



# 智能卡概论

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数量都在成倍增加，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，需要携带多种票证、现金、单据，给我们带来很多不便和不安全感。

于是，人们寻求一种具有支付、查询、密码查验等多种功能及安全可靠的“卡”。由于磁卡部分具有上述功能，且其结构简单、价格低廉，因而在全世界得到广泛的应用，其应用环境及产业所提供的服务日臻完善和普及。进入本世纪 90 年代后，磁卡本身存储量小、安全保密性差、易被伪造、多次使用数据易损坏等不足之处逐步暴露，限制了它的进一步应用。这时，一种存储量更大，安全性更好，更耐用的新工具得到了人们的普遍关注，并已开始逐步推广使用。这就是本书将要介绍的智能卡。

## 1.1 智能卡的定义

智能卡的名称来源于英文“SMART CARD”，又称集成电路卡（Integrated Circuit Card），即 IC 卡。它是将集成电路芯片镶嵌于塑料基片之中制成的，并被封装成卡片的形式，其外形与磁卡相似，尺寸大小符合 ISO 7816 标准（54 mm×86 mm×76 mm）。本书中，我们将这种卡统称为 IC 卡。

IC 卡的概念是 70 年代提出的。法国 BULL 公司首创 IC 卡产品，并将这项技术应用到金融、交通、医疗、身份证明等多个方面。IC 卡的核心是集成电路芯片，一般为 3 μm 以下半导体技术制造。IC 卡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的供外部读取，或供内部信息处理和校验用。

根据卡中的集成电路的不同，IC 卡可分为以下三类：

(1) 存储器卡：卡中的集成电路为 EEPROM(电可擦除可编程只读存储器)，它仅有数据存储能力，没有数据处理功能。

(2) 逻辑加密卡：卡中的集成电路具有加密逻辑和 EEPROM。在对卡中的数据进行操作前，必须验证每个卡的操作密码。密码的验证是由卡中的芯片完成，而不是由读卡终端完成。卡中有一个错误计数器，如果连续三次验证密码失败，则卡中数据被自动锁死，该卡不能再使用。

(3) CPU 卡：卡中的集成电路包括 CPU(中央处理器)、EEPROM、RAM(随机存储器)以及固化在 ROM(只读存储器)中的 COS 片内操作系统，其唯一工作方式“用户方式”，分为通用型和专用型两种。专用型是指其中的 CPU 为专用的、保密的，与通用型的主要差别在于其有很好的物理保护措施。智能卡的发展方向是保密的专用型。

如按卡与外界的数据传送形式来分，IC 卡可分为接触型和非接触型两种。当前广泛使用的是接触型 IC 卡，在这种卡的左上角有印制版，上面有 8 个触点可与外部接触。非接触型 IC 卡的集成电路不向外引出触点，因此它除了有上述 IC 卡的电路外，还带有射频收发电路及其相关电路。

由于目前磁卡的使用非常广泛，为了从磁卡平稳过渡到智能卡，考虑到两者的兼容性，所以很多智能卡上也有磁条。因此，IC 卡也可同时作为磁卡使用。IC 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给予明确规定。

## 1.2 IC 卡与磁卡的比较

IC 卡与磁卡外形差不多，但两者在许多方面存在差异。

(1) 抗破坏性和耐用性：磁卡是靠磁条来存储信息的，在遇到强磁场、静电、扭弯、刮伤等情况下，存储在磁条里面的信息容易丢失；另外，磁条上的信息存放时间较短及读写次数较少，修改不方便。IC 卡是由硅片来存储信息的，先进的硅片制作工艺完全可以保证 IC 卡的抗磁性、抗静电及各种射线的能力；由于硅片的体积很小，里面有环氧树脂的保护，外面有 PCB 板及基片的保护，因此，其抗机械、抗化学破坏能力也很强。目前，IC 卡的信息保存期都在 100 年以上，而且读写方便，读写次数高达 10 万次以上。

(2) 存储量和灵活性：磁卡的存储容量最大只有几百个字节，一般磁条只有几十个字节。IC 卡的容量可以做到几千个字节，而且其存储区还可以划分，允许有不同的访问级别，为信息处理和一卡多用提供了方便。

(3) 保密性：由于磁卡存储量有限，内部没有对数据内容的安全控制或对读写控制的逻辑电路，读取技术是顺序和机械的。所以，磁卡的保密性较差，容易被复制。IC 卡具有很强的保密性，首先体现在芯片的结构和读取方式上。IC 卡的容量比较大，而且存储器的读取和写入区域可以任意选择，因此灵活性较大。一般的存储器卡，采用特定的技术，具备较强的保密性。加密存储器卡，其存储区的访问受逻辑电路控制，只有密码正确，才能进行读写，而且密码的核对次数有限，超过规定次数，卡将被锁死。CPU 卡的保密性更高，除了密码控制外，还有信息处理功能，可利用各种硬件手段加密，也可利用软件的各种加

密算法加密。

(4) 读写设备成本：磁卡的读写设备中含精密机械和信号转换部件，成本高，一个简单读卡器价格达几百元，复杂点的要到几千元，而且可靠性低、维护量大；另外，由于磁卡容量小，许多信息不能存到卡上，为了保证系统的安全性，对计算机网络的要求高，软件工作量大。IC 卡因其本身就能提供数字信号，所以读写只需一个插卡的卡座，简单的卡座价格在十几元，高级的也只要几百元，而且使用寿命长，可靠性高，基本不须维护；由于 IC 卡的容量大，保密性好，许多信息可以放到卡上，因此对系统网络的要求也不高，系统设计和使用也很方便。

