脱离网络的情况下，不需人工干预，即可对IC卡进行鉴别，以确定该卡是否是本系统所许可的，是否可在该应用场合中使用等。通过持卡人输入PIN(个人标识号)，与卡内一组密码比较，可以确认持卡人的身份。这些特点，使IC卡能成为传导媒介，再加上认证和数据加密等功能，使卡能脱离网络使用。

3. 大容量的数据存储能力使IC卡成为数据载体

在一个应用系统使用中，系统必需对所有持卡人建立一份身份与使用的档案。在磁卡系统中，这组档案存放在中心数据库系统内，持卡人每次使用都必需通过终端，以网络形

式从数据库系统中提出那份与自己相关的档案。现IC卡的存储能力增加了，这份相关的使用档案可以存放在IC卡中，终端设备无需联网即可得到使用者的相关信息，使用的灵活性大大增强了，交易的实时性也明显改善。

以上三大特点的结合，构成了IC卡应用的强大优势，它一方面降低了对网络的依赖程度，提高了响应速度。另一方面它对发行商、应用商和持卡者三方面的利益提供了有效的保护手段，解决了以前所难于解决的关键问题，为IC卡的广泛应用铺平了道路。

IC卡应用范围相当广泛，这里仅根据现有的应用提供部分应用领域。

(1) IC卡应用于金融领域，可以作为信用卡、现金卡、证券卡或电子资金转帐卡等。

(2) IC卡可以作身份证明卡使用，如身份证、驾驶执照、会员证等。

(3) 在医疗、保健等领域，IC卡可以用于健康卡，少儿疫苗卡，就诊卡等。

(4) 在商业及服务业领域，可以用IC卡作为优惠卡、结算卡、服务卡等。

(5) 在交通领域，可以用IC卡取代现有的公交或地铁月票，它可以改变原有对月票的当月有效限制为有效次数限制，为改善公交管理提供了有效的工具。另外，它可用于公路付费和停车付费等场合。

(6) IC卡电话卡，这是至目前为止IC卡用量最大的一种应用。用IC卡公用电话，替代磁卡电话与投币电话，既可杜绝欺诈行为，又可省去携带零钱所带来的麻烦。此外，IC卡在蜂窝式数字移动通信网中(GSM)，以身份卡及保密卡方式投入使用，避免了因冒用用户电话号码而给用户带来的损失，成为IC卡在通信系统中又一蓬勃发展的行业。

(7) IC卡可在门禁系统、设备使用等情形中，以钥匙卡的形式出现，使"锁"有了更新一个层次的概念。

(8) IC卡还可集各种服务功能于一身，企业的员工卡，校园卡即属此类。持卡者可以用卡进行考勤、开门、就餐、借阅图书等。

9.2 IC卡的应用模式与特点

现在市场上提供的IC卡种类有上百种之多，正是这些种类繁多的IC卡，给我们带来了许多便利的条件。这些卡根据存储容量的不同、安全等级的不同，其价格亦不相同，从不足一美元一张到几十甚至上百美元一张的IC卡都有，因而，在构造一个应用系统时，必须仔细分析IC卡在系统中所扮演的角色，并合理地利用编码或其它压缩技术，使所选用的IC卡的价格在一个可行的范围，以提高系统的性能价格比。在选择IC卡的过程中主要从安全性、存储模式和存储容量这三个方面来综合考虑。

1. 数据的安全性与卡的选用

如果一个应用系统仅以IC卡作为数据的转储介质或以软件加密方式对数据进行加密而不必担心他人进行篡改或复制时，普通的存储器卡是用户的最佳选择，它的每位价格最低，而且容量范围亦较大，从1K bit(位)到16K bit(位)的产品都有，支持的厂家也很多。如果卡是在以储值、金融及其它使发行商或持卡人担心卡会被别人非法复制与篡改的场合，那么就必须采用带有保密逻辑的卡或COS卡了。保密逻辑卡可分为二类：一类是小额储值卡(Token Card)；另一类是密码保护存储器卡。它们的特点是在卡上引入了固化

内容和不可读、只可核对的密码区域，并由密码核对的正确与否来控制卡的读写特性。它可有效地防止一般情形下对卡的非法攻击，而且价格适中，与系统结合使用还可以防止一般的侦破手段，目前这类卡的应用数量最大，应用范围也最宽。COS 卡由于自身带有 MCU 及加密算法，可以用随机数与密钥结合的方式来进行卡与设备间的相互认证，可以有效地防止冒用和窃听等攻击手段，是金融系统及安全系统选择的佳品，它的缺点是卡的价格较高。

2. IC 卡的存储模式选择

有些人认为 IC 卡的存储空间的使用像普通随机存储器一样，可以随意构造一个数值写入卡中，其实这样的理解只对存储器卡来说是正确的。为了保证卡的安全特性和缩小卡的芯片面积，IC 卡的设计者们往往刻意定义 IC 卡的存储结构。例如，一次性计数卡主要是用在小额储值卡上，它将用户存储空间与外围逻辑结合，构成了一个减法计数器，用户在使用时，只能对其进行减法计数，一旦计数器减至零，该卡就不能再次使用了。COS 卡是以文件方式来对卡的存储空间进行组织的，文件的数据记录模式可以有多种选择（ISO-7816 第四部分定义了四种记录模式，但并不是所有的卡都实现了这四种模式），一旦确定并发行后，其读与写的模式也就固定了。从安全角度上，随意读写也是一种不可取的方式。

3. 存储容量的选择

IC 卡的存储容量的大小直接影响着芯片面积和工艺的复杂度，因而也直接影响着卡本身的价格。有些用户总是想把所有的包括变动的和非变动的信息以及改动过程都存于一张卡片上，这样的做法往往把大量资金投放到一个并不值得的存储空间上。正确的规划方法是划定哪些数据是卡在使用中所必需的；哪些是可以存放在系统数据库中的；哪些数据又在数次使用后便不很重要可以替换掉的。在这些数据确定后，再考查一下所有信息是否可以通过编码方式进行压缩。然后根据每一部分内容的需要确定其存储模式，并选择相适应的卡型。值得一提的是，一张卡的标定空间并不一定是用户的可用空间，必须依据其用户空间和可提供的存储方式来选定一种卡型。

4. 特殊环境要求下 IC 卡的选用

如果一张卡要在多个不同的部门使用，而且每个部门都有其独立的安全性要求，那么 M-COS 卡（多功能卡，Multifunction Card）是您最佳的选择，它允许用户将卡内空间划分为多个具有独立认证与密码核对的专用文件 DF（Dedicated File）。每一个 DF 下又可连接多个基本文件 EF，（Element File）或 DF，它使一卡多用成为可能，但价格较为昂贵。如果应用场合有严重的水汽或其它不利于使用带触点的 IC 卡时，应考虑使用非接触式 IC 卡，较具典型的是 RF 卡（射频卡），它采用射频方式与设备进行通信，有效距离可达 10—100cm，它的缺点是价格较高，且我国尚未指定其使用频率，是否与其它无线设备产生相互干扰，尚无法得知。

5. IC 卡的应用数据处理模式

综合各种应用情况，对存储器中的用户应用数据的处理方法可归纳为三类：

（1）按位计数方式：例如逻辑加密卡用作电话卡时，通常将用户数据区划分成两个区，其中一个是大额区，另一个是小额区，在用户购买预付费电话卡时，发卡商将大额区与

小额区全部擦除(即个人化操作),其结果是将 EEPROM 的用户数据区全部置成"1",数据区中每一个"1"代表一个计数单位,代表一定金额,例如小额区的一个"1"可以代表一次市内通话的最低费用,大额区的一个"1"代表小额区金额的总和。如果小额区有 512 位,最多可打 512 个市内电话或相应金额的长途电话。每打一次电话将小额区的一个"1"或若干个"1"(通话时间长或打长途电话)置成"0"。当小额区全为"0"时,自动将大额区的一个"1"置成"0",并将小额区全部擦除,如此重复,直到大、小金额区均为全"0"时,应去发卡商处重购电话卡,对于可以多次重复使用的卡,到发卡商处交费并进行个人化后即可继续使用。

预收费水表卡/电表卡、汽车加油卡、汽车停车计费卡,过桥过路收费卡等都可采用这种数据处理模式。

(2) 金额计算方式:适用于大部分金融卡(信用卡、现金卡)和储蓄卡等。卡内数据区内存放现金额(对信用卡还可能存放有关允许超额使用金额的信息)。在持卡消费时除了进行安全验证外,还要从当前现金额中减去本次消费额,写入新的余额(或欠款额),同时还可能要保留最近若干次消费记录,因此希望有较大存储容量。用智能卡作为金融卡是比较理想的。

(3) 存储方式:例如健康卡和身份证等,在用户应用区中记录个人的一些重要信息。对健康卡来说,可记录姓名、地址、血型、对药物过敏情况及重要病史等,甚至可考虑作为简单病历使用。对身份证而言,除了姓名、地址、性别、出生年月以外,还可以录入相片、指纹等生物特征,以及个人简历。这种使用方式的主要特点是存储数据,不允许持卡人修改数据。

以上三种方式几乎囊括了全部应用。

此外,在选用 IC 卡时,还要对 IC 卡的机械强度、封装质量、抗静电强度以及电气指标等进行核定。总之,IC 卡的选用必须综合多种因素,切不可盲目选用。只图节约资金去牺牲应用性能或盲目追求大而全的做法都是不可取的。

9.3 IC 卡的应用领域

IC 卡的应用领域可以说非常广泛,它除了覆盖传统磁卡的全部应用领域外,还拓展了许多磁卡所不能胜任的领域,这很大程度上归功于 IC 卡的大容量的数据储存能力与强有力的安全特性。

IC 卡的应用可分为金融系统应用和非金融系统应用两大类,在某些场合下,这两类应用又有着紧密的联系。

9.3.1 IC 卡在金融领域的应用

首先讨论一下磁卡用作信用卡时在金融系统中的应用情况。

磁卡的磁条上只记录着持卡人的信用卡号,开户行帐号和通过机具加密的 PIN(个人认证码,即:个人密码),所有的交易必须通过终端设备与中心数据库联通后,经中心数据库系统的验证与授权后,方可实现一次交易。当网络不畅或异地交易时,这种交易过程必

须付出相当大的时间或金钱代价才能完成，给商户和持卡人都带来了许多不便。当使用IC卡作为信用卡时，这一情况有了很大改观，它将认证与授权关系由中心数据库系统转移到终端设备上，而信息的安全性不变，这样，每一笔交易发生时可以不必再与中心数据库系统发生实时联系，仅通过日汇总方式进行结算和数据副本的传递服务，网络的负荷大大降低了，每一笔交易的代价也同样降低到一个最低水平。IC卡内可存放最近几次(2次—数十次)的交易记录、现存资金数值和现行透支额度信息，既方便了客户查询，又杜绝了利用网络不健全所进行的恶性透支等犯罪活动的发生。

1. 信用卡的交易方式与过程

信用卡的交易过程由三部分内容组成，第一部分是身份确认过程，这一过程中，终端设备是以发卡商的身份出现，它与卡，持卡人进行相互的核对与认证，只有三方面都正确无误时，以后的过程才可能进行。三个方面所认同的标准是相互间密码与密钥的一致性，卡对密码的可试探次数是安全性的又一保证。

在第一部分工作完成后，终端设备开始进行第二部分工作，即进行额度判断。卡内存放着该卡的全部信用信息，包括当前余额，最大一次性使用额度、最大透支额度信息和当天允许支付的次数等。终端设备根据这些信息可以作出本次交易是否可以进行的判断，如果本次交易被终端判断为有效交易，则转入到第三部分交易过程，否则退出本次交易。

第三部分是交易记录过程，终端设备将本次交易信息用保密信报方式传递给IC卡，IC卡则在其内部存储器上登录本次交易的信息，并修改当前余额，写入成功后，再以签名信息方式将信息返回到终端设备，终端设备将交易记录和签名信息存入在本地存储器内，以备汇总、清算使用。

2. 信用卡系统的构成

信用卡系统由中心数据库系统、发卡中心、清算中心、挂失、失效登录系统和终端管理系统(如一台独立单机、又称前置机)和ATM、POS等终端设备组成。

终端设备与中心数据库的汇总清算工作可以通过批处理作业方式来完成，这种方式与实时联网授权系统比较起来，可大大降低对主机与信息网络的性能要求，甚至一台基于486的微机作为前置机就可以管理数以千计的销售终端，租用的电话网络线路数量与通信时间也降低到原有的1/5—1/10，系统的使用费用和维护费用都降低到一个非常低的水平，仅此项节约的开支就足以抵消IC卡与磁卡之间的差额支出，因而在信用卡系统中使用IC卡是一个安全、方便而又节约资金的方案。

发行商发给用户一张新卡时，在将编码、用户的开户银行等信息存入卡的同时，亦将该持卡人的信用等级、最大消费和透支额度等存入卡中，这时，这张卡便可以使用了，该卡可以在该信用卡中心注册的任何一台ATM或POS等终端设备上进行存款，支取或消费活动。这些终端设备再以汇总方式将交易数据传递给数据中心，中心数据库系统根据持卡者编码和签名信息将每一个有效信息以借或贷的关系存入该持卡人的交易档案中。清算中心则依此进行各银行间，持卡人与商户间、商户与银行之间的清算服务，同时也对每一持卡者的信用程度进行评估，若某一持卡者违反信用准则时，该卡的编码会立即打入到黑名单中，这一黑名单通过中心数据库系统下载到各终端设备中，各终端设备则依据这一编码将正使用的一张在黑名单中的卡置为无效。

