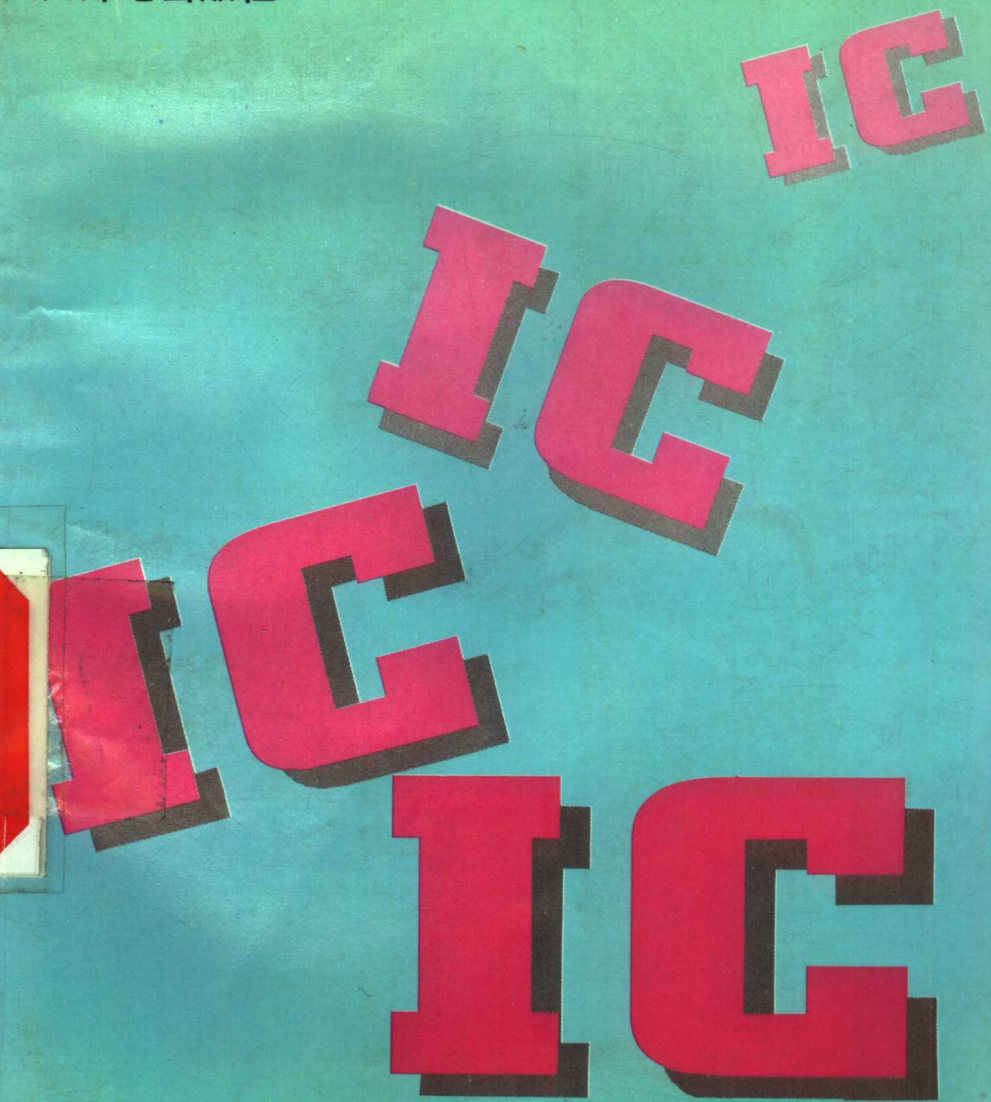
IC卡实用化技术

李津生 张一平 戴英侠等 编著

人民邮电出版社



IC 卡实用化技术

李津生　张一平　戴英侠　等编著

人民邮电出版社

登记证号(京)143号

内 容 提 要

IC 卡是继磁卡之后的新一代数据卡，卡内嵌入了含有 CPU 和存储器的芯片。除存储数据外，它还具有运算、处理、控制能力，堪称世界上最小的个人计算机。高度的安全性和大存储量是 IC 卡的两大特点，它已广泛应用于金融、交通、国防等领域。本书全面地阐述了 IC 卡的软硬件技术、发行和存取技术、加密算法等 IC 卡的基础知识，此外，还在第六章介绍了 ISO 7816 的 ID 卡接口技术规范，最后，以移动通信为例详细说明 IC 卡的具体应用。读者在阅读本书过程中可参阅《金融行业国际标准译文汇编》(第一集 银行卡)，以加深理解。