综上所述，IC 卡优于磁卡，正在或将要逐步取代磁卡，并将开拓出新的应用领域。

## 1.3 IC 卡的安全问题

IC 卡是存储现金、票据、持卡人个人或单位资料等重要信息的媒体。IC 卡具有的安全技术必须足以保证信息的安全。

### 1.3.1 信息安全的特性

一般来讲，信息安全必须具有以下几个方面的特性：

- (1) 保密性，防止未经授权的信息获取；
- (2) 完整性，防止未经授权的信息更改（修改、删除、增加）；
- (3) 可获取性，防止未经授权的信息截取；
- (4) 真实性，利用技术手段验证信息的真实性，如数字签名；
- (5) 持久性，长时间保存信息的可靠性，准确性。

### 1.3.2 威胁 IC 卡信息安全的因素

威胁 IC 卡信息安全的因素主要来自两个方面：

#### 一、人为因素

人为因素具有主动性，它涉及到信息的保密性、完整性、可获取性、真实性，是对信息安全的主要威胁。具体可表现为以下几种情况：

- (1) 截取 IC 卡和接口设备之间的信息流，分析、复制或插入假信号；
- (2) 伪造 IC 卡，由于流入或流出 IC 卡及接口设备的信息是可以模拟的，因此，接口设备无法判断信息是来自合法的 IC 卡还是非法的 IC 卡；
- (3) 在交易中更换 IC 卡，由于在刷卡交易中，可能存在时间上的迟延，在该迟延时间内，将已授权的 IC 卡在响应信号写入之前换成另一张卡或一张假卡，将响应信号（即交易数据）写入该卡中；
- (4) 对 IC 卡提供错误的控制信息，如修改余额更新日期，从而可获取最高授权余额；
- (5) 销售方或承兑方的作弊；
- (6) 接口设备被借用，私自拆卸、改装；

(7) IC 卡的发卡过程，发卡机构的工作人员的安全管理；

(8) 持卡人的非法使用。

任何依赖用户的安全措施都是不可靠的，所以必须对持卡人、IC 卡和接口设备的合法性作相互校验，还需具有授权保护功能、审计跟踪功能、日志功能及设置止付名单（黑名单）。

## 二、客观因素

客观环境对 IC 卡的干扰、破坏，会影响到信息的持久性和准确性，因此，在封装设计上应考虑保护措施，使芯片免受化学、电气、静电损害。此外，对电触点也须采取措施使之免受玷污。

### 1.3.3 IC 卡的安全技术

#### 一、IC 卡卡基表面的安全技术

(1) 荧光安全图像印刷技术；

(2) 微线条技术：肉眼看来是一段直线，实际为一系列很小的具有一定安全标识意义的字母、数字序列；

(3) 激光雕刻签名：利用激光将有关图形、字母、数字等签名信息直接“刻入”IC 卡卡基中，而不是仅仅印刷在卡的表面；

(4) 激光雕刻可触摸向量字符；

(5) 激光雕刻图像，利用激光将持卡人照片以不同辉度完全印刷嵌入卡基内；

(6) 安全背景结构，类似于纸币的回纹图案等；

#### 二、硬件安全

芯片保护，包括金属化结构、熔断丝、探测器、随机数产生、存储器逻辑保护和协处理器提供加密运算等措施。芯片安全是 IC 卡安全的基础。其反物理攻击的方法主要有下面几种：

(1) 通过烧断熔丝使测试功能不可再激活；

(2) 高 / 低电压检测；

(3) 低时钟工作频率的检测；

(4) 通过监控程序防止对地址和数据总线的截听；

(5) 逻辑实施对存储器的保护，设置错误计数器，连续三次口令错误，锁死芯片；

(6) 总线和存储器的物理保护层。

#### 三、软件安全

##### 1. IC 卡存储区的保护

利用软件将 IC 卡的数据存储区划分为若干个区，对每个区都设定各自的访问条件；只有在满足设定条件的情况下，才允许对相应的数据存储区进行访问。通过存储区域的划分，普通数据和重要数据被有效地分离，相应地提高了逻辑安全的强度。

##### 2. IC 卡通信安全与保密

主要是涉及通信过程中的信息完整性、可获取性、真实性和机密性。

(1) 对完整性的保证，即保证所交换报文内容不被非法修改，一般在报文内加入报头

或报尾，即鉴别码。鉴别码由发送方计算产生，和报文一起加密后发送。接收方收到后进行解密，然后用约定的算法算出鉴别码，将其与报文中的鉴别码进行比较。如相等，则报文完整。

对报文可获取性的保证，防止对曾经发送过或存储过的信息的再利用。其实质是对报文时间性的鉴别，即保证所传送的每一条信息都是唯一的，其后产生的重复信息全是非法的。一般在报文中加入一个以时间变量产生的随机数。

(2) 对真实性的保证，即对报文发送方和接收方的鉴别。这一鉴别采用数字签名及身份认证 (Authentication) 的概念，也就是说 IC 卡和接口设备之间只有相互认证之后才能进行数据的读、写等具体操作。认证的主要目的在于鉴别伪造的 IC 卡及应用终端。

认证有以下几种工作方式：

内部认证：应用终端阅读 IC 卡中的固定数据，计算出认证密钥。终端产生随机数并送给 IC 卡，同时指定下一步应用的密钥。IC 卡用指定密钥对该随机数进行加密，然后将加密的随机数送回终端。终端对该随机数进行解密，比较是否一致，若一致则内部认证成功。

外部认证：终端设备从 IC 卡中读取卡数据并算出认证密钥。因为 IC 卡本身不能发送此数据，所以由终端设备控制。终端设备从 IC 卡中取得一随机数 (通常为 8 字节)，用认证密钥对之进行加密并发送到 IC 卡。IC 卡对此加密值进行对比。

相互认证：终端设备从 IC 卡中读取卡数据并从中算出认证密钥。终端设备从 IC 卡中取得一随机数 (通常为 8 字节) 并产生其自己的一随机数 (通常为 8 字节)，这两个随机数和卡数据由认证密钥一起加密。终端设备将此加密值送到 IC 卡。IC 卡用终端设备指定的认证密钥对此加密值进行解密、比较。若正确，IC 卡用认证密钥加密终端设备的随机数和自己的随机数，并将此加密值发送回终端设备。终端设备解密此加密值再与自己的随机数进行对比。