IC 卡的挂失(丢失或被窃)、损坏服务也是IC 卡服务系统的一个重要环节。若一个持卡人报失一张卡,则该卡会被登录到黑名单中,并在核对该持卡人交易数据后,补发一张重新编码的 IC 卡。IC 卡的报损有三种情况,即卡物理上损坏,卡超出了有效的服役期限和持卡人忘记了个人密码(PIN)。对于头两种情况,发卡中心可以以补发新卡方式来解决。对于第三种情形,发卡中心通过卡的信封管理(在 ISO-7816-4 中定义,现已在多种卡中以不同方式实现),来将卡中原有密码删除,并以新密码重新封起一个信封即可。

3. 非实时网络所引起的数据不一致性及其解决办法

由于 IC 卡的交易系统是以非实时的汇总方式与中心数据库系统进行信息传递的。卡中的数据与数据库中数据之间会有一个时间差,在这个时间差内,数据是不一致的。当一张卡报失或报损时,由于持卡人(或检到卡的人)在报失或卡损坏前可能已进行了一连串的交易活动,而这些交易信息尚未反映到数据库中心系统,便出现了数据的不一致性,若按当时的数据档案中的交易数据补发新卡,就会造成以后的交易错误,这个问题的一种稳妥的解决办法是待到一个交易汇总周期(包括异地汇总)结束后,再补发新卡,持卡人必须耐心等待一段时间才能重新用卡进行交易,这将对信用卡中心的信誉产生负面影响,解决这一问题的唯一方法是缩短汇总周期,但这样又无疑加重了网络的负荷,而必须在其间选择一个较为折衷的方案。欧洲的 IC 卡信用卡系统的汇总周期普遍选择 3—5 天时间,这样持卡人基本上可在一周内得到一张补发的新卡,而网络的负荷也在一个允许的范畴之内。

黑名单是在终端与主机汇总时,才下载到终端的,因而也存在着时间差问题,好在信用卡使用时都需输入一个个人密码(PIN)。而正常情况下 PIN 和卡同被一个人偶然得到的可能性极小,除非是故意的犯罪。且信用卡在有限时间内只能进行有效额度的消费,其损失也在一个允许的范围内。

图 9.1 为"IC 卡销售点转帐系统"的作业过程图。图中还示出了金融机构(银行)、商店和持卡人之间的相互关系。作业流程如下:

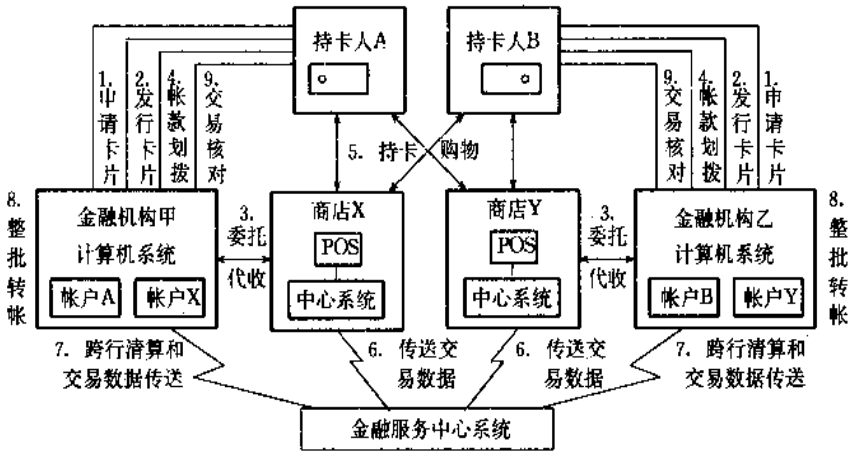


图 9.1 销售点转帐系统作业过程图

1. A、B 两人分别向金融机构甲、乙申请卡片。

2. 金融机构甲、乙分别向 A、B 发行卡片。

3. 商店X、Y分别与金融机构甲、乙建立联系，设立帐户。

4. 帐款划拨：持卡人划拨消费用的圈存金额、预付金额或偿还透支金额。

5. 持卡人A、B可持卡到商店X或商店Y购物消费。

6. 商店X、Y将交易数据传送给金融服务中心系统。

7. 金融服务中心系统与金融机构之间进行跨行清算及数据传送。

8. 整批转帐：金融机构将交易数据集中处理，校验交易有效性后即予以转帐。

9. 持卡人可以向金融机构核对交易数据。

在上例中，IC卡的识别工作由商店进行，如交易金额大，需要通过金融机构向商店授权后才能成交。商店应持有止付卡的黑名单。

9.3.2 IC卡在非金融领域的应用

1. 电度表IC卡预收费系统

包括电度表IC卡发行系统和电度表IC卡使用系统两部分。

(1) 电度表IC卡发行系统

由供电局管理，该系统由IC卡读写设备和微型计算机组成。承担向用户发行IC卡的任务。

用户到IC卡发行部门预交费(售电)，发行部门在IC卡内写入允许用电的数量及用户标识码，该标识码与装在用户处的电表是唯一对应的。同时将用户的用电情况记录在本系统微型计算机的数据库中，以备日后查询。

用户将IC卡插入电表中，即可用电。

IC卡发行系统的主要功能如下：

① 发卡与售电：用户安装使用IC卡的电表后，到指定的地点购卡，发行系统为每一用户建立一份记录。

② 查询：供电局管理人员可以随时查询指定用户或所有用户在某段时间内的用电情况，并能打印输出。

③ 设置每度电的价格：管理人员输入正确密码后，可以设定或更改电价。

为安全起见，操作人员只有在持有专门的操作卡或(和)专门的密码后才能进入本系统。

(2) IC卡使用系统：由电度表和IC卡组成。其主要功能如下：

① 验证：IC卡插入电表后，首先验证在IC卡中的用户标识码，以确定此IC卡是否有效，同时检查卡上的电量，并将它记录在电表内，然后允许将卡拔出，并保证如再次插入，卡上的电量不能重复计入，保证供电部门不受损失。

② 数据保护：表中的数据在停电后仍能保存相当长时间(若干年)，各个用户的IC卡不能互相通用。

③ 防窃电。

④ 显示：用户可查询表中剩余电量，并显示出来。

⑤ 报警及自动断电：当表中电量小于指定值时，应发出警告，提醒用户去购电，并允许超额使用一定度数的电，用户购电后，将IC卡插入电表，此时可把超额使用的电扣除，

这样既为用户提供方便，又不使双方受损失。如超过指定用电量后仍不购电，则自动断电。

本系统通过查询数据库，可了解各用户的用电情况和本地区的用电规律，以利于供电部门控制用电和计划用电。

2. IC卡门锁

IC卡门锁是用IC卡来开启门锁的装置，由门锁和写卡机两部分组成，写卡机用于向IC卡内写入密码，门锁部分用于读取IC卡上的密码，并与存放在门锁内的密码比较，如相等，则向电控门锁发出开门命令。

如IC卡门锁系统在宾馆内使用，可将写卡机放在总服务台，客人登记住宿，可用写卡机将某房间的密码和客人身份证号写入IC卡，并写入住宿日期等信息，客人交纳一定数量押金后即可拿到IC卡，到指定的房间，插入IC卡，门锁即可打开。客人离开宾馆，进行结算后，将IC卡交还给总服务台。IC卡可重复使用(写入新的密码和身份证号)。

客人离开宾馆时如忘了归还IC卡，也不会影响宾馆的治安，因为门锁的密码是可以随时更改的。同时因为各人的身份证号不同，因此非本房间客人即使知道密码也不能打开其他客人住宿的房间的门锁。旧客人回宾馆时，如果房间已换了新客人，则因身份证号不同，门锁内的存储电路内已存入新客人的信息，即使密码未变，旧客人也不能打开门锁。

IC卡门锁一般使用逻辑加密卡。

IC卡门锁可加快实现宾馆现代化管理，如客人进宾馆时，写入一定数量金额，可供客人在宾馆内消费用(进餐、购物和打电话等)，这样可减少现金流通量，方便了客人。客人离开时，将IC卡插入总服务台的写卡机内(此时需要有读卡功能)进行结算，并打印出帐单。一卡多用最好使用智能卡。

IC卡门锁可以是多功能的，可以是一门一卡(如宾馆使用)，可以是一门多卡(如多人使用的办公室)也可以是多门一卡(如进大楼门和房间门)。

假如门锁统一由上位机控制(如图9.2所示)，则各门锁的开启密码的设置、修改均可以在上位机上进行。

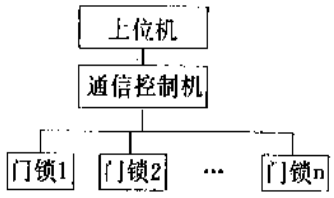


图 9.2 门锁管理系统

3. IC卡食堂收费系统

IC卡食堂收费系统由发卡管理系统和凭卡进餐系统组成。

就餐者在发卡系统购得一定金额的IC卡后，可到餐厅凭卡进餐，餐费从IC卡中扣除，这样就可避免传统售饭过程需收取钱票的种种弊端，并可减少收费差错，提高卫生水平和售饭速度，对各种信息可正确快速地进行处理，便于食堂进行管理和成本核算。该系统主要功能如下：

(1) 发卡管理系统完成卡的发行管理、成本核算、金额统计和报表打印等。

(2) 凭卡进餐系统对卡的合法性进行核对，可显示卡上的金额，对少于一定金额的卡给出提示，对超过卡上金额的消费予以拒绝，并能对当天的收入进行汇总。如遇停电，仍应继续工作，为方便就餐者，这一功能是需要的。

4. IC卡考勤管理系统

IC卡考勤管理系统广泛应用于公司、工厂、银行和宾馆等，对职工的出勤进行考核，实现自动化管理。考勤机可以有独立工作和连结微机工作两种方式。独立工作的考勤机

平时不需要与微机连结，数据存储在考勤机内，仅当微机要求数据或考勤机存储器不够使用时才向微机传送信息。与微机连结的考勤机本身很简单，从IC卡读得的考勤数据(姓名和时间)实时向微机传送。微机根据每个人的出勤情况(上、下班时间)和管理人员制定的考勤规则进行统计处理。

IC卡考勤管理系统的主要性能如下：

(1) 准确记录每个员工的上、下班时间及日期。

(2) 允许记录的员工人数应满足考勤单位的要求。

(3) 允许24小时连续工作。

(4) 断电后仍能继续工作。

(5) 有查询功能。

(6) 对管理系统设定密码，以保证安全。

5. IC卡娱乐消费计算系统

现在城市中涌现出了如娱乐城、会员俱乐部等高消费场所。IC卡娱乐消费系统正是为满足消费者的需要而设计的。该系统包括IC卡、发卡机和收费机(读卡机)三部分，其作用如下：

(1) IC卡：记录顾客预交费额或消费余额，也可以与会员卡合二为一，记录会员身份，这种卡在国外已作为现金卡使用。

(2) 发卡机：将顾客预交费额写入卡中，并将卡发给顾客。

(3) 收费机：顾客进行每项消费活动后，将消费额从卡中减去。顾客离开时可打印收据，并可对会员实行优惠。

该系统可随时统计营业情况，并消除使用现金时的许多弊端。

6. IC卡宾馆服务系统

将上面讲到的IC卡娱乐消费计费系统和IC卡门锁相结合，即可构成IC卡宾馆服务系统。目前宾馆已向多种经营和综合服务方向发展，住宿、进餐、电话、传真、娱乐和洗衣等多种费用都可以记录在卡中。如客房门上安上IC卡门锁，还可替代房门钥匙。

7. 电话卡计费系统

对电话卡计费方式已在9.2节中予以说明，在这里再补充一下有关长途电话计费情况，长途电话根据距离的远近而有不同的收费标准，因此在读卡机(可以和电话机安装在一起)中还应该有一张收费表及查表功能，同时长途电话收费相差比较大，因而采取前述的按位计数方法不一定合适，可考虑采用9.2中所讲的金额计算方式。或在卡内设置两个区，一个区(小金额区)用于市内电话，一个区(大金额区)用于长途电话。从这里可以看出，设计IC卡中的逻辑电路(逻辑加密卡)或编写应用程序(智能卡)时要考虑到实际应用系统的要求。

8. IC卡交通收费系统

最近几年来，我国桥梁、高速公路等建设发展很快，这些建设往往采取国内集资、中外合资或贷款等方式筹集资金，因此建成后需要在使用中回收资金，即需要收费，如能采用IC卡系统，则可减少现金收费时的种种弊端，并可加快收费过程，避免在收费处形成瓶颈口。

由于桥梁造价不同、高速公路距离不同，过路汽车(卡车、大轿车、小轿车等)大小重量不同，因此收费标准不同。再加上车是在公路上跑，可能要经过几个地区、甚至几个省，因此最好能设计全国通用的IC卡，或者先在部分地区试用，成功后再在全国推广。

要建立较通用的发卡系统必须有统一领导，制定出合理的收费标准，然后要考虑很多技术问题，诸如安全问题(发卡系统的安全、读写设备的安全和IC卡的安全)、数据记录问题、查询问题、卡的发放、回收和报废问题等。

