智能(IC)卡技术全书

于宏军　赵冬艳　编著

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
URL:http://www.phei.co.cn

智能(IC)卡技术全书

于宏军　赵冬艳　编著

電子工業出版社

内 容 提 要

本书详细提供了 IC 卡技术、IC 卡安全技术、智能 IC 卡操作系统、IC 卡标准、IC 卡芯片技术等资料，论述了 IC 卡在国内外的一些技术应用现状及今后的发展趋势，结合我国金卡工程分析、介绍了 IC 卡在我国的一些应用模式及应用前景。另外，书中还介绍了我国在 IC 卡技术、有关设备等方面的一些最新研究、开发成果。本书融理论分析、实用技术、技术资料等为一体，图表数据详实、丰富，易于阅读理解。

本书可作为卡基应用研究开发部门的技术、管理人员，金融、保险、电信、医疗卫生、运输、安全等部门的应用研究人员、管理人员的参考书；也可作为各高等学校有关专业的学生、教师参考书。

智能(IC)卡技术全书

于宏军　赵冬艳　编著

责任编辑　吴浩源　贾　贺

*

电子工业出版社出版(北京市万寿路)

电子工业出版社发行　各地新华书店经销

北京大中印刷厂印刷

*

开本：787×1092 毫米　1/16　印张：21.25　字数：544 千字

1996 年 10 月第 1 版　1996 年 10 月第 1 次印刷

印数：4000　册　　定价：28.00元

ISBN 7-5053-3747-5/TP·1592

前　言

1993 年 6 月 1 日，江泽民总书记在视察人民银行沙河卫星清算总中心时，提出了全民推广使用信用卡，以减少大量的现金流通，加强国家对经济的宏观调控，以“电子货币”工程为重点启动的卡基应用系统工程，即“金卡”工程。

IC 卡作为卡基应用的卡型和磁卡等其它种类卡相比具有很多优越性，在国外已有较为广泛的应用。有关专家预计，IC 卡必将在世界范围内逐步取代磁卡等卡种，在金融、电信、保险等领域有大量的应用，并在我国“金卡”工程中扮演重要角色。

IC 卡进入我国时间较晚，许多人（包括相关专业技术人员）对 IC 卡这一技术尚不了解，人们迫切需要一本较为全面的介绍 IC 卡技术方面的书籍。正基于此，我们编著此书。其中覆盖了 IC 卡软硬件技术、IC 卡标准、IC 卡应用、IC 卡用芯片等各个方面的详细资料。本书图表数据详实、丰富，易于阅读理解。阅读本书之后，相信会对您在 IC 卡的应用、研发领域的工作有重大帮助，这也正是我们所希望的。

本书适用于卡基应用研究开发部门的技术、管理人员，金融、保险、电信、医疗卫生、运输、安全等部门的应用研究人员、管理人员，各高等学校有关专业的学生、教师参考。

由于 IC 卡技术发展十分迅速，新技术、新产品、包括不断完善制订中的 IC 卡国际标准必将层出不穷、不断更新。我们将持续追踪 IC 卡的世界发展潮流，不断为广大 IC 卡应用、研究开发、管理人员提供最新、全面可靠的 IC 卡技术应用资料，以在我国的“金卡”工程中尽微薄之力。

尽管我们付出了相当大的劳动，由于时间仓促，难免出现差错，望读者批评、指教。同时，我们希望通过本书和广大读者建立广泛持久的联系，互相学习，互相促进，共同推动我国 IC 卡事业的发展。

编　者

1995 年 11 月

目　录

第 1 章　IC 卡概述

很久以前，人类就开始使用各种卡片：名片、身份证、通行证，以至现代的信用卡等。人们之所以广泛接受并使用各种卡片，说明它的用途十分广泛，并和人们的日常生活息息相关。随着社会的进步、科学技术的发展，人们期望新型卡片的出现，以满足日常生活、工作以及社会发展的需要。

