

智能(IC)卡技术全书

于宏军 赵冬艳 编著



电子工业出版社

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

电子工业出版社

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	(1)
1.1 IC 卡基本知识	(1)
1.2 IC 卡的分类	(2)
1.2.1 卡片的分类	(2)
1.2.2 IC 卡分类	(2)
1.3 IC 卡使用的 IC 芯片	(3)
1.4 IC 卡的特点及和磁卡等其它卡的性能比较	(5)
1.5 IC 卡技术及其应用系统的组成	(6)
1.5.1 IC 卡技术	(6)
1.5.2 IC 卡应用系统的典型组成	(6)
1.6 IC 卡标准化和专利申请状况	(8)
1.6.1 有关 IC 卡的标准及标准化组织	(8)
1.6.2 有关 IC 卡技术和应用的专利申请状况	(10)
1.7 IC 卡的可靠性分析	(11)
1.8 提高 IC 卡可靠性的一些技术、方法简介	(12)
1.8.1 芯片制造技术和工艺	(12)
1.8.2 IC 卡封装、印刷	(13)
1.8.3 IC 卡读写设备	(13)
1.8.4 持卡人的正确使用	(14)
1.9 IC 卡的生存周期及制造、发行等流程	(14)
1.9.1 IC 卡的生存周期	(14)
1.9.2 IC 卡的制造、发行等流程	(14)
1.9.3 IC 卡的个人化	(16)
第 2 章 IC 卡的安全策略及信息安全技术	(17)
2.1 磁卡应用及其安全性概述	(17)
2.2 IC 卡的安全技术	(18)
2.2.1 IC 卡用芯片的安全技术	(18)
2.2.2 IC 卡卡基表面采用的安全制造技术	(19)
2.2.3 IC 卡软件方面的安全技术	(20)
2.3 IC 卡发行和使用过程中的安全性	(25)
2.3.1 存储器 IC 卡安全性实例分析	(25)
2.3.2 智能 IC 卡安全性实例分析	(26)
2.4 应用于 IC 卡上的生物认证技术简介	(28)
第 3 章 智能 IC 卡操作系统	(29)

3.1 有关智能 IC 卡操作系统的基本概念	(29)
3.2 智能 IC 卡操作系统的主要功能	(30)
3.2.1 硬件资源管理	(30)
3.2.1.1 用户存储器的数据结构	(31)
3.2.1.2 用户存储器的文件组织形式	(31)
3.2.1.3 文件类型及其特性	(32)
3.2.1.4 文件属性	(33)
3.2.2 通讯传输管理功能	(35)
3.2.3 应用控制管理功能	(36)
3.2.4 安全控制管理功能	(37)
3.2.4.1 安全传输控制	(37)
3.2.4.2 内部安全控制管理	(37)
3.3 智能 IC 卡操作系统的信息结构	(40)
3.3.1 信息结构	(40)
3.3.1.1 命令信息结构	(40)
3.3.1.2 响应信息结构	(41)
3.3.2 智能 IC 卡操作系统命令	(42)
3.4 几种典型的智能 IC 卡系统简介	(43)
3.4.1 CP 8 系列智能 IC 卡系统	(43)
3.4.2 STARCOS 智能 IC 卡系列	(45)
3.4.3 COS 系列智能 IC 卡	(45)

第 4 章 密码技术及其在 IC 卡上的应用

4.1 密码技术	(47)
4.1.1 数据加密标准 DES	(48)
4.1.1.1 DES 密码算法	(48)
4.1.1.2 DES 密码的破译	(59)
4.1.1.3 DES 密码反破译的策略	(60)
4.1.1.4 其它分组密码简介	(61)
4.1.2 RSA (Rivest-Shamir-Adleman) 算法	(62)
4.1.2.1 RSA 算法简介	(63)
4.1.2.2 其它公开密钥算法简介	(64)
4.1.3 DSA 算法简介	(64)
4.1.4 密钥管理简介	(65)
4.1.5 密码分析	(66)
4.2 密码技术在 IC 卡上的应用模式	(66)
4.2.1 信息的传输保护	(66)
4.2.2 信息认证	(67)
4.2.3 信息授权	(68)

