综 述

智能 IC 卡中的信息加密技术

孙克辉 ,盛利元 ,杨 宏
(中南大学物理科学与技术学院 ,湖南长沙 410083)

摘 要: 智能 IC 卡的信息安全是其生存和发展的基础。本文在介绍了智能 IC 卡基本结构、分析当前的信息加密技术现状的基础上 ,详细讨论了智能卡中常用的信息加密算法(DES、RSA)原理及其实现 ,对新的混沌加密技术作了简要分析。

关键词: 智能卡; 信息安全; DES; RSA; 混沌加密
中图分类号:TN409 **文献标识码**:A **文章编号**:1008 - 0147(2003)03 - 11 - 04

Information Encryption Techniques in Smart IC Card

SUN Ke - hui ,SHENG Li - yuan , YANG Hong
(*College of Physics Science and Technology , Central South University , Changsha Hunan* ,410083 , *China*)

Abstract : The information security of smart IC card is the base of its existing and developing. In this paper ,the basic structure of smart IC card is introduced ,and on the basis of the analysis for present state of information encryption techniques ,the principles of several usual information encryption algorithms ,such DES ,RSA ,and their realization are discussed in detail ,At last ,a new encryption method - chaos sequence encryption is analyzed bricfly.

Keywords : Smart IC card; Information security; DES; RSA; Chaos encryption

1 引言

1977 年 ,Motorola 与它的一个计算机客户合作开发了世界上第一张智能卡 ,此后 ,智能卡开始迅猛发展 ,智能卡所采用的技术也日新月异地发生着变化。进入 20 世纪 90 年代后 ,在通信、卫生、交通等方面 ,智能卡的应用也开始蓬勃发展 ,每年以 34 % 的速度增长[1]。

智能卡在 IC 卡家族中出现最晚、也最具生命力。由于其具有较强的数据处理能力和较大存储容量 ,因此应用的灵活性、适应性较强。而在硬件结构、操作系统、制作工艺上所采取的多层安全措施 ,则保证了其极强的安全防伪能力[2]。它不仅可验证卡和持卡人的合法性 ,而且可鉴别读写终端 ,已成为一卡多用和对数据安全保密性特别敏感场合的最佳选择 ,如金融信用卡、手机 SIM 卡等。

智能卡硬件结构包括:CPU、存储器(含 RAM、

基金项目: 中南大学文理基金资助项目部分研究内容
收稿日期: 2002-08-28

ROM、EEPROM)、卡与读写终端通讯的 I/O 接口以及加密运算协处理器 CAU。其硬件结构如图 1 所示[3]。

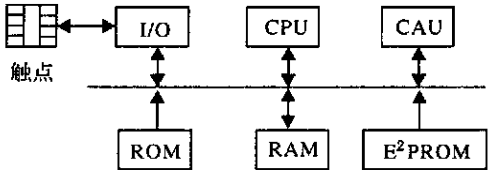

图 1 智能 IC 卡结构图

智能卡通常采用 DES、RSA 等加/解密算法来提高系统安全性能,采用 RSA 算法时要进行对运算速度要求很高的大指数模运算,8 位 CPU 难以胜任。因此,在一些高安全性加密微控制器卡芯片中(如 AT90SC1616C),均设置有专用加/解密运算协处理器 CAU。

2 信息加密现状

目前信息加密多采用基于密钥的方法。这种方法又可分为对称方法和非对称方法。DES、3DES, Blow fish, IDEA 等属于前者,其中 IDEA 使用 128 位长度的密钥,被认为是较好的方法。对称方法的特点是解密密钥和加密密钥相同。这种结构使得用对称方法实现的保密通信系统容易被破译,此外,密钥管理比较复杂。

典型的非对称方法是 RSA。它基于整数分解原理,采用了模数运算的方法。非对称方法的信息保密程度取决于求解指定数学问题的难度。目前涉及有指数分解、离散对数问题等。所解数学问题难度越大,则保密程度越高。和对称方法不同,非对称方法同时采用私钥和公钥。公钥可以象电话号码一样公开,发送方用公钥加密,接收方用私钥解密。这种方法安全性高,密钥管理方便,在商业系统中有广泛的应用前景。