1970 年，法国人罗兰德·莫瑞诺(Roland Moreno)第一次将可进行编程设置的 IC (Integrated Circuit)芯片放于卡片中，使卡片具有更多的功能。当时他在专利申请书中，对这项发明作了如下阐述：卡片上具有可进行自我保护的存储器。就在同一年，日本人有村国为也发明了集成电路卡，他称这项发明是：卡片内装有一个或多个芯片，可以产生特殊的信号。在此后的时间里，随着超大规模集成电路技术、计算机技术以及信息安全技术等的发展，IC 卡技术也更趋成熟，目前在国外得到了较为广泛的应用。1993 年，各种存储器 IC 卡销量为 2.6 亿张，带有微处理器的智能 IC 卡销量为 3500 万张，预计 96 年将分别达到 8 亿张和 1.5 亿张，年增长率达 40%。

自 IC 卡出现以后，国际上对它有多种叫法。英文名称有“Smart Card”、“IC Card” 等；在亚洲特别是港、台地区，则多称为“聪明卡”、“智慧卡”及“智能卡”等；而在我国，人们一般称之为“IC 卡”或“智能卡”，本文统称为 IC 卡。

1.1　IC 卡基本知识

什么是 IC 卡？目前业界人士尚无统一、全面的定义，但以下三种解释性说明从不同方面描述了 IC 卡。

(1) 外型和信用卡一样，但卡上含有一个符合国际标准化组织(ISO)有关标准的集成电路芯片(IC)。

(2) 由一个或多个集成电路芯片组成，并封装成便于人们携带的卡片；具有暂时或永久性的数据存储能力，其内容可供外部读取或供内部处理、判断；具有逻辑和数学运算处理能力，用于识别和响应外部提供的信息和芯片本身的处理需求。

(3) 实际上，IC 卡就是集成电路卡。它是一种随着半导体技术的发展和社会对信息安全性等要求的日益提高而应运而生的，具有微处理器及大容量存储器等的集成电路芯片且嵌装于塑料等基片上制成的卡片。它的外形与普通磁卡做成的信用卡十分相似，只是略厚一些，具体为：(85.47～85.72) × (53.92～54.03) mm^2，厚 0.76 ± 0.08 mm(ISO 标准)。

“IC 卡”和“磁卡”一样，都是从技术角度起的名字，不能将其和“信用卡”、“电话卡”等从应用角度命名的卡相混淆。例如，信用卡是银行等金融部门发行的一种金融卡，它可以用 IC 卡制成，也可以由磁卡制成，一般用户没必要了解信用卡是用 IC 卡技术还是磁卡技术制成的。

IC 卡上可以印有彩色相片、图案及说明性文字等信息。有的对安全性要求较高的 IC 卡，在其表面上印有个人签名、全息图像及类似纸币上的回纹等安全标识信息。在 IC 卡的左上角

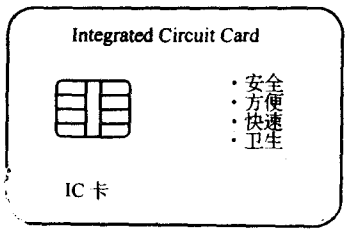

图 1-1 IC 卡示意图

封装有 IC 芯片，其上覆盖有 6 或 8 个触点和外部设备进行通讯，如图 1-1 所示。

按 ISO 标准，部分触点及其定义为：

(1) *Vcc*：IC 卡工作电源；

(2) GND：地；

(3) *Vpp*：存储器编程电源(可选)；

(4) CLK：有关信号的定时与同步；

(5) I/O：IC 卡中串行数据的输入/输出；

(6) RST：复位信号(可选)；

剩余的两个触点视不同情况则可在有关应用标准中予以定义。

1.2 IC 卡的分类

1.2.1 卡片的分类

目前，用于信息处理的卡片基本上都采用了较先进的现代电子技术，可以分成半导体卡和非半导体卡两大类。

非半导体卡有磁卡，PET 卡，光卡，凸字卡等。

(1) 磁卡：将磁条贴在塑料卡片上制成的卡片。现有许多的银行自动提款卡和信用卡均为此种卡片。

(2) PET 卡：卡片的某一整面均涂有磁性物质。现有的许多电话卡，电子自动售票卡均为此种卡片。PET(Polyethylene telephtalate)即聚对苯二甲酸乙二酯。