第 5 章 IC 卡的应用状况及其发展模式

5.1 IC 卡在部分国家或地区的应用发展概况	(71)
5.1.1 IC 卡在德国的应用	(71)

5.1.2 IC 卡在法国的应用	(71)
5.1.3 IC 卡在美国的应用	(72)
5.1.4 IC 卡在日本的应用	(73)
5.1.5 IC 卡在台湾地区的应用	(74)
5.1.6 IC 卡在新加坡的应用	(74)
5.1.7 IC 卡在泰国的应用	(74)
5.2 IC 卡发展模式	(75)
第 6 章 IC 卡应用模式及典型应用	(77)
6.1 健康保险卡	(77)
6.2 IC 卡在电信方面的应用	(78)
6.2.1 IC 卡在电信领域应用的可能性及必要性	(78)
6.2.2 IC 卡在电信领域中应用的几种模式	(79)
6.2.2.1 IC 电话卡	(79)
6.2.2.2 IC 卡和移动电话	(79)
6.2.2.3 IC 卡在电信领域中应用的前景和多样性	(80)
6.3 IC 卡在金融领域的应用	(81)
6.3.1 IC 卡在金融领域应用的必要性	(81)
6.3.2 IC 卡在金融领域的应用模式	(82)
6.4 IC 卡在智能建筑物中的应用	(83)
第 7 章 IC 卡在国内的技术及应用发展概况	(85)
7.1 国内 IC 卡的发展概况	(85)
7.1.1 我国 IC 卡应用概况	(85)
7.1.2 我国 IC 卡技术概况	(86)
7.2 几种典型的中小规模应用简介	(86)
7.2.1 IC 卡门控系统	(86)
7.2.1.1 IC 卡门控系统的组成及结构	(87)
7.2.1.2 IC 卡门控系统的功能及管理特点	(88)
7.2.2 IC 卡电表收费系统	(88)
7.2.3 IC 卡企业职工管理系统	(89)
7.2.4 IC 卡公路收费系统	(91)
7.2.5 IC 卡食堂售饭机	(93)
7.2.6 IC 卡娱乐消费管理系统	(94)
第 8 章 IC 卡和金卡工程	(95)
8.1 目前我国信用卡应用系统的功能	(95)
8.2 信用卡应用系统的需求	(96)
8.2.1 主要功能	(96)
8.2.2 脱机与联机应用	(96)
8.3 金卡工程概况	(97)
8.3.1 金卡工程的总体目标	(98)
8.3.2 金卡工程的实施步骤	(98)

8.3.3 试点阶段工程任务和要求	(98)
8.4 IC 卡在金卡工程中的应用前景	(99)
8.5 IC 卡应用实例	(100)
8.6 维萨国际组织简介	(101)
第 9 章 无接触式 IC 卡	(102)
9.1 射频技术简介	(102)
9.1.1 射频识别技术简介	(102)
9.1.2 射频识别技术的应用	(104)
9.2 无接触式 IC 卡技术及典型应用简介	(104)
9.2.1 无接触式 IC 卡技术简介	(104)
9.2.2 无接触式 IC 卡的典型应用	(105)
9.3 射频识别技术中的应答器	(106)
9.3.1 概述	(106)
9.3.2 PIT 的组成、功能及部分电气参数	(108)
9.3.2.1 PIT 的功能描述	(108)
9.3.2.2 极限值及电气特性	(109)
9.3.3 集成电路部分的功能描述	(112)
9.3.3.1 存储器组织	(112)
9.3.3.2 无接触接口(Contactless Interface)	(114)
9.3.3.3 从 PIF 到基站的数据传输(读模式 Read-Mode)	(114)
9.3.3.4 模式切换(Program - Mode - Check)	(116)
9.3.3.5 从基站到 PIT 的数据传输(编程模式 Program-Mode)	(117)
9.3.4 PIT 上电及逻辑组成	(119)
9.3.4.1 PIT 的上电	(119)
9.3.4.2 PIT 的逻辑组成	(120)
9.4 与 PIT 通讯的基站器件	(121)
9.4.1 概述	(121)
9.4.2 电路主要功能简述	(122)
9.4.3 一些工作参数	(122)
第 10 章 存储器 IC 卡芯片技术	(124)
10.1 通用存储器 IC 卡芯片技术	(124)
10.2 智能存储器 IC 卡芯片技术	(125)
10.2.1 智能存储器中存储区域的技术特点	(125)
10.2.1.1 存储区域的分类及功能	(125)
10.2.1.2 几种典型的智能存储器芯片	(127)
10.2.2 ATR 简述	(128)
10.2.3 有关通讯传输协议简介	(131)
第 11 章 通用存储器 IC 卡芯片技术	(132)
11.1 两线串行链接协议 EEPROM 芯片技术	(132)
11.1.1 概述	(132)

