第二版

王爱英　主编

智能卡技术

—IC卡—

清华大学出版社
http://www.tup.tsinghua.edu.cn

智能卡技术

—IC卡—

（第二版）

王爱英　主编

清华大学出版社

(京)新登字 158 号

内 容 简 介

智能卡是一种集成电路卡(IC card),以电子货币形式流通于市场,也可用作身份证明或健康卡。它继承了磁卡以及其他 IC 卡的所有优点,并有极高的安全、保密、防伪能力。本书对三种 IC 卡(存储器卡、逻辑加密卡和智能卡)和磁卡的物理结构、逻辑特性、实现技术和应用系统等进行了较为全面的论述,较详细地阐明了有关的国际标准、安全保密体制和读写设备(读卡器)等,并以自动柜员机 ATM 和销售点终端 POS 为重点介绍了卡的应用技术和应用系统。

本书对从事 IC 卡及其配套设备的设计、维护、制造的工程技术人员,以及从事与卡有关的应用系统的开发工作人员很有帮助。本书编写简明、易懂,因此也可作为高等院校师生以及有关工程技术人员、金融界人士的学习参考书。

图书在版编目(CIP)数据

智能卡技术:IC 卡/王爱英主编.—2 版.—北京:清华大学出版社,2000
ISBN 7-302-03971-2

Ⅰ.智… Ⅱ.王… Ⅲ.集成电路-磁卡片 Ⅳ.TP333.3

中国版本图书馆 CIP 数据核字(2000)第 35189 号

出版者:清华大学出版社(北京清华大学学研大厦,邮编 100084)
http://www.tup.tsinghua.edu.cn
印刷者:清华大学印刷厂
发行者:新华书店总店北京发行所
开 本:787×1092 1/16 印张:23.25 字数:535 千字
版 次:2000 年 10 月第 2 版 2000 年 10 月第 1 次印刷
书 号:ISBN 7-302-03971-2/TP·2324
印 数:10001～15000
定 价:29.00 元

前　言

1995 年清华大学计算机科学与技术系师生在从事 IC 卡的集成电路设计和读写设备的设计制造过程中，深切感到国内这项工作尚处在起步阶段，无论是资料、设备和开发工具都很缺乏；另一方面又感到凭我们国内的计算机系统的设计制造水平和半导体工艺水平，完全能将 IC 卡及其配套设备的设计制造任务承担起来。“金卡工程”规划用 10 年左右时间，在全国 400 个城市的 3 亿人口中推广应用卡基支付系统，应用范围普及银行、商业、旅游、饭店以及各种预收费系统等，而且会永无止境地开发新的应用系统。因此，在全国将需要一大批有相应技术水平的人来从事各类卡及其配套设备和应用系统的设计、开发、制造、发行、维护和服务工作。为了适应这一需要，我们在收集资料的基础上经过消化、吸收、补充、提高，于 1996 年 1 月整理出版《智能卡技术》一书。后来用该书作为教材，为清华大学学生开了两次课，另外还向社会开办了两次培训班。

4 年过去了，IC 卡的应用无论在国外和国内都得到了前所未有的迅速发展，与此相适应的新的国际标准和国内标准不断涌现，作者通过几年的工作和学习，对 IC 卡的认识不断深入，于是萌发了修订《智能卡技术》一书的想法，在清华大学出版社的大力支持下，《智能卡技术》(第二版)终于与读者见面了。

清华大学计算机科学与技术系先后参与 IC 卡研制工作以及为本书原著出过力的研究生有张力同、孙军、陈华、汤斌浩和顾清等，现在他们都已奔赴各自工作岗位，这次修订工作主要由王爱英完成，但是没有他们的努力，原书的质量得不到保证，也就不会有第二版了。

本次修订工作除了对原书各章进行了修改和充实以外，还增加了三章，它们是非接触式集成电路(IC)卡的国际标准、IC 卡的测试标准和中国金融集成电路(IC)卡规范。这也反映了 IC 卡的发展动向，即 IC 卡从接触式向非接触式方向发展，金融卡由磁卡向 IC 卡过渡，同时随着应用的推广，测试标准也建立起来了。

由于使用 IC 卡具有流动性与全球性的特点，迫切要求实现开放性，相应的国际标准和国家标准也就显得特别重要，因此有关的标准在本书中占有大量篇幅。同时由于标准是可能修改的，例如本书第 3 章中的国际标准 ISO/IEC 7816-3，已几经修改，这次本书按最新的版本进行了修改。

在编写本书过程中根据我们的学习、工作经验，力图全面反映智能卡技术各方面的知识、理论和实践经验，注意系统性和易读性，但由于作者知识的局限性，再加上技术发展快，又在一定程度上存在保密等原因，本书肯定会存在不少缺点，甚至错误，殷切希望领导、专家和广大读者提出宝贵意见和建议。

王爱英

写于清华园

2000 年 4 月

第1章 智能卡概论

1.1 智能卡基础知识

1.1.1 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卡(integrated circuit card)。它将一个集成电路芯片镶嵌于塑料基片中，封装成卡的形式，其外形与覆盖磁条的磁卡相似。

IC卡的概念是20世纪70年代初提出来的，法国布尔(BULL)公司于1976年首先创造出IC卡产品，并将这项技术应用到金融、交通、医疗、身份证明等多个行业，它将微电子技术和计算机技术结合在一起，提高了人们生活和工作的现代化程度。

IC卡芯片具有写入数据和存储数据的能力，IC卡存储器中的内容根据需要可以有条件地供外部读取，或供内部信息处理和判定之用。根据卡中所镶嵌的集成电路的不同可以分成以下三类：

1. 存储器卡　卡中的集成电路为EEPROM(可用电擦除的可编程只读存储器，也可写作E^2PROM。)

