电子信息类新技术丛书

智能卡技术

邹俊伟 著

北京邮电大学出版社
www.buptpress.com

智能卡技术

邹俊伟　著

北京邮电大学出版社
www. buptpress. com

内 容 简 介

智能卡(Smart Card)是一种具有微处理器和存储器等微型集成电路芯片的标准规格卡片。智能卡已应用到银行、电信、交通、社会保险、电子商务等领域,具有极高的安全、保密、防伪能力。本书对智能卡的相关国际标准、接触式智能卡、CPU 卡、Java 卡、非接触式智能卡以及智能卡安全技术进行了较为全面的论述,并给出了相关实验指导和示例程序,使读者掌握智能卡的基本原理、相关标准、应用技术和智能卡开发技术。

本书可作为高校电子信息专业及相关专业本科生的教材,也可作为从事智能卡技术的有关工程技术人员的参考书。

图书在版编目(CIP)数据

智能卡技术/邹俊伟著. --北京:北京邮电大学出版社, 2012.8

ISBN 978-7-5635-3206-3

Ⅰ. ①智… Ⅱ. ①邹… Ⅲ. ①IC 卡 Ⅳ. ①TN43

中国版本图书馆 CIP 数据核字(2012)第 205233 号

书　　名:智能卡技术

作　　者:邹俊伟

责任编辑:何芯逸

出版发行:北京邮电大学出版社

社　　址:北京市海淀区西土城路 10 号(邮编:100876)

发 行 部:电话:010-62282185　传真:010-62283578

E-mail:publish@bupt.edu.cn

经　　销:各地新华书店

印　　刷:北京联兴华印刷厂

开　　本:720 mm×1 000 mm　1/16

印　　张:7

字　　数:126 千字

版　　次:2012 年 8 月第 1 版　2012 年 8 月第 1 次印刷

ISBN 978-7-5635-3206-3　　定　价:20.00 元

前　言

智能卡(Smart Card),是一种带有微处理器和存储器等微型集成电路芯片的、具有标准规格的卡片。智能卡已应用到银行、电信、交通、社会保险、电子商务等领域,IC 电话卡、金融 IC 卡、社会保险卡和手机中的 SIM 卡都属于智能卡的范畴。

本书主要讲述了智能卡技术的理论和实践,全书共分 8 章,第 1 章介绍智能卡概述;第 2 章全面总结了智能卡相关国际标准,主要包括国际标准化组织(International Standard Organization,ISO)和国际电子技术委员会(International Electrotechnical Commission,IEC)的相关标准;第 3 章介绍了接触式智能卡技术,包括接触式智能卡的芯片技术和接口设备;第 4 章介绍了 CPU 卡技术,主要包括 CPU 卡的基础知识、逻辑结构和 COS 系统;第 5 章重点介绍了 Java 卡技术,主要包括 Java 的基础知识、Java 卡的系统结构、Java 的生命周期以及 Java 的应用开发等;第 6 章介绍了非接触智能卡技术,主要主要介绍了 MIFARE 卡;第 7 章主要介绍了智能卡安全技术,包括密钥管理系统、智能卡安全访问机制和智能卡的安全使用;第 8 章介绍了相关实验安排和指导。最后,给出了 Java 卡示例程序。

本书取材广泛,理论联系实际,讲解深入浅出,可以作为通信与信息类和电子科学与技术类专业高年级本科生的参考书,也可供从事相关领域研发工作的工程技术人员参考。

在本书的撰写过程中,得到了所在研究室的教师和部分研究生的支持和帮助,在此表示深深的谢意。

由于作者水平所限,加之时间仓促,错误和不妥之处恳请广大读者批评指正。

作　者

2012 年 7 月

目　录

第 1 章　智能卡概述

智能卡(Smart Card) 是指内嵌有微芯片的一种便携式塑料卡的通称。卡内的集成电路包括中央处理器(CPU)、可编程只读存储器(E^2PROM)、随机存储器(RAM)和固化在只读存储器(ROM)中的卡内操作系统(Chip Operating System,COS)。这些组件提供了资料的运算、存取控制及储存功能。

1.1　智能卡基础知识

1. 什么是智能卡

智能卡的名称来源于英文名词“smart card”,又称集成电路卡,即 IC(Integrated Circuit)卡(如图 1-1 所示)。IC 卡将集成电路芯片嵌入塑料基片中,封装成卡的形式。严格来说,只有具备 CPU 的 IC 卡才是真正的智能卡,但在很多应用场景中也使用 IC 卡代替智能卡的名称。