(3) 光卡：激光卡，利用光进行数据记录，每张光卡上可以存储几兆、几十兆乃至上百兆字节的数字信息且不受电磁干扰、安全可靠。目前，光卡在国外已有部分应用，但应用数量、应用领域却较有限，因为光卡及其读写设备较为昂贵，目前还难以大量应用。我国有关人士正在探讨有关光卡在我国的应用。

(4) 凸字卡：在卡片上刻压有凸字。

IC 卡属于半导体卡。半导体卡片采用微电子技术进行信息的存储、处理。它又可分为有接触点卡和无接触点卡两类。前者由读写设备的触点和卡片上的触点相接触，进行信息的读写；后者则与读写设备无电路接触，由非接触式的读写技术进行读写(例如，光或无线电技术)。

有接触点卡又可分为存储卡和智能卡(带 MPU)两类。存储卡又可分成 RAM 卡(可读写)和 ROM 卡(不可写)两种。IC 卡从不同的角度也有不同的分类，在下面章节中将详细讨论。

预计，随着新技术和新工艺的不断发展、进步，今后还会不断出现新的卡型。

1.2.2 IC 卡分类

一般将 IC 卡从功能上分成存储器 IC 卡，智能 IC 卡(带 MPU 的卡)和超级智能 IC 卡三类。三种 IC 卡的基本特性，在不同国家或地区的称呼及应用领域见表 1-1。

表 1-1　三种 IC 卡的简单定义、称呼及应用领域

		存储器卡	智能卡	超级智能卡
基本特性		由一个或多个集成电路组成，具有记忆功能，个别类型的卡具有简单的安全功能	在卡上具有 MPU、较大容量的存储器(ROM、RAM、EEPROM 等)、安全逻辑、数学运算协处理器等	在卡上具有 MPU 和存储器并装有键盘、液晶显示器和电源，有的卡上还具有指纹识别装置等
称呼	日本	IC Memory Card	Smart Card、智能卡、IC 卡(含 MPU)	N/A
	美国	IC Card、Chip Card	Smart Card	
	法国	N/A	Micro Circuit Card	
	台湾地区	晶片卡、记忆卡、微电路卡、IC 卡	精敏卡、Smart 卡、智慧卡	N/A
应用领域		简单资料的保存、身份证卡、电话卡	电子付款、清帐、信用卡	银行 POS 系统

存储器卡由于价格便宜、开发应用相对简单等原因，目前在各个领域已有大量的应用，一般还可以再分为普通存储器 IC 卡、智能存储器 IC 卡两种。

一般，存储器卡只有“硬件”组成，包括数据存储器、安全控制逻辑等；而智能卡(带 MPU)则由硬件及软件共同组成，包括硬件 MPU、RAM、ROM，软件 IC 卡监控程序或操作系统(IC Card Operating System)等。

此外，还有一种卡将 IC 芯片和磁卡同做在一张卡片上，一般称为“混合卡”。可以认为，它是由磁卡过渡到 IC 卡过程中的一种中间产品。

1.3　IC 卡使用的 IC 芯片

一般 IC 卡所使用的主要芯片分为通用芯片和专用芯片两大类。所谓通用芯片，就是普通的集成电路芯片，如美国 ATMEL 公司的 AT 24C01 两线串行链接协议存储芯片。其出厂时就有两种供货形式，一是封装成集成电路直接提供给最终用户使用，二是以裸芯片的形式提供给 IC 卡生产厂商封装成 IC 卡。裸芯片几乎没有安全性设计，也不完全符合目前 IC 卡的国际标准，但因其开发使用简单、价格便宜，比较适合于初期的对安全性要求不高的 IC 卡应用。所谓专用芯片，就是专为 IC 卡而设计、制造的芯片，如荷兰 Philips 公司的 PCB 2032/2042 芯片。这种芯片符合目前 IC 卡的 ISO 国际标准、具有较高的安全性。本节主要介绍以上芯片所采用的技术种类，有关芯片技术将在以下章节中详细介绍。