2. 逻辑加密卡　卡中的集成电路具有加密逻辑和EEPROM。

3. CPU卡　卡中的集成电路包括中央处理器CPU、E^2PROM、随机存储器RAM以及固化在只读存储器ROM中的片内操作系统COS(chip operating system)。

另外还有一种ASIC(专用集成电路)卡，它是在逻辑加密卡基础上增加一些专用电路，例如完成加密/解密运算的电路等，但由于卡内设有CPU，所以完成的功能是固定的，没有灵活性。在本书中对这种芯片没有进行专门讨论，因为在讨论了前面三种卡以后，ASIC卡的结构与功能也就明确了。

严格地讲，只有CPU卡才是真正的智能卡，但在本书中，为了论述全面，更为了应用的需要，我们将研究讨论上述三种IC卡。

按应用领域来分，IC卡有金融卡和非金融卡两种。金融卡又有信用卡(credit card)和现金卡(debit card)等。信用卡主要由银行发行和管理，持卡人用它作为消费时的支付工具，可以使用预先设定的透支限额资金。现金卡又称储蓄卡，可用作电子存折和电子钱包，不允许透支。非金融卡往往出现在各种事物管理、安全管理场所，如身份证明、健康记录和职工考勤等。另外一些预付费卡，例如用于公交系统中的交通卡和电表上的IC卡等，各由相应的管理单位发行(当然也可委托银行收费)。这种卡兼有一部分电子钱包的功能，在本书中我们仍将它列为非金融卡。

按卡与外界数据传送的形式来分，有接触式IC卡和非接触式IC卡两种。当前使用广泛的是接触式IC卡，在这种卡片上，IC芯片有8个触点可与外界接触。非接触式IC卡的集成电路不向外引出触点，因此它除了包含前述三种IC卡的电路外，还带有射频收发电

路及其相关电路。非接触式卡出现较晚，但由于它具有一些接触式 IC 卡所不能替代的优点，因此在某些应用领域发展很快。

在 IC 卡推出之前，从世界范围来看，磁卡已得到广泛应用，为了从磁卡平稳过渡到 IC 卡，也是为了兼容，在 IC 卡上仍保留磁卡原有的功能，也就是说在 IC 卡上仍贴有磁条，因此 IC 卡也可同时作为磁卡使用，图 1.1 为 IC 卡的外观图，正面中左侧的小方块中有 8 个触点，其下面为凸型字符，背面有磁条。正面还可印刷各种图案，甚至人像。卡的尺寸、触点的位置与用途、磁条的位置及数据格式等均有相应的国际标准予以明确规定。