从以上三种认证工作方式可以看出，加密解密密钥只存在于 IC 卡和有关应用终端的内部，一旦形成决不外露。因此，密钥十分安全。每次认证以随机数为媒介，且每次认证数据均不相同 (相同概率很小) 因而破译难度大 (几乎不可能)，所以这种工作方式具有很高的安全性。其中加密解密算法一般均采用国际通用的 DES 或 RSA 算法。这两种算法均具有很高的安全性。

(3) 对机密性的保证，利用密码技术对报文进行加密处理。

### 1.3.4 密码算法

通常的有两种密码算法：第一种为对称密钥密码算法或秘密密钥算法 (DES)；第二种为非对称密钥密码算法或公共密钥算法 (RSA)。

(1) 对称密钥密码算法或秘密密钥算法 (DES)：

对称密码体制，就是加密密钥和解密密钥是相同的，即使不同，也容易由其中一个导出另一个。也就是说，在这种密码体制中，能加密也就能解密，所以密钥的管理成为影响系统安全的关键。目前，这种特点已难以适应现在计算机系统开放性的要求。

DES 密码是 1977 年由美国国家标准局公布的一个分组密码算法。

分组密码是将明文按一定的位长度分组，明文组和密钥组全部经过加密运算得到密文组。解密时密文组和密钥组经过解密运算（加密运算的逆运算），还原为明文组。

分组密码的优点是：密钥可以在一定时间内固定，不必每次变换，因此给密钥配发带来了方便。但是，由于分组密码存在着密文传输错误在明文中扩散的问题，因此在信道质量较差的情况下无法使用。

## (2) 非对称密钥密码算法或公共密钥算法 (RSA):

1976 年有人提出了公共密钥密码体制，其原理是：加密密钥和解密密钥分离。这样一个具体用户就可以将自己设计的加密密钥和算法公诸于众，而只保密解密密钥。任何人利用此加密密钥和算法向该用户发送的加密信息，该用户均可以将之还原。因此，人们通常也将这种密码体制称为双密钥密码体制或非对称密码体制。

公共密钥密码的优点是：不需要经安全渠道传递密钥，大大简化了密钥管理。所以，又可称为公开密钥算法或简称为公钥算法。

1978 年有人提出了公共密钥密码的具体实施方案，即 RSA 方案。

1991 年提出的 DSA 算法也是一种公共密钥算法，在数字签名方面有较大的应用优势。

目前，国际上在智能 IC 卡上应用得较多的加密解密算法是 DES 算法、RSA 算法及 DSA 算法。下面重点介绍这三种算法。

### 一、数据加密标准 DES

1973 年，美国国家标准局开始研究除国防部外的其它部门的计算机系统的加密标准（加密算法要达到的目的（通常称为 DES 密码算法要求）主要有以下几点：

- 提供高质量的数据保护，防止数据未经授权的泄露和未被察觉的修改；
- 具有相当高的复杂性，使得破译的开销超过可能获得的利益，同时又要便于理解和掌握；
- DES 密码体制的安全性应该不依赖于算法的保密，其安全性仅以加密密钥的保密为基础；
- 实现经济、运行有效，并且适用于多种完全不同的应用。

1977 年 1 月，美国政府颁布：采纳 IBM 公司设计的方案作为非机密数据的正式数据加密标准（DES—Data Encryption Standard）。

#### 1. DES 密码算法

DES 密码实际上是 Lucifer 密码的进一步发展。它是一种采用传统加密方法的分组密码。它的算法是对称的，既可用于加密又可用于解密。

图 1.1 中  $k_i (i=1\sim 16)$  是初始密钥  $K$  经分解、移位后生成的 48 位长的子密钥； $f$  为密码函数。子密钥  $k_i$  的生成如图 1.2 所示。初始密钥  $K$  为 64 位，其中 8、16、24 …、64 ( $8 * N$ ) 位是奇偶校验位，所以  $K$  的有效位只有 56 位。对有效位的数据 56 位按换位规则  $P$  (见表 1.1) 进行换位，再将得到的结果分为左右两部分  $C_0$ 、 $D_0$ ，各 28 位。 $C_0$ 、 $D_0$  分别经循环左移得到  $C_1$ 、 $D_1$ ，左右合并，按换位规则  $CK$  (见表 1.2) 进行缩小换位，得到 48 位子密钥  $k_1$ 。同样  $C_1$ 、 $D_1$  分别经循环左移得到  $C_2$ 、 $D_2$ ，左右合并，按换位规则  $CP$  进行缩小换位，得到 48 位子密钥  $k_2$ 。同理可得  $k_3, \dots, k_{16}$ 。这里循环左移的位数按表 1.3 进行。

