国防科技大学学报
JOURNAL OF NATIONAL UNIVERSITY OF DEFENSE TECHNOLOGY
第15卷第1期 1993年3月 Vol. 15 No. 1

一种设计八进六出“S”盒的方法

郑林华*
(电子技术系)

摘 要 本文叙述了一种同时考虑扩散性和均匀性的设计86S－box的方法，并给出了程序流程图及非线性强度和随机性的论证。

关键词 密码体制，S盒，八进六出法
分类号 TN918.4

1977年，美国国家标准局公布了数据加密标准（DES）。此后，虽然全世界的破译分析者对此进行了许多次破译尝试，但目前在原则上仍以为它的保密性是可以信赖的。

DES的核心是六进四出的“S”盒。人们通过长期的研究，发现了不少关于S－box的设计原则。虽然，“S”盒没有最终破译出来，但其许多设计原则对我们研制新的加密算法是大有用处的。本文中86S－box的设计就是根据其最普遍的扩散性与均匀性原则设计的。

1 设计方法

本文中86S－box扩散性的要求是以输入改变一位、输出改变两位或两位以上来满足的。均匀性要求每行或每列中“0”、“1”个数的相等。每列应含12个“0”和12个“1”，每行应含32个“0”和32个“1”。因为变换的一行是0～63的排列，所以，各位输出总的0、1数目是相等的，都等于32. 如果0和1是间隔地排列，这时0，1均匀性最好。如果0或1都集中地出现在某部分，这样的0、1分布是均匀的。0、1分布不均匀就很容易被破译。所以，必须同时考虑行列的均匀性，保证“S”盒内0、1均匀分布。

本文86S－box的结构是4行64列的矩阵形式。其结构如图1所示。

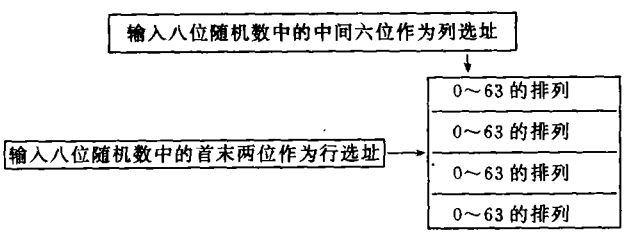

图 1

* 1992年2月22日收稿

矩阵的每行都为0～63的排列，即为000000～111111的排列。这样，行均匀性恒满足。在用软件产生86S－box的过程中，采用将均匀性和扩散性结合起来考虑的方法。这样，大大节省了计算时间。其具体方法如下：

把被输入的8位随机数中间的六位作为列选址：000000，000001，…，111111分别对应1至64列；首末两位作为行选址：00，01，10，11分别对应1至4行。可以发现：第一行和第二、三行的对应列输入改变一位，第四行和第二、三行的对应列输入改变一位，有列扩散性的要求；第二、第三行的对应列输入改变二位，没有列扩散性要求。所以，可先根据行扩散性确定第二、三行（行均匀性恒满足），然后，再确定第一行。在确定第一行的每一位时，需要同时兼顾行扩散性以及它与第二、三行对应位的列扩散性，还得兼顾到列均匀性满足的可能条件下，即在完成第四行时有满足均匀性的可能。这样，前三行“1”的个数必须满足6≤N≤12。在第一、二、三行确定下来以后，最后确定第四行。在确定第四行时，除象确定第一行时满足行扩散性和列扩散性以外，还必须兼顾每一列的“0”、“1”的个数完全相等，即满足均匀性。

在考虑行扩散性的时候，我们观察到，输入中间六位改变一位时有下列规律，如表1示。

表中相邻行与行之间每个输入的位数都改变一位。将表1中具体数值栏用二进制表示，更易看出其中的规律，如图2所示。

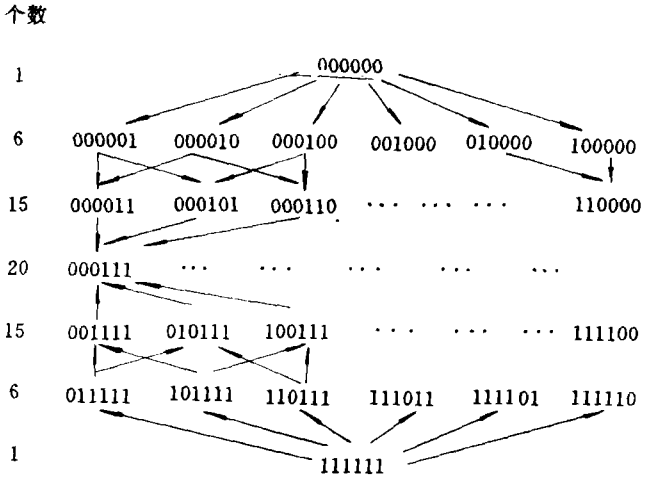

图 2

从图2中可明显地观察到输入位数改变一位时输入数值之间的关系。图中箭头起点位的数确定箭头终点位的数。从图2中的上半部分可以看出，将某位数值中的“0”逐个变成“1”，即可得到它所确定的位数的值。同样，图2下半部分是将某位数值中的“1”逐个变成“0”，即可得到它所确定位数的值。另外，图2上、下两半部分具有对称结构。这样，可采用先确定