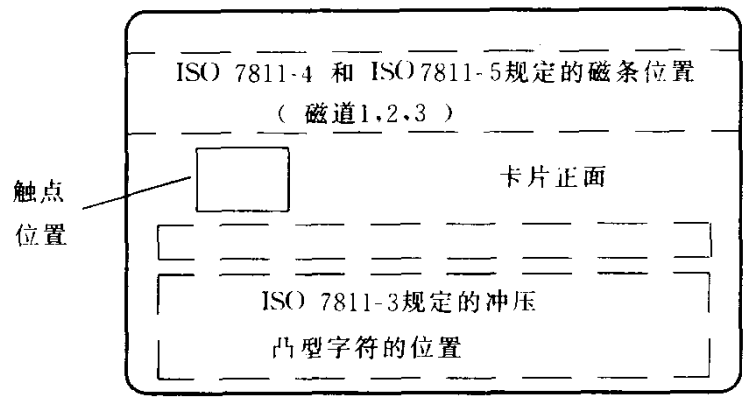

图 1.1　IC 卡的外观图

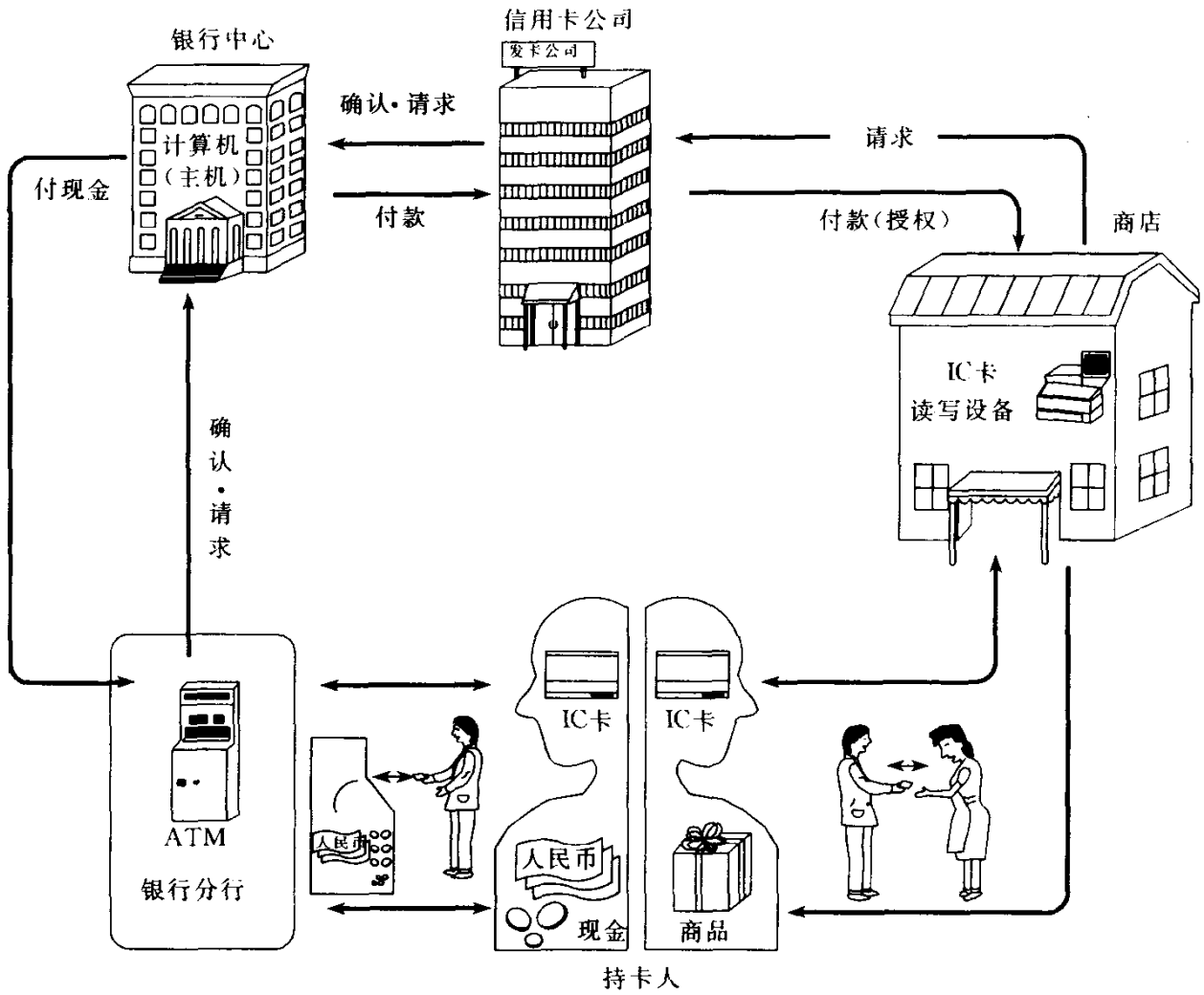

图 1.2　IC 卡应用过程

无论是磁卡还是IC卡，卡上都有唯一的发行人和持卡人的识别标志，这种卡称为“识别卡”。

1.1.2 IC卡的接口设备

为了使用卡片，还需要有与IC卡配合工作的接口设备IFD(inter face device)，或称为“读写设备/读写器”。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，该接口设备通过IC卡上的8个触点向IC卡提供电源并与IC卡相互交换信息。IFD也可以是一个简单的接口电路，IC卡通过该电路与通用微机相连接。无论是磁卡或IC卡，在卡上能存储的信息总是有限的，因此大部分信息需要存放在接口设备或计算机中。当用信用卡购物时，如在允许透支范围内，则可以先取走商品，事后再结算；如需一笔大款，则需经银行确认，授权于商店后，才能取走商品。由于银行、发放信用卡的公司以及商店不在同一处，因此需要经过通信线路和计算机(主机)联系才能实现上述过程。

图1.2(右半部)示出使用信用卡购物的过程，图1.2(左半部)是在ATM(自动柜员机)上自动取款(稍后说明)。

为了快速而又可靠地进行处理，计算机网络与通信线路的安全与响应时间是关键。

1.2 金融卡的应用基础

IC卡主要用作金融卡，金融卡的主要功能是存储数据和处理数据。

1.2.1 IC卡提供的信息

1. 印在卡上的可供人阅读的信息　用以标识卡发行人的标志、使用期限、客户姓名、账号和签名等，这些信息是卡能作为金融交易中的支付工具的基础。

2. 机器可读数据　卡上的凸出字符用于压印账单，以便向售货商和客户提供交易凭证。卡上还可提供金融交易的账目。

3. 提供机器可读的授权信息和数据收集系统的标识符。

1.2.2 举例——在自动柜员机上实现取款

下面以自动柜员机ATM为例进行说明。

自动柜员机是放在银行或商店大堂中供客户自动提款的机器(有的ATM还有自动存款功能)。执行从ATM提取现金的操作仅需十几秒钟，总共只需要做出4个输入动作：

1. 插入金融卡；
2. 输入个人标识码(PIN)；
3. 选择交易类型(取款)；
4. 给出申请提取的金额。

当ATM判别没有问题时，自动输出卡和现金，并打印凭证。由此可见，ATM是一种操作方便的信息处理系统，可以24小时提供服务。

ATM 是安装在柜里的计算机系统，它要处理卡片、货币、收据和信封（存款用）四种介质，并能与相连接的远程计算机相互通信。它的内部有严密的可靠的物理和逻辑安全措施。它的每一笔交易通常接受正确的授权和严格的控制，因此 ATM 系统既是一个操作简单的系统，又是一个构造复杂的系统。由于历史原因，目前 ATM 主要使用磁卡。

ATM 将磁条上（对磁卡）的数据，诸如发行人和客户账号识别码（用来获取自动授权信息的基础）通过通信线路与发卡单位的计算机及其账户数据库相连，用以检查金融卡的编号（查对黑名单），以防止他人使用已挂失的或偷窃来的金融卡，同时核对客户的账面记录，以查明可供支用的金额，并根据交易的金额随即更新账面记录，供金融卡下次使用。此外，为了避免某些可能发生的弊端（如已挂失但尚未列入黑名单），还要限制金融卡在一天内允许使用的次数和一天内允许提取现金的总金额。

绝大多数 ATM 机取款时还需输入个人标识符 PIN，并将 PIN 送到计算机，用来核对持卡人是否是卡的主人。如在通信线路上明文传送 PIN，存在被窃听的危险，为此有时需对 PIN 进行加密，这就要提供一个加密算法和“密钥”，让经过加密后的 PIN 在通信线路上传送，在接收端解密，因此在接收端提出了密钥的管理和保护的要求（参考第 7 章）。

