公钥密码学

曹珍富 著

黑龙江教育出版社
1993年·哈尔滨

（黑）新登字第5号

公 钥 密 码 学

曹珍富 著

责任编辑：韩殿发
封面设计：安玉滨

黑龙江教育出版社出版（哈尔滨市道里区九站街1号）
齐齐哈尔铁路印刷厂印刷·新华书店北京发行所发行
开本 850×1168 毫米 1/32·印张 6.625·插页 2·字数 150 千
1993年10月第1版·1993年10月第1次印刷
印数：1—1 500

ISBN 7-5316-2045-6/O·8 定价：4.80元

目　录

第一章

公钥密码学的理论基础

§1.1 Shannon信息论

1.1.1 Shannon保密系统

1949年，Shannon[1]在“保密系统的通信理论”一文中，提出了一整套如今被称为信息论的基础理论的概念和方法，并且用来度量密码体制的保密性. Shannon将一个密码体制表示为如图1—1的保密系统.

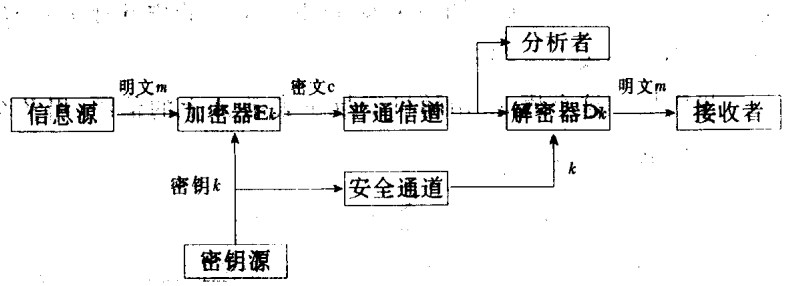

图1—1 Shannon保密系统框图

其中信息源(简称信源)是若干消息或明文的集合，故也称为消息空间或明文空间，记为M. 密钥源是若干供加、解密使用的密钥空间，记为K. 发送者欲将明文$m\in M$秘密发送给接收者，双方首先通过安全信道约定好一个密钥$k\in K$，发送者通过加密器获

得密文 $c=E_k(m)$，并将 c 通过普通信道发送出去. 接收者通过解密器获得明文 m，即

$$D_k(c) = D_k(E_k(m)) = m,$$

其中对$\forall\ k\in K$，D_k 与 E_k 是一对互逆变换. 密码分析者(也称破译者)从普通信道上只能截获到密文 c，所以，他们的任务就是从密文 c 求出明文或密钥. 这是一个完整的传统的密码系统.

1.1.2 保密性度量——信息量与熵

设信息源的输出符号取值于一离散集合 $A=\{a_1,a_2,\cdots,a_n\}$，其中符号 a_i 出现的概率记为 $p(a_i)(i=1,\cdots,n)$，且 $\sum_{i=1}^{n}p(a_i)=1$. 对$\forall\ a\in A$，以 $I(a)$记符号 a 的信息量，通常定义

$$I(a) = -\log p(a),$$

这里对数的底通常是 2，相应的信息量的单位为比特(bit). 十分显然，a 的"不确定性"与 a 的信息量 $I(a)$有着密切的关系. 例如 a 表示"1+1=2"，这时由于 a 是一个众所周知的确定性事件，所以提供给人们的信息量是零；如果 a 表示哥德巴赫(Goldbach)猜想[注]，则 a 包含了很多未知的东西，因此 a 的不确定性要大一些，信息量 $I(a)$也要大一些.