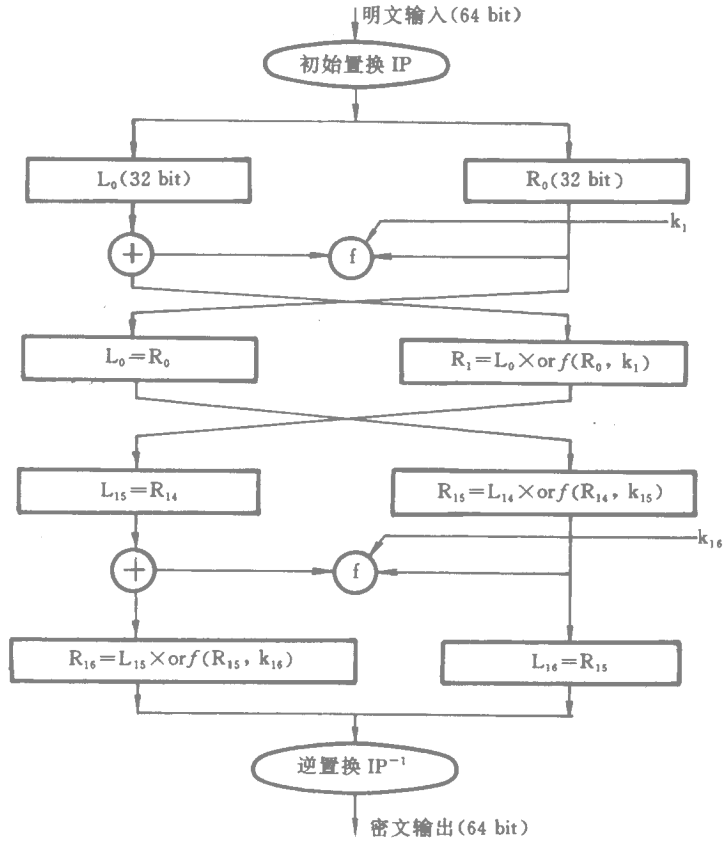


图 1.1 DES 密码算法粗框图

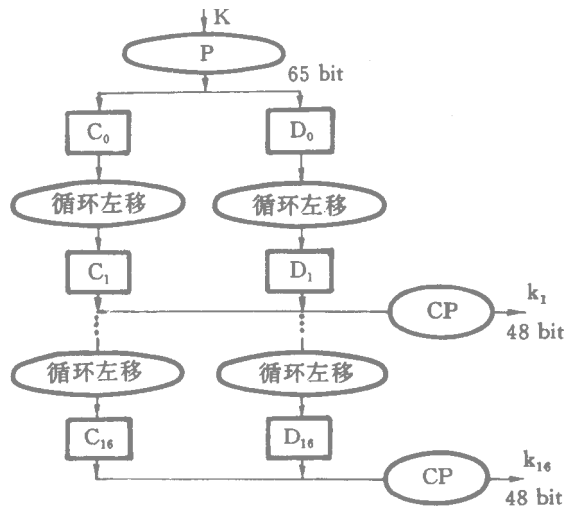


图 1.2 子密钥 k<sub>i</sub> 的生成

表 1.1 换位规则 P

57	49	41	33	25	17	9
1	58	50	42	34	26	18
10	2	59	51	43	35	27
19	11	3	60	52	44	36
63	55	47	39	31	23	15
7	62	54	46	38	30	22
14	6	61	53	45	37	29
21	13	5	28	20	12	4

表 1.2 换位规则 CP

14	17	11	24	1	5
3	28	15	6	21	10
23	19	12	4	26	8
16	7	27	20	13	2
41	52	31	37	47	55
30	40	51	45	33	48
44	49	39	56	34	53
46	42	50	36	29	22

表 1.3 循环左移的位数

迭代次数	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
左移位	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

要加密的明文经过初始置换 IP (见表 1.4) 的处理, 然后再经一系列迭代运算, 所得结果由 IP 的逆置换  $IP^{-1}$  (见表 1.5) 给出加密结果。IP 的功能是将输入的 64 位数据按位重新组合, 分为  $L_0$ 、 $R_0$  两部分, 位长皆为 32 位。表 1.4 为初始置换 IP 的换位规则, 表 1.5 为逆置换  $IP^{-1}$  的换位规则。 $f$  为密码函数, 其结构如图 1.3 所示。它的功能是利用放大换位 EP (见表 1.6) 将 32 位的  $R_{i-1}$  扩展到 48 位。在与子密钥  $k_i$  按位作模 2 加后, 将所得结果分为 8 个 6 位长的数据块, 分别经替代函数  $S_1, S_2, \dots, S_8$  (即所谓的 S 盒) 变换产生 8 个 4 位长的数据块, 合并为 32 位再经简单换位 SP (见表 1.7) 得到  $f(R_{i-1}, k_i)$ 。表 1.8 为替代函数  $S_i$ 。

表 1.4 初始置换 IP 的换位规则 表 1.5 逆置换  $IP^{-1}$  的换位规则

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
32	1	41	9	49	17	57	25

表 1.6 放大换位 EP

32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

表 1.7 简单换位 SP

16	7	20	21
29	12	28	17
1	15	23	26
5	18	31	10
2	8	24	14
32	27	3	9
19	13	30	6
22	11	4	25

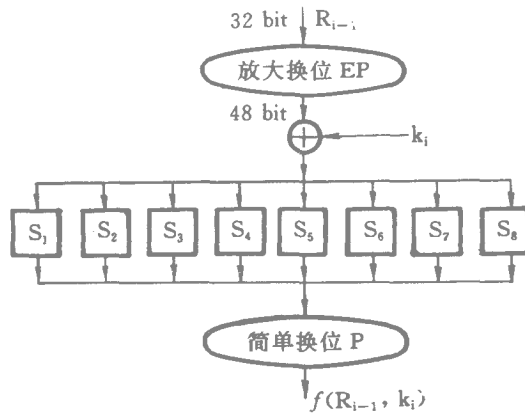


图 1.3 密码函数  $f$  结构图

表 1.8 替代函数  $S_i(S_{\text{盒}})$

R/h	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7	$S_1$
1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8	
2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0	
3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13	
0	15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10	$S_2$
1	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5	
2	0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15	
3	13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9	
0	10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8	$S_3$
1	13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1	
2	13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7	
3	1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12	
0	7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15	$S_4$
1	13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9	
2	10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4	
3	3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14	
0	2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9	$S_5$
1	14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6	
2	4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14	
3	11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3	
0	12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11	$S_6$
1	10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8	
2	9	14	15	5	2	8	12	3	7	0	4	10	1	3	11	6	
3	4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13	

续表

R/h	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
0	4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1	$S_7$
1	13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6	
2	1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2	
3	6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12	
0	13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7	$S_8$
1	1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2	
2	7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8	
3	2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11	