智能卡可以一卡多用，如能将IC卡加油功能也包括进去就更理想了。

以上讲的IC卡指的是接触型IC卡，其缺点是路过桥梁的入口处或高速公路的入/出口时，仍需停车、如能改用非接触性IC卡则就不用停车了，可考虑用红外线探测车型以确定收费标准，或根据车重收费，后者可在车通过的路上设置压力传感器，自动测得重量(其原理与电子秤相似)，通过IC卡的读写设备确定所收费用，记入IC卡。

IC卡的读写设备记录下过路车辆的情况，利用这些数据可以进行分析统计，例如可统计出车辆高峰时间、车辆类型等，从而制定出不同时间不同的收费标准，利用经济规律来调度车辆，使车跑得更快、道路更畅通。

9. 其他

IC卡的应用范围很广，其他诸如IC卡加油系统、替代公共汽车月票、地铁月票的IC卡系统、汽车停车收费系统、图书证、身份证等不再一一介绍了。

IC卡实际上是将一台计算机(除I/O设备)装入到了一张名片大小和厚度相似的卡片中，可以装在衬衣的小口袋中。随着芯片集成度的提高，片内的存储器容量会越来越大，IC卡的用途会越来越广，从这点出发、IC卡实际上是一块尚未开发的处女地，其前途无可限量。

9.4 IC卡应用系统的开发

为便于应用，设计制造IC卡的公司往往同时可供应IC卡的读写设备，以供发卡商发卡时使用和商户收费时使用。为了适应某些用户自行开发应用系统的要求，有些公司还提供了通用读写器，可对市场上某些常用的IC卡进行读写操作，同时还提供开发工具(例如菜单选择和用高级语言编写的卡操作接口函数等)，用户可用它来开发应用系统。在后面将介绍适用于存储器卡和逻辑加密卡的操作接口函数。但需注意，尽管IC卡与读写器的触点已标准化，但IC卡内部逻辑与存储器区域的分配并未标准化，因此真正通用的读写器是很难实现的，所谓通用读写器也只能在一定范围内通用，所以用户在开发应用系统之前，必须对读写器的性能和特点有所了解，应该使用与IC卡相配的读写器。

读写器是IC卡和计算机之间的传输媒介，它与计算机之间是通过RS-232串行接口相连的，这里所说的计算机一般指微机，将读写器的串口与微机的串口(COM1或COM2)相连。

通用读写器可以有内置式和外置式两种类型。内置式读写器的外形尺寸与标准的三吋软盘驱动器一致，可直接安装在机内软驱的位置上。外置式读写器是一个独立的盒子，相当于一个串行接口外设。

读写器的电源可以由微机提供，也可以直接取自 220V/110V 交流电源，经整流稳压后得到的+5V 电源。IC 的电源一般由读写器提供。

本节要讲到的"IC 卡应用系统的开发"实际上仅涉及读写器的一些基本操作，读写器制造商已为这些基本操作编制好程序(即卡操作接口函数)，可供用户编写读写器的应用程序时直接调用。至于读写器的主程序以及与应用有关的程序仍需用户编写，如果读写器中的 CPU 芯片采用 i87c51，则可选用 Intel 公司的相应的开发系统，如采用 MC68HC05，则可选用 Motorola 公司的相应的开发系统。

综上所述，可以假设通用读写器与微机相连，用户开发应用系统时在微机的键盘上进行操作，通用读写器制造商已在微机上编制好菜单，例如第一级菜单(主菜单)可设置如下：

主菜单

1. 微机串口选择(COM1 或 COM2)
2. IC 卡卡型选择
3. 用户密码
4. 数据处理(读、写、擦除)
5. 上电操作
6. 下电操作
7. 熔断熔丝
8. 退出

菜单中的串口选择和卡型选择可预先设定默认值，如用户的 IC 卡已确定，且仅有一种，那末可不必再选择卡型。

如为逻辑加密卡，用户使用时需输入用户密码，与已存在卡中的密码进行比较，仅当输入密码正确时才能进行下一步操作，密码核对正确与否应在屏幕上给出提示，但不该显示密码。

数据处理指的是读、写和擦除操作，对于逻辑加密卡，要根据其存储器各区位置分配及各区读、写、擦除条件分别予以处理，并与熔丝(FUSE2)是否熔断有关(参见第 6 章)，在发卡处的 IC 卡，其熔丝 FUSE1 在出厂时已熔断。用户密码区的内容在 FUSE2 熔断以前，允许进行读、写或擦除操作，而在 FUSE2 熔断以后，虽允许从存储区读出，但不允许从芯片输出，密码比较只能在片内进行，当输入正确的用户密码后，允许用户修改密码，这样用户感到该密码只有他本人知道，会增强安全感，实际上也是如此。

上电操作与下电操作都是对 IC 卡进行的。

熔断熔丝操作指的是将 FUSE2 熔断，该操作是在卡发行时进行的，发卡机将用户密码和擦除密码写入卡后，将 FUSE2 熔断。从此以后，擦除密码不得修改，也不允许从卡中输出。

从主菜单选择下一步操作后进入下一级菜单。今以制造商提供的、用 C 语言实现的操作程序接口为例，介绍如下：

1. C 语言接口函数

(1) 串口选择(串口接通)

link com(int port)

参数：port 可选择 COM1 或 COM2

返回值：无

说明：此函数用于选择 COM1 或 COM2 和初始化串口，并通过串口向读写器提

供电源，传输速率为 9600bps。读写器加电后执行初始化程序需要有一段时间，

(2) 串口断开

unlink_com(int port)

参数：port 可选 COM1 或 COM2

返回值：无

说明：断开某一串口提供给读写器的电源。

(3) 上电操作

power on()

参数：无

返回值：为 0，操作正确，1 有错。

(4) 下电操作

power_off()

参数：无

返回值：为 0，操作正确，1 有错。

(5) 选择卡型

sel card (int cardtype)

参数：cardtype 为卡型

返回值：为 0，操作正确，1 有错。

(6) 核对密码

chk_secret (int cmd, char secret)

参数：cmd=SC，用户密码；

cmd=EZ，擦除密码；

secret，密码字符串。

返回值：为 0，密码核对正确，1 有错。

(7) 查询读写器状态

inquire (int cardtype, cardin, power)

参数：cardtype 为卡类型；cardin 表示读写器中有无卡，1 有卡，0 无卡；power 表示卡是否上电，1 上电，0 下电。

(8) 读卡操作

read_card (int cmd, addrh, addrl, len, race[32])

参数：cmd：选择卡中哪一区(如 FZ、…)

addrh：所选区高位地址

addrl：所选区低位地址

len：读出字节个数

race：存放读出数据的数组名

返回值：0 正确，1 有错。

(9) 写卡操作

write_card (int cmd, addrh, addrl, len, send[32])

参数：cmd：选择卡中哪一区

addrh：所选区高位地址

addrl：所选区低位地址

len：写入字节个数

send：所写数据存放的数组名

返回值：0 正确，1 有错。

(10) 擦除操作

erase_card (int cmd, addrh, addrl, len)

参数：cmd：选择卡中哪一区

addrh：所选区高位地址

addrl：所选区低位地址

len：擦除字节个数

(11) 熔断操作

fuse()

参数：无

返回值：0 正确，1 有错。

9.5 IC 卡应用系统的安全性和可靠性

在本书的前面几章，我们对 IC 卡的安全、防伪等问题已进行了充分讨论，但是作为应用系统，尤其是金融领域中的应用系统，涉及银行(或商店)和客户双方利益，系统的安全性和可靠性必须给以充分重视。

系统的安全性和可靠性包括 IC 卡和硬件环境的安全可靠性、网络通信设备及数据传输过程的安全可靠性、系统软件和应用软件的安全可靠性等，并应有严密的安全保密管理措施。

1. 硬件安全

IC 卡芯片及卡片制作质量要符合国际标准所提出的物理特性和电气特性，芯片中的 EEPROM 的擦写次数和信息保存时间(一般为 10 年)要予以保证。

从安全观点出发，在应用系统中的 IC 卡可分成三种：

(1) 持卡人拥有的 IC 卡。

(2) 操作读写设备使用的 IC 卡，称为设备卡，必须插入这种卡，读写设备才能工作，除此以外还可要求操作人员输入口令，以防冒用。

(3) 发行商使用的 IC 卡，必须插入这种卡，发行设备才能工作，也可要求发行人输入口令，以防冒用。

在金融领域中应用的计算机系统，其供电系统及主机系统都应有备份，一旦出故障，故障部件单独被隔离，冗余的电源或主机立即投入工作，保证系统正常运转。

与业务有关的数据也应有备份，系统中任何部件出问题，都要保证数据的完整性和正确性，因此存储数据的设备(例如硬盘驱动器)应有备份，且应处于备份工作状态(即在正

常工作时，处于备份的数据存储设备与处于工作状态的存储设备同时接收数据）。网络通信设备及通信线路要保证完好畅通，也应有备份或可转接的通信线路。

2. 软件安全

IC 卡和读写设备中的操作系统和应用程序要确保功能完善，数据安全，任何操作错误，都不应造成灾难性的后果。而且要验证持卡人的身份，并确认卡片及读写设备不是伪造的。

对于主机系统和网络系统，为维护数据的保密性和完善性，对于传输的数据，系统应有数据加密和文电鉴别功能来防止数据被非法截取、插入或更改。对于进入系统的数据要加以核对，存取权限要加以验明。

系统应采取措施去防止和处理各种异常情况，作出错误标记并以适当方法提请操作员或管理人员及时作出处理。

清算中心对收到的每条信息进行检查，例如发信息者的身份，信息的来源和目的地等，并将信息记录下来以备查对。要保证每条信息成功地送到目的地，因此目的地收到信息后要发出回答信息，对于没有回答的信息，应记录备案。清算中心收到回答信息后才允许将该回答信号转发给发出信息的来源点，源点在收到回答信号后才能完成转帐、提款或消费过程。

3. 建立严格的安全保密制度

对卡片的制作，读写设备的制作和使用要严格遵循保密制度。

对系统的主机及有关设施要符合安全条件（如温度、湿度等），并应有相应的应急防护措施。严格控制进入机房的人员和操作人员。对存储数据的介质要严加保管。

对有关人员进行严格的技术培训和保密教育。以保证有良好的技术素质和保密习惯。

思 考 题

1. IC 卡技术与磁卡技术相比具有哪些优势，从而使得在磁卡已占有广大市场的情况下还能发展 IC 卡。
2. IC 卡与磁卡相比，哪种卡对网络的要求高？请说明原因。
3. 当逻辑保密卡用作市内电话预付费卡时，应用区是怎样设置的？设应用区为 256 位，且仅有 1 个应用区，最多可打多少个电话？
4. 接上题，如设置有 2 个应用区，第一应用区为 256 位，第二应用区为 32 位。试问这两个应用区应如何设计使得此 IC 卡能用于打较多电话？最多能打多少个电话？
5. 请说出下述各卡采用何种 IC 电路较为合适：
   现金卡、信用卡、身份证卡、健康卡、病历卡、电话卡、加油预付卡、电费计费卡、门锁卡。
6. 什么是黑名单，其作用何在？
7. 持卡人如忘了个人密码（PIN），此卡是否应该作废，持卡人是否会蒙受损失？你觉得如何处理比较合适？
8. 为了 IC 卡能推广应用，为用户着想，应考虑哪几方面问题？
9. 预付费卡和信用卡有何实质差别？
10. 请写出在电话卡一次使用过程中，读写器的工作流程。

附录 A　有关识别卡的国际组织及识别卡标准

1. 有关国际组织

(1) ISO/IEC JTC1 SC17 分技术委员会

国际标准化组织/国际电子技术委员会，信息技术第一联合技术委员会第 17 分技术委员会，负责行业间和国际交换中使用的识别卡(如磁卡、IC 卡和光卡)、相关装置和识别卡管理的标准化工作。目前共有 37 个成员国，我国为成员之一。该分技术委员会的组织结构如图 A.1 所示。

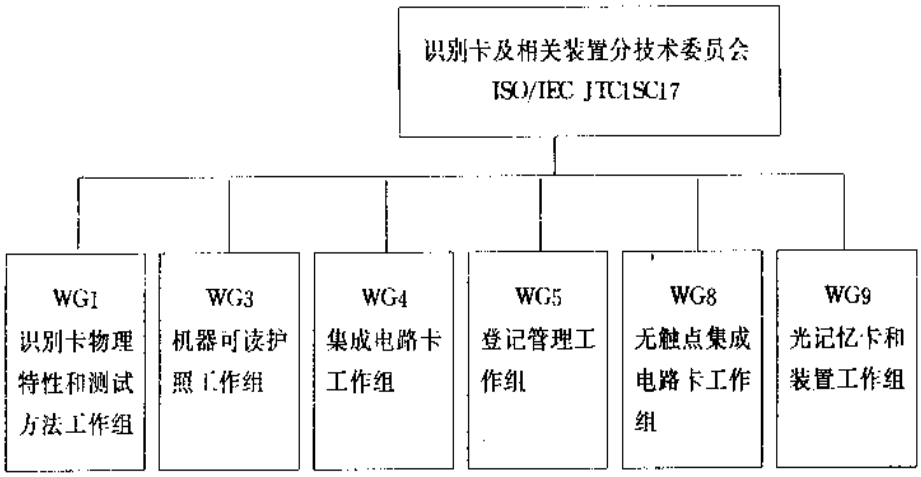


图 A.1　ISO/IEC JTC1 SC17组织结构

与 SC17 相对应的国内归口组织为“全国信息技术标准化技术委员会”，秘书处设在电子工业部标准化研究所。

(2) ISO/TC 68

银行及相关金融服务(ISO/TC 68)负责银行及相关金融服务领域的标准化工作，目前共有 41 个成员国，我国为成员之一。TC68 下设三个分技术委员会，其组织机构如图 A.2 所示。