1.2.3 IC 卡存储区的分配和功能简介

IC 卡的存储量比磁卡大得多，一般分四个存储区：

1. 公开的（不保密的）存储区　内含公用信息，诸如发行标识符、持卡人的账号等。

2. 外部不可读的存储区　存储的内容是供内部决策用的，如 PIN 值，该值是在卡片发行时进行个人化处理写入的，用户在输入正确的 PIN 值后，允许输入新 PIN 值进行修改，但在任何情况下，都不允许将存储在卡中的 PIN 值向外界传送。在本存储区内还可能存放密钥。

3. 保密存储区　内含账面余额、允许卡使用的服务类型及限额等。当持卡人输入正确的 PIN 值后，允许读取本存储区数据，进行交易，并根据应用情况写入正确数据（如修改余额）。

4. 记录区　内含每次交易细节，称为“日志”，可供查询。

除了存储器卡外，在其他 IC 卡中还有逻辑电路或微处理器，提供安全可靠的服务。

1.2.4 接口设备存储器内容简介

与智能卡配合使用的接口设备（或称为读写设备、读卡器）应该提供附加的存储器和逻辑电路，它本身可能就是一台微机。

用于商店中的接口设备的存储器中包含如下内容：

1. 交易数据　内含每次交易记录，一般于每天晚上将当天交易细节汇总后传送到开户银行或发卡银行，供转账和清算之用。银行应保证及时将应付款存入售货商账户。

2. 非法卡表（或称为黑名单、止付名单）　列出所有挂失、被窃或透支超过限额的账户清单，在每天向银行递交交易细节时，也递交此清单。同时银行经汇总后，应将修改后的黑名单提供给售货商。凡登在黑名单上的账户或透支超额的账户要进行交易时，须由售货商通过网络或用专用电话和银行进一步授权核实后，方可受理。也可拒绝处理，甚至可根

据实际情况将卡没收。

3. 保密数据　密钥和授权电话号码即属于保密数据，密钥用以生成校验码以防交易日志被修改。至于授权电话，在售货商希望成交某些超额交易时，用它接通用户银行，经银行授权后方可受理，如果电话通信线路很忙，那么等待授权的时间可能很长，甚至能让客户觉得无法容忍，这就会影响到金融卡的推广应用。较先进的系统应靠计算机网络和通信线路来完成授权功能。

1.2.5　使用智能卡完成一次购物的操作过程

操作顺序如下：

1. 客户拿着金融卡和购买的商品(或付款单)来到付款处。并将金融卡插入能输入PIN的小键盘设备中。

2. 售货员通过他本人工作的键盘输入交易金额。

3. 交易金融显示在小键盘设备的显示板上。

4. 客户在小键盘上按下某个指定键，表示对交易金额的认可。

5. 小键盘设备的显示板上指示客户输入PIN。然后客户输入PIN。输入后自动与卡中的PIN比较，如一致，就将金融卡自身打开，准备受理交易。

6. 接着接口设备内部进行一连串处理，如查对黑名单、核实资金是否够用、计算交易后的余额，将它登入交易日志记录里并计算出安全校验码加在日志记录中以保证数据的安全。同时把这笔交易记录也写到金融卡中，最后给客户打印收据。

7. 显示板指示交易结束，客户取走商品和卡。

1.2.6　发展智能卡与人有关的因素

参与智能卡操作的相关方面有：持卡人或用户，商店，卡片的发行者及销售部门，卡片的设计者、出售商及安全维护。

1. 持卡人或用户

用户要求：

(1) 使用方便：装置的地点、使用的时间和操作的步骤等力求方便。操作一学就会。

(2) 启用手续简易：发行和基于PIN号的卡片个人化处理手续简易。

(3) 加快交易时间：进行一次交易或授权等待时间尽量缩短。

(4) 安全可靠：每次交易正确无误，操作错误后的重新启动方便可靠，卡片的丢失、被窃和PIN值的更换等容易处理。

(5) 清楚简单的操作提示：卡片上清楚表明接口方向，显示屏幕清楚易读，避免使用计算机术语和复杂的交互式操作。

2. 商店

商店期望：

(1) 人员培养容易，操作过程和例外处理简单。

(2) 故障处理简单：故障处理包括出错后的重新启动、例外情况或交易被拒绝时的处理，以及在正常的解决办法失灵时，其他可供选择的措施。

(3) 安全可靠：对丢失、被窃以及未付账款的卡片处理办法简单且安全，对各类不安全因素易于检测。

3. 卡片的发行者和销售部门

除了满足商店和用户的要求以外，应做好有关方面(银行、商店、用户)之间的信息交换工作，以及用户忘了 PIN 后的处理工作等。

4. 设计者、出售商及安全维护

设计目标应满足用户及商店的要求。电子设备应保证能够每天 24 小时不间断工作，并能很容易测试判断智能卡是否工作正常。机械设计要保证设备和零件工作可靠。设计好对例外情况的处理办法，并能迅速排除故障。

1.2.7 智能卡的种类

1. 信用卡　卡中预先建立允许透支的限额，即预先设置好可借用的资金额度，承诺到期归还并支付利息的责任。根据持卡人信用程度的不同，有两种信用卡：金卡和普通卡。前者的透支限额高。

2. 现金卡(付款卡)或储蓄卡　供储蓄账户使用，持卡使用的资金是客户已经存放在银行中的存款。

3. ATM 卡　只能在 ATM 中使用的现金卡或信用卡。

4. 预付卡　按卡面价值购买，先购买，后使用，例如电话和公共系统用的预付卡、电表预付卡等。

另外，还有诸如大饭店内部使用的卡，客人进入饭店后，住宿、用餐、娱乐等都可凭卡记账，离开饭店时结账。

1.3 智能卡的安全问题

智能卡的作用是替代流通领域中的现金或支票，随着智能卡的推广使用，利用它进行欺诈或作弊的行为也会不断增加，对于出现的不安全问题的解决办法需要在提供合理的效果和防护的保证与所需的成本和投资之间进行平衡，从而提出一个折衷的解决办法。