11.1.2 AT 24 系列芯片工作原理	(135)
11.1.2.1 总线状态及时序	(135)
11.1.2.2 器件寻址操作	(135)
11.1.2.3 操作模式	(137)
11.1.3 参数	(139)
11.2 三线串行链接 EEPROM 芯片技术	(141)
11.2.1 概述	(141)
11.2.1.1 主要功能及特点	(141)
11.2.1.2 引脚分配及功能	(142)
11.2.2 工作原理	(143)
11.2.2.1 操作模式	(143)
11.2.2.2 操作时序	(144)
11.2.2.3 操作指令	(147)
11.2.3 工作参数	(148)
第 12 章 面向位操作的智能存储器 IC 卡芯片	(152)
12.1 ATMEL 公司的芯片	(152)
12.1.1 AT 88SC06	(152)
12.1.1.1 主要特性及逻辑结构	(152)
12.1.1.2 存储器组织	(153)
12.1.1.3 个人密码比较	(154)
12.1.1.4 个人化操作	(155)
12.1.1.5 芯片操作模式	(156)
12.1.1.6 有关参数	(157)
12.1.2 AT88SC101/102	(158)
12.1.2.1 主要特性及逻辑结构	(159)
12.1.2.2 封装及 IC 卡触点配置	(159)
12.1.2.3 存储器组织	(160)
12.1.2.4 工作模式	(163)
12.1.2.5 参数	(167)
12.2 Siemens 公司的芯片	(169)
12.2.1 SLE 4406	(170)
12.2.1.1 主要特性及引脚、封装	(170)
12.2.1.2 逻辑结构及存储器组织	(170)
12.2.1.3 计数规则	(171)
12.2.1.4 计数范围	(172)
12.2.1.5 地址设定和读操作	(172)
12.2.1.6 写操作	(172)
12.2.1.7 删除带进位存储器字节	(172)
12.2.1.8 开启过程	(172)
12.2.1.9 参数	(173)
12.2.2 SLE 4436	(175)
12.2.2.1 主要特性及触点配置	(175)

12.2.2.2	功能概述	(176)
12.2.2.3	带有用户状态的存储器组织	(176)
12.2.3	SLE 4404	(177)
12.2.3.1	主要特性及引脚配置	(177)
12.2.3.2	功能概述	(178)
12.2.3.3	功能特性	(178)
12.2.3.4	芯片操作	(179)
12.2.3.5	参数	(180)
12.2.4	SLE 4412	(182)
12.2.4.1	主要特性及触点配置	(182)
12.2.4.2	功能概述	(183)
12.2.4.3	功能特性	(183)
12.2.4.4	器件操作	(183)
12.2.4.5	操作模式	(184)
12.2.4.6	参数	(185)
12.3	Philips 公司的芯片	(186)
第 13 章	面向数据存储的智能存储器 IC 卡芯片	(193)
13.1	ATMEL 公司的 AT88SC200 智能存储器	(193)
13.1.1	主要特性及逻辑结构	(193)
13.1.2	触点配置	(194)
13.1.3	功能概述	(194)
13.1.4	参数	(195)
13.2	Siemens 公司的智能存储器芯片	(195)
13.2.1	Siemens 公司的 SLE 4432/4442	(195)
13.2.1.1	特性	(195)
13.2.1.2	功能概述	(196)
13.2.1.3	逻辑结构及功能描述	(196)
13.2.1.4	传输协议	(197)
13.2.1.5	命令模式	(197)
13.2.1.6	处理模式	(198)
13.2.1.7	数据输出模式	(199)
13.2.1.8	PSC 的用法(仅 SLE 4442)	(199)
13.2.1.9	复位	(200)
13.2.1.10	命令格式	(200)
13.2.1.11	工作参数	(201)
13.2.2	Siemens 公司的 SLE 4418/4428	(203)
13.2.2.1	主要特性	(203)
13.2.2.2	功能描述	(204)
13.2.2.3	操作命令	(205)
13.2.2.4	复位	(207)
13.2.2.5	工作参数	(208)
13.3	Philips 公司的 PCB 2032 / 2042	(209)

