第一章 概 论

随着社会的进步和现代化程度的不断提高，人类所拥有的信息种类和信息数量都在成倍增加。在远古时代，我们的祖先只需要极简单的语言就可以交换他们的全部信息。而今，包括政治、经济、军事、科技、文化等方方面面的信息充斥着我们的生活，信息媒介也从简单的语言发展为书刊、报纸、电视、电话、电脑、广播、电报、电传、传真、计算机网络等形形色色的载体，信息交流的广度和深度都在与日俱增。勿庸置疑，这是信息大爆炸的时代，是人类社会信息革命的开始。

在这样的社会里，我们每天都要处理许多与个人有关的信息，如购物、打电话、到银行存款取款等。为了处理的方便，我们需要随身携带多种票证、单据、卡片，包括购物用的现金、支票和收据，证明身份用的身份证、工作证、借书证和会员证，社交活动用的名片、记事本，到银行存取款用的存折、信用卡，等等。如此众多的卡片，必然会给我们的日常生活带来不便和不安全感。这就亟须一种多用安全卡，能够把生活中单项使用的电话卡、预付卡、金融卡、信用卡等融为一体，只要一卡在手，便能买到各类物品或得到各种服务，甚至走遍天下，畅通无阻。

应运而生的“磁卡”已在全世界普及，一般人已逐渐习惯使用，且磁卡的应用环境及产业所提供的服务，已日臻成熟和普及。

但磁卡只能是一种功能卡，而后起之秀“智能卡”更加安

全，功能也更多，能广泛应用于金融、医疗、交通和教育等领域，可以身兼数职，满足上述大众化信息处理的要求。因此，各先进国家纷纷采用智能卡，形成了智能卡的研究和开发热潮。

第一节　智能卡的定义

一、什么是智能卡

智能卡是由一个或多个集成电路芯片组成的，并封装成便于携带的一种多功能“电脑卡”。

智能卡中的集成电路芯片是一种单片机(MCU)。这种单片机唯一的工作方式是“用户方式”，分为通用和专用两种。专用的单片机是指其中的微处理器为专用的、保密的单片机。它与通用的单片机差别很大，主要差别在于“保密”的单片机有很好的物理保护措施。智能卡的发展方向是保密的单片机。

智能卡的外形一般同信用卡的大小一样，但为便于用户携带、插入、取回以及与设备的连接，也可制成形状、大小和厚度各异的卡片。智能卡所采用的封装可从最简单的单张芯片到具有键盘、显示器、电源和通信接口的“工作站”。

智能卡的功能是多样化的，它具有暂时或永久的数据存储能力，存储器的内容可以供外部读取，或供内部信息处理的判定用。它比磁卡具有更大的存储容量和更多的“智能”，使用起来更安全、方便。

二、世界各地的名称对照

智能卡在各国的名称和定义略有差异，表 1.1 是各国和台湾地区对各种智能卡的名称对照。

表 1.1 智能卡在世界各地的名称对照

	IC 存储卡	智能卡	超级智能卡
特性	由一个或多个集成电路组成，具有存储能力	在集成电路中具有微电脑(CPU)和使用者存储能力	在智能卡的基础上，装置有键盘、液晶显示屏(LCD)和电源
日本	IC 存储卡	智能卡 IC 卡(含 CPU)	可视卡 GPC 卡 超级智能卡
美国	IC 卡 芯片卡	智能卡	超级智能卡 可视卡
法国		微电路卡	通用卡 活动卡
英国		芯片卡	
台湾	晶片卡、存储卡、微电路卡、IC 卡	精敏卡、电子金融卡、灵巧卡、智能卡	超级智能卡
常用领域	资料保存(资料卡)、电话卡、身份证登记、强化记忆等	电子付款、清款或结算用	离线信用购物、飞机票、火车票预订、家庭批量交易、电话购物

三、结构与生命周期

1. 物理结构

智能卡的物理支撑一般是一个塑料长方卡。它的结构如图 1.1 所示。

智能卡的尺寸从通用磁卡衍生而来，磁卡又遵从相关的国际标准 ISO 7810，即大小为：85.47～85.72mm×53.92～54.03mm，厚度为 0.76mm±0.08mm。从而确保了与现存硬件的兼容。

智能卡上可以印有发行者的信息(如广告)和卡片持有者的可读信息(如姓名、有效期及照片等)；左上角有印制板，上面有 8 个触点；触点印制板的下面是智能卡芯片。由于目前磁

