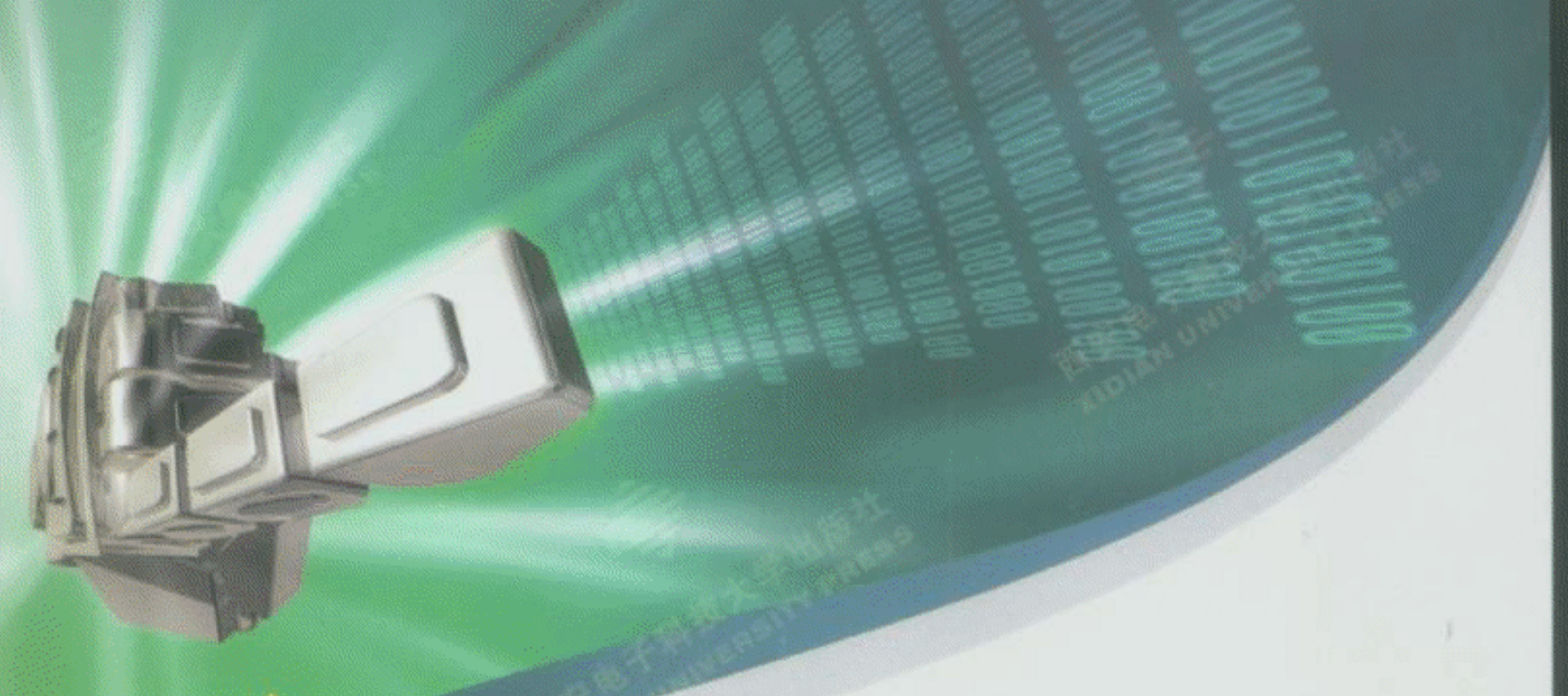


面向21世纪高级应用型人才

中国高等职业技术教育研究会推荐

高职高专系列教材

智能卡技术

刘守义 主编

毛丰江 苏全 副主编

西安电子科技大学出版社

http://www.xduph.com

□中国高等职业技术教育研究会推荐

高职高专系列教材

智 能 卡 技 术

刘守义　主　编

毛丰江　苏　全　副主编

西安电子科技大学出版社

2004

内 容 简 介

作为信息化社会的标志之一，智能卡技术已形成涉及全球众多著名电子巨头的新兴技术产业，并普及到现代经济和日常生活的各个方面。

本书从高职教育和工程应用的角度出发，面向产品，注重实际应用，通过核心实例贯穿、实训引路、逐步深入的方法，全面讲述智能卡的理论和实用技术。本书共分 5 章，内容包括智能卡概述、接触式 IC 卡技术、非接触式 IC 卡技术、智能(CPU)卡技术和智能卡应用系统。