13.3.1.1	主要特点	(209)
13.3.1.2	功能概述	(209)
13.3.1.3	引脚信息	(209)
13.3.1.4	功能描述	(210)
13.3.1.5	复位模式	(216)
13.3.1.6	工作参数	(216)
第 14 章	智能 IC 卡芯片技术	(218)
14.1	ATMEL 公司的 AT88SC54C	(219)
14.1.1.1	主要功能及特性概述	(219)
14.1.1.2	逻辑结构及其功能说明	(220)
14.1.1.3	公共密钥算法协处理器	(221)
14.1.1.4	串行编程接口	(222)
14.1.1.5	工作参数	(224)
14.2	Siemens 公司的智能 IC 卡芯片技术	(225)
14.2.1	8 位安全控制器 SLE 44C40	(225)
14.2.1.1	主要功能及特性	(225)
14.2.1.2	EEPROM 技术	(225)
14.2.1.3	安全特性	(226)
14.2.1.4	芯片管理系统(CMS)	(226)
14.2.1.5	封装类型及 IC 卡触点配置	(226)
14.2.2	8 位安全控制器 SLE 44C80	(226)
14.2.2.1	主要功能及特性	(226)
14.2.2.2	EEPROM 技术特性	(227)
14.2.2.3	安全特性	(227)
14.2.2.4	芯片管理系统(CMS)的主要功能	(228)
14.2.2.5	封装形式及 IC 卡触点配置	(228)
14.2.3	带加密协处理器的 8 位微处理器 Siemens SLE 44C200	(228)
14.2.3.1	主要功能及特性	(228)
14.2.3.2	加密协处理器的主要特性	(229)
14.2.3.3	EEPROM 的主要技术特性	(229)
14.2.3.4	CMS/CCMS 系统的主要特性	(229)
14.2.3.5	封装形式及 IC 卡的触点配置	(229)
14.3	Philips 公司的 8 位安全微控制器 83C852	(229)
14.3.1.1	主要特性及功能概述	(230)
14.3.1.2	功能描述	(231)
14.3.1.3	特殊功能寄存器	(250)
14.3.1.4	指令集	(252)
14.3.1.5	ISO 有关 IC 卡的参数信息	(256)
14.3.1.6	有关工作参数	(257)
14.4	MOTOROLA 公司的智能 IC 卡芯片	(258)
14.4.1.1	主要功能及特性	(259)
14.4.1.2	引脚功能描述	(260)

14.4.1.3 存储器组织映象及有关功能描述	(261)
14.4.1.4 安全特性	(265)
14.4.1.5 电气参数	(265)
第 15 章 I²C 总线技术	(271)
15.1 I ² C 总线技术概述	(271)
15.1.1 I ² C 总线出现的前提及必然性	(271)
15.1.2 I ² C 总线的基本概念	(272)
15.1.3 一般特性	(273)
15.1.4 位传送及数据的有效性	(274)
15.1.5 开始和结束信号	(274)
15.2 I ² C 总线的数据传送	(275)
15.2.1 字节格式	(275)
15.2.2 响应(确认)	(275)
15.3 总线仲裁和时钟同步	(276)
15.3.1 时钟同步	(276)
15.3.2 总线仲裁(竞争)	(276)
15.3.3 利用时钟同步机制作为一种握手信号	(277)
15.4 数据格式	(278)
15.5 寻址	(279)
15.5.1 第一个字节各位的定义	(279)
15.5.2 广播呼叫地址	(280)
15.5.3 开始字节	(281)
15.5.4 CBUS 兼容性	(282)
15.6 总线定时	(282)
15.7 低速方式	(283)
15.8 I ² C 总线规范的扩展	(284)
15.8.1 高速模式	(285)
15.8.2 10 位寻址	(286)
15.8.2.1 第一、二字节中的有关位定义	(286)
15.8.2.2 具有 10 位地址的数据格式	(286)
15.8.2.3 通用呼叫地址和起始字节	(288)
15.8.3 高速模式器件的电流增减控制输出级	(288)
15.8.4 高速模式器件的开关上拉电路	(288)
15.8.5 高速模式下电阻 R_P 和 R_S 的参数选择	(289)
15.9 串行总线的走线结构	(291)
15.10 I ² C 器件输入输出电气特性	(291)
15.11 I ² C 总线的电气规范和有关时序	(293)
15.12 I ² C 器件的主要种类及地址分配	(295)
15.12.1 I ² C 器件的主要种类	(295)
15.12.2 I ² C 总线的地址分配	(296)
15.13 时钟/日历和 RAM 芯片 PCF 8583	(298)