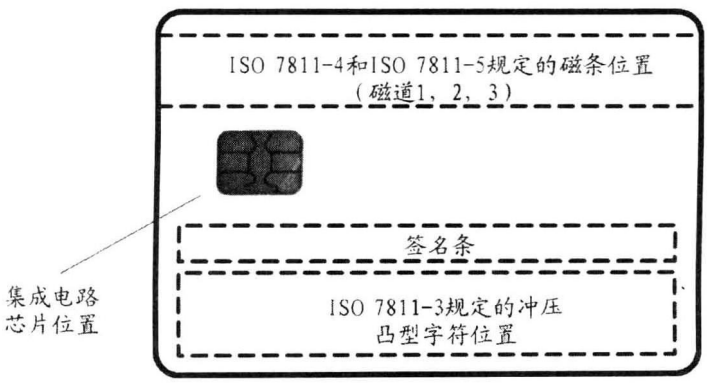

图 1-1　IC 卡的外观图

智能卡因配备有 CPU 和 RAM,可自行处理数量较多的数据而不会干扰到主机 CPU 的工作。智能卡还可过滤错误的数据,以减轻主机 CPU 的负担,适应于端

口数目较多且通信速度需求较快的场合。卡中数据分为外部读取和内部处理部分。卡片的大小、接点定义目前是由 ISO 规范统一，主要规范在 ISO 7816 中。常见的有电话 IC 卡、身份 IC 卡，以及一些交通票证和存储卡。

2. IC 卡发展史

1950 年，美国开始使用塑料卡体，而原先使用的纸板卡体被逐渐淘汰。第 1 代卡功能简单，称为凸码卡；第 2 代卡被称为磁卡，数据以可读的形式存储在卡的磁条内，作为可视数据的补充；第 3 代卡被称为 IC 卡，能将集成电路结合到识别卡中。

- 1972 年 Roland Mereno(法)提出 IC 卡设想；
- 1976 年 Bull 公司(法)研制第一张 IC 卡，开始微电子技术与计算机结合的应用；
- 1991 年全球 IC 卡发行突破 1 亿张；
- 1993 年中国政府启动金卡工程；
- 2000 年中国 IC 卡发行量达 2.3 亿张；
- 截至 2003 年年底，全球 IC 卡发行总量达 63 亿张；
- 截至 2007 年年底，中国 IC 卡发行总量达 40 亿张；
- 截至 2009 年年底，中国各类 IC 卡发行总量达 70 亿张。

3. IC 卡的分类

IC 卡按集成电路类型分存储器卡、逻辑加密卡和 CPU 卡。存储卡中的集成电路为 E^2PROM 的称为存储器卡；卡中的集成电路为加密逻辑＋E^2PROM 的称为逻辑加密卡；卡中的集成电路包括中央处理器 CPU、E^2PROM、RAM 以及 ROM 的称为 CPU 卡。实质为单片机的嵌入式应用。

IC 卡按用途分为金融卡和非金融卡。金融卡指信用卡和储蓄卡，信用卡(借贷卡)一般由银行发行和管理，作为支付工具，可按预先设定额度透支。储蓄卡(借记卡)又称现金卡，作为电子钱包或者电子存折，不能透支。非金融卡包括身份证、社保卡、交通卡等。非金融卡主要用于各种事物管理。

IC 卡按卡与外界数据传送的形式分接触式 IC 卡和非接触式 IC 卡。接触式 IC 卡通过 IC 芯片上的 8 个触点与外界相连，进行数据的读、写。非接触式 IC 卡又称射频卡，卡与外部无触点接触，通过射频技术实现非接触式的数据通信。卡内带有射频收发电路。此外，还有双界面卡，即将接触式 IC 卡与非接触式 IC 卡组合到一张卡中，集两者优点于一身。

1.2　智能卡应用基础

1. IC 卡存储区的分配和功能简介

IC 卡一般分四个存储区：公开区、不可读存储区、保密存储区和记录区。公开区（不保密的存储区）内含公用信息，如发行标识符、持卡人账号等。外部不可读存储区仅供内部使用，如 PIN 值、密钥，一般不允许将 PIN 值向外界传送。保密存储区含账面余额、卡使用的服务类型及限额，允许读取数据进行交易，并修改（如余额等）。记录区内含交易细节，称为日志，可供查询。