IC 卡实用化技术

李津生 张一平 戴英侠 等编著

责任编辑：王亚明 陈万寿

*

人民邮电出版社出版发行

北京朝阳门内南竹杆胡同 111 号

北京市丰华印刷厂印刷

新华书店总店科技发行所经销

*

开本：850×1168 1/32 1995 年 2 月 第 一 版

印张：6.5 1995 年 2 月 北京第 1 次印刷

字数：167 千字 印数：1— 4 000 册

ISBN 7-115-05478- 9-/TN・828

定价：8.20 元

前　言

早在60年代后期，一些发达国家已将磁卡用做信用卡和现金卡。此后，在交通和通信领域用做月票和电话卡；在健康保险服务和企业内部用做医疗卡和考勤卡；在门禁系统中用做电子钥等，其应用范围不断扩展。在上述应用中磁卡暴露出两个不可克服的缺陷。首先是安全性能差，磁条上的数据很容易被改写、伪造。据统计，美国在发行磁条信用卡的头十年中，平均每年的损失为10亿美元，占信用卡销售总金额的百分之一。其次是磁卡的数据存储量小，难以实现大数据量信息的存取和实现一卡多用。

1972年法国的R. Moreno发明了集成电路卡(IC Card)，并由法国电信部门率先推广使用。IC卡是在与磁卡尺寸相同的塑料卡上嵌入了大规模集成电路(LSI)芯片的新一代数据卡。芯片内含有处理器(CPU)、程序存储器(ROM)、工作存储器(RAM)和数据存储器(EEPROM)，因此，IC卡被认为是世界上最小的个人计算机。其存储容量为8千字节至64千字节，是磁卡的数十倍至数百倍；还因其CPU的运算、处理和控制能力使IC卡具有突出的3S特点，即Standard(国际标准化)、Smart(智能化)和Security(安全性)。高度的安全性是IC卡的最重要的特征，即使进行脱机处理也能确保数据的可靠性。因此，IC卡不仅在金融领域中将取代磁卡，在通信、交通、教育、卫生、安全和企业管理方面也日益发挥其重要作用。

IC卡的应用前景引起了我国政府和有关部门的高度重视。在国务院办公会议批准的"金卡"工程总体方案中明确了我国的金融交易卡"从防伪及技术发展考虑，以IC卡为主导，以磁卡为过渡"的指导

思想。在此之前，它已被列为国家重点科技项目攻关计划“金融电子化”的核心内容和国家产学研联合开发工程高技术产业计划“数据卡及配套电子设备”项目的重点课题。这些举措对推动我国 IC 卡的研究与应用，发展我国 IC 卡产业产生了深远的影响。在这一背景下我们编写了这本读物供从事 IC 卡应用研究与开发的科技工作者参考。其中第一章由张一平执笔，第二、三、四、五、八章由李津生执笔，第六、七、九、十、十一章分别由王星、戴英侠、王东林、仲安妮、王云生执笔，王瑞智帮助作图并打印了部分手稿。全书由李津生、张一平、戴英侠主编。鉴于我们对 IC 卡的研究起步不久，肯定会有不妥之处，望批评指正。