本书面向实际应用，叙述深入浅出，可作为高职高专、成人教育计算机与电子类相关专业的教材及智能卡从业人员的参考书。

图书在版编目（CIP）数据

智能卡技术／刘守义主编. —西安：西安电子科技大学出版社，2004.8

(高职高专系列教材)

ISBN 7–5606–1425–6

Ⅰ. 智… Ⅱ. 刘… Ⅲ. 智能卡—高等学校：技术学校—教材 Ⅳ. F830.46

中国版本图书馆 CIP 数据核字（2004）第 062408 号

策　　划　马乐惠

责任编辑　王　瑛　马乐惠

出版发行　西安电子科技大学出版社（西安市太白南路 2 号）

电　　话　(029)88242885　88201467　邮　编　710071

http://www.xduph.com　E-mail: xdupfxb@pub.xaonline.com

经　　销　新华书店

印刷单位　西安交通大学印刷厂

版　　次　2004 年 8 月第 1 版　2004 年 8 月第 1 次印刷

开　　本　787 毫米×1092 毫米　1/16　印张 18.125

字　　数　424 千字

印　　数　1～4000 册

定　　价　20.00 元

ISBN 7 – 5606 – 1425 – 6／TP・0760（课）

XDUP 1696001-1

＊＊＊ 如有印装问题可调换 ＊＊＊

本社图书封面为激光防伪覆膜，谨防盗版。

前　言

“金卡工程”规划用 10 年左右的时间，在全国 400 个城市的 3 亿人口中推广应用卡基支付系统，应用范围普及银行、商业、交通、医疗、税务、身份认证及各种预收费系统。随着微软等高科技巨头的积极介入，智能卡的技术和应用正朝着更深、更广的方向发展。因此，在全国将需要一大批具有相关技术应用能力的人来从事各类卡及其配套设备和应用系统的设计、开发、制造、发行、维护和服务工作。为了适应高职院校开设相关课程的需要，结合近年来的技术发展和教学经验，我们组织编写了这本教材。

智能卡技术是一门应用性很强的专业课，要求理论与实践密切结合。本书以智能卡门禁系统作为一个核心实例贯穿始终，从第 2 章的接触式 IC 卡门禁机，到第 3 章的快递公司非接触式安全门锁控制，再到最后的智能卡门禁系统设计，随着技术的发展逐步展开，内容不断深入。

本书的一个重要特点是强调教、学、做相结合，每章均由认知性训练引出相关概念，随着理论教学的深入再进一步展开要求较高的技能实训。理论与实践环环相扣，由浅到深，不断递进。

全书共安排了 6 个实训项目和 1 个综合性的课程设计与 1 个综合性的课程训练。由于市面上尚没有专用的智能卡训练教学系统，本书设计的训练均采用实际应用系统来完成。使用者可根据自己的需求配备类似的应用系统。

本书的参考学时为 68～90 学时(含实训)，使用者可根据具体情况增减学时。本书可作为高职高专电子与计算机类智能卡技术课程的教材，也可作为智能卡系统开发、制造、使用和维护人员的培训参考书。

刘守义对本书的编写思路与大纲进行了总体策划，指导全书的编写，并对全书统稿。毛丰江和苏全协助刘守义完成上述工作，并分别编写了第 1～3 章与第 5 章，唐建东编写了第 4 章。

深圳职业技术学院冯明发副教授、深圳清华比高信息技术有限公司王连魁高级工程师审核并校对了全书，深圳明华澳汉科技股份有限公司、深圳达实智能股份有限公司也为本书的编写提供了很大的帮助，在此表示深切的感谢。

在本书编写的过程中，我们力图全面反映智能卡技术各方面的知识、理论、技术和实践经验，但由于智能卡技术发展日新月异，又在一定程度存在技术保密与知识产权保护等因素，因此一些技术尚未在教材中涉及，有待今后进一步完善。