在本书的第 7 章将详细讨论安全问题。

1.3.1 影响智能卡安全的若干基本问题

在众多智能卡安全问题中有下列基本问题需要解决：

1. 智能卡和接口设备之间的信息流通　这些流通的信息可以被截取分析，从而可被复制或插入假信号。

2. 模拟智能卡(或伪造智能卡)　模拟智能卡与接口设备之间的信息，使接口设备无法判断出是合法的还是模拟的智能卡。

3. 在交易中间更换智能卡　在授权过程中使用的是合法的智能卡，而在交易数据写入之前更换成另一张卡，因此将交易数据写入替代卡中。

4. 修改信用卡中控制余额更新的日期　信用卡使用时需要输入当天日期，以供卡判

断是否是当天第一次使用，即是否应将有效余额项更新为最高授权余额（也即是前面讲到的，允许一天内支取的最大金额），如果修改控制余额更新的日期（即上次使用的日期），并将它提前，则输入当天日期后接口设备会误认为是当天第一次取款，于是将有效余额更新为最高授权余额，因此，利用窃来的卡可取走最高授权的金额，其危害性还在于（在银行提出新的黑名单之前）可重复多次作弊。

5. 商店雇员的作弊行为　接口设备写入卡中的数据不正确，或雇员私下将一笔交易写成两笔交易，因此接口设备不允许被借用、私自拆卸或改装。

1.3.2　安全措施

为了安全防护，一般采取以下措施：

1. 对持卡人、卡和接口设备的合法性的相互检验。

2. 重要数据加密后传送。

3. 检验数据的完整性。

4. 卡和接口设备中设置安全区，在安全区中包含有逻辑电路或外部不可读的存储区，任何有害的不合规范的操作，将自动禁止卡的进一步操作。

5. 有关人员明确各自的责任，并严格遵守。

6. 设置止付名单（黑名单）。

1.3.3　密钥与认证

1. IC 卡系统中常用的两种密码算法

（1）对称密钥密码算法或秘密密钥密码算法（DES）；

（2）非对称密钥密码算法或公共密钥密码算法（RSA）。

对持卡人、智能卡和接口设备之间的相互认证以及数据的加密，均可采用这两种密码算法中的一种。

与加密有关的还有解密和密钥管理，密钥管理包括密钥的生成、分配、保管和销毁等。

对传输的信息进行加密，以防被窃取、更改，从而避免造成损失。对存储的信息进行加密保护，使得只有掌握密钥的人才能读取信息。

2. 认证

为防止信息被篡改、伪造或过后否认，特别是对被传输的信息，加密认证就显得更为重要。

（1）信息验证　防止信息被篡改，保护信息的完整性，要求在接收时能发现被篡改的数据，例如可采用一定的算法产生附加的校验码，在接收点进行检验。

（2）数字签名（电子签名）　要求：收方能确认发方的签名；发方签名后，不能否认自己的签名；发生矛盾时，公证人（第三方）能仲裁收发方的问题。

为实现数字签名，一般要求用公共密钥解决。

（3）身份认证：用 password 或个人标识号 PIN 进行认证，更可靠的是利用生物特征。

本处讨论的密钥与认证问题将在第 7 章详细讨论。

1.3.4 卡片的作弊问题

从磁卡使用情况来看，造成发卡行损失的有两种情况：

1. 呆账　持卡人到时不付账。

2. 作弊　是由于犯罪行为引起的，因此在塑料卡上采取了一些防范措施。例如 VISA 卡采取了以下措施：正面有全息飞鸽图形；精细的底版印刷；非凸形的标识号；卡片上有签字条，当签字被更改时，签字条立即显示出 VOID(作废)。

其他根据需要还可以作出照片、指纹等个人标识。

除了卡片外，磁条更有问题，因为磁条上的记录具有以下特点：可读出，可更改，可伪造，可模拟，可擦掉。

为了避免由于作弊造成的损失，使用磁卡时(尤其是超过现额时)需经过授权验证。

读取 IC 卡中的信息较磁卡为难，尤其是智能卡，可通过加密验证等手段使得冒用或伪造变得困难起来，因此，与磁卡相比可使用在脱机情况下。但是，实际上没有绝对的秘密可言，因为客观上存在着能力很强的对手，即使有加密方法，也肯定能找到解密的方法，只不过是要耗费多大代价，需要多少时间，是否值得的问题，即使是好的设计也会存在不同程度的易被击破的弱点。

1.4 识别卡的国际标准

由于信用卡可在国内各地使用，某些还能在国外使用，因此制定国际和国家标准是迫切需要的，国家标准应该尽量与国际标准一致，同时也应制订适合本国实情的新标准。

识别卡是一种可识别其发行者和持有者的卡。金卡支付业务中用得最多的是信用卡，它是一种识别卡。识别卡分磁卡和 IC 卡两类。

1.4.1 磁卡的国际标准

1. 物理特性　包括卡的材料、构造、特性、标称尺寸等，均应符合国际标准 ISO 7810：1985。

2. 凸印　卡正面显著地凸起的字符称为凸印，用于数据传送，这种传送可以通过压印机，也可以用目视或机器阅读。凸印字符包含标识号、持卡人的姓名和地址。常用的 ID-1 型卡上凸印字符的位置应符合国际标准 ISO 7811-3：1985 的规定。

凸印字符及其字体的选择应符合 ISO 1073-1、ISO 1073-2 和 ISO 7811-1 附录 B、附录 C 描述的 7B 字体的规定，凸印字符的字符间距、高度等符合国际标准 ISO 7811-1：1985 的规定。凸印字符的印刷规范符合 ISO 1831：1980 的规定。