本书在编写过程中得到中国工商银行和中国科学院应用研究与发展局的支持和帮助，并得到中国科学院 C&C 总体部主任王行刚教授的指导，在此表示诚挚的谢意。

作者

1994 年 9 月

目　录

第一章　绪　论 …… 1
第二章　IC 卡硬件技术 …… 7
2.1　卡的分类及其特点 …… 7
2.2　IC 卡的分类 …… 9
2.2.1　按功能分类 …… 11
2.2.2　按与终端设备连接方式分类 …… 12
2.3　IC 卡中所用存储器的种类 …… 14
2.3.1　易失性存储器 …… 14
2.3.2　非易失性存储器 …… 14
2.4　ISO 规范的 IC 卡 …… 15
2.4.1　ISO 规范的 IC 卡标准结构 …… 15
2.4.2　IC 卡的生产工艺 …… 18
2.5　IC 存储卡 …… 24
2.6　非接触式 IC 卡 …… 26
2.6.1　带触点的 IC 卡的缺点 …… 26
2.6.2　非接触式 IC 卡的类型 …… 26
第三章　IC 卡软件技术 …… 30
3.1　IC 卡存储器的分层结构 …… 30
3.1.1　文件 …… 30
3.1.2　区 …… 32
3.1.3　记录 …… 32

3.2 IC卡中存放信息的分类 …… 34
3.2.1 系统信息与用户信息 …… 34
3.2.2 从应用观点分类 …… 34
3.2.3 从安全观点分类 …… 35
3.3 安全技术 …… 35
3.3.1 存储器锁 …… 37
3.3.2 文件锁 …… 38
3.3.3 区锁 …… 42
3.4 从外部对IC卡存储器的存取法 …… 44
第四章 IC卡发行技术 …… 49
4.1 IC卡制造处理 …… 49
4.2 IC卡初始化处理 …… 49
4.3 IC卡发行处理 …… 50
4.4 IC卡再生处理 …… 54
第五章 IC卡存取技术 …… 56
5.1 IC卡读写器的基本功能 …… 56
5.2 IC卡读写设备的构成 …… 57
5.2.1 接口方式 …… 58
5.2.2 读写/控制器 …… 60
5.3 微机的初始化 …… 61
5.4 控制器的初始化 …… 62
5.5 通信规程 …… 62
5.6 程序的编制 …… 64
第六章 面向信号传输和信息交换的ID卡接口技术规范 …… 67
6.1 概述 …… 67
6.2 机械接口规范 …… 68
6.3 信号传输协议 …… 68
6.3.1 各个触点的电特性 …… 68
6.3.2 操作过程 …… 69

6.4 T=0,异步半双工字符传输协议 …… 73
6.4.1 工作等待时间 …… 73
6.4.2 命令的结构和处理过程 …… 73
6.5 用于信息交换的行业间命令 …… 78
6.5.1 消息结构 …… 78
6.5.2 对 APDU 与 TPDU 间相互转换的约定 …… 82
6.5.3 具体的行业间命令 …… 88
第七章 IC 卡加密技术 …… 91
7.1 加密技术简介 …… 91
7.2 DES 算法 …… 95
7.3 数字签名及公钥算法 RSA …… 102
第八章 IC 卡应用系统 …… 106
8.1 引言 …… 106
8.1.1 IC 卡的作用 …… 106
8.1.2 IC 卡的应用领域 …… 107
8.2 IC 卡预付款业务 …… 109
8.3 IC 卡在线通信 …… 110
8.4 IC 卡电话机及其应用 …… 113
8.4.1 IC 卡电话机的结构及特点 …… 113
8.4.2 IC 卡电话机的应用实例 …… 114
8.5 无线 IC 卡应用系统 …… 116
8.6 IC 卡管理体系 …… 119
第九章 移动通信中的 SIM 卡 …… 122
9.1 引 言 …… 122
9.2 GSM 的基本结构 …… 123
9.2.1 GSM 网络 …… 123
9.2.2 发往移动站的呼叫建立 …… 125
9.3 GSM 系统的安全保密特性 …… 125
9.3.1 用户身份保密 …… 126