表 1

个数	含n个“1”、“0”	具体数值(十进制表示)
1	0个“1”	0
6	1个“1”	1,2,4,8,16,32,(=2^n,n为0～5)
15	2个“1”	3,5,6,9,10,12,17,18,20,24,33,34,36,40,48
20	3个“1”/3个“0”	7,11,13,14,19,21,22,25,26,28,35,37,38,41,42,44,49,50,52,56
15	2个“0”	15,23,27,29,30,39,43,45,46,51,53,54,57,58,60
6	1个“0”	31,47,55,59,61,62,(=63－2^n,n为0～5)
1	0个“0”	63

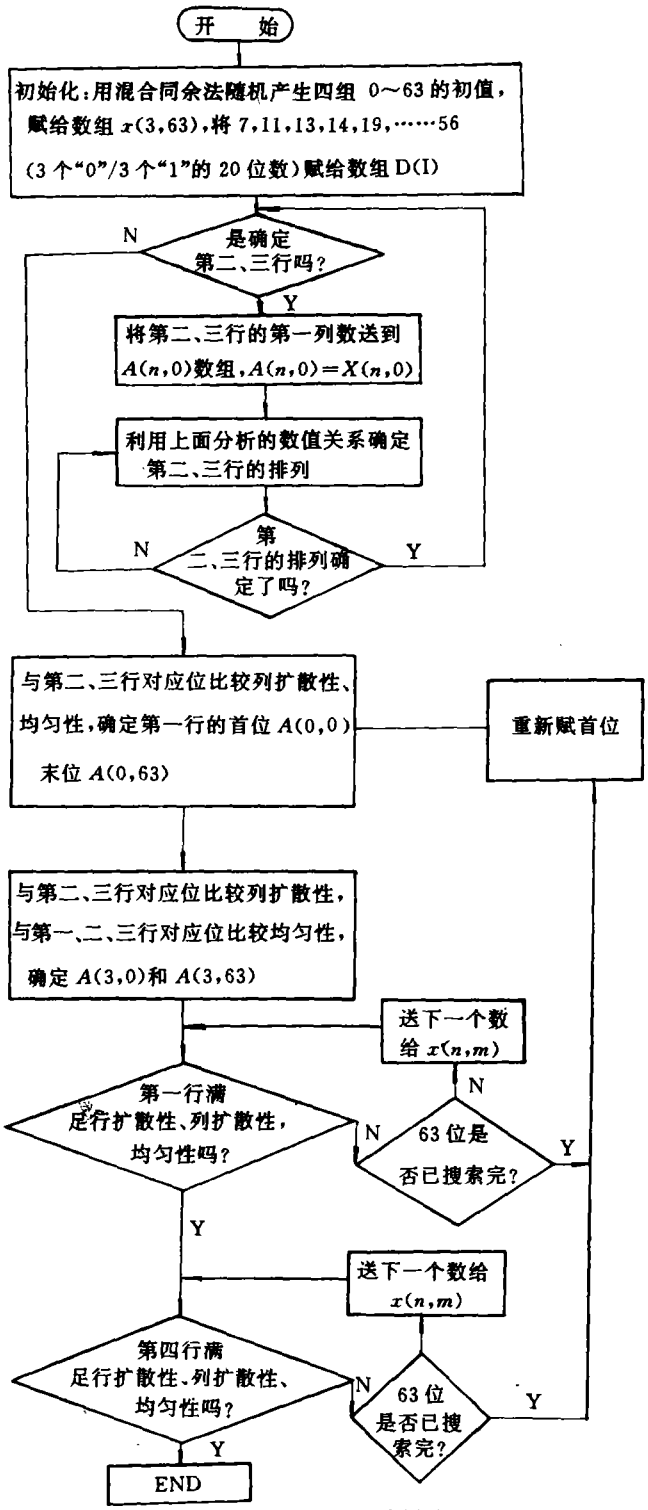

图 3　产生 86S－box 的程序框图

首末两位，由两头往中间挤的办法确定出满足扩散性的行来。确定 86S—box 的程序流程图如图 3 所示。由此方法确定的一个 86S－box 如表 2 所示。

表 2　一个 86S－box 的组合

N＝2

59 4 34 45 3 23 14 48 60 16 12 55 38 44 49 41 62 2 36 57 32 29 63 51 26 13
6 24 22 42 43 31 19 15 56 0 25 46 21 30 35 37 18 28 11 8 52 50 61 40 20 47
58 5 33 10 1 54 39 9 53 27 17 7
2 45 28 9 63 8 44 7 33 59 61 46 16 41 47 4 19 15 22 40 35 27 29 53 52 17
12 51 58 38 34 14 21 18 49 54 26 48 50 42 55 3 5 32 57 31 11 39 37 20 62
1 23 60 24 36 56 13 25 10 30 0 6 43
26 21 14 0 15 52 17 5 41 11 31 49 51 32 10 22 2 37 40 23 57 43 20 29 13 62
25 3 8 56 53 42 35 30 18 63 28 19 40 44 7 60 45 34 1 47 4 55 16 50 38 9 39
46 27 54 36 33 58 61 6 12 24 1
57 55 31 59 8 45 54 49 26 60 1 2 23 25 56 15 58 46 53 50 7 9 40 16 39 22
43 52 44 5 20 3 6 10 37 28 34 21 17 38 32 13 12 63 11 36 29 0 51 41 42 19
33 4 14 47 27 24 48 30 18 61 62 27

2　非线性强度及随机性的检验

检验过程是首先产生一个 m 序列。经过 86S—box 变换后，检验输出序列的周期性和局部统计特性。

2.1　局部统计特性的检验

我们用 H・贝克、F・派普尔著的《密码体制——通信保护》一书的频数检验、序列检验、扑克检验、游程检验、自相关检验来衡量局部统计特性。以上各种检验全在 PC 机上进行。检验结果表明：对于 86S－box，当其输入具有良好的统计特性时，其输出也具有良好的统计特性。

2.2　86S－box 的非线性强度

由 86S－box 的真值表可以求出其输出开关函数的最简逻辑表达式。由 86S－box 的第一位输出的最简逻辑表达式可以看出，它的非线性最高次数可达 7 次，项数为 55 项，并且含有单项式。其输入与输出存在复杂的非线性关系，每一位输出与所有输入都有关系。

2.3　86S－box 输出序列的周期

关于输出序列的周期性，我们有以下定理。