2. IC 卡应用系统

由 IC 卡、IC 卡接口设备、PC、网络、后台主机组成，如图 1-2 所示。IC 卡由持卡人掌管，记录有持卡人的特征代码、文件资料的便携式信息载体；IC 卡接口设备（Interface Device，IFD），或称为读写设备/读写器，配合 IC 卡工作，是卡与 PC 进行信息交换的桥梁以及 IC 卡的能量来源。IFD 可以是一个由微处理器、键盘、显示器与 I/O 接口组成的独立设备。PC 是系统的核心，完成信息汇总、统计、计算、处理、报表生成输出和指令的发放、系统的监控管理以及卡的发行、挂失、黑名单的建立等。在金融服务等相对大的系统中，网络是使前端 PC 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。后台系统/主计算机保存所有参与系统的银行和持卡人账目，并登记所有到来的交易数据，同时它还能控制所有后方勤务的处理（分发新黑名单、发送软件更新给终端等）。IC 卡应用举例如图 1-3 所示。

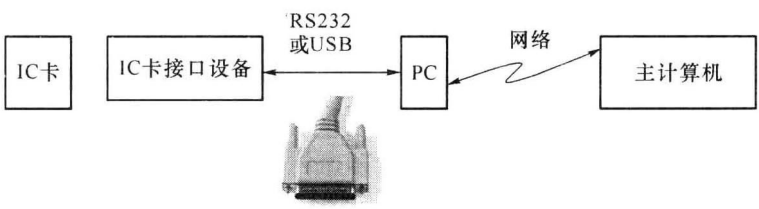

图 1-2　IC 卡应用系统

3. IC 卡的生存周期

IC 卡的生存周期主要包括制造、发行、应用、回收。制造指芯片与卡的制造；发行指具有应用功能的卡的发行；应用指持卡人在特定部门管理下的使用；回收指回收处理损坏卡、失效卡。

一般来说，卡制造商提供的卡都是仅具备基本软、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。

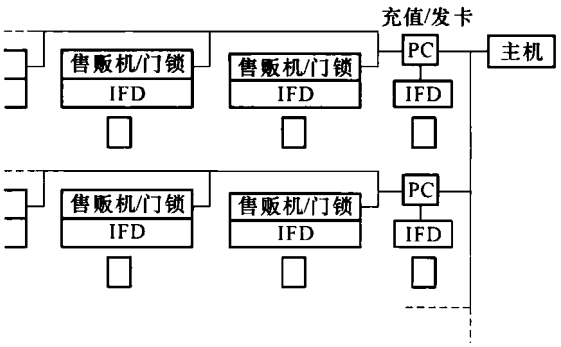

图 1-3　应用举例

4. 金融卡的用卡过程

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,诸如账户金额、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账号作为索引信息,方便在数据库中迅速找到用户数据。例如,某银行(发卡行)核对客户账目后,发给客户一张储蓄卡,卡内存有该客户的账号。客户持该卡到某商店(受卡方)购物的操作顺序如下所示。

① 将卡插入商店的 POS 机中。

② 售货员通过他本人工作的键盘输入交易金额,并提示客户输入 PIN。

③ 客户输入 PIN 后,POS 机读出卡中磁条上的数据(如客户账号),并通过网络将客户账号、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账号(查对黑名单),同时核对客户的账面记录,查明可供支配的金额,核对 PIN,以确认持卡人是否是卡的主人。

④ 核查客户账号和 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 机将客户账号、所购物金额数记录下来,给客户打印收据。客户取走商品和卡。

⑤ 在适当的时间(如晚上),商店的开户银行(代理方)就会通过信息交换系统与发卡的银行联系,发卡银行根据代理方发来的交易细节将交易金额转入商店在开户银行的账户,整个交易过程结束。

使用磁卡金融卡的特点包括:

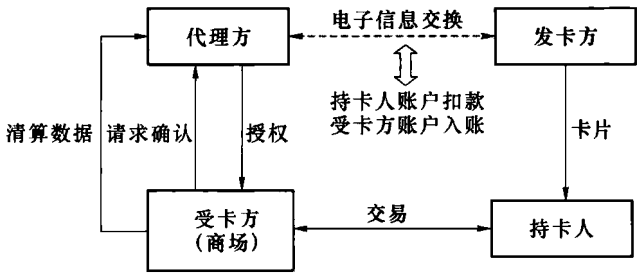

图 1-4　磁卡金融卡完成一次购物的过程示意图

• 磁卡的应用需有其他条件的支持，如强大可靠的计算机网络系统、中央数据库等，且受限于网速。

• 磁卡中磁条存储容量小。

• 磁条容易读出和伪造，保密性差。

某银行（发卡方）发给客户一张 IC 卡储蓄卡，卡内存有客户账号，银行接受客户上交的现金后在不可读存储区写入客户 PIN 码，在保密存储区写入账面余额等，完成卡的个人化。客户持 IC 卡储蓄卡到某商店（受卡方）去购物的操作顺序如下：

① 将储蓄卡插入商店的 POS 机中。

② 售货员通过他本人工作的键盘输入交易金额，并提示客户输入 PIN。

③ 客户输入 PIN 后，由 POS 机自动与智能卡中存储的 PIN 号相比较，如比较一致，准备受理交易。

④ POS 机内部进行如下处理：读出卡中账号，并与 POS 机中的黑名单进行比对；读出卡中余额，核实资金是否够用；计算交易后余额，修改卡中余额；将交易金额登入 POS 机的交易日志记录，同时把这笔交易记录也写到储蓄卡中。给客户打印收据后，客户取走商品和卡。

⑤ 在适当的时间（如晚上），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，发卡银行根据代理方发来的交易细节将交易金额转入商店在开户银行的账户，整个交易结束。

使用 IC 卡金融卡的优点在于：IC 卡容量大、保密性好，持卡人的账目信息可直接存储在卡中，受卡方只需查看卡中的信息并直接在卡中处理交易，过一段时间受卡方再同异地银行进行清算。方便了用户，缩短了交易时间。表 1-1 介绍了磁卡和 IC 卡用作金融卡的区别。

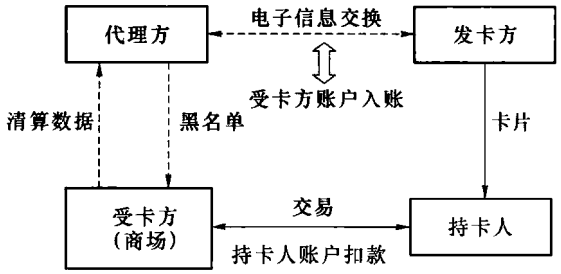

图 1-5　用 IC 卡金融卡完成一次购物的过程示意图

表 1-1　磁卡与 IC 卡用作金融卡的区别

项目	磁卡	智能卡
是否联机	是	否
网络实时性要求	高	低
账号存放位置	磁条	芯片
黑名单存放位置	后台数据库	POS 机/后台数据库
PIN 存放位置	后台数据库	卡中/后台数据库
余额/交易记录存放位置	后台数据库	卡中/后台数据库
特点	磁条容量小，安全性差，受限于网速； 采用集中式数据处理方式	容量大，保密性好，交易时间短； 采用分布式数据处理方式

1.3　智能卡的安全问题

智能卡系统拥有其他卡系统无法比拟的安全可靠性，它集成了当今较为先进、成熟的诸多安全技术和研究成果，已成为实现信息安全存储和传输的重要屏障。

1. 信息安全需具备的特性

保证数据信息在确定的时间、确定的地点和条件下只能被确定的人所使用。需要具有：保密性(Confidentiality)、完整性(Integrity)、真实性(Authenticity)和持久性(Durability)。

2. 威胁信息安全的因素

客观因素主要表现为对信息载体的干扰、破坏等，如静电、辐射、腐蚀、温度、湿度等因素。英文术语称为“Safety”，关系到信息的持久性。

人为因素具有主动性及蓄意性，英文术语称为“Security”，是对信息安全的主

要威胁，关系到信息的机密性、完整性及真实性等。人为因素对智能卡信息安全的威胁主要包括：截取智能卡与读写器间的信息流，分析、复制或插入假信号；使用伪造卡；交易过程中更换卡等。