我们推广这个概念. 用随机变量 x 表示 A 上的信源，用各个符号信息量的平均值

$$H(x)=-\sum_{i=1}^{n}p(a_i)\log p(a_i)$$

来度量信源 x 的不确定性，并将 $H(x)$称为该信源的熵，也称 $H(x)$为信源 x 的熵函数. 十分显然，当诸 $p(a_i)$均相等时 $H(x)$达到最大值，此时 $p(a_i)=\frac{1}{n}(i=1,2,\cdots,n)$且

[注] 哥德巴赫猜想是：对任给的偶数 $N\geqslant 4$，都存在两个素数 p_1，p_2，使得 $N=p_1+p_2$. 这是一个没有证明的著名难题.

$$\max H(x)=-\sum_{i=1}^{n}\frac{1}{n}\log\frac{1}{n}=\log n.$$

当某个 $p(a_i)=1$ 时，$H(x)$达到最小值 $\min H(x)=0$. 因此熵函数满足

$$0\leqslant H(x)\leqslant\log n.$$

设随机变量y的可能值位于集合$B=\{b_1,b_2,\cdots,b_m\}$中，$\sum_{i=1}^{m}p(b_i)=1$. 令$p(x|y)$表示对于给定y后，随机变量x的条件概率，并用 $p(x,y)$表示给定 x,y 的联合概率. 根据概率的乘法定理，我们有 $p(x,y)=p(x|y)p(y)$. 记 $H(x|y)$为给定 y 后 x 的条件熵，其定义是

$$H(x|y)=-\sum_{x,y}p(x,y)\log p(x|y),$$

其中和号$\sum_{x,y}$ 表示对所有 $x\in A,y\in B$ 求和，即上式也可以改写为

$$\begin{aligned}H(x|y)&=-\sum_{i,j}p(a_i,b_j)\log p(a_i|b_j)\\&=-\sum_{j=1}^{m}p(b_j)\sum_{i=1}^{n}p(a_i|b_j)\log p(a_i|b_j).\end{aligned}$$

定义 x,y 的联合熵为 $H(x,y)$，其表达式为

$$H(x,y)=-\sum_{x,y}p(x,y)\log p(x,y).$$

则直接验证有

$$\begin{aligned}H(x,y)&=H(x)+H(y|x)\\&=H(y)+H(x|y),\end{aligned}$$

并且

$$H(x|y)\leqslant H(x),\quad H(y|x)\leqslant H(y).$$

由此显然，如果 x,y 是互相独立的两个事件，则

$$H(x,y)=H(x)+H(y).$$

如果事件 y 完全被事件 x 所确定，则

$$H(x,y)=H(y).$$

类似地，可定义 n 个随机变量 $x_1,x_2,\cdots,x_n$ 的联合熵

$$H(x_1,x_2,\cdots,x_n)=H(x_1)+H(x_2|x_1)+\cdots+H(x_n|x_1,\cdots,x_{n-1}).$$

若将 $a\in A,b\in B$ 分别看成是一个系统对应的输入与输出，则输出 b 提供给输入 a 的信息量 $I(a;b)$ 定义为

$$I(a;b)=\log(p(a|b)/p(a)).$$

显然 $I(a;b)=I(b;a)$. 这表明两个事件 a,b 可以互相提供的信息量相等，所以 $I(a;b)$ 也称为 a 与 b 间的互信息. 对 $I(a;b)$ 统计平均，则得到 x 与 y 的平均互信息

$$I(x;y)=\sum_{x,y}p(x,y)I(x;y),$$

这里随机变量 x,y 的可能值分别位于 A,B 中，和号 $\sum_{x,y}$ 表示对所有 $x\in A,y\in B$ 求和. 由此定义可得 $I(x;y)$ 与 $H(\cdot)$ 的关系，我们有

$$\begin{aligned}I(x;y)&=H(x)-H(x|y)\\&=H(y)-H(y|x)\\&=H(x)+H(y)-H(x,y)\\&\geqslant 0.\end{aligned}$$

在密码学中，密码分析员的任务是，在截获密文 c 后，求出密钥 k 或明文 m. 因此，相应地有两种条件熵，即给定密文 c 后，密钥 k 的条件熵 $H(k|c)$ 与明文 m 的条件熵 $H(m|c)$：

$$H(k|c)=-\sum_{c}p(c)\sum_{k}p(k|c)\log p(k|c),$$

$$H(m|c)=-\sum_{c}p(c)\sum_{m}p(m|c)\log p(m|c).$$

因为可能存在多个密钥把一个明文 m 加密成相同的密文 c，即满足 $c=E_k(m)$ 的 k 值可能不止一个，所以 $H(k|c)\geqslant H(m|c)$. 密码设计员同样依据 $H(k|c)$ 与 $H(m|c)$ 来设计密码体制，例如，当 H

