国防科技大学学报
JOURNAL OF NATIONAL UNIVERSITY OF DEFENSE TECHNOLOGY
第10卷第4期 1988年12月 Vol.10.No.4

DES算法中S-盒的输入输出周期性研究

肖 戎

(电子技术系)

摘 要

DES应用于序列密码体制，其周期性问题没有一般的结论。文中证明了：DES中最关键部分—S盒对输入输出周期具有一个下界。

关键词：密码通信，DES算法，周期性

1 引 言

众所周知，序列密码体制的保密性取决于密码序列的一系列特性，其中包括：序列的周期长短、随机性等。即判断一个序列密码体制是否保密，存在一些包括上述两个问题在内的必要条件。但对于一个任意给定的体制，现在没有成熟的、严格的理论去证实它是否满足这一系列的必要条件，这不能不说是密码学理论中的一个不足之处。本文作者对此问题作了一些工作[1]。

可以把举世闻名的DES算法经过改造、组合后产生一个序列密码体制所需的密码序列，如图1所示：

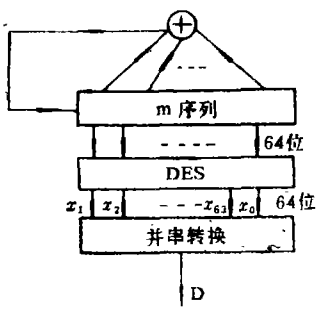

图 1

工作原理：m序列相邻的64比特作为DES的64位输入，经过DES算法得到相应的64比特输出，x_1，x_2，…，x_{63}，x_0。然后再经过并串转换，得到系统的串行输出D的64位。在下一时间单位，m序列右移一位，再对此时的64比特，重复以上过程，又得D的64比特，……。如此循环不已，则得密码序列D。

在研究D的周期性之前，注意到以下的已知事实：DES的64位输出是相互统计独立的。即：若把DES的每一个输出头的输出看成一个序列，记为$\{x_{1,n}\}$，$\{x_{2,n}\}$，…，$\{x_{63,n}\}$，$\{x_{0,n}\}$，D为这64个序列依比特位“嵌套”，即$D_n=x_{\mathrm{mod}(n,64),\ [n-1/64]+1}$，则这64个序列互相统计独立。

若把这64个序列看成一个二值平面，并记它们的周期分别为d_1，d_2，…，d_{63}，d_0，则二值平面的周期为$[d_1,\cdots,d_{63},d_0]$。故由统计独立性知，D的周期为$64\cdot[d_1,d_2,\cdots,d_{63},d_0]$。此处$[\ ]$表示最小公倍数。

故D的周期性问题转化为各个序列$\{x_{i,n}\}$的周期性问题。

1987年4月3日收稿

显而易见，DES 中的初始排列、逆初始排列、左右交换 32 位和 E 扩展 等过程对输入、输出周期的影响很容易决定，而影响最大、最关键的是其非线性变换，即S-盒。故我们将注意力集中于S-盒的研究上。

同理，S-盒的 4 位输出在统计上也是独立的，故我们可将问题简化为只用如下简单模型，来研究输入、输出的周期性。

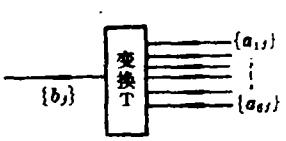

图 2

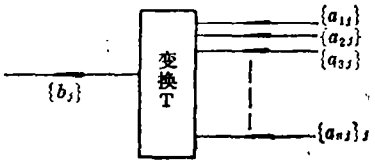

图 3

2 理 论 模 型

在进行研究S-盒对输入周期性的影响之前，为叙述简便，使用一些术语。这些概念及结论是作者在文[1]中提出及得到的。为方便阅读此文，摘抄于此。

一般理论模型：如图 3 。

此处$\{a_{ij}\}_j$，$i=1$，2，…，n 为 n 个相互统计独立的序列，它们作为系统的 输入，$\{b_i\}_i$为系统的输出，T 为具有 n 个变元的变换，并且

$$b_i=T\begin{pmatrix}a_{1i}\\a_{2i}\\\vdots\\a_{ni}\end{pmatrix}\qquad i=1,2,\cdots$$