由于编者水平有限，书中的错误和不妥之处在所难免，殷切希望专家和广大使用者对本书提出宝贵的意见和建议。

深圳职业技术学院电子应用实验室智能卡分室为本教材配备了全套实训所需的硬件设备与应用软件，使用本教材的院校如自己配备训练系统有困难，可与深圳职业技术学院电子通信工程系联系。

编　者

2004年3月

目　　录

第1章 智能卡概述

根据2003年中国IC卡(智能卡)博览会统计，2003年中国IC卡市场总出货量约在3.97亿张，销售额达到32亿元人民币。预计在2006年将会达到6.89亿张的发售量，销售额达82.7亿元人民币。

未来中国IC卡市场将出现快速增长。首先，是居民身份证市场巨大。按照国家有关部门计划，基于IC卡技术的国家第二代身份证项目已于2004年正式启动，并于2008年之前完成9.8亿张的发放量，仅卡片一项就会带来将近200亿元的市场，如果包括系统在内，市场更加惊人。IC卡市场的另一个热点则来自银行卡，即将于2005年出台的EMV标准(国际三大银行组织Europay、MasterCard和Visa共同制定的智能卡技术标准)将会使银行磁条卡逐渐被IC卡所代替。此外，手机SIM卡仍将保持增长的势头，特别是随着2005年3G(第三代数字移动通信)的启动，SIM卡将出现一个较快的增长，而公用电话卡由于手机的逐渐普及和小灵通的挤占将会呈现逐步下降的趋势。同时，社保卡由于政府的推动，参加社会保险的人数会越来越多，因而会稳步增长；交通卡则随着城市公交一卡通的实施将会出现一个大幅的增长。

本章旨在对智能卡技术的相关概念、技术要素、国际标准和应用概况加以粗略描述，以使读者建立一个总体的概念，并大致了解智能卡系统的基本组成与工作过程。

1.1 智能卡基础

自1972年法国人罗兰·莫雷诺(Roland Moreno)首先提出IC卡的设想，1976年法国布尔(Bull)公司研制出世界第一张IC卡以来，IC卡技术飞速发展，已经形成一涉及全球众多著名电子巨头的新兴技术产业。国际标准化组织(ISO，International Standardization Organization)与国际电工委员会(IEC)的联合技术委员会(JTC1)为之制定了一系列的国际标准、规范，极大地推动了IC卡的研究和发展。目前，IC卡的应用已遍布全球。据统计，仅2000年，全球就发行IC卡36亿张，2003年达63亿张。

那么，究竟什么是智能卡？

1.1.1 什么是智能卡

在当今这个信息时代，“智能卡”(Smart Card)这个词在我们的日常生活中已随处可见，然而这个词在一定意义上是模糊的，常常又被称为IC卡、聪明卡、灵巧卡、智慧卡(Intelligent Card)、微电路卡(Microcircuit Card)、微芯片卡(Microchip Card)等。国际标准化组织使用术语ICC(Integrated Circuit Card)，即“集成电路卡”来涵盖所有在一个符合ISO ID1定义的塑料卡片内封装了一个集成电路的器件，卡的外形尺寸是85.6 mm×53.98 mm×0.76 mm，与

银行所使用的磁卡相同。当然，也可封装为标签、纽扣、钥匙、饰物等特殊形状，也被称为智能(IC)卡。

在智能卡推出之前，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智能卡，也为了兼容，通常在智能卡上仍贴有磁条，为此，卡中封装集成电路芯片的位置受到磁条位置的限制。图 1.1 为 IC 卡的外观图，正面左侧的小方块中封装有集成电路芯片，其下面为签名条；最下面为凸印字符，用于压印帐单；背面上部有磁条。正面还可印刷各种文字、图案、照片等。卡的尺寸、触点位置与用途、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。