9.3.2 用户身份认证 …… 127
9.3.3 用户数据加密传输 …… 128
9.3.4 信令信息加密 …… 130
9.4 SIM 卡及其功能 …… 130
9.4.1 SIM 卡的两种形式 …… 130
9.4.2 SIM 卡的功能 …… 131
9.4.3 PIN 的处理 …… 131
9.4.4 SIM 卡支持的业务 …… 132
9.5 SIM 卡存储器的结构 …… 132
9.5.1 SIM 卡存储器的逻辑结构 …… 132
9.5.2 目录项及数据域首标结构 …… 134
9.5.3 SIM 卡的目录结构 …… 135
9.5.4 SIM 卡的数据域 …… 137
9.6 SIM 卡的指令系统 …… 149
9.6.1 指令格式 …… 150
9.6.2 MS 指令编码 …… 150
9.6.3 状态编码 …… 151
9.6.4 MS 指令说明 …… 154
9.6.5 SIM 卡的传输规程 …… 162
9.6.6 SIM—ME 进程结构 …… 164
第十章 金融交易中的 IC 卡 …… 169
10.1 电子货币及金融交易卡 …… 169
10.1.1 电子货币的概念 …… 169
10.1.2 金融交易卡 …… 169
10.1.3 金融磁条卡与金融 IC 卡的比较 …… 170
10.2 金融 IC 卡的应用 …… 171
10.2.1 金融 IC 卡应用系统 …… 171
10.2.2 IC 卡实现的信用卡业务 …… 178
10.2.3 IC 现金卡——电子存折 …… 181

10.2.4 电子钱包…… 181
第十一章 IC卡标准化 …… 183
11.1 IC卡标准化的意义 …… 183
11.2 IC卡标准化的主要领域 …… 184
11.3 制定IC卡标准的国际组织 …… 184
11.4 ID卡及IC卡国际标准概况 …… 186
11.5 国际标准ISO 7816简介 …… 188
11.5.1 ISO 7816第一部分主题内容 …… 188
11.5.2 ISO 7816第二部分主题内容 …… 189
11.5.3 ISO 7816第三部分主题内容 …… 189
11.5.4 ISO 7816第四部分主题内容 …… 189
11.5.5 ISO 7816第五部分主题内容 …… 190
11.6 国际标准ISO 9992简介 …… 190
11.6.1 ISO 9992第一部分主题内容 …… 191
11.6.2 ISO 9992第二部分主题内容 …… 191
11.7 国际标准ISO 10202简介…… 192
11.7.1 ISO 10202第一部分主题内容 …… 192
11.7.2 ISO 10202第二部分主题内容 …… 193
11.7.3 ISO 10202第三部分主题内容 …… 194
11.7.4 ISO 10202第四部分主题内容 …… 194
11.7.5 ISO 10202第五部分主题内容 …… 195
11.7.6 ISO 10202第六部分主题内容 …… 196
11.7.7 ISO 10202第七部分主题内容 …… 196
11.8 小结…… 197

第一章 绪 论

随着电子信息技术的飞跃发展和迅速普及应用，人类进入了一个全新的高度信息化的社会。电子信息技术与人类社会生活的广泛深入的融合，大大改变了人们的生产和生活方式，产生了诉许多多的新概念、新工具、新手段。信息化社会是以电子计算机的全方位普及和深层次应用为特色的。在未来的10～20年内，电子计算机将从不同的应用领域，以不同的规格性能进入人类社会生产和消费活动的各个方面，真正达到无处不在，无处不用，给人类社会生产创造出巨大的效益，给人们的消费活动带来极大的方便。

智能卡是当今世界日新月异发展的信息化社会中出现的一颗新星，它被公认为世界上最小的个人计算机。智能卡的概念最初是法国的新闻工作者R. Moreno先生于1972年首先提出的。此后法国布尔公司率先投入了对这一革命性的高技术产品的研究与开发。1976年布尔公司高级研究员Ugon先生所领导的研究小组首先研制了世界上第一张由双晶片（微处理器加存储器）组成的智能卡，接着又于1978年制成了单晶片智能卡，取得了技术专利。国际标准化组织在此基础上制定出了智能卡的国际标准——ISO 7816，为智能卡的发展普及创造了条件。在此后的十几年间，除法国布尔公司之外，世界上先后有Motorola，Thomson，Hitachi，OKI，Toshiba，Sharp，Gemplus，Schlumberger等十多家公司企业相继投入了智能卡芯片或卡片成品的开发生产，形成了一个世界性新兴的技术产业。Ugon先生由于其重要成就，于1992年被评选为世界智能卡先生。