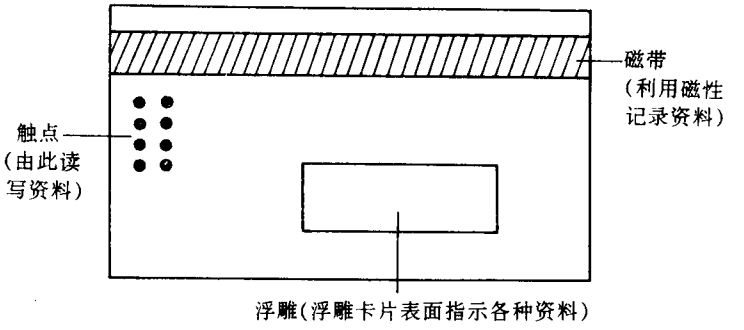

图 1.1 智能卡的物理结构

卡使用很广泛,所以很多智能卡上也具有磁条,可作为某种应用的磁卡使用。

智能卡 8 个触点的排列是按照国际标准定位的,其中 6 个触点同芯片连接。这 6 个触点用来提供电源、地线、时钟、复位及一条串行数据通信线路。另外 2 个触点留作将来使用。

2. 芯片结构

智能卡的芯片结构包含 5 个主要部分(见图 1.2),各部分的功能是:

(1)微处理器(CPU)

它通常是一个 8 比特的处理器,最常见的是摩托罗拉的 6805 及英特尔的 8048。还将出现新的、功能更强的处理器。

(2)工作存储器(RAM)

主要用来存储卡片在使用过程中的临时数据。

(3)只读存储器(ROM)

该存储器包含有由处理器执行的永久性代码。要注意的

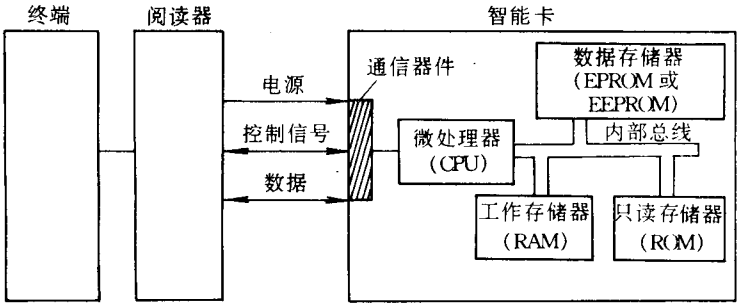

图 1.2　智能卡的芯片结构

是，这个程序是通过一种掩膜存储的，不能以任何方式更改。

(4)数据存储器(EPROM 或 EEPROM)

第一代数据存储器是 EPROM，需要外加 25V 电源。最新的智能卡包含 EEPROM，仅需要单一的 5V 电源。这种类型的存储器可在很短时间内写入和抹除。

(5)通信器件

通信器件用于在智能卡和外部访问终端之间交换数据和控制信息。该通信单元以串行异步方式工作，最常用的比特率是 9600bps。

为保证智能卡的安全，上述五大要素是集合到一块芯片上的。否则，芯片间的外部布线会为非法访问或非法使用智能卡提供可能通路。

3. 生命周期

智能卡的生命周期是指从智能卡的制造、发行、使用直到回收为止的时间。

在制造阶段，主要是决定智能卡的技术要求以及卡片的设计。发行阶段，与用户签约，决定卡片应用业务范围并交付使用。使用阶段，主要是管理卡片遗失及信息管理。回收阶段，主要是回收损坏卡片，处理和回收过期卡片以及用户解约卡片。

第二节　智能卡的技术演变过程

智能卡是信息处理系统和微电子系统设计技术共同发展的产物。

首先，二次世界大战后不久推出的、以真空管为基础的数字计算机，即电脑，还是一座几吨重、需要有高度专业知识的人方能操作的庞然巨物。随着数字技术从真空管发展为晶体管，再发展为现代的集成电路芯片，电脑的体积越来越小，现在已进入单片式微型计算机的时代了。事实上，1950 年最早的电子数字计算机的体积竟是今天单片微机的 200 万倍（1000 平方英尺比 1 1/4 平方英寸）。而且，单片微机的运算速度更快，容量更大，可靠性更高，使用也更为灵活方便。