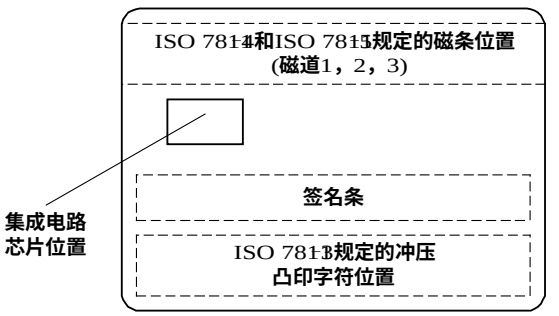


图 1.1　智能(IC)卡的外观

1.1.2　智能卡的分类

智能卡种类繁多，可以按不同形式分类。

1．按镶嵌芯片的不同分类

按卡内镶嵌芯片的不同可将智能卡分为存储器卡、逻辑加密卡和 CPU 卡三类。

1) 存储器卡

存储器卡卡内嵌入的芯片为存储器芯片，这些芯片多为通用 EEPROM(或 Flash Memory)；无安全逻辑，可对片内信息不受限制地任意存取；卡片制造中也很少采取安全保护措施；不完全符合或支持 ISO/IEC 7816 国际标准，而多采用 2 线串行通信协议(I^2C 总线协议)或 3 线串行通信协议。

存储器卡功能简单，没有(或很少有)安全保护逻辑，但价格低廉，开发使用简便，存储容量增长迅猛，因此多用于某些内部信息无需保密或不允许加密(如急救卡)的场合。

2) 逻辑加密卡

逻辑加密卡由非易失性存储器和硬件加密逻辑构成，一般均为专门为 IC 卡设计的芯片，具有安全控制逻辑，安全性能较好；同时采用 ROM、PROM、EEPROM 等存储技术；从芯片制造到交货，均采取较好的安全保护措施，如运输密码 TC(Transport Card)的取用；支持 ISO/IEC 7816 国际标准。

逻辑加密卡有一定的安全保证，多用于有一定安全要求的场合，如保险卡、加油卡、驾驶卡、借书卡、IC 卡电话、小额电子钱包等。

3) CPU 卡

CPU 卡也称智能卡、保密微控制器卡、加密微控制器卡(片内带加密协处理器)，在 IC

卡家族中出现最晚，也最具生命力。CPU 卡的硬件构成包括 CPU、存储器(含 RAM、ROM、EEPROM 等)、卡与读写终端通信的 I/O 接口及加密运算协处理器 CAU，ROM 中则存放有 COS(Chip Operation System, 片内操作系统)。

由于 CPU 卡具有很高的数据处理和计算能力以及较大的存储容量，因此应用的灵活性、适应性较强。同时，CPU 卡在硬件结构、操作系统、制作工艺上采取了多层次的安全措施，这保证了其极强的安全防伪能力。它不仅可验证卡和持卡人的合法性，而且可鉴别读写终端，已成为一卡多用及对数据安全保密性特别敏感场合的最佳选择，如金融信用卡、手机 SIM 卡等。

虽然通常将所有 IC 卡都称作智能卡，但严格地讲，只有 CPU 卡才真正具有智能特征，也即只有 CPU 卡才是真正意义上的“智能卡”。

由于工艺技术要求苛刻等因素，目前世界上仅有少数几家著名半导体芯片制造商能设计和生产 CPU 卡芯片，如美国的 Motorola、Atmel，韩国的三星，德国的 Siemens，法国的 Bull，荷兰的 Philips 等。多数卡制造商均选择这几家芯片制造商的产品，经封装并灌以自行开发的 COS，而成为拥有各自注册版权的 CPU 卡。

国内接触式 IC 卡的产品现状是流行产品多为进口产品。部分国内卡商可对进口芯片进行卡封装，甚至对 CPU 卡灌装自产 COS。上海、北京等实力较强地区则已自行研制多种 IC 卡芯片，如上海贝岭微电子公司的 BL 7432/7442 2 Kb 存储器卡/逻辑加密卡芯片、中国华大集成电路设计中心的 CIU91/92 系列 CPU 卡芯片(2～8 KB EEPROM、256 B RAM、10～12 KB ROM)及与之配套、适用于不同应用的多种 COS(适用于交通、医疗、保险、管理的 M-COS ;针对金融、预付费、电子钱包的 S-COS ;专用于组织机构信息卡的 CNOS-COS；针对中国人民银行 IC 卡规范的 B-COS 和适用于安全、灵活性要求较高领域的 Z-COS 等)。清华大学、长丰、华虹、航天金卡、华旭金卡、长城计算机集团公司等也都开展了卡用芯片及 COS 的研制开发。它标志着我国已结束了单纯依赖进口芯片、模块的状况。