从严格的意义上讲，智能卡（Smart Card）只是集成电路卡（IC

Card)的一个分支。集成电路卡就是一张由一个或多个集成电路芯片所组成，外部封装成便携式卡片的塑料卡。IC 卡按其内部封装芯片的种类及功能的不同可分为智能卡(Smart Card)和存储卡(Memory Card)。智能卡由一块包含有微处理器(CPU)和存储器(Memory)的集成电路芯片、接触键表面及塑料卡式片基构成。存储卡与智能卡的唯一区别就在于存储卡内部不包含微处理机，只具有存储数据信息的功能。本书中将基本遵循这种严格的分类和定义。

一张典型的智能卡的各部分构成及功能如下：

微处理机单元：

——8 位微处理器(CPU)。

存储器单元：

——随机存储器 (RAM)；

——只读存储器 (ROM)，用来存放智能卡的操作系统(OS)；

——可编程存储器，用于存放智能卡的应用信息及与持卡人有关的个人信息。目前智能卡中所使用的可编程存储器有以下两种：

- EPROM，可擦除可编程只读存储器；
- EEPROM，电子可擦除可编程只读存储器。

输入/输出部分：

——可实现与接口设备的单线双向、面向字符的 I/O 通信，传输速率达 9600 波特。

智能卡本身具有中央处理器和存储器，因此可以建立多种应用，存放多种信息，并实现对数据信息存取的高可靠性、高安全性控制，可以独立操作和随身携带，确实堪称一部最小的个人计算机。

IC 卡作为一种高效实用、方便安全的智能化工具，十几年的时间中已在金融业务、商业服务、医疗保险、交通、电信、资料管理、身份验证、安全控制以及军事领域等各个方面获得了广泛的应用。目前世界上 IC 卡的应用广度和深度还正在迅速不断地发展之中。

在IC卡的发源地法国，近年来已研制应用了一种智能卡公路自动收费系统。该系统的特点是在汽车驾驶者持有的智能卡中嵌入了一个小型环状天线，在高速公路和桥梁隧道的收费站装设一个特制的天线盒，收费站以无线通信的方式向通过的汽车发出信息，对所过的汽车进行鉴别分类和计费结算。汽车可以不减速地通过收费口，不需要停车等待时间，这样就大大提高了车辆通过率，有效地减少了交通堵塞。对于持无效卡或非法卡闯关的汽车，自动收费站的高速自动摄影机可以留下非法通过的汽车的照片，事后可以追踪处罚。对于不使用自动收费智能卡的汽车，收费站则为其另开一条慢车道，实行停车人工收费，大家可以“各得其所，相安无事”。这种采用智能卡不停车即可自动收费的系统受到人们的欢迎，发展前景十分看好。

随着人们对通信手段的要求不断提高，世界各国的手持式移动电话得到迅速发展，各种区域性的漫游电话通信给人们的信息交流带来极大的方便，跨国界的全球性漫游电话也在酝酿之中。与此同时，各种针对移动式电话的高技术智能性犯罪也应运而生。各种偷窃用户密码、大量恶意透支电话费的案件层出不穷，给电信部门及用户都造成了巨大的损失。为了解决既使用方便又安全可靠这一难题，国外已开始将智能卡引入移动式电话中，智能卡中存储有用户的个人标识等有关机密信息以及用户的财务信息，通过智能卡可对通话进行严密可靠的控制，通信网络借助智能卡可方便地识别电话用户并按照通话次数、距离、时间自动地在卡上计费结算，从而极大地方便了使用和管理。

智能卡技术在军事领域的应用也取得了极大的发展。据有关资料介绍，美国军方已将智能卡技术实际应用于其作战指挥系统。其庞大的作战指挥信息系统通过卫星及无线通信方式覆盖到第一线的作战连队，每个连队都装备有采用无线方式联网的终端，连队指挥官持有一张载有各种个人标识及机密信息的智能卡，通过其本人使用的密码、指纹及其他特殊信息的验证方可进入系统与上级联络或者接收作战指示。智能卡系统不仅能识别连队指挥官的密码及指纹信息，