$(m|c)=H(m)$时，相应的密码体制被称为绝对安全的，因为此时截获到的密文没有给分析员提供任何附加信息．被称为一次一钥的密码体制是绝对安全的．这种体制虽然在唯密文攻击下是安全的，但不能保证在已知明文或选择明文攻击下也是安全的．

使用互信息的概念，我们有

$$I(m;c)=H(m)-H(m|c),$$

因为 $H(m|c,k)=0$，故

$$\begin{aligned} I(m;c,k) &= H(m) - H(m|c,k) \\ &= H(m). \end{aligned}$$

对任何密码体制，由于

$$\begin{aligned} H(k|c) &= H(k|c) + H(m|k,c) \\ &= H(m,k|c) \\ &= H(m|c) + H(k|m,c) \\ &\geqslant H(m|c), \end{aligned}$$

及

$$H(k)\geqslant H(k|c),$$

故

$$\begin{aligned} I(m;c) &= H(m) - H(m|c) \\ &\geqslant H(m) - H(k|c) \\ &\geqslant H(m) - H(k). \end{aligned}$$

这表明，当密钥熵越大，则密文中包含的明文信息量就越小．若密文与明文间的互信息 $I(m;c)=0$，则窃密者在唯密文破译下无论截获多大密文，均不能得到有关明文的任何信息．所以，绝对安全的密码体制也可以被定义为适合 $I(m;c)=0$ 的密码体制，这种体制存在的必要条件是 $H(m)\leqslant H(k)$．

§1.2 计算复杂性理论

对给定问题，研究求解的方法并分析执行此方法需要操作的次数是复杂性理论的重要内容. 因此，很自然地，复杂性理论对于设计密码体制、分析破译方法的计算需求以及研究破译的困难程度，均是十分重要的.

1.2.1 基本概念——算法分类

一个要求给出解答的一般提问称为一个问题. 它由两个要素组成：具体实例与询问. 求解问题的过程如果能用一组明确指定操作顺序的规则描述，则说该问题是算法可解的，其中全体明确指定的操作顺序的规则构成了一个算法. 执行算法所需要的时间 T 与空间 S 称为算法复杂性. 假设 n 是输入规模，则 T 与 S 都可以表示为 n 的函数.

通常 $T(n)$ 与 $S(n)$ 均用其自身的阶来表示. 设 $f(n)$，$g(n)$ 均是正整数集 $\mathscr{Z}_{>0}$ 到 $\mathscr{Z}_{>0}$ 的函数，如果存在常数 c 和 N，使得当 $n>N$ 时 $f(n)\leqslant cg(n)$，则说 $f(n)$ 具有阶 $g(n)$，记为 $f(n)=O(g(n))$. 这样做具有与系统独立的优点，例如没有必要知道各种指令的精确执行时间和各种数据类型具体占用的空间，但却能看到，当 n 增大时，时空需求是如何增长的.

根据算法的时间(或空间)复杂性将算法分成两类：一是当算法的执行时间是 $T(n)=O(n^t)$，t 为常量时，称该算法是多项式时间算法或有效算法；另一是当 $T(n)$ 不能囿界于多项式时的算法称为指数时间算法. 通常把找不到有效算法的问题称为难解问题.

算法可分为确定性算法与非确定性算法. 确定性算法在图灵机(或其它抽象的计算模型)上每执行一步计算都有确定的下一步动作，因此，每一个操作的结果都是唯一确定的. 对于一个非确定性算法，在图灵机上每执行一步可有选择地进行下一步动作，即算

法中的某些操作的结果不是唯一确定的，而只限制在某个特定的可能结果的集合中. 因此，非确定算法也称为概率算法. 对非确定性算法，可以选择一个序列能导致算法成功地完成，则达到成功地完成所需的最少步数叫做非确定性算法所需要的时间. 很显然，确定性算法可以看成非确定性算法的特例.