2．根据卡与外界数据交换界面的不同分类

根据卡与外界数据交换界面的不同可将智能卡分为接触式 IC 卡(如图 1.2 所示)和非接触式 IC 卡(如图 1.3 所示)。接触式 IC 卡以符合 ISO/IEC 7816 标准的多个金属触点为卡芯片与外界的信息传输媒介，成本低，实施相对简便；非接触式 IC 卡则不用触点，而是借助无线收发传送信息，因此在前者难以胜任的交通运输等诸多场合有较多应用。此外，还有兼备接触式和非接触式两种接口的组合卡。

图 1.2 接触式 IC 卡外观

图 1.3　非接触式 IC 卡外观

3．根据应用领域的不同分类

根据应用领域的不同可将智能卡分为金融卡和非金融卡(即银行卡和非银行卡)。金融卡又分为信用卡和现金卡。前者用于消费支付时，可按预先设定额度透支资金，后者可用做电子钱包和电子存折，但不得透支。而非金融卡的涉及范围极广，实质上囊括了金融卡之外的所有领域，如门禁卡、组织代码卡、医疗卡、保险卡、IC 卡身份证、电子标签等。

4．根据与外界数据传输形式的不同分类

根据与外界数据传输形式的不同可将智能卡分为串行通信卡和并行通信卡。串行通信卡即为目前最常用的卡，也是目前国际标准中所规定的接口方式。由于采用串行方式与外界交换信息，卡芯片引脚较少，因此易于封装和接口。但随着芯片存储容量的增大，引发了两个问题：一是芯片面积急剧增长，给卡的封装带来困难；二是读写时间过长，读写 1 Mb 的容量需要 12 分钟。而并行通信卡由于采用并行通信，故无此二弊，但国际标准中尚无此类接口标准。深圳艾柯电子公司研制的 P 型 IC 卡的引脚数多达 32 个，不仅速度极快，而且容量增大，采用地址数据线分离，可寻址 4 Mb 空间；采用地址数据多路复用，则可达 32 Mb 寻址空间。与串行通信卡一样，它也有存储型(1 Mb、2 Mb、4 Mb、8 Mb、32 Mb 容量)、逻辑加密型(1 Mb、2 Mb 容量)和 CPU 型(1/4 Mb、1/2 Mb、1 Mb 容量)，并已在纳税申报等系统中得以应用。

1.1.3　IC 卡与磁卡的比较

磁卡自 20 世纪 60 年代末问世以来，就因其简单、价廉、使用方便而在金融、邮电等领域得以广泛运用。但由于它依靠容量有限的外露磁条存储信息，因此在保密性、抗损性、可靠性及脱机工作等方面存在诸多不足。由于美国等国已建立了基于磁卡的强大的授权通信网络，难以抛弃已有的大量设备资源，因此目前在金融领域仍主要采用磁卡。而欧洲各国(如法国、芬兰等国)的 IC 卡应用则比较普遍，技术水平也较为领先。然而，随着芯片技术的迅猛发展，IC 卡凭借其 3S(Standard、Smart、Security，即标准、智能、安全)优势将逐步替代磁卡的趋势已成为共识。

相对于磁卡，IC 卡具有以下特点：

(1) 存储容量大：可存储文字、图像、声音等各种信息。

(2) 安全性高：物理层、硬件、软件三方面均采取了相应的安全策略。

(3) 对网络要求不高：其安全性决定了可以脱机/非实时联机使用。

表 1.1 给出了 IC 卡与磁卡特性差异的对比。

表 1.1　IC 卡与磁卡的比较

性　能	IC 卡	磁　卡	
抗机械损伤	好	差	
抗电磁干扰	是磁卡的 10 倍	差	
抗静电	好	差	
抗辐射	好	差	
防潮防污	好	差	
存储容量	已达 4 Mb	小于几百字节	
数据保存期限	100 年	1～2 年	
使用寿命	10 万次	几千次	
卡的价格	较高	低	
作业模式	脱机/非实时联机	脱机	实时联机
网络要求	较低	低	高
对主机的要求	较低	低	高
系统投资	中等	低	高
卡的复制与伪造	很难	容易	
读写安全措施	读写保护、数据加密保护	无	
使用保护	个人密码、卡与读写器双向认证	个人密码	