而且能根据其手指上体液的分泌情况准确判定是不是活人的指纹。这样就严格地保证了作战指挥信息系统的安全保密性，可靠地防止泄密和窃密等破坏活动，大大提高了部队指挥作战的机动性和正确性。

智能卡技术另一个成功的应用典型是在1992年西班牙塞维利亚世界博览会上用作个人参观证进行出入控制。在这次博览会上共售出智能卡参观证50万张。智能卡中存储有持卡人的指纹信息，被称为"生物统计信息身份证"。凡是想参观博览会并打算停留4天以上的人都可以办理智能卡参观证。参观者可以先在西班牙的三个指定银行支付入场费，然后在装备有45部工作站的售票点获取入场卡。智能卡具有64千字节的存储容量，利用有关的管理信息及持卡人的指纹特征信息对卡进行个人化处理。在博览会的5个入口处，持卡人只要把智能卡插入读卡机，并把手指放在指纹识别终端上，计算机将卡中存储的数字化的指纹信息与实际指纹进行比较，全部判别过程不超过5秒种，检验正确即可放行，让合法的参观者进入大厅。所有丢失卡和被窃卡都不能使用，入场卡也不能转借。这样一个现代化的门禁系统就有效地保证了整个博览会的出入控制和安全管理。

众所周知，智能卡应用的一个极为广阔的领域是金融交易。用智能卡来代替目前仍在通用的磁条卡，尽管卡本身的成本比较高，但由于其本身具有极强的安全保密功能，具有存储和管理信息的功能，可以采用完全的分布式处理模式实现银行交易的通存通兑，许多原来必须采用联机实时处理的作业可以改为脱机加批处理的作业，从而大大降低了银行计算机业务处理系统的设备和通信费用，而且系统的安全性和可靠性得到了充分的保证。正因为如此，智能卡不仅受到了西方发达国家银行界的青睐，在一些东方发展中国家的银行业中也引起了极高的兴趣。这方面的一个典型实例就是马来西亚伊斯兰银行的智能卡应用系统。伊斯兰银行是马来西亚国内第二大商业银行，其下属的31家分行中均采用高档DOS系统微机作为主机，构

成分行业务处理系统，下面连接分行的柜员工作站及 ATM 自动柜员机。全行向客户共发行智能金融交易卡 5 万多张。各分行的系统平时以脱机方式分布式处理，银行客户凭借自己的智能卡可以在所有分行的营业点、ATM 以及代理客户办理业务或消费转帐，实现脱机通存通兑。各分行的系统营业点采用电话拨号线批处理方式与总行的 UNIX 系统小型机结算对帐，交换信息。这个基于分布式处理的银行智能卡系统投产运行不到十年的时间中仅节约通信方面的费用已达 2000 多万美元，取得了十分可观的经济效益和社会效益。

智能卡的出现给已流通使用半个多世纪的金融交易卡注入了新的生机与活力。金融交易卡的应用发展走过了凸印字符卡和磁条卡两个历史阶段。目前正在世界范围兴起其革命性的第三代智能金融交易卡。第一代的凸印字符卡由于仅限于手工处理，因而从 60 年代起，逐渐被机器可读的第二代磁条卡所取代。但磁条卡由于其信息量有限及可靠性和安全性方面的不足，在推广和发展中也出现了不少问题。据统计，像维萨、万事达这样的世界性信用卡公司由于受伪造窃密、恶意透支危害所造成的金钱损失大约为其信用卡总交易额的 0.6%，每家公司在亚太地区的损失每年约 1～2 亿美元。而智能卡芯片内部采用微处理器结构和特别研制的防复制防入侵的存储区域，其 ROM 之中固化有可靠性极高的安全控制程序，从技术性能上讲是对磁条卡的重大改进和发展。智能卡从其制造阶段开始，就采取了一系列严格的安全措施，在其不同的个人化处理及启用的各个阶段，每张卡内都设立了相应的跟踪记录密码，不同的阶段使用不同的加密密钥，逐级鉴别，严防假冒。智能卡中有关客户的交易信息以及客户密码(PIN) 的存取传输都是通过专用密钥以加密方式进行的，可有效防止被窃取和被破译。在某些特别用途的智能卡中，还可以采用多媒体技术存入持卡人的图像及指纹等信息，更加提高其使用的安全可靠性能。正是由于智能卡的这种特强的安全保密性能及其可以存储处理信息的方便性使其在金融交易卡领域中引起了各方面的高度重视，显示了巨大的优越性和生命力。智能卡不仅在传统的信用卡