说明：假设输入 6 位二进制数  $D = d_1d_2d_3d_4d_5d_6$ ，则表中  $h = d_2d_3d_4d_5$ ， $R = d_1d_6$ ，根据  $R$ 、 $h$  可得  $S = s_1s_2s_3s_4$  (4 位二进制数) 完成将 6 bit 的输入变换为 4 bit 的输出。

DES 算法可以使用四种操作模式，这四种操作模式是：电子密文、密码分组链接、输出反馈及密文反馈。其中，电子密文是最简单的模式，安全性也最差；密码分组链接经常以软件方法实现；输出反馈和密文反馈往往在硬件实现的算法中实现。

DES 公布之后，制造有关 DES 设备的厂商已达几十家。随着 DES 应用的日益扩大，各种 DES 专用芯片也应运而生，这种 DES 芯片价格便宜，加密解密速度快，在有关产品中使用时十分广泛。

## 2. DES 密码的破译

首先考虑用穷举法破译 DES 密码的问题。设已知一段密码文  $C$  及与它对应的明码文  $M$ ，用一切可能的密钥  $K$  加密  $M$ ，直到得到  $E(M) = C$ ，这时所用的密钥  $K$  即为要破译的密码的密钥。穷举法的时间复杂性是  $T = O(n)$ ，空间复杂性是  $S = O(1)$ 。对于 DES 密码， $n = 2^{56} \approx 7 \times 10^{16}$ ，即使使用每秒钟可以计算 100 万个密钥的大型计算机，也需要算  $10^6$  天才能求得所使用的密钥，因此看来是很安全的。

## 3. DES 密码反破译的策略

自 DES 算法公诸于世以来，人们一直对 DES 的安全性持怀疑态度，对密钥的长度、迭代次数及  $S$  盒的设计众说纷纭。从技术上说，对 DES 的批评主要集中在以下几个方面：

(1) 作为分组密码，DES 的加密单位仅有 64 位（二进制），这对于数据传输来说太小，因为每个分组仅含 8 个字符，而且其中某些位还要用于奇偶校验或其他通讯用途；

(2) 密钥仅有 56 个二进制位未免太短，各次迭代中使用的密钥  $K(i)$  是递推产生的，这种相关性降低了密码体制的安全性。目前，有人认为：在现有的技术条件下用穷举法寻找正确密钥已趋于可行，若要安全保护 10 年以上的数据最好不用 DES 算法；

(3) 实现替代函数  $S$  所用的  $S$  盒的设计原理尚未公开，其中可能留有隐患。更有人担心 DES 算法中有“陷阱”，知道秘密的人很容易进行密文解密。

针对以上 DES 的缺陷，人们提出了几种增强 DES 安全性的方法，主要有以下几种：

- 三重 DES 算法：此方法为密码专家 Merkle 及 Hellman 推荐。
- 具有独立子密钥的 DES 算法：每一轮迭代都使用一个不同的子密钥，而不是由一个 56 个二进制位的密钥产生。由于 16 轮迭代的每一轮使用一个 48 个二进制位的密钥，所以这一方法可以增强 DES 的加密强度。

· 带用交换 S 盒的 DES 算法: Biham 和 Shamir 证明, 通过优化 S 盒的设计 甚至 S 盒本身的顺序, 可以抵抗差分密码分析, 以达到进一步增强 DES 算法的加密强度的目的。

## 二、RSA (Rivest - Shamir - Adleman) 算法

1976 年, Diffie 和 Hellman 在斯坦福大学发表了在密码学史上有深远意义的论文《密码学的新方向》。他们指出, 可以适当选择加密算法 E 和解密算法 D, 使得即使知晓加密算法 E 也无法推出解密算法 D。他们的论文使密码工作者耳目一新, 开辟了密码学研究的一个新方向。他们提出的密码体制要满足以下三个要求:

- (1)  $D(E(M)) = M$ ;
- (2) 从 E 推出 D 在计算上是不可能的;
- (3) 用选择明码文破译 E 在计算上是不可能的。

第一条要求说明, 如果把 D 运用于加密后的消息  $E(M)$  将恢复明码文消息 M。第二条要求是公共密钥密码体制的关键, 否则就不能将 E 公开。第三条要求也是完全必要的, 因为在已知 E 的情况下, 密码分析员肯定会选择一些明码文, 用 E 对它加密, 并千方百计地破译它。

满足这些要求后, 就没有理由再不把 E 公布于众。在利用公共密钥密码体制时, 需要进行秘密通讯的用户首先设计出满足以上三个要求的 E 和 D。然后把 E 公布于众, 比如刊印在文件中或登记在手册上。任何想与他通讯的用户都可以用他的公开变换加密消息 M 生成  $E(M)$  他收到  $E(M)$  后, 再用他的秘密变换 D 解密  $E(M)$ , 得到明码文消息  $M = D(E(M))$ 。

在传统密码体制中, 由于加密密钥和解密密钥可以简单的互导, 因此密钥必须首先经由安全通道分发给通讯双方, 随后才能利用公共通道建立起安全通讯, 因而密钥分配问题是传统密码体制的薄弱环节。公共密钥密码体制不存在这个问题, 因此特别适合于在计算机网络中建立分散于各地的用户之间的秘密通讯联系。

公共密钥密码体制的上述优点, 使得设计者的论文问世之后立即受到密码学界的普遍关注。许多研究人员进行了认真的研究, 目前已发表了一些实用的算法。RSA 方法就是其中一种。