在本文中所述的序列都为 0 ， 1 序列。

把输入看成如右边所示的退化的二值平面（即纵轴方向有限）。

$$\begin{pmatrix}a_{11}\ a_{12}\cdots\cdots\\a_{21}\ a_{22}\cdots\cdots\\\vdots\ \ \vdots\\a_{n1}\ a_{n2}\cdots\cdots\end{pmatrix}$$

记行序列周期分别为d_1，d_2，…，d_n，二值平面周期为 d ，则$d=[d_1,d_2,\cdots,d_n]$。

定义 1：二值平面中连续 t 列所成$n\times t$阶 0 ， 1 矩阵称之为一个(n,t)—状态。

定义 2：二值平面称为 1 —遍历平面，若对任意l d，$l<d$，满足：

(i) 若$d_i\nmid l$，$i=1,2,\cdots,n$，则当 i 跑遍 1 ，2，3，…， d 时，$(2n,1)$—状态：

$$\begin{pmatrix}a_{1i}\\a_{2i}\\\vdots\\a_{ni}\\a_{1i+l}\\\vdots\\a_{ni+l}\end{pmatrix}$$

跑遍所有2^{2n}种不同的$(2n,1)$—状态；

(ii) 若$d_{i_j}\mid l$，$j=1$，2，…，ρ，而$d_h\nmid l$，$h\neq i_1$，i_2，…，i_ρ，$h=1$，2，…，n。则当i跑遍1，2，…，d时，$(2n,1)$－状态：

$$\begin{pmatrix} a_{1i} \\ a_{2i} \\ \vdots \\ a_{1\,l+i} \\ \vdots \\ a_{i_1\,l+i} \\ \vdots \\ a_{ni+l} \end{pmatrix} \qquad (\text{此时}a_{i_j i}=a_{i_j i+l},\ j=1,2,\cdots\rho)$$

跑遍所有可能的形如上述状态的$2^{2n-\rho}$种$(2n,1)$—状态。

结论 1[1]：在模型图3中，若$\{a_{ij}\}_j$都为m－序列，$i=1,2,\cdots,n$，并且其阶数两两互素，则它们所构成的二值平面必为1－遍历平面。

定义 3：若变换T为具有n个变元的变换。如果任意取定j个变元的值后所得的$n-j$元变换不为常数，并且j为满足此条件的最大值，则称T为j—变元变换。

定理[1]：对模型图3来说，不妨记$d_1<d_2<\cdots<d_n$。若$\{a_{ij}\}_j$都为m－序列，$i=1,2,\cdots,n$，并且$d_1,d_2,\cdots,d_n$两两互素，T为j－变元变换，则系统的输出序列周期l必满足：$l\geqslant d_1 d_2\cdots d_j$。

3 S-盒的输入、输出周期性

在以上理论基础上，我们利用计算机，即可研究S-盒对输入周期的影响，解决所提出的问题。

此时，$n=6$。

S-盒的结构：

S-盒为一个6进4出的变换，它把6位输入变成4位输出，它可由一个4行16列的表来说明，举例如下[2]：

行数 \ 列数	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
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

如果S_1是这个表规定的函数，B是一个6比特组，则$S_1(B)$确定如下：B的第一位及最后一位以2进制数代表0到3中间的一个数，假定为i。B的中间4位以2进制数代表0到15中的某个数，假设为j。然后在表上查找第i行、第j列的这个数，它是0到15中的某数，用一个4比特组来唯一表示这个数，即为输入为B时的输出$S_1(B)$。