IC 卡所使用的专用芯片一般分为存储器芯片和微处理器芯片两大类。存储器卡使用存储器芯片作为卡芯；智能卡则使用微处理器芯片作为卡芯。

IC 卡经常使用的存储器芯片种类及特性见表 1-2。

表 1-2　IC 卡经常使用的存储器芯片种类及特性

存储器类型	功　能
ROM (Read Only Memory)	只读存储器，一次写入后不可更改或删除。一般由芯片制造商进行掩膜写入信息，价格便宜，适合于大量的应用
RAM (Random Access Memory)	随机存取存储器，掉电后信息丢失，卡片上需电源。一般和其它种类的存储器共同使用，作为信息处理时的临时存储
PROM (Programmable ROM)	一次编程多次读出存储器，可由用户编程写入应用信息，价格较便宜，适合于较大量的应用
EPROM (Erasable PROM)	可在紫外线擦除之后写入信息。目前，在 IC 卡中已经很少应用
EEPROM (Electronically EPROM)	电可擦除、写入存储器。目前，在 IC 卡上应用得最多

IC 卡经常使用的微控制器芯片的种类及特性见表 1-3。

表 1-3　IC 卡经常使用的微控制器芯片种类及特性

类　型	功　能	举　例
带加密运算的微控制器 (MPU+CAU)	逻辑控制、管理功能，加密、解密等运算功能	飞利浦公司的 83C852 等
不带加密运算的微控制器(MPU)	逻辑控制、管理等功能	日立公司的 H8 系列等

IC 卡使用的 IC 芯片以带有安全逻辑的存储器芯片和带有加密运算的微控制器芯片最为普遍，这两种芯片的典型逻辑结构见图 1-2 和图 1-3。

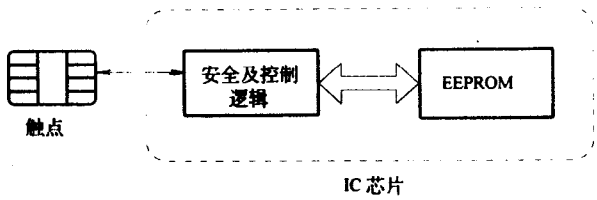

图 1-2　带有安全逻辑的 IC 卡用存储器芯片

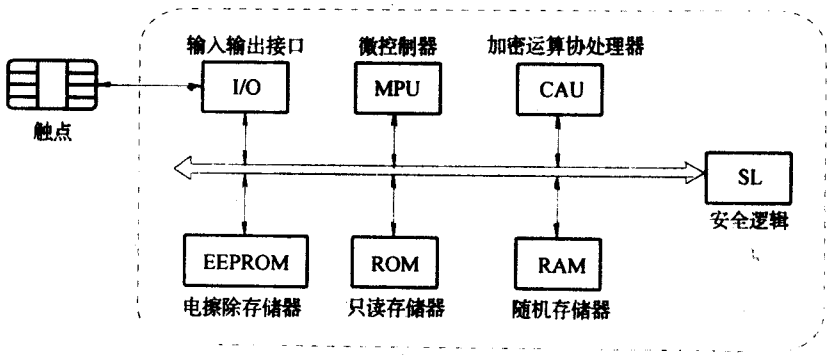

图 1-3　带有加密运算及安全逻辑的 IC 卡用微控制器芯片