RSA 算法于 1978 年首次推出, 以三位发明者 Rivest、Shamir 及 Adelman 的名字命名, 并在以后经受住了多年广泛的密码分析破译。

RSA 算法的安全性来自于分解大数因子的困难。大数分解 (将一个大合数分解成其素数因子的乘积) 和素性检测 (判定一个给定的正整数是否为素数) 是著名的数论难题之一, 高斯曾称之为“算术中最重要最有趣的问题之一”。古往今来, 曾吸引不少的中外学者以浓厚的兴趣为此付出了艰辛的努力, 然而由于其本身所固有的难度及指数阶的计算复杂度, 一直困扰着人们进行更深入的探索。本世纪 50 年代以来, 随着计算机技术的飞速发展以及有关理论方法的不断提出, 对这个古老的难题研究又重新兴起, 许多研究成果被直接应用于密码学中, 导致了密码学研究的第二大成就的代表——RSA 公共密钥密码体制的出现, 并广泛应用于金融、商业等领域。

在 RSA 算法中 解密密钥 (专用) 和加密密钥 (公用) 是一对非常大 (100~200 位十进制数或更大) 的素数的函数, 该算法由素数计算出两个密钥, 而且猜想由一个密钥确定另一个密钥相当于分解两个素数乘积的因子。目前, 为实现 RSA 算法, 需要寻找大质数, 这个

问题已基本解决，但大数分解的问题则进展十分缓慢，因而 RSA 算法可以成为一个较为成熟、实用的方案。

RSA 算法也有不足之处，就是计算复杂，影响加密、解密速度。近年来有不少人研究如何提高 RSA 的幂模运算速度。几年前日本人曾提出，多模数  $N$  为 512 位(154 位十进制数)可以用 2.5 万门的集成电路芯片实现，使 RSA 的加、解密速度达到每秒 5 万二进制位。

### 三、DSA 算法简介

1991 年 8 月 NIST (美国国家标准和技术学会)提出了符合其新的数字签名标准 DSS (Digital Signature Standard) 的数字签名算法 DSA (Digital Signature Algorithm)。DSA 和 DSS 之间的关系是 DSA 为算法，DSS 为标准，标准实现算法，算法是标准的一部分。

DSA 算法是 Schnorr 和 El Gamal 签名算法的变形。DSS 本身不能用于加密，它只是一种签名标准，当然 DSA 算法也是一种签名算法。

NIST 公布 DSA 招来了一片抨击和谴责：

抨击之一是认为 DSA 算法比 RSA 慢。事实上也确实如此，据估计产生签名约慢 40% 验证签名约慢 100 倍。但随着计算机技术的飞速发展，这倒不会成为一个永久性的严重问题。RSA 算法是事实上的标准，即使许多公司已经使用了 RSA 标准，可是谁又能保证不必支付专利权费用的 DSA 算法不会赢得广大用户的青睐呢。

抨击之二是 DSS 是美国国家保密局 (NSA) 制定的算法中可能有“陷阱”这对我国有关用户，特别是对金融、电信等涉及国家宏观经济领域的应用来讲，确实是一个值得研究和重视的问题。

## 1.4 金卡工程

金卡工程是我国金融电子化建设的重要组成部分。它是以电子货币的形式，将计算机、通信技术应用于金融和商业流通，实现电子货币跨部门、跨地区的结算流通的系统工程。

### 1.4.1 金卡工程总体构想

我国的金卡工程总体构想是建立统一的金卡工程专用全国网络系统，建立全国性的金卡网络服务中心，建立全国统一的金卡发行体系，以便从现在起，在十年左右的时间内，在全国三亿城市人口中推广普及金融交易卡，进而实现支付手段的革命性变化，使我国国民经济和社会生活迈入到电子货币时代。通过严格控制现金额流通量的做法，减少偷税漏税发生率和堵塞非法金融活动，并通过完善金融立法和制度的必要手段，实现稳定和规范化金融秩序的全面建立。

金卡工程的实质是在全国范围内通过计算机技术、现代通信技术、现代金融电子化技术成果的应用，使我国传统的纸币和纸面票据的流通与交换转变成无纸化电子货币的流通与交换，进而推动我国国民经济信息化的进程，促进金融领域、财税领域和现代商业领域管理活动的现代化，并带动我国信息产业有一个较大的发展。

为实现这一目标，首先要在我国建成一个完善的银行卡巨型网络系统，这种网络系统

能够确保国家各级金融机构之间、金融银行机构与各个商户之间、各地区之间以及国内与国外金融机构之间，具有可靠的、有效的、方便快捷的电子货币交易。在同一个城市或同一地区，同一银行系统内部的各种金融计算机系统连结成网，使其网内的各个业务点之间可以通存通兑；在不同银行系统之间，通过网络系统交换中心进行互联，使用户可以实现跨行通存通兑；在全国范围内的不同地区，也可通过金融广域网络，实现各地区银行间的通存通兑；通过与国际金融银行卡网络系统相连，可以在全球范围内实现电子货币交换。

在我国主要城市和一些发达地区，将广泛使用银行磁卡或银行智能卡（IC卡），按照在三亿城市人口中广泛使用银行卡计算，达到香港地区九十年代中期的使用水平（平均每四个人一张），要比日本九十年代中期全国发卡总量多一倍。

尽管与许多发达国家相比，我国的银行卡业务起步较晚，但是发展却十分迅速。据统计，到1993年底，我国信用卡的发行量和交易额分别为430万张和1400亿元人民币。按照金卡工程的预计目标，我国在今后十年左右的时间内，将会出现数量巨大的持卡者队伍，并使用各种电子货币进行交易活动。

#### 1.4.2 金卡工程规划和布署

整个工程为期十年，分为三个阶段。这三个阶段是试点阶段、推广阶段、普及阶段。

第一阶段（1994年~1996年）已实施。第一阶段先在十多个省、市进行试点，取得经验，渐次扩展。通过这一试点阶段，使我国一些沿海、沿江发达城市和地区的发卡总量达到3000万张，相应的城市人口覆盖量达到约3000万人。在上述试点城市和地区，要求每百万人口拥有200台自动柜员机（ATM）、2000台联网销售点终端机（POS）及一批必要的配套设施。

为了向全国推广银行卡应用系统，在各试点城市和地区正在建设城市（或地区）的银行卡授权交换中心。这些授权中心将与各所在城市（或所在地区银行）清算中心连成网络，实现同城、同地区的银行卡跨行通存通兑业务。