其次，随着微电子系统设计技术的持续发展，把单片微机中的集成电路芯片嵌入只有 0.76mm 厚的软塑料卡中，就产生了成本更低、功能更强且适应性更灵活的电脑——智能卡。

具体地说，单片微机（MCU）是综合在单片硅上的完全微处理系统。它几乎包含所有要实现特殊应用的资源，或一系列应用。除了中央处理单元（CPU）及其控制电路，它通常包含各种类型的存储块，硬件功能的选择项，优选通用的、或者有时是非常专用的应用领域。它唯一缺乏的、类似计算机的资源是外部人工或机器接口设备，如键盘、显示器、磁盘驱动器、转

换程序和传感器。大部分 MCU 至少包含随机访问存储器(RAM)和只读存储器(ROM)。MCU 的固定存储器综合排列,如 EPROM(由 UV 光擦除)和 EEPROM(电子可擦除)适于各种数据必须保持较长时间的应用。

大部分典型的单芯片微机的设计都是在几种不同的操作模式下工作,模式可由用户选择。在单芯片用户模式(即大部分应用的正常操作模式)下,CPU 在 ROM 的用户软件控制下运行。在一些 MCU 的支持扩展模式操作中,内部数据和地址总线连接到 I/O 针,允许 CPU 访问附加存储器和 MCU 外部的 I/O。其它的操作模式用于测试。

类似地,保密的单芯片微机,即智能卡,可以包括上述任一或全部特性,但是它还具有内装能力,可以通过多种手段随时防止非授权访问 CPU、存储器排列、用户/应用软件、设备内正在处理或存储的任何数据。半导体制造商测试和通过全部功能后,保密微机唯一可行的操作模式必须是用户模式,即在只读存储器(ROM)中用户软件的完全控制之下。

第三节　智能卡的分类

根据智能卡与阅读器的连接方式,它分为接触型和非接触型两种。在接触型智能卡中,它又分为存储卡、智能卡和超级智能卡三种。各种卡的分类及其特性如表 1.2 所示。

表 1.2 智能卡的分类及其特性

			触点数	CPU	构成	尺寸、规格	芯片的种类	组成零件	举例
接触型	智能卡	M/S 对比(ISO)卡	8	V	CPU + 存储器	ISO 规格	8bit CPU + 16～64K EPROM 16～64 K EEPROM	芯片、R、制板、卡片基体	法、日、美开发的大部分智能卡
		ROM 卡				54×85.6×(2～3)mm			
		RAM 卡				同上	8bit CPU + CMOS·SRAM	同上·电池	
	超级智能卡		8	V	CPU +存储器+液晶显示屏(LCD)+键盘	ISO 规格	8bit CPU + 16K ROM 8K RAM	同上 电池	VISA (东芝)
	存储卡	ROM 卡	8	×	存储器	54×85.6×2.2mm 左右	Mask ROM (1M×1～4)	芯片 RC 制板 卡片基体	法国公共电话卡
							EPROM (256K ×2)		
							EEPROM (64K ×4)		
		RAM 卡				54×85.6×3.4mm 左右	CMOS·SRAM (64K ×16) 周边电路用 IC	芯片、RC、制板、卡片基体、电池	

（续表）

		触点数	CPU	构成	尺寸、规格	芯片的种类	组成零件	举例
非接触型	近接结合卡	1	V	CPU+存储器	ISO 规格	—	—	日本LSI卡社
		4	×	存储器	54×85.6×(1～5)mm			
	远隔结合卡	1	V	CPU+存储器	54×85.6×(1～5)mm		—	
		4	×	存储器				

注："V"表示"有"，×表示"无"。

第四节　智能卡与其它卡片技术的比较

在目前的卡片市场中，除了磁卡和智能卡以外，还有一种被称为“激光卡”的非磁质高密度记录媒体。三种卡的结构和功能的比较如表 1.3 所示。

表 1.3　磁卡、智能卡和激光卡的比较

项目	磁卡	智能卡	激光卡
构造	将磁性储存媒体嵌入塑料卡内	将芯片嵌入塑料卡内	将光储存媒体嵌入塑料卡内
尺寸	ISO 规格 54mm×85mm×0.76mm	ISO 规格 54mm×85mm×0.76mm	ISO
存储容量	1.2K	8K（千字） 16K（2 千字） 64K（8 千字） 256K（32 千字） 1M（发展中）	2M 字节
CPU	无	8bit 内藏	无
记录媒体	磁带	IC 存储器	聚碳酸酯
安全性	容易读取记载内容、易伪造、窜改等	记载资料不易被伪造或窜改	记载资料不易改变
外在伤害	可能被电器制品或皮包内的铁器制品等具有磁性的材料所破坏	不受磁性影响，但会因静电受伤害	刮伤破坏
记录媒体发展性	安全性和存储容量受限制	可作密码运算和增加存储容量	存储容量仍有可能增大
连线作业	CD/ATM 存提款	CD/ATM 存提款信用卡授权销售点转帐家庭/企业银行	N/A （较适合医疗系统）