(Credit card)和借记卡(Debit Card)两个业务类别中逐渐担当起重要的角色,而且又产生了一种新型的金融交易卡——现金卡(Cash Card)。这种智能现金卡高度安全可靠,可完全脱机使用,完全可以代替现金进行消费和支付,成为名副其实的"电子货币"。

今天智能卡这一新型的信息技术结晶正在迅速地进入中国社会生活和人们消费活动的各个方面。当前正在大力开展的"金卡工程"吸引了越来越多的国人的注意力和兴趣,也引起了社会各界对智能卡这一略带神秘色彩的小玩艺的极大重视和青睐。科研产业界人士以及社会大众都在以不同的侧面和角度对它进行研究和揣测。人类社会生产生活实践活动已无数次地证明了一个无可辩驳的真理:任何一项成熟的新技术只有在能为广大未经专门培训过的普通民众都能使用,能使那些不具备这种新技术详尽知识的人能够接受时,它才能得到社会的公认,才能转化为改变人们工作生活方式的巨大力量。正像亿万电视观众并不需要理解彩色电视复杂的编码解码技术就能正确地使用欣赏电视,汽车驾驶者不需理解内燃机和汽化器的工作原理就能正常开车,而银行储户也不需要知道自动柜员机(ATM)的控制程序就可以方便地用它存款取款一样。今天电视、汽车和ATM已日益成为现代社会须臾不可离开的工具,与之相应的研制生产已形成了庞大的社会产业。可以说,今天的智能卡技术也面临同样的局面。本书是以工程技术的角度介绍IC卡软硬件技术的各个方面,目的在于为国内从事IC卡应用开发的技术人员提供一套基本的参考资料。而有关电子信息技术人员面临的任务则是如何去规划和开发智能卡技术与人们社会应用需求之间的衔接界面,努力促进这一尖端技术在当今社会生活中的广泛应用。

第二章　IC卡硬件技术

2.1　卡的分类及其特点

卡片是作为个人身分识别的手段而导入的。最初，在纸质卡片上印有持卡人的姓名和单位名称，进入50年代演进成冲压有凸字的塑料卡，例如美国曾大量使用的一种塑料金融交易卡(Financial Transaction Card：FTC)即属此类，可以利用机械方法把这些带有凸字的卡片的发行人和客户帐号压印到纸质单据上。

到了60年代中期，人们把这种FTC卡的背面贴上磁条，发展成能够自动读取信息进行在线处理的磁卡。磁卡的结构简单，价格低廉，得以迅速推广。到1988年美国磁卡发行量已超过10亿张，平均每人拥有5张。日本发行了2.3亿张，其中信用卡为8700万张。另一方面，磁卡的存储容量小(三个磁道存储字符的总和不过200余个)，安全保密性差，限制了它的应用和发展。

近年来，IC卡和光卡等多功能卡开始实用化。IC卡是在与磁卡尺寸相同的塑料卡中埋设了LSI芯片的新一代数据卡。卡内装有CPU、程序存储器掩膜ROM、工作存储器RAM和数据存储器EEPROM(电可擦除的存储器)。其存储容量为8～64KB，是磁卡的数十倍至数百倍，还因其CPU的运算、处理和控制能力使IC卡具有突出的3S特点，即Standard(国际标准化)、Smart(灵巧智能化)和Security(安全性)，因而发展迅速，在金融、销售和企业管理等应用领域有取代磁卡之势。一些企业家把IC卡称作“开创市场之卡”，也就是说，