3. 磁条　磁条上磁性材料的物理特性和性能特性、编码技术和编码字符集有相应的国际标准 ISO 7811-2：1985。磁条上共有三个磁道，第一、二磁道为只读磁道，第三磁道为读写磁道，分别有国际标准 ISO 7811-4：1985 和 ISO 7811-5：1985。

有关磁卡的较为详细的介绍请见本书第 2 章。

1.4.2 IC卡的国际标准

IC卡分接触式和非接触式两种。接触式IC卡应用较早，其国际标准比较完善。非接触式IC卡近年来开始推广应用，其标准有些已经通过，有些正在制定与讨论过程中。另外，有关的测试标准也是值得注意的。

标准是IC卡设计制造与应用的支撑点，符合标准是IC卡赖以生存的条件。因此，了解标准和学会使用标准是本书的主要重点之一。有关标准的表示方法请阅本书附录A的注解。

1. 接触式IC卡的国际标准

ISO/IEC 7816是IC卡遵循的主要国际标准，该标准也引用了以前制定的有关识别卡的标准，有关ISO和IEC国际组织的介绍见本书附录A。

ISO/IEC推出的7816国际标准已有10个部分。它们对IC卡的物理特性、卡上触点尺寸与位置、电信号与传输协议、行业间交换命令、数据元以及IC卡注册管理办法等做出了详细的规定。

ISO/IEC 7816国际标准在本书第3、4章论述。

2. 非接触式IC卡的国际标准

非接触式卡表面无触点，因此接口设备与非接触式卡的通信方式与接触式卡不同，提供电源的方式也不同，为此国际标准化标准根据接口设备与IC卡作用距离的不同而定义了三个国际标准，分别为ISO/IEC 10536、ISO/IEC 14443和ISO/IEC 15693，每个国际标准又由几个部分组成，但到写稿时为止，大部分标准尚未正式通过，还是草案，其中某些标准(例如ISO/IEC 14443)的若干部分可望在2000年正式通过。

ISO/IEC 7816中的大部分内容仍适合于非接触式IC卡。有关非接触式IC卡的标准将在本书第5章中介绍。

3. 测试标准

IC卡是否符合国际标准在应用前要进行测试(某些测试项目可抽样进行)。

ISO/IEC 10373是对各种卡进行测试的国际标准，包括磁卡、接触式卡、非接触式卡和光卡。本书的第7章将讨论接触式IC卡和非接触式卡的测试标准及其实现方法。

值得一提的是：国际标准是不断充实和完善的，即使是已经通过的国际标准，仍有修改的可能性，读者应注意国际标准的最新版本。

1.5 金卡工程(电子货币工程)

金卡工程(电子货币工程)是我国金融电子化建设的重要组成部分。电子货币是现代化货币流通的形式，它集计算机、通信、金融和商业专用机具为一体，以金融交易卡(信用卡和现金卡)为介质，并通过电子信息转账形式实现货币流通。金卡工程就是为实现电子货币大范围流通的跨部门、跨地区和跨世纪的系统工程。

金卡工程的实现可减少社会上现金的流通量和货币的发行量，加强国家对资金的宏观调控和决策能力。这对国家掌握各种金融活动和资金的流动情况，加速资金的周转提供

了现代化技术手段；并对抑制通货膨胀、稳定社会治安、减少经济犯罪起良好作用。

本节内容未经核实，纯按技术问题讨论，仅供参考。

1.5.1 金卡工程的总体设想

1. 金卡工程的发展(1994 年制订)

先从金融卡(银行卡)起步，用 10 年(1994 年—2003 年)时间，在全国 400 个城市及部分经济发达的县城推广使用。在 3 亿城市人口地区，计划发卡量达到 2 亿张。

将 10 年时间划分成 3 个阶段：试点阶段(3 年)、推广阶段(3 年)和普及阶段(4 年)。

(1) 试点阶段　选择 12 个省市进行金卡工程试点。这 12 个省市是：北京、上海、广州、杭州、江苏省、青岛、厦门、天津、辽宁省、海南省、大连和山东省。具体目标为：

① 制定发展信用卡市场的规划，建立以金融部门为主体的信用卡业务管理体系。

② 建立法律法规，统一银行卡标准，实现信用卡跨地区、跨部门通用。

③ 建立全国金卡信息交换服务中心和各试点城市金卡信息交换服务中心，并与人民银行国家处理中心联网。实现同城或异地授权信息的即时转接和资金的适时结算。

① 全国计划发卡量为 3000 万张。

(2) 推广阶段　具体目标为：

① 进一步完善试点城市的发卡、联网、应用和服务环境。

② 选择一些城市推广，分别建立城市(区域)金卡信息交换服务分中心并联网。

③ 全国计划发卡量为 6000 万张。

(3) 普及阶段　具体目标为：

① 完善有关银行卡业务的法律、法规、制度和监督体系。

② 全国 400 个城市联网，实现即时授权和适时结算。

③ 相当多城市将信用卡业务推广到周围经济较发达的县、镇。

① 到 2003 年，全国计划发卡量超过 2 亿张。

2. 金卡工程的实现技术

建立现代化银行卡电子货币系统，银行卡通用，可凭卡在同城或异地购物、消费、存取款和转账结算，要达到这一目标，需建立先进的信用卡技术支撑系统，主要指信用卡授权清算系统、计算机网络、通信系统、卡及其读写机具。

(1) 建立信用卡授权系统　这是加强信用卡管理、减少信用卡风险的一项重要措施。信用卡授权是指发卡银行授予特约商户向持卡人支付资金(商品)的权力，即授权单位对支付行为负责，因此必须是经营信用卡业务的金融机构或其代理才有资格授权。需建立全国性的电子授权中心，例如设立全国和城市(或区域)两级授权交换中心。