国内与 TC68 相对应的组织为“全国金融标准化技术委员会”，秘书处设在中国人民银行支付与科技司。

TC68/SC2 的技术归口单位为中国工商银行。

TC68/SC4 的技术归口单位为中国银行。

TC68/SC6 的技术归口单位为中国工商银行。

(3) SWIFT(The Society for World Interbank Financial Telecommunication)

它是国际上各银行之间的连接中心，进行国际金融业务。SWIFT 组织通过世界各银行通用的 SWIFT 协定，提供国际金融银行间信息自动交换的有效解决方案，目前连接着全球 300 家以上的金融机构，并提供 130 种以上电脑可辨识的信息标准以支持所有金融作业的规则，且拥有 ISO 授权许可的银行认证码(Bank Identifier Codes-BISS)，是国际各

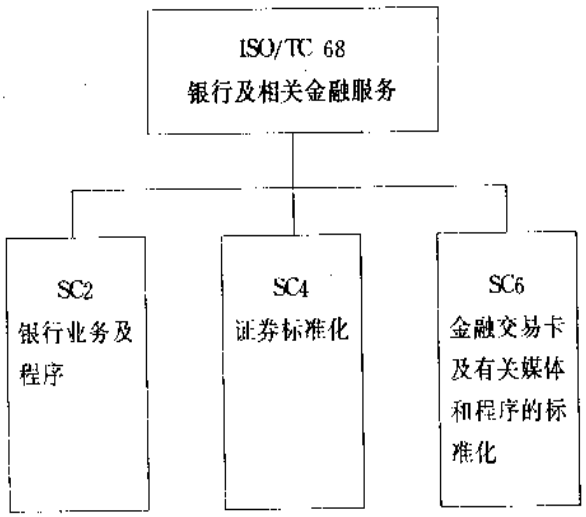


图 A.2 TC68组织机构图

金融机构在电信上认证的唯一方法。

2. 有关识别卡的标准

(1) 识别卡

ISO 7810:1985 (GB/T14916-94)

识别卡 物理特性

ISO 7811-1:1985 (GB/T15120.1-94)

识别卡 记录技术 第1部分：凸印

ISO 7811-2:1985 (GB/T15120.2-94)

识别卡 记录技术 第2部分：磁条

ISO 7811-3:1985 (GB/T15120.3-94)

识别卡 记录技术 第3部分：ID-1型卡上凸印字符的位置

ISO 7811-4:1985 (GB/T15120.4-94)

识别卡 记录技术 第4部分：只读磁道的第1磁道和第2磁道的位置

ISO 7811-5:1985 (GB/T15120.5-94)

识别卡 记录技术 第5部分：读写磁道的第3磁道的位置

ISO 7816-1:1987

识别卡 接触型集成电路卡 第1部分：物理特性

ISO 7816-2:1987

识别卡 接触型集成电路卡 第2部分：触点的尺寸和位置

ISO 7816-3:1987

识别卡 接触型集成电路卡 第3部分：电信号和传输协议

ISO 7816-4:1994 (待发布)

识别卡 接触型集成电路卡 第4部分：交换用行业间命令

ISO 7816-5:1994

识别卡 接触型集成电路卡 第5部分：应用标识符的编号系统和注册过程

ISO/IEC 7812-1:1987

识别卡　发卡方的标识　第1部分：编号体系

ISO/IEC 7812-2:1993

识别卡　发卡方的标识　第2部分：申请和登记规程

(2) 用于金融交易的识别卡

ISO 7813:1990　(SJ/Z9028-94)

识别卡　金融交易卡

ISO 4909:1987

银行卡　磁条第3磁道的数据内容

ISO 7580:1987

识别卡　卡产生的信息　金融交易的内容

ISO 8583:1987　(GB/T15150-94)

产生报文的银行卡　交换报文规范　金融交易内容

ISO 9992-1:1990

金融交易卡　集成电路卡与卡接受设备之间的信息　第1部分：概念与结构

ISO 10202-1:1991

金融交易卡　使用集成电路卡的金融交易系统的安全体系结构　第1部分：卡的生命周期

(3) 相关资料

ISO 1177:1985　(SJ/Z9081-87)

信息处理　面向起止式和同步式字符传输的字符结构

ISO 1831:1980　(SJ/Z9079-87)

光学字符识别打印规范

GB 2659-86　(ISO 3166:81)

世界各国和地区名称代码

GB 12406-90　(ISO 4217:87)

表示货币和资金的代码

GB 12053-89　(ISO 1073-1:1976)

光学识别用字母数字字符集　第一部分：OCR-A字符集　印刷图象的形状和尺寸

GB 12508-90　(ISO 1073-2:1976)

光学识别用字母数字字符集　第二部分：OCR-B字符集　印刷图象的形状和尺寸

注：GB为国家标准，SJ为行业标准。

附录 B　台湾 IC 金融卡规格(参考)

台湾内部金融机构发行的供客户使用的金融卡片称为金融卡,下面制订的是金融卡 IC 部分的规格,即 IC 卡的规格,遵循 ISO 7816 标准。

1. 电气信号及传输协议

IC 卡具有 8 个接触点,定义如下:

接触点	功能
C1	Vcc(电源)
C2	RST(复位信号)
C3	CLK(时钟)
C4	保留
C5	GND(地)
C6	Vpp(编程电压)
C7	I/O(数据输入/输出)
C8	保留

本规格采用异步半双工传输协议(T=1),符合 1991 年 6 月发布的 ISO 7816-3 Amendment. 1(草案)标准。

2. 复位应答(Answer To Reset)信号

复位应答信号的结构如图 B. 1 所示。

图中各参数的意义参见本书第 3 章 ISO/IEC 7816-3。

本规格对各参数的具体规定见表 B. 1。

表 B. 1　复位应答参数值(十六进制表示)

参　数	值	说　明
TS	3B	采用正向约定,LSB(低位)先发送
T0	FF	TA_1 TB_1 TC_1 TD_1 均存在,15 个历史字节
TA_1	11	IC 与 IFD 之间的传输速率为 9600bps
TB_1	00	Vpp 不使用
TC_1	00	传输两连续字节最小时间间隔为 12 单位
TD_1	81	TA_2、TB_2、TC_2 不传,且采用 T=1 传输协议
TD_2	71	TD_3 不传,且采用 T=1 传输协议
TA_3	40	信号字段长度为 64 字节
TB_3	42	BW1 取 4(缺省值),CWI 取 2(即 CNT=15)
TC_3	00	校验码采用 LRC,1 字节

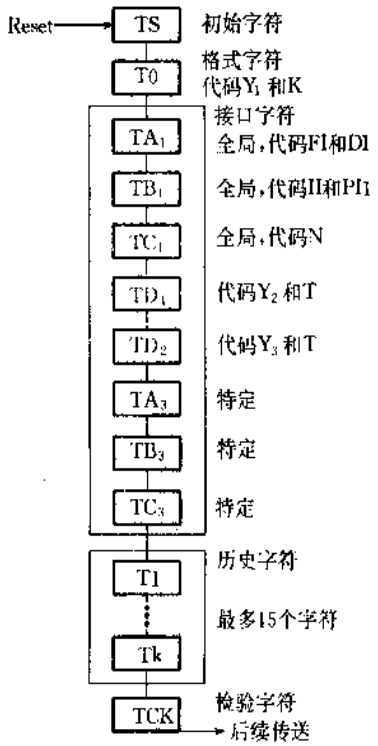


图 B.1　复位应答的结构

表中 LRC(Longitudial Redundancy Checksum)为纵向冗余校验和。

历史字符

T1：'00'，

T2：'21'，下接发卡单位授权代码

T3：'01'，金融卡识别代码

T4：'31'，下接数据文件选择代码

T5：'42'，数据文件代码，即 DIR 文件标识符＝'2F00'

T6：'52'，下接发卡单位代码(2 字节)

T7：'XX'，发卡单位代码第一字节，以十进制表示

T8：'XX'，发卡单位代码第二字节，以十进制表示

T9：'63'，下接卡片制造商代码(3 字节)

T10：'B0'(GEMPLUS)，卡片制造商编号

T11：'25'(ST16623)，卡片芯片编号

T12：'01'，卡片芯片 ROM MASK 版本编号

T13：卡片生命状态，'02'初始化，'06'个人化之前，'0E'已个人化。

T14：SW1 状态位，'90'正常，'66'异常(存储器完整性问题)。

T15：SW2 状态位，'00'正常，'40'异常(存储器完整性问题)。

检验码

TCK：表示自 T0 到 TCK 前一位的所有字节的 LRC 校验码。

3. IC 卡与 IFD(接口设备)之间的命令及应答

终端与接口设备 IFD 和 IC 卡接通时的信息流如图 B.2 所示。

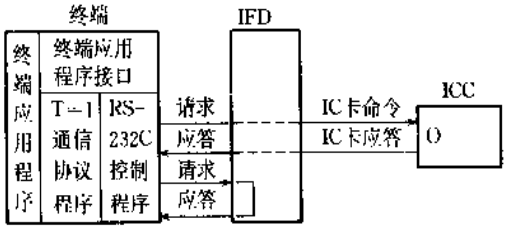


图 B.2 终端应用程序与 IFD 和 ICC 的信息流

终端可向 IFD 或 ICC 发请求命令,然后由 IFD 或 ICC 发应答信息,命令和应答的信息格式分别如图 B.3 和图 B.4 所示。

开始字段			信息 INF							结尾字段
			头				体			
NAD	PCB	LEN	CLA	INS	P1	P2	Lc	Data	Le	EDC

图 B.3 请求命令信息格式(命令 APDU)

开始字段			信息 INF			结尾字段
			体	尾		
NAD	PCB	LEN	Data	SW1	SW2	EDC

图 B.4 应答信息格式(应答 APDU)

由 NAD(Node Address)指示是发向 IFD 的命令还是发向 ICC 的命令。

信息字段内含协义控制或应用程序使用的详细数据,称为应用协议数据单元,简称 APDU。

各字段的长度及意义符合 ISO/IEC 7816-3 A.1 协议。

以下分别介绍适用于台湾金融卡的命令和应答代码。

(1) 命令(参见第四章 ISO/IEC 7816-4 交换用行业间命令),

命令名、命令头和功能说明见表 B.2。

表 B.2 行业间命令

命令名	头				功能说明
	CLA	INS	P1	P2	
Create file	00	E0	00	00	建立 DF 或 EF
Select_DF	00	A4	01	00	选择 DF
Select_EF	00	A4	02	00	选择 EF
Select_PF	00	A4	03	00	选择父文件
Lock_DF	00	76	00	00	锁定 DF

续表

命令名	头				功能说明
	CLA	INS	P1	P2	
Unlock DF	00	78	00	00	解除 DF 之锁定状态
Read_Rec	00	B2	RecN	04	读 EF 记录
Read_EF	00	B2	RecN	05	读 EF 当前记录以下的所有记录
Read Curt	00	B2	00	04	读 EF 当前记录
Read Next	00	B2	00	06	读 EF 中下一个记录
Read Prev	00	B2	00	07	读 EF 中上一个记录
Write Rec	00	D2	00	05	在指定的 EF 中加一个记录
Write Rec W TAC	00	E6	00	Kq	指定 EF、Record、Key ID 以 DES 运算法则按 ANSI×9.9 之处理流程产生 8 字节交易鉴别码 TAC(Transaction Authentication Code),将数据及交易鉴别码均写入指定位置,并输出交易鉴别码。
Update_Rec	00	D2	RecN	04	在指定 EF 内更新一个记录
Update Curt	00	D2	00	04	在指定 EF 内更新当前记录
Update_Next	00	D2	00	06	在指定 EF 内更新下一记录
Update Prev	00	D2	00	07	在指定 EF 内更新上一记录
Erase_EF	00	0E	00	00	清除指定 EF 数据
Binary_ADD	00	E8	00	04	二进制数据累加
Verify PIN	00	20	00	p_q	验证个人密码 PIN
Generate_Random	00	86	00	00	产生随机数
Terminal_Authentic	00	82	00	Kq	卡片认证终端
Unlock_Key/PIN	00	2C	00	00	解除基码(Key)或密码(PIN)基本文件的锁定状态
Card Authentic	00	88	00	Kq	终端认证卡片
Read_Binary	00	B0	00	00	读二进制
Set_Key Session	00	84	00	Kq	建立交易间的 Session Key
Update_Rec_ciphered	00	E4	01	04	用已被 Session Key 解码的数据去更新 EF 中指定记录的数据

说明:RecN 为记录号,Kq 为 Key Qualified 的缩写,Pq 为 PIN Qualifier 的缩写。

(2) 应答代码

SQ1 SW2

90 00 正常处理

应答以下代码,命令失效。

SW1	SW2	
66	00	尚未定义的错误
	01	参数或数据不一致
	02	寻址或访问问题
	04	存储器容量问题
	08	安全问题
	10	安全状态不正确
	20	锁定位置
	40	系统数据问题(LRC,ID,……)
	80	硬件问题
67	00	长度错(Lc 或 Le 不正确)
		APDU 不正确或不接受

应答以下代码,命令不执行。

SW1	SW2	
6B	00	参数错(P1 或 P2 不正确)
6D	00	指令错(INS 不正确)
6E	00	类型错(CLA 不正确)
6F	00	尚未定义的错误