1.1.4　智能卡应用系统的构成要素

毫无疑问，智能卡本身并不能单独或直接使用，它必须与相关设备组合，才能共同构成符合某种需求的应用系统。那么，一个完整的智能卡应用系统究竟包括哪些构成要素？可采取哪种结构模式呢？

一个标准智能卡应用系统的最基本的构件包括智能卡、智能卡接口设备(智能卡读写器)、PC 机，较大的系统还包括通信网络和主计算机等，如图 1.4 所示。

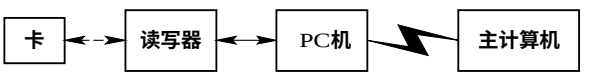


图 1.4　标准 IC 卡应用系统的最基本的构成

1) **智能卡**(ICC，IC Card)

智能卡即由持卡人掌管，记录有持卡人的特征代码、文件资料的便携式信息载体。

2) **接口设备**(IFD，InterFace Device)

接口设备即通常所说的 IC 卡读写器，是卡与 PC 机进行信息交换的桥梁，而且常常是 IC 卡的能量来源。其核心通常为工作可靠的工业控制单片机，如 Intel 的 51 系列等。IFD 与 IC 卡间遵循 ISO/IEC 国际标准的通信协议，通过自身的机械卡座或射频(RF)、红外等无线信道，以接触或非接触方式对卡读写，并通过 RS232 串行接口等以实时或非实时方式与 PC 机通信，实现卡与 PC 机间信息的上传下送。

3) PC 机

PC 机是系统的核心，完成信息汇总、统计、计算、处理、报表的生成、输出和指令的发放、系统的监控管理以及卡的发行与挂失、黑名单的建立等。

4) 网络与计算机

在金融服务等相对大的系统中，网络是使前端 PC 机与上级控制/授权/服务/管理中心，即中央电脑(主计算机)连接的必备条件。其借助通信线路、设备和完善的网络通信软件，将地理位置不同的各个子系统，有机相接为一功能完备的大系统；主计算机则是对此大系统实施监控管理的核心，是重大决策管理要素的源头。

综上所述，智能卡应用工程融微电子与芯片技术、单片机应用技术、数据库管理技术、网络技术、安全技术、射频识别技术、嵌入式操作系统以及数字印刷技术等多种高新技术于一身，是一个综合性的高新技术产业。