基于密钥的方法有其局限性。首先它是一种静态方法,不能用于信息的实时处理。其次,它的运算速度是密钥长度的函数,即运算速度随着密钥长度的增加而降低,使其破译难度的提高受到制约。

混沌加密属于序列密码加密,是一种动态加密方法,由于其处理速度和密钥长度无关,因此这种方法的计算效率高。用这种方法加密的信息很难破译,具有很高的保密度。尤其是它可用于实时信号处理,同时也适用于静态加密的场合。尽管目前这项新技术的研究尚处于实验阶段,由于它的实时性强、保密性高、运算速度快等明显优势,已显示出其在信息加密中的强大生命力。

3 智能卡中的信息加密方法

目前,在智能卡中应用较多的加密技术有对称密码体制和非对称密码体制,其中较典型的加密算法是 DES 算法和 RSA 算法。随着技术的进步和安全性要求的不断提高,序列密码加密越来越受到人们的重视,特别是混沌加密算法的研究,将为信息加密技术带来新的革命。

3.1 DES 加密

DES 是迄今为止世界上最广泛使用和流行的一种分组密码算法。该算法使用长度为 56 比特的密钥,加密长度为 64 比特的明文,获得长度为 64 比特的密文,其加密过程如下:

①给定一个明文 x,通过一个固定的初始置换 IP 置换 x 获得 x_0,记 $x_0 = IP(x) = L_0R_0$,这里 L_0 是 x_0 的前 32 比特,R_0 是 x_0 的后 32 比特。

②然后进行 16 轮完全相同的运算,在这里,数据与密钥相结合。计算规则如下:

$$L_i = R_{i-1} \qquad (1 \leq i \leq 16) \qquad (1)$$

$$R_i = L_{i-1} \oplus f(R_{i-1}, k_i) \qquad (2)$$

其中 $\oplus$ 表示比特串的异或,f 是一个函数,$k_1, k_2, \cdots, k_{16}$ 都是密钥 k 的函数,长度均为 48 比特,$k_1, k_2, \cdots, k_{16}$ 构成了密钥方案。一轮 DES 加密过程如图 2 所示。

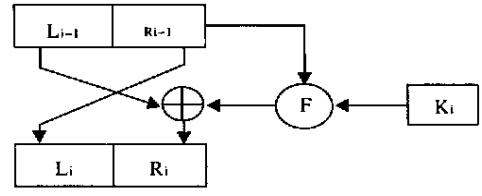

图 2 一轮 DES 加密过程

③对比特串 $R_{16}L_{16}$ 应用初始置换 IP 的逆置换 IP^{-1},获得密文 y,即 $y = IP^{-1}(R_{16}L_{16})$。注意最后

一次迭代后,左边和右边未交换,而将 $R_{16}L_{16}$ 作为 IP^{-1} 的输入,目的是为了使算法可同时用于加密和解密。

函数 f(A,J) 的第一个变量 A 是一个长度为 32 的比特串,第二个变量 J 是一个长度为 48 的比特串,输出是一个长度为 32 的比特串。f 的计算过程如下:

①将 f 的第一个变量 A 根据一个固定的扩展函数 E 扩展成一个长度为 48 的比特串。

②计算 E(A) ⊕J,并将所得结果分成 8 个长度为 6 的比特串,记为 $B = B_1B_2B_3B_4B_5B_6B_7B_8$。

③使用 8 个 S - 盒 $S_1, S_2, \cdots, S_8$。每一个 S_i 是一个固定的 4 ×16 阶矩阵,它的元素来自 0 - 15 这 16 个整数。给定一个长度为 6 的比特串,如 $B_j = b_1b_2b_3b_4b_5b_6$,按下列办法计算 $S_j(B_j)$:用两比特 b_1b_6 对应的整数 r(0 ≤r ≤3) 来确定 S_j 的行,用 4 比特对应的整数 c(0 ≤c ≤15) 1 来确定 S_j 的列,$S_j(B_j)$ 的取值就是 S_j 的第 r 行第 c 列的整数所对应的二进制表示。记 $C_j = S_j(B_j)$,1 ≤j ≤8。