定理　设 x_1，x_2，…，x_n 为输入变量，输出 y 的开关函数多项式表达式为

$$y = c_1x_1 + c_2x_2 + \cdots + c_nx_n + f(x_1,x_2,\cdots,x_n)$$

其中多项式 $f(\cdot)$中没有 x_1，x_2，…，x_n 的一次项。若输入序列周期性为 L，则当 c_1 不全为“0”时，输出序列的周期也为 L。

证明　因 $y=c_1x_1+c_2x_2+\cdots+c_nx_n+f(x_1,x_2,\cdots,x_n)$　　(1)

此处 c_i 不全为 0，$f(\cdot)$为多项式。

设 y 的输出周期为 $\bar{c}$，则显然 $\bar{c}/l$(即 $\bar{c}$ 可被 l 整除)采用反证法。

若 $l\times\bar{c}$,记 y 的输出序列为 $Z_1,Z_2,\cdots$。

则有 $$Z_i=Z_{i+\bar{c}},\ (i=1,2,3,\cdots)$$

即 $$(c_1x_{i+1}+c_1x_{i+\bar{c}+1})+\cdots+(c_nx_{i+1}+c_nx_{i+n+\bar{c}})$$
$$+f(x_{i+1},x_{i+2},\cdots,x_{i+n})+f(s_{i+\bar{c}+1},x_{i+\bar{c}+2},\cdots,x_{i+\bar{c}+n})=0$$

记 $M(x)$为线性部分,$N(x)$为非线性部分

则 $$M(x)+N(x)=0 \qquad i=1,2,\cdots\cdots$$

即 $$P[M(x)+N(x)=0]=1 \tag{2}$$

对 $i=1,2,\cdots$,成立

又: $$P(x_i=0)=\frac{1}{2}$$

且因 c_i 不全为 0

故 $$P[M(x)=0]=\frac{1}{2}$$

则 $$P[M(x)+N(x)=0]$$
$$=P[M(x)=0]\cdot P[N(x)=0]+P[M(x)=1]\cdot P[N(x)=1]$$
$$=\frac{1}{2}\{P[N(x)=0]+P[N(x)=1]\}=\frac{1}{2} \tag{3}$$

由(3)式与(2)式矛盾。故知:$l/\bar{c}$.

我们证得 $l/\bar{c}$,且 $\bar{c}/l$. 所以 $l=\bar{c}$.

根据此定理可知 86S—box 输出序列的周期为 L.

参 考 文 献

1 H·贝克,F·派普尔. 密码体制——通信保护

2 H·迈耶、M·马特斯. 计算机数据保密的新领域——保密系统设计和实现指南. 国防工业出版社

3 Rainer A. Rueppel. Analysis and Design of stream Ciphers. 西北电子科技大学出版社

4 戴世虎. 布尔代数. 湖南教育出版社

A Method of 8 Input 6 Output "S" Box Design

Zheng Linhua

(Department of Electronic Technology)

Abstract

This paper discusses a method of 86S—box design which considers the diffusibility and the homogeneity. It also gives the flow scheme of the program and the demonstration of nonlinear intensity and radomization.

Key words cipher system,S—box,8 input 6 autput S box