1.2　智能卡的用卡过程

1.2.1　智能卡的生存周期

1．智能卡的生存周期

智能卡的生存周期是指智能卡从制造到失效的过程，主要包括制造、发行、使用、回收四个阶段。

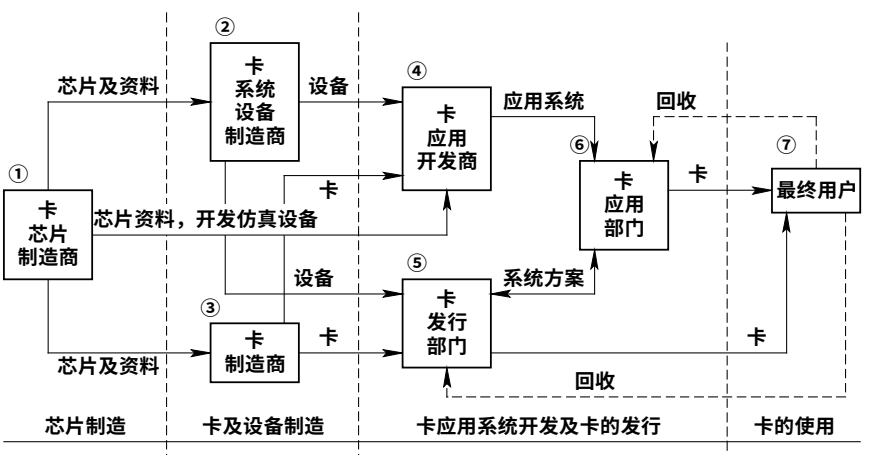
(1) 制造阶段：包括芯片、卡及设备的制造。

(2) 发行阶段：指生成相应应用目的的卡，并提供给持卡人的过程。

(3) 使用阶段：持卡人用卡及相关部门对之监督管理的过程。

(4) 回收阶段：对损坏卡、过期卡、解约卡等的回收处理过程。

对这四个阶段的进一步理解可由图 1.5 流程获悉。



注：① 卡芯片制造商；② 卡系统设备制造商；③ 卡制造商；④ 卡应用开发商；⑤ 卡发行部门；⑥ 卡应用部门；⑦ 最终用户

图 1.5　智能卡的生存周期

其中：

① 卡芯片制造商：从事 IC 卡及相关机具的芯片设计和制造，一般不参与卡、设备的制造和应用开发，如 Motorola 公司。

② 卡系统设备制造商：主要从事卡的封装、测试、印刷等设备及应用开发设备的设计制造。

③ 卡制造商：从事卡的封装、测试、印刷及应用开发设备的设计制造，应用系统工程的承包，如法国 Bull 公司。

④ 卡应用开发商：从事应用系统的设计、开发、制造，甚至小规模的卡封装和印刷。

⑤ 卡发行部门：行使跨行业、跨地区、跨部门应用的统一管理，在中小规模应用中其职能由卡应用部门行使。

⑥ 卡应用部门：负责卡的应用、发行，部分技术、经济实力较强的该类部门也同时扮演角色④。

⑦ 最终用户：持卡人。

虽然不同领域、不同规模应用时的 IC 卡生存周期的划分和流程可能有很大不同，但一般均可归纳为如下三种形式：

(1) 小规模应用：如考勤/门禁等。由应用开发商开发并提供相关服务。其中 IC 卡可从卡制造商或其代理处购得。相关机具则从卡设备制造商处获取或自行研制。流程为①→②／③→④→⑥→⑦。

(2) 中规模应用：常常与某一行业有关，如各种公用事业收费卡。因涉及行业内部对标准、规划、实施的统一性要求，应用开发商一般很难“挤入”，流程为①→②／③→⑥→⑦。

(3) 大规模应用：具有跨行业、跨地区、跨部门的特点，如身份证、医疗卡等。流程为①→②／③→⑤→⑥→⑦。

2．智能卡的个人化

一般来说，卡制造商提供的卡都是仅具备最基本软、硬件配置的“白卡”，必须在发行阶段对之个人化(Personalization)后才能实际应用。所谓“个人化”，是指相关部门根据系统设计要求，将系统应用信息及持卡人个人信息写入或制作于卡上，使具有普遍通用意义的白卡变为具有个人特殊意义的可用卡的过程。

个人化的内容通常包括：

(1) 卡的软、硬件逻辑格式化。

(2) 系统应用信息和个人应用信息的初始化写入。前者包括表明卡的来源的发行商代码、用作金融交易的充值凭证、保护发行商利益的发行商密码等；后者则包括持卡人密码、姓名、年龄、应用数据等。

(3) 在卡面上印刷卡和发行单位名称、持卡人照片等。

对于大规模应用，个人化可由卡制造商或发行部门完成，例如公交卡由公交公司发行；而中小规模应用则由应用部门或应用开发商完成，例如智能小区门禁/停车卡可由物业管理公司来发卡。

1.2.2　智能卡的用卡过程

上面介绍了智能卡从制造、发行到使用、回收的过程，那么，用户持有卡以后，如何使用？受卡方和发卡方的关系怎样，如何协调呢？金融卡是我们日常生活中用得最多的卡，下面就以金融卡为例，来说明智能卡的用卡过程。

1．使用磁卡金融卡完成一次购物的过程

在金融行业，作为金融交易卡的磁卡，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，诸如帐户金额、交易记录等，均保存在金融机构计算机的数据库中，磁卡一般仅提供用户的主帐号作为索引信息，方便在数据库中迅速找到用户数据。

例如，某银行(发卡方)核对了客户(持卡人)的帐目(如余额为 1000 元)后，发给客户一张储蓄卡(也称扣款卡、现金卡、电子存折)，卡内存有该客户的帐号、最多可一次使用的金额等。客户持这张卡到某商店(受卡方)去购物的操作顺序如下：