3. 智能卡的安全技术

智能卡的安全技术包括芯片的安全技术、卡片的安全制造技术和智能卡软件的安全技术。

1.4　智能卡的应用领域

智能卡主要在电信领域，身份证领域；交通领域，商业及服务业领域，医疗、保健等领域，金融领域，门禁系统等领域有着广泛的应用。

(1) 电信领域

智能卡在电信领域的应用主要包括公用电话卡和移动电话卡。

(2) 身份证领域

第二代身份证于 2004 年起正式在几个城市换发，当年仅发行 400 万张。截至 2005 年年底，国内累计换发第二代身份证达 1 亿多张，开始影响我国 IC 卡的整体市场。截至 2009 年年底，制发第二代居民身份证超过 10 亿张。

(3) 交通领域

随着公交卡应用的推广，城市公共交通领域(含公交、出租、轮渡、轨道等)的 IC 卡得到了市民的欢迎。

(4) 门禁系统

(5) 商业及服务业领域

(6) 金融领域

目前国内银行绝大多数使用磁卡，只有少数卡种使用 IC 卡(如牡丹交通 IC 卡)。

中国银联是经中国人民银行批准、由 80 多家国内金融机构于 2002 年 3 月共同发起设立的股份制公司，注册资本 16.5 亿元人民币，总部设在上海。“银联”卡是由国内各发卡金融机构发行，采用统一业务规范和技术标准，可以跨行跨地区使用的带有“银联”标识的银行卡。

VISA(维萨)是目前世界上最大的信用卡组织，由国际上各银行会员组成，无股份，属于非营利机构，总部设在美国加利福尼亚州旧金山。

MASTER(万事达)是全球第二大信用卡国际组织。管理总部设在美国纽约市。

(7) 医疗、保健等领域

第 2 章　IC 卡国际标准

在信息技术领域，国际标准化组织(International Standard Organization，ISO)和国际电子技术委员会(International Electrotechnical Commission，IEC)共同建立了一个技术委员会，即 ISO/IEC JTC1，被该委员会所采纳的国际标准草案由各国家团体投票，被发布作为国际标准至少需要得到 75%参加投票的国家团体的赞成。

2.1　概述

1. 接触式 IC 卡

所谓接触式 IC 卡，就是在使用时，通过有形的金属电极触点将卡的集成电路与外部接口设备直接接触连接，提供集成电路工作的电源并进行数据交换的 IC 卡。其特点是在卡的表面有符合 ISO/IEC 7816 标准的多个金属触点。

接触式 IC 卡国际标准的总名称为：识别卡——接触式集成电路卡；国际标准为 ISO/IEC 7816。

- ISO 7816-1 规定了它的物理特性。
- ISO 7816-2 规定了它的触点尺寸和位置。
- ISO/IEC 7816-3 规定了它的电信号和传输协议。
- ISO/IEC 7816-4 规定了它的行业间交换用命令。
- ISO/IEC 7816-5 规定了它的应用标识符号系统和注册过程。
- ISO/IEC 7816-6 规定了它的行业间数据元。
- ISO/IEC 7816-7 规定了它的关于结构化卡询问语言的行业间命令。
- ISO/IEC 7816-8 规定了它的与安全有关的行业间命令。
- ISO/IEC 7816-9 规定了它的附加的行业间命令和复位应答。
- ISO/IEC 7816-10 规定了它的用于同步卡的电信号和复位应答。

2. 非接触式 IC 卡

非接触式 IC 卡，又称射频卡、感应卡，通信时不需要触点接触。非接触式 IC 卡由 IC 芯片和感应天线组成，并完全密封在一个标准尺寸的卡片中，无外露部分。非接触式 IC 卡的读、写通过射频电磁波的发射与接收来完成。非接触式 IC 卡的国际标准主要包括：

- ISO/IEC 10536。
- ISO/IEC 14443。
- ISO/IEC 15693。

3. 与应用相关的标准

在卡片国际标准的基础上，国内的行业监管部门都在此基础上制定了多个行业应用规范，指导本行业的智能卡应用发展，具体包括：

- 中国金融集成电路(IC)卡规范(1998 年)。
- 社会保障(个人)卡规范(2000 年)。
- 中国石化加油集成电路(IC)卡应用规范(2001 年)。

2.2　接触式 IC 卡的物理特性(ISO 7816-1)