4. 文件结构

有三种文件:主文件 MF、专用文件 DF、基本文件 EF,遵循 ISO/IEC 7816-4 协议。

(1) MF:在 IC 卡中必须存在,且是唯一的。用来控制 IC 卡内所有的 DF 和 MF 所属的 EF,并管理卡片制造和卡片发行单位对卡片各阶段处理的状态。

MF 内含 MF 识别数据(FD ID,即 DF 标识符),建立 DF 权限、MF 的可使用状态等。

使用时,MF 为公用文件 CDF(Common Date File)。

(2) DF:DF 文件的数量与存储器容量有关,最多可达 16 个,存储的是该 DF 所属 EF 的相关管理资料,用来控制管理 EF。

DF 内含该 DF 的识别资料(DF 标识符:DF ID 或 DF 名:DF NAME)及该 DF 的存取权限控制信息。

DF 可作为应用数据文件 ADF(Application Data File),使用时经 Select File 命令方可进入,进入 DF 后,只能在该 DF 下作业,当需转至 MF 或其他 DF 时,需再用 Select File 命令。

(3) EF:EF 的文件数量最多可以有 253 个,以记录形式存放内容,每一 EF 下最多可有 253 个记录,每一记录最多可以有 240 字节,在 DF 下使用 Select File 命令选定 EF。采用线性变长结构。

EF 按其所存内容分成以下几类:

① 应用数据基本文件(Data EF)

② 交易记录数据基本文件(Transaction EF),记录采用线性固定长方式。

③ 使用者密码数据/乱码基码数据基本文件(Secrets EF)。

按其使用分为两类：

- 由卡片认证其处理结果的基本文件(Active Secrets EF)。
- 供外界认证其处理结果或用以产生交易验证码的基本文件(Neutral Secrets EF)。

④ 特殊数值基本文件(Special Value EF)：仅有一个记录，字长固定为3字节。

注意：本规格未经证实，仅供参考。

附录 C　T=0 的 APDU 传输

（资料来源：国际标准草案 ISO/IEC 7816-4 的附录 A）

C.1　情形 1

通过将值'00'赋于 P3 将命令 APDU 映射到 T=0 TPDU。

命令 APDU (C-APDU)	CLA　INS　P1　P2	
命令 TPDU (C-TPDU)	CLA　INS　P1　P2	P3='00'

应答 TPDU 无需任何改变即映射到应答 APDU。

应答 TPDU (R-TPDU)	SW1　SW2
应答 APDU (R-APDU)	SW1　SW2

C.2　情形 2　短型 (2S)

在这种情形下，Le 的值从 1 到 256，并在字节 B_1（B_1='00'表示最大，即 Le=256）中编码。

命令 APDU 无需任何改变即映射到 T=0 的 TPDU。

C-APDU	CLA　INS　P1　P2	Le=B_1
C-TPDU	CLA　INS　P1　P2	P3=B_1

应答 TPDU 根据 Le 的接收和命令的处理而映射到应答 APDU。

情形 2S.1-Le 被接受

应答 TPDU 无需任何改变即映射到应答 APDU。

R-TPDU	Le 字节	SW1　SW2
R-APDU	Le 字节	SW1　SW2

情形 2S.2-Le 不被接受

如果长度出错，Le 不会被卡接受，卡将不支持提供数据的服务。

来自卡的应答 TPDU 指出由于长度错误：(SW1)='67'，卡拒绝了该命令。应答 TPDU 无需任何改变映射到 APDU

R-TPDU	SW1='67'　SW2
R-APDU	SW1='67'　SW2

情形 2S.3-Le 不被接受，La 被指示

Le 不被卡所接受，并且卡指出可用长度 La。

来自卡的应答 TPDU 指出由于长度错误，命令被拒绝，并指出正确的长度为 La；

(SW1)='6c',SW2 编码 La。

如果接口设备的传输系统不支持重发相同命令的服务,则无需任何改变可将应答 TPDU 映射到应答 APDU。

R-TPDU	SW1='6c'	SW2=La
R-APDU	SW1='6c'	SW2=La

如果接口设备中的传输系统支持重发相同命令的服务,它应当重发已将 La 值赋给参数 P3 的相同命令 TPDU。

C-TPDU	CLA INS P1 P2	P3=SW2

应答 TPDU 由 La 个字节及后接的两个状态字节来构成。

如果 La 小于或等于 Le,则应答 TPDU 无需任何改变即映射到应答 APDU。

R-TPDU	La 个字节	SW1 SW2
R-APDU	La 个字节	SW1 SW2

如果 La 大于 Le,则应答 TPDU 仅保留开始的 Le 个字节和状态字节 SW1、SW2 映射到应答 APDU。

R-TPDU	La 个字节	SW1 SW2
R-APDU	Le(<La)字节	SW1 SW2

C.3 情形 3 短型 (3S)

在这种情形下,Lc 的值在 1 到 255 之间,并在字节 B_1(≠'00')中被编码。

命令 APDU 无需任何改变即映射到 T=0 的 TPDU。

C-APDU	CLA INS P1 P2	Lc=B_1	Lc 个字节
C-TPDU	CLA INS P1 P2	P3=B_1	Lc 个字节

应答 TPDU 无需任何改变即映射到应答 APDU

R-TPDU	SW1 SW2
R-APDU	SW1 SW2

C.4 情形 4 短型 (4S)

在这种情形下,Lc 值在 1 到 255 之间并且在 B_1 中编码。Le 值在 1 到 256 之间且在 B_L 中编码(B_L='00'意为最大数,即 Le=256)。

命令 APDU 通过切掉最后一个字节的方法映射到 T=0 TPDU。

C-APDU	CLA INS P1 P2	B_1=Lc	Lc 个字节	B_L
C-TPDU	CLA INS P1 P2	B_1	Lc 个字节	

情形 4S.1——命令不被接受

由卡发出的第1个应答TPDU指出卡拒绝了该命令：SW1='6×'，除了'61'。

应答TPDU无需任何改变即映射到APDU。

R-TPDU	SW1='6×'	SW2
R-APDU	SW1='6×'	SW2

情形4S.2——命令被接受

由卡发生的第1个应答TPDU指明卡已完成了命令：SW1—SW2='9000'。

接口设备的传输系统通过把Le值赋给参数P3把GET RESPONSE命令TPDU发给卡。

C-TPDU	CLA	INS=GET RESPONSE	P1	P2	P3=B_1

取决于发自卡的第2个应答TPDU，接口设备中的传输系统应当如同上面2S.1，2S.2和S2.3所描述的那样作出反应。

情形4S.3——命令被接受，有附加信息

来自卡的第1个应答TPDU指明卡已完成命令处理，并给出可用数据字节长度的信息：SW1='61'，SW2编码Lx。

接口设备中的传输系统应通过把Lx和Le的最小值赋给参数P3把GET RESPONSE命令TPDU发给卡。

C-TPDU	CLA	INS=GET RESPONSE	P1	P2	P3=min(Le,Lx)

第2个应答TPDU无需任何改变即映射到应答APDU。

R-TPDU	P3个字节	SW1 SW2
R-APDU	P3个字节	SW1 SW2

C.5 情形2 扩展型(2E)

在这种情形下，Le的值由1到65536，并编码成3字节：(B_1)='00'，(B_2 ‖ B_3)=任意值(B_2和B_3值为'0000'意思为最大，即Le=65536)。

C-APDU	CLA INS P1 P2	B_1='00'	B_2B_3=Lc	

情形2E.1——Le≤256，B_1='00'，B_2B_3从'0001'到'0100'。

命令APDU通过将B_3的值赋给参数P3映射到命令TPDU。传输系统的处理应根据情形2S来进行。

C-TPDU	CLA INS P1 P2	P3=B_3		

情形2E.2——Le>256，B_1='00'，B_2B_3='0000'或从'0101'到'FFFF'

命令APDU通过将值'00'赋给参数P3映射到命令TPDU。

C-TPDU	CLA INS P1 P2	P3='00'		

a) 如果来自卡的第1个应答TPDU指示由于长度错误(SW1='67')卡拒绝了该命令，那么这个应答TPDU无需任何改变即映射到应答APDU。

R-TPDU	SW1='67'	SW2
R-APDU	SW1='67'	SW2

b) 如果来自卡的第 1 个应答 TPDU 指出由于长度错误而拒绝该命令，并指出正确的长度是 La(SW1='6C' 及 SW2=La)，则接口设备的传输系统应象情形 2S.3 描述的那样完成处理。

c) 如果第 1 个应答 TPDU 是 256 字节的数据后接 SW1SW2='9000'，这就意味着该卡没有大于 256 字节的数据，和/或不支持 GET RESPONSE 命令。传输系统将此应答 TPDU 映射到应答 APDU 而无需任何改变。

R-TPDU	256 字节	SW1='90' SW2='00'
R-APDU	256 字节	SW1='90' SW2='00'

d) 如果来自卡的第 1 或后续应答 TPDU 的 SW1 为'61'，则 SW2 编码 Lx，它是从卡可获得的额外数据(值为'00'的 SW2 指示 256 或更多字节的数据)，传输系统应当计算 Lm=Le−(先前接收到的应答 TPDU 的长度之和)，以确定可从卡中查询的剩余的字节数。

如果 Lm=0，则传输系统应将所有接收到的应答 TPDU 的体(数据)和最后接收到的应答 APDU 的尾部(SW1,SW2)级联，形成应答 TPDU。

如果 Lm>0，则传输系统应发出参数 P3 设置为 Lx 和 Lm 的最小值的 GET RESPONSE 命令 TPDU。来自卡的相应应答 TPDU 应进行如下处理

——如果 SW1='61'，根据情形 d)。

——如果 SW1='90'，则如同上述 Lm=0 的情形。

C.6 情形 3 扩展型 (3E)

在这种情形下，Lc 值从 1 到 65535，且编码成 3 字节：$(B_1)='00'$，$(B_2 \| B_3)\neq'0000'$。

C-APDU	CLA INS P1 P2	$B_1='00'$ B_2B_3=Lc	Lc 个字节

情形 3E.1——$0<Lc<256$，$B_1='00'$，$B_2='00'$，$B_3\neq'00'$

命令 APDU 通过将 B_3 值赋于参数 P3 映射到命令 TPDU。

C-TPDU	CLA INS P1 P2	P3=B_3	Lc 个字节

在这种情形下，Lc 值从 1 到 255，为一个字节编码。

应答 TPDU 无需任何改变即映射到 APDU。

R-TPDU	SW1 SW2
R-APDU	SW1 SW2

情形 3E.2——$Lc>256$，$B_1='00'$，$B_2\neq'00'$，B_3=任意值。

如果传输系统不支持 ENVELOPE 命令，它应当返回一个出错应答 APDU，表示长度出错：SW1='67'。

R-TPDU	SW1='67' SW2

R-APDU	SW1='67'	SW2

如果传输系统支持 ENVELOPE 命令，它应将 APDU 划分为长度<256 的段，并将这些连续的段送到连续的 ENVELOPE TPDU 体中。

C-TPDU	CLA	INS=ENVELOPE	P1	P2	P3	P3 个字节

如果来自卡的第 1 个应答 TPDU 指出卡不支持 ENVELOPE 命令(SW1='6D')，该 TPDU 无需任何改变即映射到应答 APDU(注：原文为 TPDU)。

R-TPDU	SW1='6D'	SW2
R-APDU	SW1='6D'	SW2

如果来自卡的第 1 个应答 TPDU 指出卡支持 ENVELOPE 命令(SW1−SW2='9000')，传输系统将根据需要发送进一步的 ENVELOPE 命令。

R-TPDU	SW1−SW2='9000'			
C-TPDU	CLA	INS=ENVELOPE	P1	P2	P3	P3 个字节

对应于最后一个 ENVELOPE 命令的应答 TPDU 无需任何改变即映射到应答 APDU。

R-TPDU	SW1	SW2
R-APDU	SW1	SW2

C.7 情形 4 扩展型 (4E)

在此情形中，Lc 值由 1 到 65535，编码成 3 字节：(B_1)='00'，$(B_2 \| B_3)\neq$'0000'，Le 值由 1 到 65536，编码成 2 字节：$(B_{L-1} \| B_L)$=任意值(B_{L-1}和 B_L 的值为'0000'表示最大，即 Le=65536)。

C-APDU	CLA	INS	P1	P2	B_1='00'	B_2B_3=Lc	Lc 个字节	$B_{L-1}B_L$=Le

情形 4E.1——Lc<256，B_1='00'，B_2='00'，$B_3\neq$'00'

命令 APDU 通过切除最后两字节 B_{L-1}和 B_L，并将 B_3 的值赋给 P3 而映射到命令 TPDU。

C-TPDU	CLA	INS	P1	P2	P3=B_3	Lc 个字节

在这种情形下，Lc 的值由 1 到 255，为一个字节编码。

a) 如果来自卡的第 1 个应答 TPDU 中 SW1='6×'，则应答 TPDU 无需任何改变即映射到应答 APDU。

R-TPDU	SW1='6×'	SW2
R-APDU	SW1='6×'	SW2

b) 如果来自卡的第 1 个应答 TPDU 中 SW1='90'，则

如果 Le<257($B_{L-1}B_L$ 值从'0001'到'0100')，则传输系统应发出把 B_L 值赋于参数 P3 的 GET RESPONSE 命令 TPDU。传输系统的后继处理应根据上述的情形 2S.1，2S.2 和