(2) 信用卡资金清算系统　信用卡资金清算是指银行通过同行业间的资金往来，按照一定程序，将持卡人使用的资金完成最终支付的一个资金流动过程。

(3) 技术装备

① 通信网络：可以采用中国国家金融网络(CNFN)，邮电部中国公用分组交换数据网 CHINAPAC 和国家公用经济信息通信网(金桥网)，实现互连、互为备份。

② 各专业银行的入网前置机应该尽早统一标准，以实现跨行授权。

③ 计算机系统：根据业务量确定规模，尽量采用开放式系统。

④ 信用卡终端设备：ATM(自动柜员机)和 POS(销售点终端)推广使用。

⑤ 磁卡和 IC 卡：目前我国发行的信用卡还是磁卡，优点是价格便宜，但易伪造，安全性差。智能卡的优点是安全、可脱机处理、对通信网络的要求较低，但价格高。我国考虑同时发展磁卡和 IC 卡，并选定试点城市，一开始就用 IC 卡。

3. 金卡工程的效益目标

提高银行卡结算业务在全社会资金结算中的比例，扭转现金结算总额上升的趋势，减少现金流通量。

4. 金卡工程的管理体系

建立和完善以金融部门为主的银行卡业务管理体系。

人民银行加强对银行卡业务的指导、管理和监督。建立并健全各商业银行联营银行卡的联合组织，并制定规章。

制定有关的法律、法规，促进银行卡业务发展。

5. 其他

依托金卡工程促进商业和旅游服务业等领域的信息化，带动配套电子信息产业的发展。

1.5.2 银行卡基本业务需求

银行卡有信用卡和现金卡两种。

1. 信用卡

是银行或金融机构发给信用良好人士使用的一种凭证，持卡人可用它来购物消费、信用借款、转账结算、汇兑和储蓄等。国内按发卡银行不同有牡丹卡、长城卡、金穗卡和龙卡等；按使用对象不同分单位卡和个人卡；按持卡人信誉程度不同有金卡和普通卡；按还款先后不同分借记卡和贷记卡；按信用卡国际组织不同有 MASTER 卡和 VISA 卡。

发卡银行加入信用卡国际组织后发行的、可在全球使用的、以本币或外币进行结算的信用卡称为国际卡。一般在国内消费时以本币或外币结算，在国外消费时以所在国货币或美元结算。

银行卡的业务范围和应用范围包括：发卡中心业务处理、在国内外商店购物消费、在银行自动柜员机(ATM)上存取现金和转账，以及在销售点终端(POS)上付款或转账等。

银行卡发卡中心业务处理范围包括：

(1) 银行卡业务档案资料管理：包括持卡人档案、商户档案、发卡机构档案、止付名单(黑名单)档案、储蓄所档案、ATM 和 POS 等有关机具的档案等。

其业务包括档案资料的收集、整理、储存和使用。

(2) 账户管理：包括单位卡活期和定期账户、个人卡活期和定期账户、商户活期和定期账户、银行内部账户等。

其业务包括开户、查询、账务处理、冻结、清户和开出有关清单等。

(3) 发卡和换卡：对新开户或过期、遗失、被窃、损坏的卡进行发放或更换。

(4) 账务处理

① 日间业务处理：本地卡和异地卡现金和转账收付业务处理；透支和还款处理；错账冲正和账户调整；查询。

② 日、月、年终业务处理：轧账、借贷款利息计算、生成报表等。

(5) 授权：商户或取现金点对超过消费限额或取现金限额的银行卡交易，必须通过发卡或代理行授权同意后才能受理，无论是否同意用卡，均应产生答复信息。

(6) 止付：银行卡信息交换中心应储存所有银行的止付名单，不联网的商户或取现金点应保存可在本处使用的止付信用卡名单。每笔交易都应该查对止付名单。

(7) 清算：本系统资金清算由发卡银行自行处理，跨系统清算由中央银行处理中心处理。

(8) 事后监督和统计打印报表。

2. 现金卡(或储蓄卡)

由于持卡人不能透支，所以不涉及持卡人信誉，发行手续简便，只要领卡人在银行有一定存款，银行即可发卡。持卡人用卡时银行应对卡的真伪进行认证。用户正确输入密码后可对密码进行修改。IC 卡上可以带有账户存款余额，因此，可以脱机操作，不需要授权。

3. 银行卡信息交换中心

为了处理本地和异地的跨系统授权业务，应成立全国银行卡信息交换中心和地区银行卡信息交换中心，本地跨系统的授权需通过地区银行卡信息交换中心转给发卡银行处理、异地跨系统授权通过全国银行卡信息交换中心转给地区银行卡信息交换中心，再由其转给发卡银行处理。

1.5.3 金卡工程总体结构

1. 金卡信息交换中心

我国金卡工程信息交换可能采用两级(国家和城市)交换，发卡单位最终授权的机制。具体可按以下规定执行：

(1) 银行卡在同城(区域)范围内的跨行交易，需要经过同城(区域)交换中心的转接。

(2) 银行卡跨地区交换，通过本地城市信息交换中心→国家信息交换中心→异地城市信息交换中心，转至发卡行(见图 1.3)。

(3) 银行卡在本行系统内交易，使用本银行系统内的网络，如图 1.4 所示。

图 1.3 中的国家信息交换中心对内连接各城市信息交换中心，对外统一与国际信用卡处理中心连接，其功能有：跨城市授权信息转接，分发全国止付名单，与国际统一接口，生成并分发结算报表，提供跨城市信用卡业务的统计、分析和预测资料。

城市信息交换中心对上与国家信息交换中心连接，对下与城市各发卡银行及 ATM/POS 中心相连，其功能有：银行卡同城跨行使用的信息转发；银行卡异地使用的信息转发；统一并分发本市止付名单；向城市清算中心提供信用卡同城跨行使用产生的清算资料；统计、生成报表等。