1.2.2 问题分类

根据确定性与非确定性算法以及时间复杂性，可以将问题分成 P 问题、NP 问题、NP 难问题、NP 完全问题、$Co-NP$ 问题等. 所谓 P 问题，是指用确定性算法，在多项式时间内解决的问题，而 NP 问题则是指用非确定性算法在多项式时间内可以解决的问题. 用 P、NP 分别表示 P 问题类、NP 问题类，则显然 $P\subseteq NP$. 但是，对每个 NP 问题，究竟有没有确定性算法在多项式时间内求解？$P=NP$？虽然许多 NP 问题看上去比 P 问题困难得多，但至今还没有证明 $P\neq NP$. 这是计算复杂性理论中的著名难题.

设 π_1 和 π_2 是两个问题，若 π_1 可用多项式时间的确定性算法转化为 π_2，而 π_2 的解又可以用多项式时间的确定性算法转化为 π_1 的解，则称 π_1 可归约为 π_2，记为 $\pi_1\propto\pi_2$. 利用归约的概念，可以将问题进行转化. 例如，若 $\pi_1\propto\pi_2$，则对 π_1 的研究可以转化为对 π_2 的研究.

设 π 是一个给定的问题，如果对 $\forall\ \pi'\in NP$ 均有 $\pi'\propto\pi$，则称 π 是 NP 困难问题. 如果 π 是 NP 困难问题，并且 $\pi\in NP$，则 π 称为 NP 完全问题或 NPC 问题. 显然，如果能证明任意一个 NPC 问题属于 P 问题，则 $NP=P$. 因此，NPC 问题是 NP 问题中最困难的问题，它们的已知最快算法在最坏情况下均具有指数阶的时间复杂性.

以 $Co-NP$ 表示由 NP 问题的否问题构成的集合，我们不知道 $NP=Co-NP$ 是否成立，但确实存在一些问题处在 NP 和 Co

$-NP$ 的交集中. 由于验证 $Co-NP$ 问题的解比验证 NP 问题的解困难，因此人们倾向于 $NP \neq Co-NP$. 但是，如果假定有某个 NPC 问题，它的否问题(属于 $Co-NPC$ 类)也属于 NP，那么就会推出 $NP=Co-NP$. 所以，学术界普遍倾向于：如果问题 $\pi \in NP \cap Co-NP$，则 π 不是 NPC 问题.

图 1—2 显示了不同类别之间的大致关系，它们之间的确切关系，至今还不甚清楚. 在图 1—2 中，$PSPACE$ 类的问题被定义为以多项式阶空间求解的问题，它包括 NP 与 $Co-NP$ 类的问题. 但在 $PSPACE$ 类中也有被认为比 NP 问题和 $Co-NP$ 问题更难的问题. 当然，最为困难的是没有任何算法能以任意复杂性求解的问题(称为不可判定问题). 例如 Hilbert 第十问题的否定回答[4*]，证明了丢番图方程 $f(x_1, \cdots, x_n)=0 (n \geqslant 3)$ 是否有解的问题是不可判定问题，其中 $f(x_1, \cdots, x_n)$ 是任给的具有整系数的多项式.

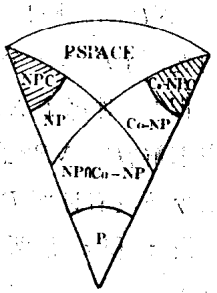

图 1—2　问题类别的关系

在设计密码体制时，常常是从已知的 NPC 问题或 NP 问题出发来构造，以保证足够的安全性.

1.2.3　一些 NP 问题介绍

(1)背包问题(Knapsack 问题)

实例：n 个整数的集合 $A=\{a_1, a_2, \cdots, a_n\}$ 和整数 s.

询问：存在 A 的一个子集，其中所有元素之和等于 s 吗？

容易知道[5*]，背包问题是 NP 问题. 进一步地，它还是一个 NPC 问题. 该问题的一个等价的说法是：设 $a_1, a_2, \cdots, a_n$ 是 n 个整数的序列，s 是一个整数，问方程 $a_1x_1+a_2x_2+\cdots+a_nx_n=s$ 是否有满足 $x_i \in \{0,1\}, 1 \leqslant i \leqslant n$ 的解？

(2)整数分解问题(简称分解问题)

实例:正整数 n.