2S.3 来处理。

如果 Le>256($B_{L-1}B_L$ 值为'0000'或大于'0100'),则传输系统应发出把值'00'赋于参数 P3 的 GET RESPONSE 命令 TPDU。传输系统的后继处理应根据上述的情形 2E.2 来进行。

c) 如果来自卡的第 1 个应答 TPDU 中 SW1='61',则传输系统应按上述情形 2E.2d)来处理。

情形 4E.2——Lc>255,B_1='00',B_2≠'00',B_3=任意值

传输系统应按上述情形 3E.2 的描述来处理,直到命令 APDU 完全送到卡为止。然后按照情形 4E.1 a)、b)和 c)的描述来处理。

附录 D　T=1 的 APDU 传输

（资料来源：国际标准草案 ISO/IEC　7816-4 的附录 B）

D.1　情形 1

命令 APDU 通过添加一个值为'00'的第 5 个字节 P3 映射到 I-分组的信息字段。

命令 APDU	CLA　INS　P1　P2	
信息字段	CLA　INS　P1　P2	P3='00'

在应答中接收到的 I-分组信息字段无需任何改变即映射到应答 APDU。

信息字段	SW1　SW2
应答 APDU	SW1　SW2

D.2　情形 2(短型和扩展型)

命令 APDU 无需任何改变即映射到 I-分组的信息字段。

C-APDU	CLA　INS　P1　P2	Lc 字段
信息字段	CLA　INS　P1　P2	Lc 字段

应答 APDU 构成如下：

…在应答中接收的 I-分组信息字段，

——或在应答中接收的连续 I-分组信息字段的级联，这些分组应当是链接在一起的。

信息字段	数据字段	SW1—SW2
或信息字段的级联	数据　…　…	
	…　…　…	
	…　字段	SW1-SW2
R-APDU	数据字段	SW1-SW2

D.3　情形 3(短型和扩展型)

命令 APDU 无需任何改变即映射到

——一个 I-分组的信息字段，

——或成链的连续 I-分组信息字段的级联。

C-APDU	CLA　INS　P1　P2	Lc 字段	数据字段
信息字段	CLA　INS　P1　P2	Lc 字段	数据字段
或信息字段的级联	CLA　INS　P1　P2	Lc 字段	数据…
	…　…　…		

… … 字段

在应答中接收的 I-分组信息字段无需任何改变即映射到应答 APDU。

信息字段	SW1 SW2
R-APDU	SW1 SW2

D.4 情形 4a(短型和扩展型)

如果 Le 字段不是全'0',则命令 APDU 无需任何改变即映射到

——一个 I-分组的信息字段

——或成链的连续 I-分组信息字段的级联。

C-APDU	CLA INS P1 P2	Lc 字段	数据字段	Le 字段
信息字段	CLA INS P1 P2	Lc 字段	数据字段	Le 字段
或信息字段的级联	CLA INS P1 P2	Lc 字段	数据…	
	… … …			
	… 字段		Le 字段	

应答 APDU 构成如下:

——在应答中接收的 I-分组信息字段,

——或在应答中接收的连续 I-分组信息字段的级联。这些分组应当是链接在一起的。

信息字段	数据字段	SW1—SW2
或信息字段的级联	数据 … …	
	… … …	
	…字段 …	SW1—SW2
R-APDU	数据字段	SW1—SW2

D.5 情形 4b(短型和扩展型)

如果 Le 字段是全'0',则没有 Le 字段的命令 APDU 映射到

——一个 I-分组的信息字段

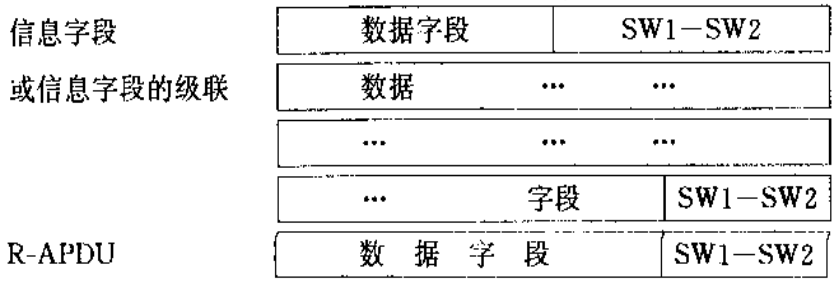
——或成链的连续 I-分组信息字段的级联。

C-APDU	CLA INS P1 P2	Lc 字段	数据字段	Le 字段
信息字段	CLA INS P1 P2	Lc 字段	数据字段	
或信息字段的级联	CLA INS P1 P2	Lc 字段	数据…	
	… … …			
	… … 字段			

应答 APDU 构成如下:

——在应答中接收的 I-分组的信息字段，

——或在应答中接收的连续 I-分组信息字段的级联，这些分组应当是链接在一起的。



D.6 链接规则

IFSC 为“卡的信息字段长度”Information Field Size for the Card 的缩写。见 ISO/IEC7816-3Amendment 1。

发送到卡且 M 位设置为 1 的 I-分组的信息字段所包含的字节数应等于 IFSC。

附录 E　RSA 密码算法的实现

RSA 密码系统为每个用户分配两对密钥，即(e,n)和(d,n)，其中(e,n)用于加密报文，(d,n)用来解密报文。

设 m 为明文，c 为密文，则下列两式成立：

$$c=m^e \mod n \quad \text{(加密运算)} \tag{1}$$

$$m=c^d \mod n \quad \text{(解密运算)} \tag{2}$$

式中 n,e 为公开密钥，d 为秘密密钥。

公开密钥 n 是两个大素数 p 和 q 的乘积，对一个安全性较高的保密系统来讲，n 的长度经常在 500 位以上，例如 512 位。

$$n=p \cdot q \tag{3}$$

e 和 d 满足关系式：

$$e \cdot d \equiv 1 \mod \phi(n) \tag{4}$$

式中

$$\phi(n)=(p-1) \cdot (q-1) \tag{5}$$

d 是和 $\phi(n)$互素的任意数(如果两个整数的公约数为 1，那么这两个整数被称为互素)。

以上这些公式在第 5 章都已进行论述，为便于下面讨论，在此扼要重述。

使用 RSA 算法将明文 m 加密成密文 c，然后又要将密文 c 解密还原成明文，由于加密算法和解密算法的公式是相同的，加密密钥和解密密钥可以互换，因此只要说明一个过程就可以了。

实现 RSA 算法需要解决两个问题

1. 如何确定 n、d、e 三个密钥。

2. 如何实现公式(1)的加密算法或公式(2)的解密算法。由于其中涉及大数的指数运算及模运算，计算量很大，因此这是实现 RSA 算法的关键。

下面分别对这两个问题进行讨论。

1. 确定 n、d 和 e 密钥

(1) 产生素数的方法

根据修改的欧拉定理，如 p 为素数，则对于 X 的所有整数值，应满足：

$$X^{p-1} \equiv 1 \mod p \tag{6}$$

这是一个必要条件而非充分条件，不过，如果有 5 个以上的 X 值能满足公式(6)，则 p 基本上可断定为素数。图 E.1 是产生素数的流程图。该流程图表示，如果 X 从 1—5 之间变化时，均能满足公式(6)，则 p 即为素数，否则将 p+1，重复计算，直到获得素数为止。

用上述方法，可得到公式(3)中的 p 和 q。其乘积即为 n。

(2) 产生秘密密钥 d

d 是与 $\phi(n)$互素的任意数，因此可以先任选一数 d，检查它是否与 $\phi(n)$互素，若不是，则执行 d=d+1，再次检查，直到与 $\phi(n)$互素为止。

检查两数是否互素的方法：

检查两数的公约数 gcd 是否为 1，若是，则两数互素。根据欧几里德算法，如果

a=bn+c，则 a 和 b 的 gcd 等于 b 和 c 的 gcd，即 gcd(a,b)=gcd(b,c)，因此 gcd(a,b)可用每次运算的余数去除该次运算的除数来计算，这样可逐渐减小参加运算的操作数的数值，最后的非零余数即为公约数。

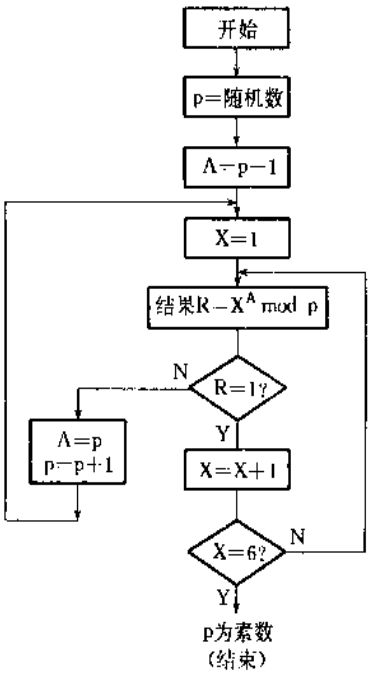


图 E.1 产生素数的流程图

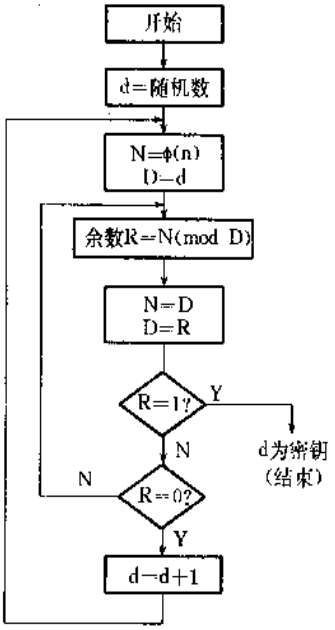


图 E.2 产生密钥 d 的流程图

例 1，计算 gcd(40,28)

第一次运算：40=28×1+12，即 40/28 的余数为 12；

第二次运算：28=12×2+4，即 28/12 的余数为 4；

第三次运算：12=4×3+0，即 12/4 的余数为 0。

因此 40 和 28 的公约数 gcd(40,28)=4。

例 2，计算 gcd(40,31)

第一次运算：40=31×1+9，即 40/31 的余数为 9；

第二次运算：31=9×3+4，即 31/9 的余数为 4；

第三次运算：9=4×2+1，即 9/4 的余数为 1。

因此 gcd(40,31)=1，40 与 31 互素。

上述算法即使对很大的整数，也只需要不多的步骤即可得结果。

图 E.2 为产生密钥 d 的流程图。

(3) 产生公开密钥 e

用欧几里德算法的一种变型产生公开密钥 e。

设：φ(n)=X(0)， d=X(1)， φ(n)和 d 是互素的数；

X(i+1)=X(i-1)/X(i)的余数；

q(i)=X(i-1)/X(i)的商(取整数)；

e(0)=0， e(1)=1。

则：e(i+1)=e(i−1)+q(i)·e(i)

递归计算，直到 X(i)=1，e(i)的值即为密钥 e。

例：设 $\phi(n)=2668$， d=157，通过计算作出表 E.1。

表 E.1 计算密钥 e

i	x(i)	q(i)	e(i)
0	2668		0
1	157	16	1
2	156	1	16
3	1	156	17

在本例中，密钥 e=17。

2. 加密/解密算法的实现

在 n、d 和 e 已确定的情况下，完成公式(1)和公式(2)的运算。

RSA 加密算法主要是进行以大整数 n 为模的大指数运算，即 $m^e \bmod n$，这一运算超出了传统智能卡 CPU 的计算能力，或者说在传统的智能卡 CPU 上计算所需的时间将使持卡人不能容忍。然而由于公钥体制的优越性，在智能卡中采用 RSA 加密算法是一种趋势。下面先介绍模数乘法运算的特点，然后介绍 RSA 算法的实现方法。

模数乘法运算的主要特点是在计算过程中，可随时去掉该模数的整数倍，而结果仍是正确的。

如要计算 $X \cdot Y = 7563 \times 278 \mod 8957$

计算时乘数 278 按位(从左到右)与被乘数 X 相乘，并随时去掉模数的整数倍，操作过程如表 E.2 所示。

表 E.2 模数乘法举例

计 算	模运算结果
7563×2−15126	6169
7563×7+6169×10=114631	7147
7563×8+7147×10=131974	6576

$X \cdot Y \equiv 6576 \bmod 8957$

表中每一步操作可用公式 $B=X \cdot y_i+A$ 表示，其中 i=2、1、0，即 $y_2=2$，$y_1=7$，$y_0=8$。

上述模数乘法运算可减小运算过程中的中间结果数值，从而减小运算数据的长度，因此可提高运算速度，并减少中间数据的存储量。

在本书的 5.4.3 节中已介绍过一种大指数模 n 运算的简单算法，可将繁重的指数计算简化为多次乘法模 n 运算，在这里不再重复，因此只要讲清楚乘法模 n 运算也就解决了大指数模 n 运算问题。

在现有的智能卡中的 CPU，受 ISO 标准所规定的芯片尺寸的限制，数据字的宽度一般为 8 位，执行两大数的乘法运算要通过很多次 8 位乘法运算才能完成，因此在智能卡的