接触式 IC 卡的基本构成如图 2-1 所示。

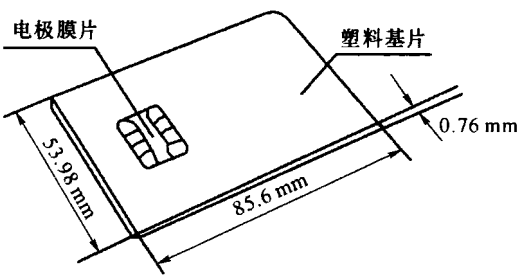

图 2-1　接触式 IC 卡的基本构成

此外，还提出了一些附加特性，具体包括：防护紫外线的能力，X 光照射的剂量，触点的表面轮廓，卡和触点的机械强度，触点电阻，磁条与集成电路之间的电磁干扰，指定强度磁场的影响，静电影响，热耗等。

2.3 接触式 IC 卡的触点尺寸和位置(ISO 7816-2)

接触式 IC 卡有 8 个触点(如图 2-2 所示),即集成电路引脚,为 C1～C8。国际标准 ISO/IEC 7816-2 对接触式集成电路卡的触点尺寸和芯片位置以及功能作了具体的规定。表 2-1 详细介绍了接触式 IC 卡各触点的功能。

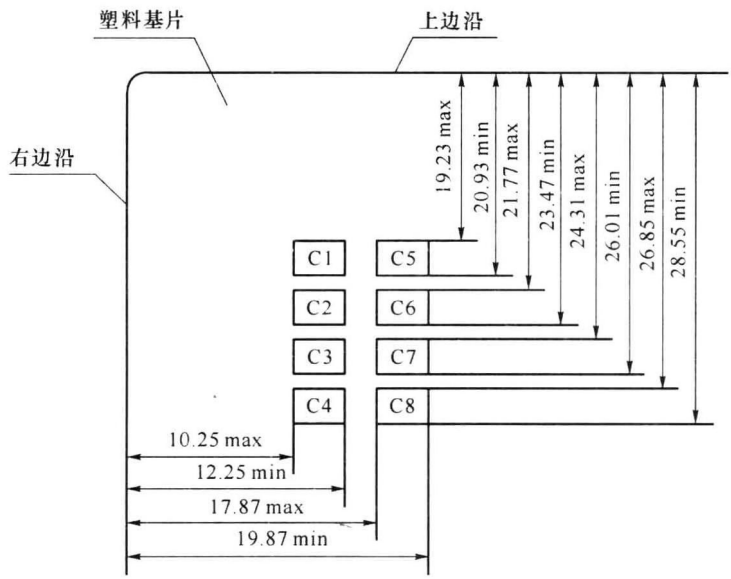

图 2-2 接触式 IC 卡的触点

表 2-1 接触式 IC 卡的触点功能

触点编号	功能
C1	Vcc(电源电压)
C2	RST(复位信号)
C3	CLK(时钟)
C4	ISO/IEC JTC1/SC17 保留使用
C5	GND(地)

续 表

触点编号	功能
C6	V_{pp}(编程电压)
C7	I/O(数据输入/输出端)
C8	ISO/IEC JTC1/SC17 保留使用

2.4 行业间交换用命令(ISO 7816-4)

ISO7816-4 规定的行业间交换用命令包括:在接口设备与 IC 卡之间传送的命令和应答信息的内容、在卡中的文件和数据的访问方法、定义在卡中的文件和数据访问权限的安全结构、安全报文的交换方法等。

2.4.1 数据结构

1. 文件的组织结构

文件的组织结构如图 2-3 所示。

- 主文件(Master File,MF)根文件,必有。
- 专用文件(Dedicated File,DF),可选。
- 基本文件(Elementary File,EF),可选。

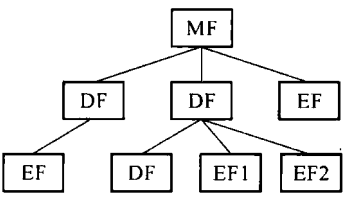

图 2-3 文件的组织结构

基本文件的结构如图 2-4 所示。

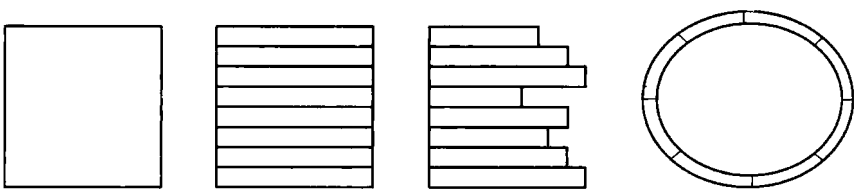

图 2-4 基本文件的结构