15.13.1 主要功能概述	(299)
15.13.2 引脚功能定义及有关技术参数	(299)
第 16 章 IC 卡的国际标准	(301)
16.1 IC 卡标准分类及简介	(301)
16.1.1 IC 卡标准的分类	(301)
16.1.2 有关 IC 卡标准简介	(302)
16.1.2.1 有关标准化组织	(302)
16.1.2.2 IC 卡技术及应用的部分主要标准	(303)
16.2 IC 卡国际标准 ISO/IEC 7816	(304)
16.2.1 ISO 7816-1	(305)
16.2.2 ISO 7816-2	(308)
16.2.3 ISO/IEC 7816-3	(310)
主要参考文献	(326)

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) 外形和信用卡一样,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: $(85.47 \sim 85.72) \times (53.92 \sim 54.03) \text{ mm}^2$, 厚 $0.76 \pm 0.08 \text{ mm}$ (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

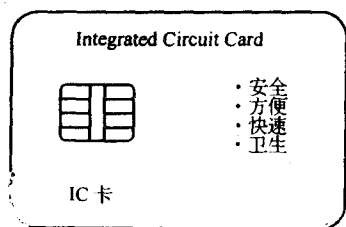


图 1-1 IC 卡示意图

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) V_{cc} : IC 卡工作电源;
- (2) GND: 地;
- (3) V_{pp} : 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 telephthalate)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 and 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、EEP-ROM 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 ATIMEL 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 (Erassable 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 FB 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。

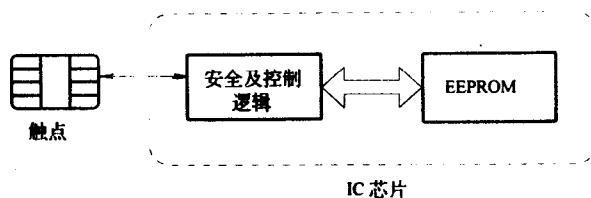


图 1-2 带有安全逻辑的 IC 卡用存储器芯片

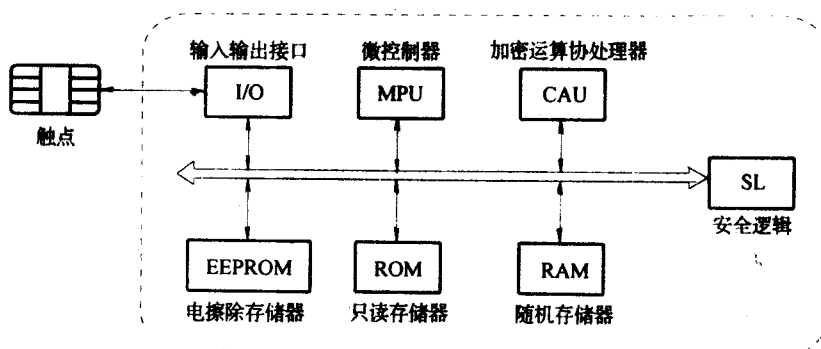


图 1-3 带有加密运算及安全逻辑的 IC 卡用微控制器芯片