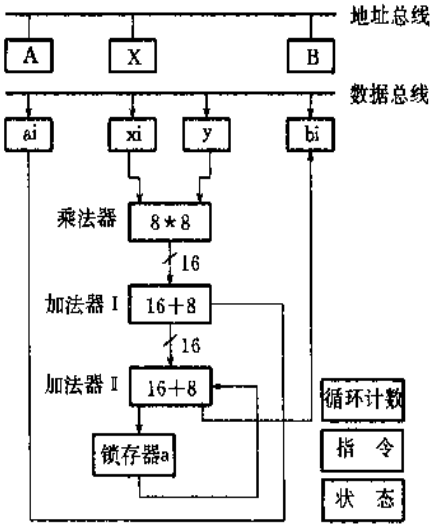


图 E.3 乘加运算逻辑单元

CPU 中实现 RSA 算法比较困难，解决问题的办法之一是采用协处理器。图 E.3 表示用 8 位乘法器(8 位×8 位)实现大数乘法运算的逻辑图。由于公式$(b-1)^2+2(b-1)<b^2$成立，因此把 2 个 8 位数加到 16 位乘积上仍然是一个 16 位数。公式可解释如下：式中$(b-1)$表示一个 8 位数，其最大值为 255，$(b-1)^2$是两个 8 位数的 16 位乘积，其最大值为255^2，由于$(b-1)^2+2(b-1)=(b^2-2b+1)+(2b-2)=b^2-1<b^2$，即$b^2-1$的最大值$=256^2-1=4096-1$，仍为 16 位二进制数。图 E.3 利用了这种特性。该图将 y 看作一个 8 位常数，而 X 由若干个字节组成，设 X 为 32 位，则由$x_3x_2x_1x_0$4 个字节组成。利用 8 * 8 乘法器需要进行 4 次乘加运算才能得到最后结果，其运算步骤如图 E.4 所示。

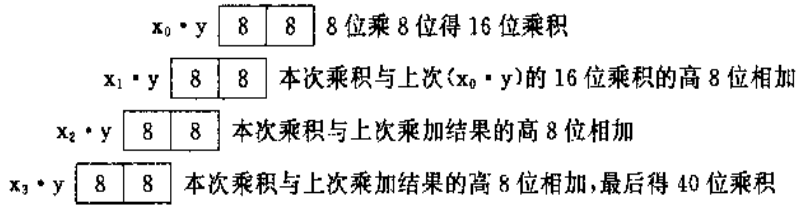


图 E.4 X·y 的运算步骤(X 为 4 字节，y 为 1 字节)

每一步执行操作$B_i \leftarrow y \cdot x_i + a$，访问 2 次存储器(读$x_i$，写$B_i$)。结果为 16 位，低 8 位为最终结果，送存储器，存储地址为B_i，高 8 位送锁存器 a，在执行下一步操作时，送到加法器进行加法运算。

如果 Y 也为 32 位，由 4 个字节$y_3y_2y_1y_0$组成，则在完成$X \cdot y_0$操作后，进行$X \cdot y_1$操作，同时还要将$X \cdot y_0$的相应位加到$X \cdot y_1$运算的中间结果中去，由于已知$X \cdot y_0$的 40 位结果已送入存储器，而且其低 8 位已是最终结果，其余 32 位，将通过存储器地址寄存器 A 逐字节选择到加法器 I 进行加法运算。这就说明了图 E.3 的乘加运算逻辑单元中有 1 个乘法器、2 个加法器。每一步操作访问 3 次存储器(读A_i和X_i，写B_i)。另一个操作数来自锁存器 a。地址寄存器 X、A 和 B 均有自动减量的功能，执行一次存/取数操作这些地址

会自动更新，变化的量正好满足运算的要求，也就是说要设计好数据在存储器中存放的规则，使得每次从存储器中取出来的数正好就是所需要的数。此外在该单元还有循环计数器、指令及状态寄存器，其初始值在指令开始执行时由 CPU 设置。

图 E.3 的逻辑图比较简单，但硬件使用效率不高，由于上述的运算很有规律，所以可考虑设计成流水线乘加部件，有关内容已超出本书范围，不再讨论。

大数模 n 运算可考虑在智能卡的 CPU 中，通过移位和减法相结合的除法运算予以实现。

上述方案是假设智能卡的 CPU 采用通用微控制器的核心部分，乘加部件用协处理器方式工作。如新设计智能卡芯片，可考虑在 CPU 内设置乘加功能模块。

附录 F　智能卡的设计、制造、个人化和发行

智能卡从设计到发行，一般可将它归纳成 6 个步骤，如图 F.1 所示。

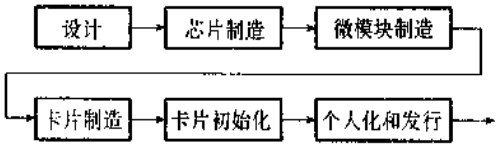


图 F.1　智能卡制作过程(从设计到发行)

今将每一步骤介绍如下：

一、设计

1. 系统设计　根据用户对卡的应用与安全要求设计卡内芯片，确定其功能与指标，并根据工艺水平与成本对卡内 CPU 的性能和存储器容量等提出具体要求，同时也对片内操作系统提出具体要求。然后就可进行具体设计。

2. 卡内集成电路设计

其设计过程与 ASIC(专用系统集成电路)设计过程相类似，包括逻辑设计、逻辑模拟、电路设计、电路模拟、版图设计与正确性验证等步骤，借助于计算机辅助设计工具(如 Workview、Mentor、Cadence 等)，争取在设计阶段发现逻辑错误、电路错误或版图错误。

目前卡内集成电路一般包括 CPU、ROM、RAM、EEPROM 和安全逻辑等内容，在国外，卡内 CPU 经常采用微控制器 MCU 核心(如 MC68HC05)，不必重新设计。在国内，则缺乏现成的设计资料和工艺条件，因而实现起来难度较大。

3. 软件设计

包括安装在芯片内部 ROM 中的操作系统(COS)和应用软件的设计。如采用国外现成的芯片，则有相应的开发工具可供选用。有关 COS 内容请参阅第六章。

智能卡中某些针对特定应用的应用程序可不进入掩膜 ROM，而进入 EEPROM 中。

常用的开发工具称为仿真器，它包含着与卡内芯片类似的硬件结构，如 CPU 和存储器等。仿真器通常与微机相连，开发者在微机上利用仿真器与微机之间的通信软件，进行编程、测试和修改，直到编出符合要求的软件为止。并将软件的代码提供给芯片制造部门用于产生 ROM 的掩膜，或作为 EEPROM 中的部分内容。

二、芯片制造

1. CMOS 工艺过程简介

今以 CMOS 反相器为例简单介绍其工艺过程。图 F.2 是 CMOS 反相器电路，其中反相管 T_1 为 N 型 MOS 管，负载管 T_2 为 P 型 MOS 管，T_1 和 T_2 的栅极 G 连接在一起作为反相器的输入端 V_{in}，两管的漏极 D 连接在一起作为反相器的输出端 V_{out}。N 管的衬底接地，P 管的衬底接电源 V_{DD}。当输入为高电平时，T_1 管导通，T_2 管截止，V_{out} 为低电平(接近地)；当输入为低电平时，T_1 管截止，T_2 管导通，V_{out} 为高电平(接近 V_{DD})。由于两管是交替导通的，所以电流小，反相器功耗小。

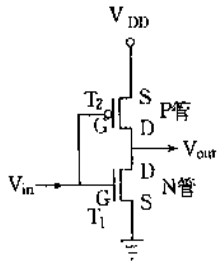


图 F.2　CMOS 反相器线路图

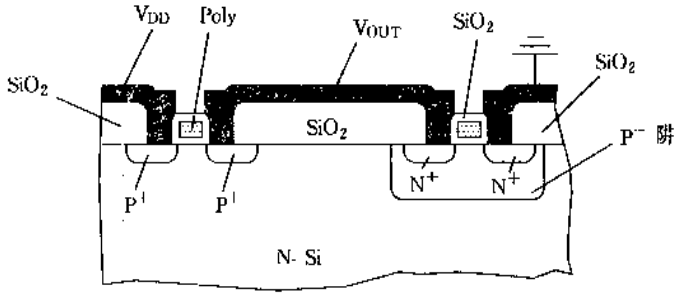


图 F.3　CMOS 反相器剖面图

图 F.3 是CMOS 反相器剖面图，图 F.4 是制作 CMOS 反相器的工艺流程图。解释如下：

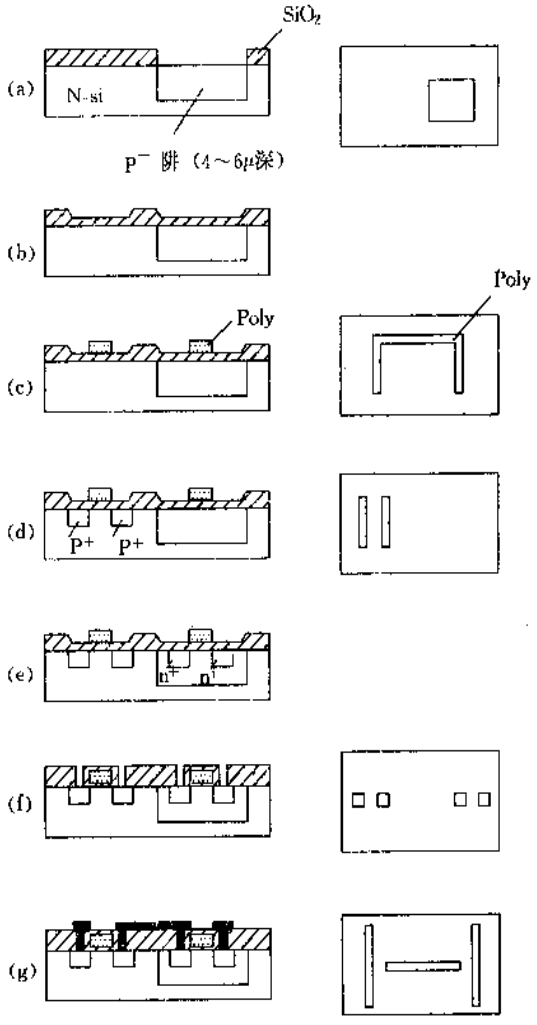
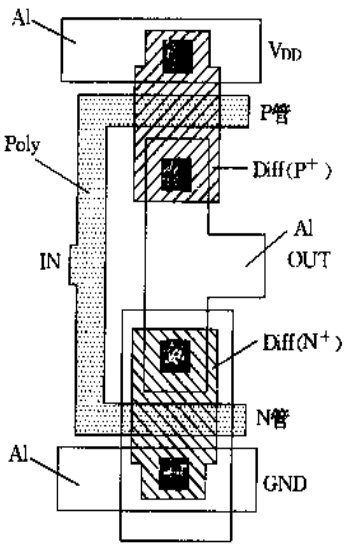


图 F.4　CMOS 反相器工艺过程(右部为顶视图)

先将含 N 型杂质(五价元素，如磷等)的硅基片(称 N-S_i 衬底)暴露在氧气气体中加热，使硅片表面上生长一层 S_iO_2 绝缘层，经光刻工艺，将一定区域的 S_iO_2 刻除，形成一个

窗口，然后在高温条件下把硅片暴露在含有三价元素（如硼）的P型杂质的气体中，硼就从窗口向硅体内扩散，由于P型杂质只能进入未覆盖S_iO_2的硅区域，从而使窗口下的区域由N型转为P^-（P型杂质浓度较低时记作P^-）型，形成P^-阱（图F.4(a)），CMOS反相管就是制作在P^-阱中的。接着把硅片表面的S_iO_2去掉，再在硅表面上形成如图F.4(b)所示的氧化层。然后在硅表面上生长上一层多晶硅（简称Poly），再用光刻工艺去掉大部分多晶硅，剩下如图F.4(c)所示多晶硅条，它们是相连的P管和N管的栅极。接着经光刻和扩散工艺形成P型杂质浓度较大的P^+区（图F.4(d)），它们是P管的源区和漏区（通称扩散区，简称Diff），再在P^-阱中以扩散的方法形成N^-扩散区，它们是N管的源区和漏区（图(e)）。接着光刻出两管源区和漏区引线孔，最后在硅片表面蒸发一层铝作为两管漏极互连以及电源引线和输出线（图(f)、图(g)）。

图F.5是CMOS反相器的布局图，可以把它看成是CMOS反相器结构的顶视图，图中显示了CMOS反相器多物理层的几何关系。其中以斜线标出的是扩散区（两管的源、漏区），它位于下层；中间一层以小点标出的是多晶硅区（栅区）；最上层的是铝连线。铝、扩散条、多晶硅条都可用作连线。铝的电阻率低，主要用于传输较大电流的场合，如电源线。一般讲，电路内部连线都应使用铝线。但是，随着电路集成度的提高，内部互连线越来越多，为了避免铝线相交，有时还用多晶硅和扩散区作互连线，虽然多晶硅的电阻率较高，但在一些传输小电流（如栅极电流）的场合，以多晶硅作为互连线是合适的。图F.5所示反相器就是以多晶硅作为两管栅极连线的。图中涂黑方孔表示金属与扩散区的接触。



图F.5 CMOS反相器的布局图

2. IC卡芯片制作过程

(1)制作圆片(Wafer)

单晶硅圆柱（直径75mm—150mm）切割成圆片，圆片厚度约为0.5mm，表面磨光，不得有任何缺陷。

(2)制作圆片上的电路

根据设计与工艺过程要求，产生多层掩膜版图（包括写入ROM代码的掩膜），对圆片进行氧化、光刻、腐蚀、扩散等处理，形成所需要的电路。在一个圆片上可制作几百—几千个相互独立的电路，每个电路即为一个小芯片（die），小片上除了有按IC卡标准（8个触点）设计的压焊块外，还应有专供测试用的探头压块。