④将长度为 32 比特串 $C = C_1C_2C_3C_4C_5C_6C_7C_8$ 通过固定的 P 置换,将所得结果 P(C) 记为 f(A,J)。函数 f 的产生如图 3 所示。

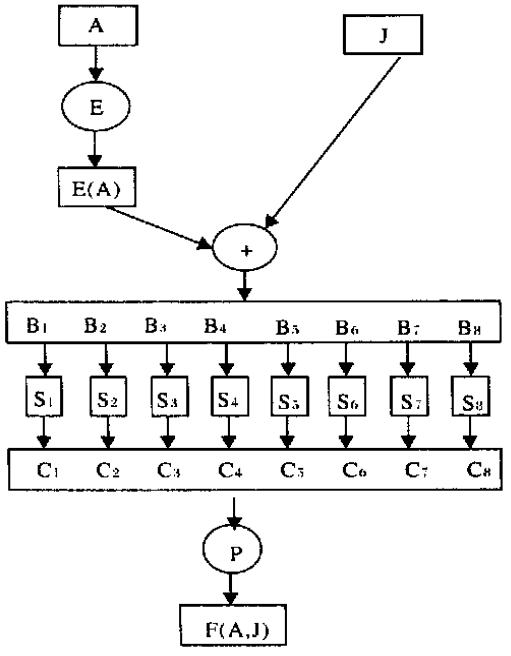

图 3　DES 的 f 函数产生

DES 算法的安全性在于攻击者破译的方法除了穷举搜索外还没有更有效的手段,而 56 位长的密钥的穷举空间是 2^{56},可见 DES 算法的保密强度还是比较高的[4]。随着计算机的运算速度越来越快,DES 算法的安全程度有所降低,所以现在倾向采用 128bit 密钥。

3.2　RSA 加密

RSA 公钥密码是一种典型的非对称密码,它由 Rivest、Shamir 和 Aolleman 联合提出,称之为 RSA 公钥密码系统。RSA 算法的理论基础是一种特殊的可逆模指数运算。它的安全性依赖于大数的因式分解的困难性。其算法描述如下:

①适当选取一组大素数(十进制位数超过 100,即 $> 10^{100}$)p 和 q(保密)。

②令 n = pq(公开),计算 n 的 Euler 函数 $\phi(n)$ = (p - 1) (q - 1) (保密)。

③随机选取一小整数 e(加密密钥,公开),使得 $(e, \phi(n)) = 1$,且 $e < \phi(n)$。

④根据 $e \times d \equiv 1 \bmod \phi(n)$,计算 d(解密密钥)。

对每一个 K = (n,p,q,e,d),公开 n 和 e,保密 p,q 和 d,定义加密变换为:

$$E_k(x) = x^e \bmod n,\ x \in Z_n \qquad (3)$$

解密变换为:

$$D_k(y) = y^d \bmod n,\ y \in Z_n \qquad (4)$$

RSA 加密算法的安全性取决于 n 分解为 p、q 的困难程度。由于大数分解在数学上是一个难题,目前还没有人能够找到一种十分有效的方法,因此可以保证 RSA 运算的安全性。RSA 的不足之处是密钥生成比较麻烦;另外,加密、解密的计算十分复杂,速度较慢;而智能卡受其外形尺寸的限制,计算能力还不强,这使 RSA 加密算法在智能卡中的应用受到限制,但,随着技术的发展,这一问题已基本得到解决。

3.3　混沌加密

混沌加密基于混沌系统所具有的独特性质:对初值极端敏感性和具有高度的随机性。混沌加密的原理与序列密码的原理相似,不同在于:一般的序列密码是利用移位寄存器为基础的电路来产生伪随机序列作为密钥序列,而混沌加密是利用混沌系统产生混沌序列作为密钥序列,利用该序列对明文加密,密文经信道传输,接收方用混沌同步的方法将明文信号提取出来实现解密。

混沌序列加密是指明文数据与一“乱数流”叠加产生密文,称该“乱数流”为加密序列,它由一个密钥产生[5]。序列加密的数学模型可作如下描述:

明文序列:

$$x^{\infty}=(x_0,x_1,x_2,\cdots),\ x_i\in GF(q) \qquad (5)$$

“乱数流”:

$$k^{\infty}=(k_0,k_1,k_2,\cdots),\ k_i\in GF(q) \qquad (6)$$

由明文序列与“乱数流”可产生密文序列:

$$y^{\infty}=(y_0,y_1,y_2,\cdots),\ y_i\in GF(q) \qquad (7)$$

其中 $y_i=x_i+k_i,\ i=0,1,2,\cdots$

“乱数流”也是一无穷序列,在密码学中通常采用随机序列或伪随机序列。混沌序列加密的主要特点是加密方式十分简单,它只要对两个序列进行叠加即可。混沌序列加密原理如图 4。

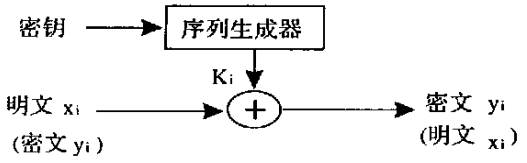

图 4 混沌(序列)加密原理

混沌序列加密,是一种很有前途的加密方法,具有随机性好,保密性强,密钥量大等特点。

4 加密算法的选择与实现

DES 和 RSA 算法均可由硬件和软件实现。目前,DES 芯片速度的最快记录保持者是由美国 DEC 公司,数据加/解密速率达 1G 比特/秒,它能在 1 秒内加密 1560 万个分组数据。在 IBM3090 大型计算机上的 DES 软件实现方法每秒能完成 32000 次加密,在微机上要慢一些,但仍相当快。目前,RSA 的最有效的硬件实现的加密速率达到每秒 600K 比特,与 DES 的硬件实现的每秒 1G 比特的加密速率相比,RSA 大约比 DES 慢了 1500 倍。在软件实现中,DES 大约比 RSA 快 100 倍。这些速率会随着技术的发展而改变,但 RSA 的速率将永远不会达到私钥密码算法的速率。这就是为什么大多数实际系统中仅用 RSA 来变换 DES 密钥,而后用 DES 加密信息的原因。混沌加密是一个新的研究课题,翁贻方[6]等人提出了混沌加密的软件实现算法,其等效密钥长度达 600 位,是很有前途的一种加密算法。

智能卡中的信息加密采用较多的是 DES 算法。由于智能卡中微处理器的计算能力限制,如果要用程序实现 RSA 算法,通常在卡内设置适合于加密/解密运算的协处理器(CAU)。实践表明,利用协处理器可大大提高密码算法的速率。如,用 8051 对 512 比特的操作数进行加密运算时需 1～4 分钟,而利用带有协处理器的智能卡,则仅需 1.5 秒左右[7]。随着技术的进步,在智能卡技术中采用非对称密码体制或混沌序列密码体制是一种必然的趋势。

5 结论

随着智能 IC 卡应用范围的不断扩大,智能 IC 卡的信息安全和保密性显得日益重要。利用信息加密技术可大大提高智能卡应用时的安全程度。由于混沌序列加密具有随机性好,保密性强,密钥量大的特点,其在智能卡中的应用,将为智能卡的信息安全提供保障。

参考文献:

[1] 王爱英. 智能卡技术[M]. 北京:清华大学出版社,2000.10.

[2] 孙克辉,盛利元. 黄德祥. 逻辑加密型 IC 卡的安全性能分析,微电子技术[J]. 2002,30(1):20 - 23.

[3] 陆永宁. IC 卡应用系统[M]. 南京:东南大学出版社,2000,5.

[4] 冯登国,裴定一. 密码学导引[M]. 北京:科学出版社,1999.4.

[5] 沈世镒. 近代密码学[M]. 桂林:广西师范大学出版社,1998,11.

[6] 翁贻方等. 混沌同步保密通信技术及软件实现,计算机工程[J]. 1999,25(10):105 - 107.

[7] 李国新等. 密码技术在智能卡中的应用,计算机工程与应用[J]. 2000,3:60～63.