(1) 将储蓄卡插入商店的 POS 机中。

(2) 售货员通过键盘输入交易金额(如 400 元)，并显示在客户设备的显示板上，同时指示客户输入个人标志符 PIN。

(3) 客户输入 PIN 后，POS 机读出卡中磁条上的数据，如客户帐号等，并通过网络将客户帐号、PIN 传送到银行的计算机，由银行的计算机在其数据库中检查该帐号(查对黑名单)，以防止他人使用已挂失或偷窃来的金融卡。同时核对客户的帐面记录，查明可供支用的金额，以及核对 PIN，以确认持卡人是否是卡的主人。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)，还要核查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。

(4) 核查客户帐号和 PIN 无误后，银行计算机将通过网络发回授权信息，授权商店进行交易。商店 POS 机将客户帐号、所购物金额数(400 元)记录下来，显示板显示交易结束，给客户打印收据。客户取走商品和卡。

(5) 在适当的时间(例如晚上)通知商店的开户银行(代理方)，告诉它该客户今天在这儿花了多少钱。随后，商店的开户银行就会通过信息交换系统与发卡的银行联系，发卡银行以客户的帐号为索引在它的数据库中找到客户在该银行中的帐目，并加以修正(扣款，余额 600 元)，同时将交易金额(400 元)转入商店在开户银行的帐户，整个交易过程结束。

交易过程如图 1.6 所示。

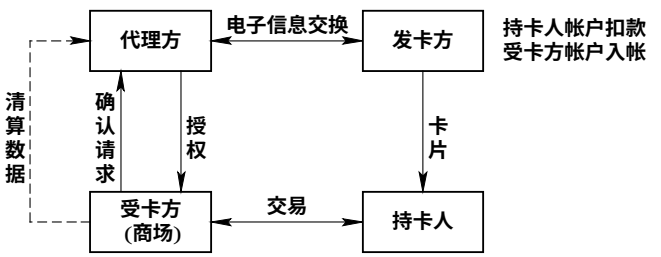


图 1.6　使用磁卡金融卡完成一次购物的过程示意图

从上述使用过程可以看到，一方面，磁卡的应用必须有其他条件的支持，例如强大可

靠的计算机网络系统、中央数据库等，其应用方式是集中式的，除需要巨大的网络投入外，还受限于网络速度、网络吞吐率等；另一方面，磁条容易读出和伪造，为了防范磁卡诈骗行为，各行业采取了一些方法对磁卡的使用加以限制，如要求授权、限制一天内的交易次数和交易金额等，这在某种程度上给客户带来了不便。所有这些问题都是由磁卡中磁条存储容量小、保密性差引起的。

2．使用智能卡金融卡完成一次购物的过程

1) 智能卡存储区的分配和功能简介

智能卡的容量比磁卡大得多，一般分为四个存储区：

(1) 公开的存储区：内含公用信息，如发行标志符、持卡人帐号等。

(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时写入的，用户在输入正确的 PIN 值后，允许输入新的 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进行交易，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。

2) 智能卡接口设备存储器内容简介

与智能卡配合使用的接口设备(如智能卡 POS 机)提供附加的存储器和逻辑电路，它本身就是一台微机。

商店中的智能卡接口设备(POS 机)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商店开户银行，供转帐或清算之用。银行应保证及时将应付款存入商店的帐户。

(2) 黑名单：即止付名单或非法卡表。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税户要进行交易时，须由售货商通过网络或用专用电话和银行进一步授权核实后方可受理，也可拒绝受理，甚至可根据实际情况将卡没收。

(3) 保密数据：密钥和授权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。至于授权号，在售货商希望成交某些超额交易时，用它通过网络连接发卡银行，经银行授权后方可受理。

3) 使用智能卡储蓄卡完成一次购物的操作过程

某银行(发卡方)发给客户一张智能卡储蓄卡(也称扣款卡、现金卡、电子存折)，卡内存有客户帐号，银行接受客户上交的现金 1000 元后在不可读存储区写入客户 PIN 码，在保密存储区写入帐面余额 1000 元等，完成卡的个人化。

客户持智能卡储蓄卡到某商店(受卡方)去购物的操作顺序如下：

(1) 将储蓄卡(余额 1000 元)插入商店的 POS 机中。

(2) 售货员通过键盘输入交易金额(如 400 元)，并显示在客户设备的显示板上，客户在