在研究S-盒的输入与输出周期性时，由第一节知，可将S-盒分解成4个如模型图2的变换T来研究。

对于DES中的8个非线性变换，即8个S-盒，可以应用计算机来研究它们的性质。此时，DES中8个S-盒总共有32个如图2所示的变换。得到本文的结论：

定理：DES中8个S-盒所具有的32个如图2所示的变换都为3－变元变换。

证明：从定义 3 可知，只需对32个变换验证：任意取定 3 个变元的值后所得的 3 元变换不为常数，而对某 4 个变元取定某些值后所得 2 元变换为常数即可。故定理的证明从本质上来说，只需对32个变换逐个进行计算、验证即 可。作者 用 计 算机来完成这一工作。

作者一次同时对一个 S- 盒所具有的 4 个变换进行验证。在用计算 机 进行以上验证时，是对定义 3 中的 j 采取逐步计算的方法来完成的。在此，8 个S-盒的数据表是以一个数据文件来存放、读取的。对于$j=1$时的计算框图如下：

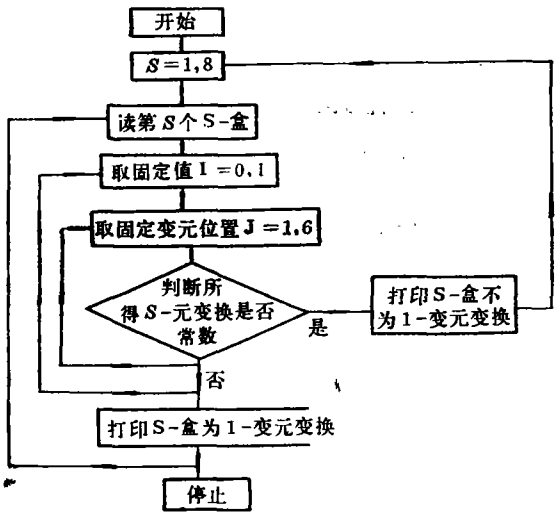

图 4

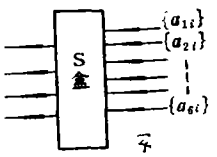

图 5

对于另外的 j 值，同理，在此省略。程序运行结果对$j=3$为肯定。即得定理结论。

结合第二节中的理论及以上定理，得最终结果，也即本文的主要结论：

定理：S-盒如图 4 模型所示。记 6 个输入序列周期分别为d_1，d_2，…d_6，不妨设$d_1<d_2<\cdots<d_6$。若 6 个输入序列都为m - 序列，并且 d_1，d_2，…，d_6两两互素，则S-盒的输出平面的周期 d 必满足：$d\geqslant d_1d_2d_3$。

4 结 束 语

从本文所得结论可以看出，S-盒的非线性对输入序列的周期性影响很大，完备的结论难以得到，本文所作的工作也仅仅是这一密码学中理论难题的初步探索。

参 考 文 献

[1] 肖戎. 密码学中的两个理论问题. 通信学会与数据通信学会学术年会资料，1986

[2] 密码体制—通信保护. 通信保密，1986

Families of Frequency-Hopping Sequences with Optimal Hamming Correlation Properties

Mei Wenhua Chen Xianfu

Abstract

Families of p^k-ary sequences with small Hamming crosscorrelation are required for hopping patterns in asynchronous frequency-hopping spread-spectrum multiple-access communication systems. Lower bounds on the out-of-phase auto correlation and on the crosscorrelation of sequences of given length and alphabet size are derived in [1], and a method of constructing families of sequences that uniformly realize these bounds is presented as well. In this paper, a commonest method of constructing families of frequencyhopping sequences with optimal Hamming correlation properties is presented, taking the method in [1] as its special case. By driving the frequency synthesizer from k inconsecutive stages Tather than from k consecutive stages, we can partially solve the Hop-and-Stay problem existing in [1].

Key words: Communication, Frequency-hopping, Sequences

Research on Periodicity of Input and Output of S-boxes in DES

Xiao Rong

Abstract

There are not any general conclusions about periodicity of DES when it is used in stream cipher system. The author discusses this problem and gives a low bound for period of S-boxes.

Key words: Cipher communication, DES method, periodi city