银行卡授权交换系统的试点建设，对我国广泛推广使用银行卡进行无纸货币支付和交易具有十分重要的作用。它将使银行卡的使用趋于实时化、高可靠和简单快捷，使持卡者乐于使用，并可使那些利用现在的银行卡使用过程中授权过程的缓慢而进行恶性透支者无所遁形。

通过这一阶段的银行卡授权交换系统的试点建设，将为全国金融银行系统实现信用卡设施资源共享、商户开放、统一收单、统一授权、准确止付、统一清算开辟道路。金卡工程覆盖面广，它将推进金融领域实现与支付、授权、清算等有关金融业务处理的高度自动化和无纸操作，进而扩展到商业消费领域业务活动的自动化和无纸操作。

第二阶段，我国将在1997年到2000年前这一阶段中，对金卡工程的已有成果和经验进行大规模的推广应用。在这一阶段中，不是一下子把银行卡和邮政储汇“绿卡”发行到全国，一步到位地在十二亿人口中推广使用银行卡等无纸支付手段，而是步步为营地先在第一阶段的试点城市的基础之上，再按照切实可行的条件，把发卡范围扩展到包括全国省会城市在内的30~50个主要城市，达到全国发卡总量为6000万张、城市人口覆盖面积为1亿、年交易额为6000亿元以上的水平。

在这一阶段中，与推广相对应的是巩固和完善已有（或已建成）的银行卡发卡、联网、

应用和综合服务环境，并进一步提高包括国家授权交换中心在内的各城市（各地区）授权交换中心的效率及可靠程度，进一步完善与国际银行卡授权交换系统的紧密联系。

在第三阶段（2000年~2003年）中，金卡工程将在全国 1/4 范围进行推广，形成普及之势。届时，我国将成为世界上使用银行卡人数最多的国家。在全国约 400 个城市和人口覆盖面约达 3 亿的地区，将完成卡基支付业务的应用和综合设施的建立，发卡总量将达 2 亿张以上，年交易额上升到 1 万亿元以上。到那个时候，全国将建立起完善的涉及卡基支付业务的法律和法规，以及与之相适应的监督系统。以上述城市为主体的银行卡应用系统，又将成为向各个县、乡扩展的主干系统。

金卡工程对全国走向金融电子货币交换这一不可逆转的重大变革，将起到不可估量的巨大作用。

### 1.4.3 金卡工程有关标准

金卡工程是我国国民经济信息化过程的主要起步工程之一。它的制定和分步实施已在国内外引起巨大反响，作为一个巨大的系统工程，人们已经认识到标准化工程的重要性。金卡工程所要建立的银行卡网络应用系统，必须有完整的系统设计、系统工程实施和系统验收等国家标准，才能保证其在全国范围内的各个不同层次、地区及不同银行系统中，具有高度的硬件可兼容性、可互换性、可扩展性和软件的可靠性、规范性及安全性。

为满足金卡工程任务的紧迫需求，在国家标准尚未制定出来之前，有关机构对照国际有关标准，并结合金卡工程现有情况，编写了《金卡工程标准化指南》。该指南既可以作为银行卡和其它金融卡用户及有关工程设计人员的工程基础性规范标准，又可作为较为权威的指导性文献。

在业已发行的“指南”第一册中，编列出识别银行卡和其它金融卡（多种磁卡或 IC 卡）物理特性的基本技术与记录技术，有关金融卡的标准规范等。尚未发行的“指南”第二册编列出智能卡（IC 卡）的数据结构、编号注册程序和安全系统等。第三册则涉及卡本身的安全和数据安全问题及相应的应用标准等。后续各册将分别编写有关自动柜员机、销售点终端设备、光卡及相关接口部件的标准规范化内容。



## IC 卡及其专用芯片

芯片是 IC 卡的基础，它的性能和成本对 IC 卡的推广使用有着很大的影响。目前，世界上有很多 IC 卡芯片生产商，已进入我国市场较为著名的有美国的 ATMEL 公司、德国的 SIMENS 公司等。本章将详细介绍他们的几种典型 IC 卡专用芯片。

### 2.1 美国 ATMEL 公司的 AT24C01/AT88SC102/AT88SC51 芯片

美国 ATMEL 公司在设计和制造 IC 卡专用高性能芯片上处于世界领先水平，其产品基本代表了该领域的最新发展水平，下面详细介绍几种芯片。

#### 2.1.1 简单存储芯片 AT24C01/02/04/08/16

##### 一、芯片说明

AT24C01/02/04/08/16 提供 1024/2048/4096/8192/16384 位串行 EEPROM，EEPROM 组态为 128/256/512/1024/2048 \* 8 位。IC 卡低电压工作时，将  $A_0$ 、 $A_1$ 、 $A_2$  接地即可。AT24C01/02/04/08/16 为低功耗 CMOS 工艺制造，可单电压工作。

##### 二、芯片特点

###### 1. 低电压

5.0 V ( $V_{cc}=4.5\sim6.0$  V)

3.0 V ( $V_{cc}=2.7\sim6.0$  V)

2.5 V ( $V_{cc}=2.25\sim6.0$  V)

2.0 V ( $V_{cc}=1.8\sim6.0$  V)

###### 2. 内部组态

AT24C01 的容量为 128 \* 8(1 KB)，AT24C02 的容量为 256 \* 8(2 KB)，AT24C04 的容量为 512 \* 8(4 KB)，AT24C08 的容量为 1024 \* 8(8 KB)，AT24C16 容量为 2048 \* 8

(16 KB).