询问:存在整数 $n_1,n_2,1<n_1,n_2<n$ 使 $n=n_1n_2$ 吗?

这是一个著名的 NP 问题,求解它的已知最快的确定性算法是 Morrison 与 Brillhart[2] 得到的,但仍需要进行 $O(\exp\sqrt{\log n\log(\log n)})$ 次算术运算.同时,由于分解问题的否问题是:对所有整数 $n_1,n_2,1<n_1,n_2<n,n\neq n_1n_2$ 吗?即 n 是素数吗?这个问题也是一个 NP 问题,所以分解问题既是 NP 问题又是 $Co-NP$ 问题.因此,倾向性的意见认为分解问题不是 NPC 问题.

(3)矩阵覆盖问题(简称 MC 问题)

实例:一个整数环 Z 上的 n 阶方阵 A,和 $s\in Z$.

询问:存在 $(x_1,\cdots,x_n)\in\{0,1\}^n$ 使得

$$(x_1,\cdots,x_n)A\begin{bmatrix}x_1\\ \vdots\\ x_n\end{bmatrix}=s?$$

已经证明[5*],MC 问题是一个 NPC 问题.背包问题可以看成 MC 问题特例,例如

$$A=\begin{bmatrix}a_1 & & O\\ & a_2 & \\ & & \ddots\\ O & & a_n\end{bmatrix}\text{时,}$$

$$(x_1,\cdots,x_n)A\begin{bmatrix}x_1\\ \vdots\\ x_n\end{bmatrix}$$

$$=a_1x_1^2+\cdots+a_nx_n^2$$

$$=a_1x_1+\cdots+a_nx_n.$$

(4)二元二次丢番图方程问题

设 $f(x_1,\cdots,x_n)(n\geqslant 2)$ 是任给的具有整系数的多项式，丢番图方程 $f(x_1,\cdots,x_n)=0$，当 $n\geqslant 3$ 时是否有解是一不可判定问题. 对于 $n=2$， A. Baker[4*]一般地定出了丢番图方程 $f(x_1,x_2)=0$ 解的上界，因此存在算法判定 $f(x_1,x_2)=0$ 是否有解. 但这种算法的复杂性常常是指数阶的. 例如，对如下的二元二次丢番图方程问题：

实例：三个正整数 a,b,c.

询问：丢番图方程 $ax^2+by=c$ 存在整数解吗？

Manders 和 Adleman[3]于 1978 年证明了这一问题属于 *NPC* 类的问题(可参阅[5*]). 从[5*]可知下面问题也是属于 *NPC* 类的问题：

实例：三个正整数 a,b,c，且 $a<b$.

询问：同余式 $x^2\equiv a(\mathrm{mod}\ b)$ 存在小于 c 的正整数解吗？

(5)陪集重量问题

设向量 $\boldsymbol{x}=(x_1,x_2,\cdots,x_n)\in\{0,1\}^n$，所谓 $\boldsymbol{x}$ 的 Hamming 重量(简称重量)是指向量 $\boldsymbol{x}$ 的各分量中 1 的个数，记为 $W_H(\boldsymbol{x})$. 1978 年，Berlekamp，McEliece 和 Van Tilborg[4]证明了下面两个问题均是 *NPC* 问题.

1)陪集重量问题

实例：$\{0,1\}$ 上的一个 $n\times m$ 矩阵 A，一个 m 维向量 $\boldsymbol{y}=(y_1,y_2,\cdots,y_m)$，及一个正整数 w.

询问：存在向量 $\boldsymbol{x}=(x_1,x_2,\cdots,x_n)\in\{0,1\}^n$，$W_H(\boldsymbol{x})\leqslant w$ 使得 $\boldsymbol{x}A=\boldsymbol{y}$ 吗？

2)子空间重量问题

实例：$\{0,1\}$ 上的一个 $n\times m$ 阶矩阵 A，及一个正整数 w.

询问：存在向量 $\boldsymbol{x}=(x_1,x_2,\cdots,x_n)\in\{0,1\}^n$，$W_H(\boldsymbol{x})\leqslant w$ 使得