项目	磁卡	智能卡	激光卡
离线作业	基于安全性，无法达成离线交易	具有处理能力和较大存储容量，可达成离线交易：·预付交易 ·记帐交易 ·信用交易	N/A（较适合医疗系统）
作业转换		作业转换期间可与磁卡并用，达成作业转换期间终端转换交易	N/A（较适合医疗系统）
网络成本	连线作业，网络成本高	可离线或连线，网络成本低	N/A（较适合医疗系统）
是否可重写	是	是	否
价格	约 50 日元	约 2000 日元	约 500 日元
优点	价格低	速度快 具有计算能力 安全性高	容量大 可储存影像 安全性高
缺点	容量小 易受伤害 资料容易改	成本较高 容量适中	读写时间长

从表 1.3 中可以看出，在某些只需要存储功能的应用中，采用激光卡是十分有利的。例如，把激光卡用来作为病历或程序的装入设备，或用来存储一张非法卡表。然而，仅有这种大容量的存储功能还不足以对智能卡的高度吸引力造成威胁。智能卡的性能价格比仍然是最优的。

第五节　智能卡的应用

一、应用举例

尽管全世界磁卡的发行量已达数十亿张，但由于智能卡具有比磁卡大得多的存储容量，可提供很高的安全性和多种功能，因而大有取代磁卡之势。

智能卡的典型应用有：

在金融行业，智能卡可以减少柜员人数，提供开发新业务的界面功能，取代简单的收提款工作并减少资料负荷过重的问题，而这些都是过去磁卡所办不到的。

由于智能卡具有微处理、存储能力和编程能力，因而可以记录持卡人的密码、银行存款余额及交易的资料。使用者购物时会自动从银行存款金额上扣除所购商品的费用。更重要的是，即使假日和夜晚银行线上系统不工作时亦可使用智能卡。

智能卡还可用作无现金购物。其方式是使用者就特定的用途先购买预付智能卡，于每次使用时逐次扣除。例如，电话卡、车票卡等均已普遍应用于先进国家。目前有些国家进而研究可用于各种用途的多用预付卡。

在先进国家中，企业银行连线应用智能卡也很普及，公司在内部以终端机与银行展开日常交易业务，智能卡扮演着操作终端机“钥匙”的角色。目前企业银行连线大都以密码作为安全保护功能。一旦企业与银行作完交易后，交易的资料就会及时存入智能卡，企业即可确认交易的正确性。

财产管理也是智能卡的应用之一。在智能卡上储存了个人财产的相关资料，如姓名、各种存款、贷款等，进而提供财产

管理咨询服务，可协助使用者对其财产作更有效的管理与投资。目前在国外的商业交易中，所有的消费行为，包括购物、订位、买票、停车等，皆利用智能卡与银行帐户之间的资料直接转帐。因此，像便利商店，大型饭店和连锁速食店等需大量现金交易的商家，均可借此大幅降低现金处理成本。

由于智能卡具有储存容量大及容易携带的特性，在医疗领域上极具应用价值。目前病人的病历资料大部分散见于各家医院，缺乏快速而有效的流通渠道，当紧急事件发生时，病人家属无法立即取得完整、正确的病历资料。智能卡则可提供有效的解决方案，因为个人的身份证明、健康保险号码、血型、过敏症、健康检查结果、过去及目前所患病症、药物治疗效果以及医生诊断结论等资料，均可储存在其中。

当病人就医时，医生可由智能卡快速地了解病人的基本资料，减少重复检查的项目，提高诊断的效率与准确性。通过智能卡上的个人资料及银行帐号，银行也可自动转帐来缴纳诊疗费。