- 双线串行接口 ( 双线为 : 时钟线 SCL 串行数据线 SDA );
- 双向数据传送协议 ;
- 支持 ISO/IEC 7816—3 同步协议 ;
- 8 字节页面 ( 1 KB, 2 KB )、16 字节页面 ( 4 KB, 8 KB, 16 KB ) 写入方式 ;
- 允许部分页面写入 ;
- 自定时写入周期 ( 最大 10 ms );
- 高可靠性, 擦写次数可达 10 万个周期, 数据保存期达 100 年 ;
- 以晶片、模块及标准封装等形式提供。标准封装有 8 个引脚的双列直插 (PDIP)、8 个引脚的表面封装和 14 个引脚的表面封装 (SOIC);
- 晶片和芯片厚度为 (6~21 密耳 (mil)<sup>①</sup>);
- 提供测试卡中芯片的测试程序 ;
- 芯片体积较小, 增加了可靠性, 降低了成本。

### 三、IC 卡芯片的触点

AT24C01 芯片触点功能见表 2.1, 其触点位置见图 2.1。

表 2.1 AT24C01 芯片触点功能说明

芯片触点	引脚	功能
C1	V <sub>cc</sub>	工作电压
C2	NC	未连接
C3	SCL(CLK)	串行时钟
C5	GND	地
C6	NC	未连接
C7	SDA(I/O)	串行数据(输入/输出)

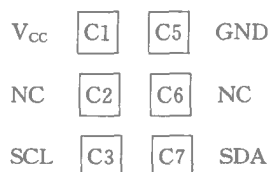


图 2.1 AT24C01 芯片触点

### 四、芯片最大额定值

工作温度 : -55 ~ +125

贮存温度 : -65 ~ +150

任一管脚对地电压 : -1.0 ~ +0.7 V

最大工作电压 : 6.6 V

DC 输出电流 : 50 mA

### 五、芯片内部功能逻辑

AT24C01 芯片逻辑图如图 2.2 所示。下面对该芯片引脚作一简要说明。

#### 1. 引脚说明

SCL( 串行时钟 ): SCL 上升沿将数据输入到 EEPROM 芯片, 下降沿将 EEPROM 中的数据输出。

SDA( 串行数据 ): 双向串行数据传送引脚, 该引脚采用漏极开路驱动, 可以与其他任何数量的漏极开路或集极开路器件进行“线或”。

A<sub>0</sub>、A<sub>1</sub>、A<sub>2</sub>( 器件 / 页地址 ): 器件地址输入端, 应用于标准封装中。IC 卡中的 A<sub>0</sub>、A<sub>1</sub>、A<sub>2</sub> 不引到触点。

<sup>①</sup> 1 mil = 25.4 × 10<sup>-3</sup> mm

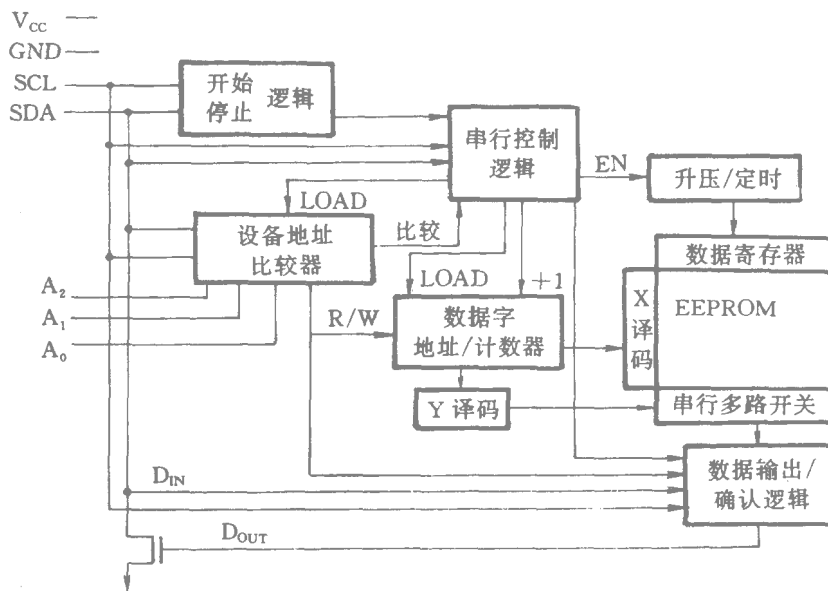


图 2.2 AT24C01 芯片逻辑图

## 2. 逻辑图组成

启动/停止逻辑：控制一次读/写操作的开始和停止。

串行控制逻辑：在 IC 卡中，SCL 为同步时钟，地址、数据和读写控制命令从 SDA 输入，由串行控制逻辑区分。

地址/计数器形成访问 EEPROM 的地址，分别送 X 译码器进行字选，送 Y 译码器进行位选。

升压/定时线路：EEPROM 的写入操作需要高电压，所以芯片内有升压线路，将标准电压提升到 12~20 V。

数据输入/应答逻辑：控制数据的输入/输出和确认应答信号。

## 3. 器件操作

时钟和数据传送：SCL 和 SDA 通常各自通过一个电阻上拉到高电平，SDA 上的数据仅在 SCL 为高电平时有效，在低电平时允许数据变化见图 2.3。当 SCL 为高电平时，数据的变化表示“开始”或“停止”两种状态。其定义如下：

开始态：SCL 处于高电平时，SDA 从高电平转向低电平表示一种操作的开始，所以该状态应在其他命令之前执行，见图 2.4。

停止态：SCL 处于高电平时，SDA 从低电平转向高电平表示一种操作的结束，将停止所有通讯。在一个读时序后，停止命令置 EEPROM 于等待状态。

确认(ACK)：所有地址和数据字以 8 位码串行输入、输出，总线上的任何接收数据设备(当与 EEPROM 通讯时)必须将 SDA 总线置于低电平，以确认它成功的接收到了每一个字，该确认必须在每个字及其他所有设备脱离 SDA 总线之后，即第九个时钟周期发生，见图 2.5。EEPROM 也通过在收到的每个地址或数据码之后，置 SDA 于低电平的方式确认。