(3)测试

利用带测试程序的计算机，控制探头测试圆片上的每个芯片，在有缺陷的芯片上作标记（涂上带色的墨水），一个芯片只需要几秒钟测试时间。

(4)研磨圆片和切割圆片

经过工艺过程的圆片可能过厚，需进行研磨，使厚度达到要求。IC卡的厚度规定为0.76mm，芯片应该更薄。

研磨后，用激光或钻石将圆片切割成众多的小芯片。

三、微模块制造

这一步是将已制造好的芯片安装在有8个触点的印刷电路板上，称作微模块。

微模块的制作有三个过程：首先制作基底(微型印刷电路板)，然后将芯片联接在基底上，最后进行团块封顶(Glob topping)。

微模块的基底是一层绝缘物质，例如聚酰亚胺或环氧树脂玻璃，在其上有连接芯片到卡表面的接触焊盘(对有触点的卡而言)。在多芯片卡中，基底上还有连接芯片的导线。基底做好后，有三种方法可以将芯片安装到基底上：细丝压焊法、磁带自动压焊法(TAB)和倒焊晶片法(Flip chip)。三种方法都有各自的设备和工艺。因卡片的传统材料PVC在潮湿的环境中会产生盐酸，其它替代材料又可能包含离子物质，对芯片产生腐蚀和污染。一种保护措施是在芯片连到基底上以后，在芯片上覆盖一层环氧树脂或其它惰性保护物质，这个过程称为"团块封顶"。

四、卡片制造

将微模块嵌入卡中。

在卡中嵌入微模块的方法有三种：

一种是层压钻孔法。通过将一层或多层的PVC(一种制卡材料)以及透明的顶层和底层封皮(这两层称为封皮层)进行辗压，形成卡片。在卡片上挖一个洞，将微模块粘进洞中。一种典型的方法是将四个不同的层迭压在一起：顶部封面层，顶部图形层，底部图形层，底部封面层。封面层是透明的，保护图形层，图形层上印刷卡的正、反面的设计图案。为微模块开的洞孔从卡的一边一直开到卡厚度的大部分(不挖透)，粘贴微模块后进行密封，只露出八个触点在卡的外表面。这种方法只适合有触点的卡。

另一种方法是将微模块嵌入压平的各层的夹层中。这种方法适合安装更大、更复杂的微模块。通常，卡片也由四层组成：两个封皮层和两个图形层。在顶层图形层和底层图形层之间夹着微模块，为了微模块不受挤压，要求图形层(PVC层)靠近微模块的一面有一凹孔，以便将微模块嵌入图形层。然后将这些层压平，形成卡片。对于有触点的卡，触点位置应有孔通到卡外。

第三种嵌入方法叫做注入成形法。这种方法是针对塑料卡制定的工艺，主要包括三个过程：注塑、粘贴和印刷。将塑料颗粒加热至熔化，注入一高温高压模具中(约300℃和2000lb/in^2)，冷却后形成的白卡有一孔。然后将微模块粘贴进这个孔中，并对芯片进行检测和编码。最后对卡片进行印刷。Gemplus公司制造有触点的卡时使用这种方法。注入成形法机器设备的制造商，位于瑞士的Wetstal正在研制一种新的工艺，可以使生产智能卡在一步内完成。这种技术将微模块直接放入模具中，再注塑，这样微模块就直接嵌入卡中了。这种方法存在一个很大的问题就是注入温度以及它对芯片的影响。

五、卡片的"激活"

将芯片的制造厂标识号、密钥等信息写入EEPROM中，经测试合格后，烧断熔丝。使IC卡从测试方式转入用户方式。为安全起见，决不允许从用户方式再回到测试方式。此时卡可发给发行者。

由于智能卡没有足够的引出端可连到内部电路，为便于测试，可增加一些连接线，而

烧断熔丝后，这些连接线不再起作用，因此内部一些保密信息和工作状态不能在外部测到，保证了安全。

六、个人化和发行

智能卡通过以上步骤制造好以后，制造商通过保密渠道将成批的卡片发给发行者（银行、邮局、医院等单位）。发行者通过读写器对卡进行个人化处理，使每张卡成为唯一能识别的卡，发行给最终的客户。

个人化工作大体包括二个方面：EEPROM 分区，写入个人信息，设定个人密码。IC 卡由制造商生产出来后，其应用存储空间（给用户用的而非卡本身使用的空间，通常在 EEPROM 中）是一片空白，只是在某些特定位置（如整个存储区的开头写入制造商的标识号码）有信息。卡到了发行商手里，发行商就要对卡的存储区进行分区。规定这个区派什么作用场，那个区作什么用。

发行商还将识别卡的一些信息写入卡内。例如标识发行者的号码、用户帐号、用户姓名、金额等等。为保护持卡人而设定的个人密码，或称 PIN（个人识别号码）也在发行时由用户输入，并存储在一块以后连发行商都无法读取的空间内，这通常是由芯片内的安全逻辑予以保证的。

完成了这些过程的卡就成为一张独立的、能唯一标识用户的卡（通过制造商标识，发行商标识，发行号或帐号就可唯一标识一张卡）。经过个人化的卡就可由发行者交给用户，用户以后就可凭卡消费了。

附录G　英文缩写词

ACK　ACKnowledge　确认
ADF　Application Data File　应用数据文件
AID　Application IDentifier　应用标识符
APDU　Application Protocol Data Unit　应用协议数据单元
APPZ　Application Zone　应用区
ASN.1　Abstract Syntax Notation one　抽象语法符号表示法1
ATM　Automatic Teller Machine　自动柜员机
ATR　Answer To Reset　复位应答

BER　Basic Encoding Rules of ASN.1　ASN.1的基本编码规则(参见ASN.1)
BGT　Block Guard Time　分组保护时间
BWI　Block Waiting time Integer　分组等待时间整数
BWT　Block Waiting Time　分组等待时间

CLA　CLAss byte　类型字节
COS　Chip Operating System　片内操作系统
CRC　Cyclic Redundancy Check　循环冗余校验
CWI　Character Waiting time Integer　字符等待时间整数
CWT　Character Waiting Time　字符等待时间

D　Data　数据
DAD　Destination node ADdress　目的结点地址
DES　Data Eneryption Standard　数据加密标准(一种加密/解密算法)
DF　Dedicated File　专用文件
DIR　DIRectory　目录
DIS　Draft International Standard　国际标准草案
DSA　Decimal Shift and ADD　十进制移位和加法(一种加密/解密算法)

EC　Erase Counter　擦除计数
EDC　Error Detection Code　差错检验码
EEPROM　E²PROM　Electrically-Erasible Programable Read-Only Memory　电可擦可编程只读存储器
EF　Elementary File　基本文件
EFT-POS　Electronic Funds Transfer at Point Of Sale　销售点电子货币转帐
EPROM　Erasible programable Read-Only Memory　可擦可编程只读存储器
EZ　Erase key Zone　擦除密码区

FAT　File Allocation Table　文件分配表

FCI File Control Information 文件控制信息
FCP File Control Parameter 文件控制参数
FMD File Management Data 文件管理数据
FTC Financial Transaction Card 金融交易卡、金融卡
FZ Fabrication Zone 制造代号区

GSM Global Special Mobile 全球专用移动电话

HCMOS High-performance Complementary Metal-Oxide-Silicon 高性能互补金属氧化硅

I-block Information block 信息分组、信息块
ICC Integrated Circuit Card、IC Card 集成电路卡
IEC International Electrotechnial Commission 国际电子技术委员会
IFD InterFace Device 接口设备、读写设备
IFS Information Field Size 信息字段大小(长度)
IFSC Information Field Size for the Card 卡的信息字段长度
IFSD Information Field Size for the interface Device 接口设备的信息字段长度
IFSI Information Field Size Integer 信息字段长度整数
IIN Issuer Identification Number 发行者标识号
INF INformation Field 信息字段
INS INStruction byte 指令字节
ISO International Standard Organization 国际标准化组织
IZ Issuer Zone 发行代码区

L Length 长度
LEN LENgth 长度
LRC Longitudinal Redundancy Check 纵向冗余校验

MCU MicroController Unit 微控制器、单片微计算机
MF Master File 主文件

NAD Node ADdress 结点地址
NVM Non-Volatile Memory 非易失性存储器

OSI Open Systems Interconnection 开放系统互连

P1-P2 Parameter byte 参数字节
PAN Primary Account 主帐号
PCB Protocol Control Byte 协议控制字节
PCOS Payment COS 支付 COS (参见 COS)
PIN Personal Identification Number 个人标识符
POS Point of Sales 销售点

PTS Protocal Type Selection 协议类型选择

RAM Random Access Memory 随机存储器
R-block Receive-block 接收分组、接收块
RFU Reserved for Future Used 保留于将来使用
ROM Read-only Memory 只读存储器
RSA Rivest、Shamir、Adleman(三人名) 一种加密/解密算法
RST ReSeT 复位、总清

SAD Source node ADdress 源结点地址
S-block Supervisory block 管理分组、管理块
SC Security Code 安全代码
SC Smart Card 智能卡
SM Secure Messaging 安全信息
SW1—SW2 Status byte 状态字节

TLV Tag、Length、Value 标志、长度、值
TPDU Transmission Protocol Data Unit 传输协议数据单元
TV Television 电视
TZ Test Zone 测试区

WTX Waiting Time eXtension 等待时间扩充

参 考 文 献

[1] International Standard ISO 7810, Identification cards, Physical characteristics, 1985

[2] International Standard ISO 7811/1, Identification cards, Recording technique, Part 1:Embossing, 1985

[3] International Standard ISO 7811/2, Identification cards, Recording technique, Part 2:Magnetic stripe, 1985

[4] International Standard ISO 7811/4, Identification cards, Recording technique, Part 4:Location of read-only magnetic tracks, Tracks 1 and 2, 1985

[5] International Standard ISO 7811/5, Identification cards, Recording technique, Part 5: Location of read-write magnetic track, Track 3, 1985

[6] International Standard ISO 7812, Identification cards, Numbering system and registration procedure for issuer identifiers, 1987

[7] International Standard ISO 7813, Identification cards, Financial transaction cards, 1987

[8] International Standard ISO 8583, Bank card originated messages, Interchange message specifications, Content for financial transactions, 1987

[9] International Standard ISO 4909, Bank cards, Magnetic stripe data content for track 3, 1987

[10] International Standard ISO 7580, Identification cards, Card originated messages, Content for financial transactions, 1987

[11] International Standard ISO 7816-1, Identification cards, Integrated circuit(s) cards with contacts, Part 1: Physical Characteristics, 1987

[12] International Standard ISO 7816-2, Identification cards, Integrated circuit(s) cards with contacts, Part 2: Dimensions and location of the contacts, 1988

[13] International Standard ISO/IEC 7816-3, Identification cards, Integrated circuit(s) cards with contacts, Part 3: Electronic signals and transmission protocols, 1989

[14] International Standard ISO/IEC 7816-3/Amd. 1, Identification cards, Integrated circuit(s) cards with contacts, Part 3:Electronic signals and transmission protocols, Amendent 1:Protocol type T=1, asynchronous half duplex block transmission protocal, 1992

[15] Draft International Standard ISO/IEC DIS 7816-4, Information technology, Identification cards, Integrated circuit(s) cards with contacts, Part 4: Interindustry commands for interchange, 1994

[16] International Standard ISO/IEC 7816-5, Identification cards, Integrated circuit(s) cards with contacts, Part 5: Numbering system and registration procedure for ap-

plication identifiers, 1994
[17] 电子工业部,国家技术监督局、中国人民银行."金卡"工程标准化指南(第一册 V1.0).电子工业部标准化研究所,1994.6
[18] Jerome Svigals. SMART CARD: The Ultimate Personal Computer, 1985
[19] 陈爱民 于康友 管海明编著.计算机的安全与保密.电子工业出版社,1992.9
[20] 卢开澄.计算机密码学:通信中的保密与安全.清华大学出版社,1990
[21] Bruce Bosworth. Codes Ciphers and Computers— An Introduction to Information Security. Hayden Book Company INC, 1982
[22] 钟林惠编译.社会生活中的信息安全问题.通信保密 1993 年第 4 期
[23] Dominigue de Waleffe & Fean-Facgues Quisguater. CORSAIR: A Smart Card for Public key, Cryptosystems. Advances in Cryptology——CRYPTO, 1990
[24] 关义章.智能卡 未来标准化的安全器件.通信保密,1993 年第 3 期
[25] M. H. Er, D. J. Wong, A. A-L. Sethu and K. S. Ngeow. Design and Implementation of an RSA Cryptosystem Using Multiple DSP Chips.《Microprocessors and Microsystems》, Vol. 15, No. 7, Sept. 1991
[26] 陆首群.为什么要建金桥工程.中国计算机用户,1995 年专刊 1
[27] 刘韵洁.中国公用数据网的发展及国家经济信息化网络的组成.中国计算机用户,1995 年专刊 1
[28] 陈 静.中国金融数据通信网建设成就与未来发展构想.中国计算机用户,1995 年专刊 1
[29] Michael Hill. The development of Semiconductor Technology Expectations For Future Smart Cards. The Smart Card Guide'95
[30] Kathleen Brown. Developing Smart Card Specific Technologies. World Card Technology, Vol. 1, Issue1, Feb/Mar 1995
[31] Atmel Corporation CMOS Integrated Circuit Data Book 1993. 1994
[32] 陈章龙编.MC6805 单片机原理、应用及技术手册.复旦大学出版社,1991 年
[33] 金井千喜编著.POS 入門,オーム社,1986