至于在企业中，智能卡可扮演一个集识别证、通行证、考勤资料于一身的角色。也可通过智能卡发放员工的薪金，储存个人工作资料等。

智能卡在教育领域的应用潜力极大。智能卡可用于学生证、课堂出勤状况记录、选修课程记录、成绩单、借阅图书、缴纳学费、使用学校设施、发行学生折扣票等，因而有利于教育的合理化。由于智能卡储存容量大，可将教材，如英语单词、句型等存入智能卡，学生可随身携带以便各种场合学习之用。

智能卡在交通方面已有许多应用的实例。目前先进国家利用磁卡作为火车车票、高速公路通行费、汽油费、停车费等的支付。譬如停车费，由于普遍使用的停车计时器缺乏智能，

停车者很难正常地估算停留的时间，因此经常不是多投了冤枉钱，就是逾时被罚。

为了解决这类困扰，可把智能卡用作预付停车记费卡，预先设置一定金额度，用完为止。智能卡也可作为驾驶执照，并记录驾驶人税金、检验等资料，而内含密码的智能卡可以替代车辆的钥匙。

由此可见，智能卡具有如此广泛的应用能力，必将成为信息社会的重要工具。

二、全球应用情况

从图 1.3 的全球智能卡应用简图可以看出，应用智能卡最多的国家是法国，应用最广泛的智能卡是银行卡、电话卡和医疗卡。

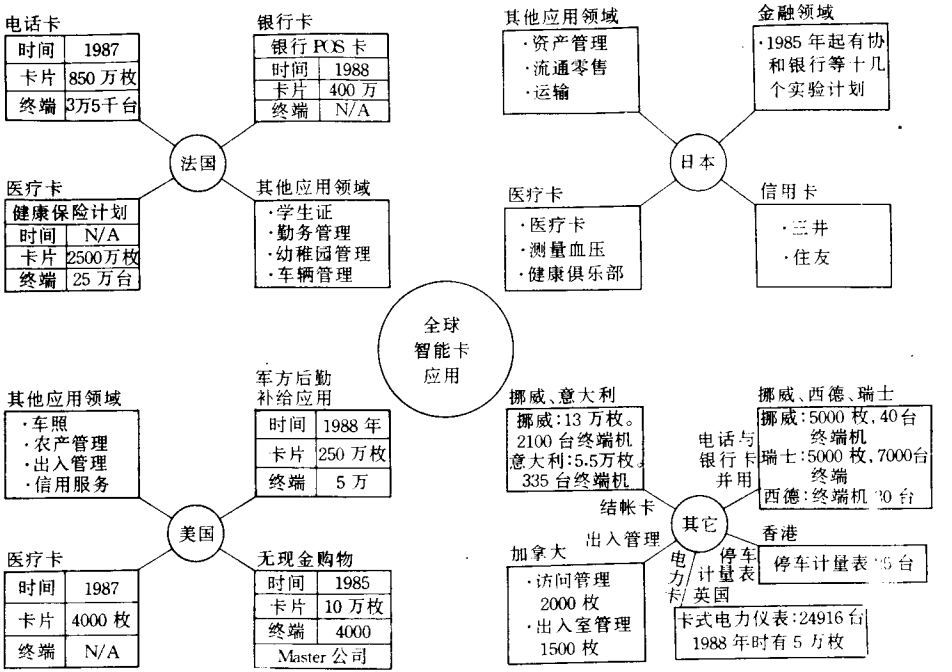

图 1.3 全球智能卡应用简图

第二章　智能卡技术

智能卡技术是指智能卡在整个生命周期内涉及到的技术。它比磁卡技术复杂得多，主要包括三个部分：硬件技术、软件技术和业务知识。硬件技术有半导体技术、制板技术、封装技术、终端技术及其它零组件技术。软件技术有软件技术、通信技术、安全技术和系统技术。

本章重点讨论智能卡的安全技术、智能卡的标准和系统设计技术，并展望智能卡技术的发展趋势。

第一节　硬件技术

一、半导体技术

(一)CMOS 集成电路

CMOS 集成电路是一种功耗低、噪声容限大、电源电压范围宽的新颖半导体集成电路。近年来发展极为迅速，已成为集成电路制造技术发展的主要趋势。数据处理和通信是CMOS 技术应用增长最快的领域，其次便是存储器和微处理器领域。用 CMOS 技术制作的单片机(MCU)是构成智能卡的主要器件。

作为一种工艺，CMOS 兼有 I^2L(集成注入逻辑)的低功耗特性和 NMOS(N 沟道金属氧化物半导体)的高速特性。它的主要特点是：