发卡行信用卡处理中心向上与城市信息交换中心相联或区域内非中心城市信用卡信息交换转发集结点相联，向下与本行信用卡营业网点(包括 ATM 和 POS 等)相连。

图 1.4 中的银行总行是银行卡业务的主管单位，发卡行也可以是为数众多的地方分行。

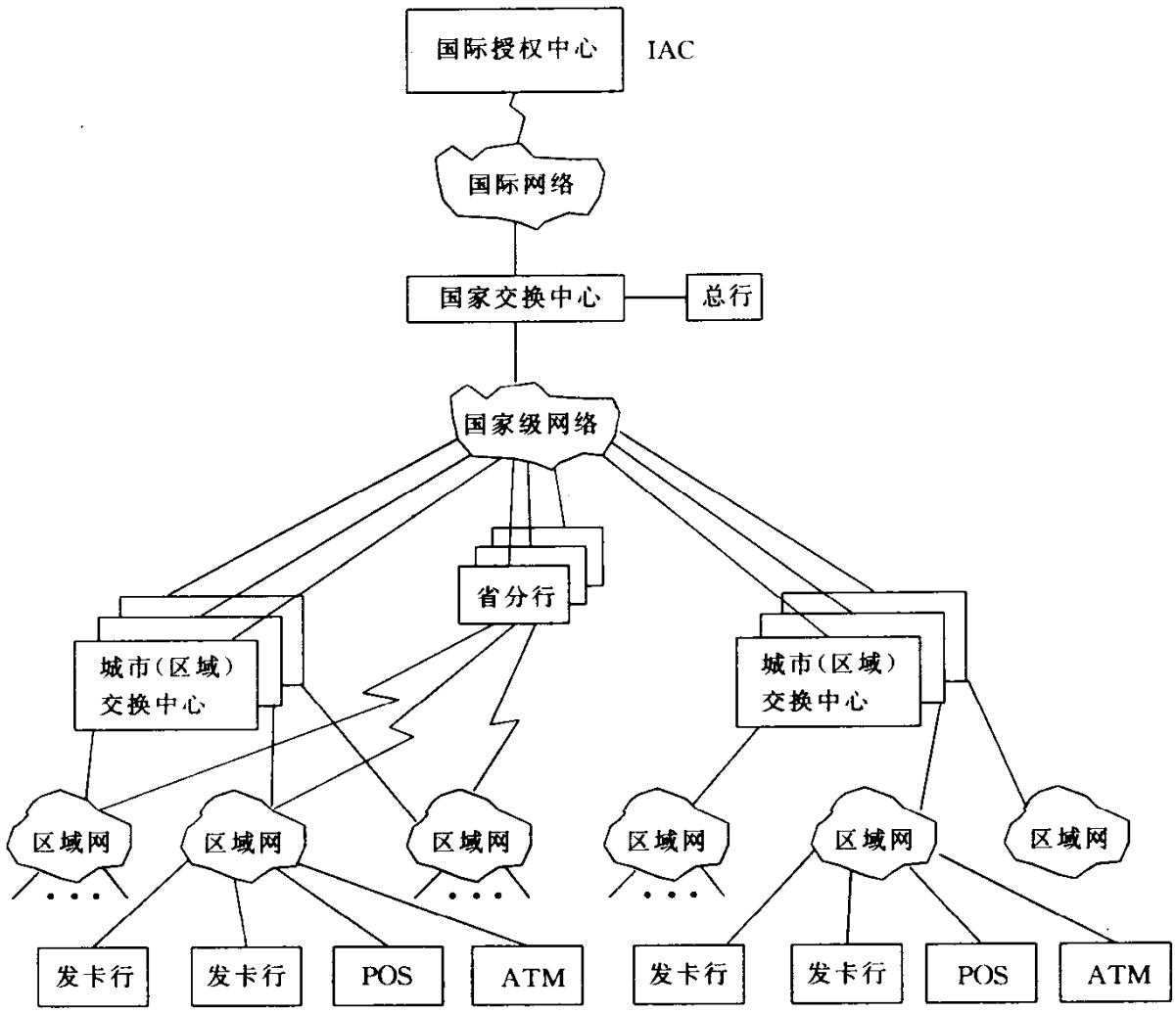

图 1.3　金卡信息交换服务网络系统

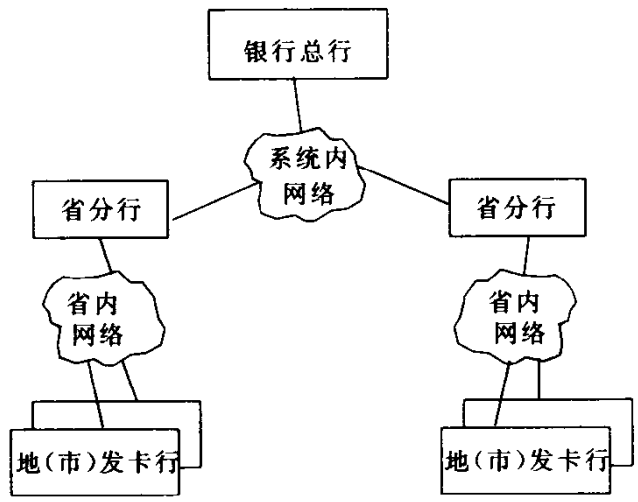

图 1.4　银行本系统的网络结构

2. 通信网络

充分利用现有资源，以先进、可靠、方便、安全和经济为原则，选用中国国家金融通信网(CNFN)、中国国家公用数据网(CHINAPAC)和国家公用经济信息网(金桥网)为主干网，上述网络互连互通、互为备份。在城市内，优先选用电信管理部门已建成的区域性网络。不应再重新组建专用网。