1989年12月 西安电子科技大学学报 Dec.1989
第16卷 第4期 JOURNAL OF XIDIAN UNIVERSITY Vol.16 No.4

DES的弱密钥的代数构造

王育民
(信息工程系)

摘要 本文分析了DES的弱密钥、半弱密钥和1/4弱密钥的代数构造，并发现了DES的1/4弱密钥远多于48种。

关键词: DES; 弱密钥; 密码学①

1 引 言

DES的密钥构造是研究DES的安全性的重要课题之一。DES的密钥是由8个字节链接而成的64bit二元数字序列，其中每字节的最后一位是奇校验位，在密钥变换和加密过程中不起作用，只在传输和存贮过程中作检错之用。DES加密过程中包含了16轮迭代，而每轮迭代所用的子密钥是变化的。为了揭示DES的密钥构造，先简要介绍DES的密钥产生器，如图1所示。有关DES算法的基本原理，这里不再赘述，可参看文[1]。

给定一64bit密钥 $\underline{k}$，经过图1中的置换选择1后，将其中的8bit校验位删去，其余56bit经过置换后形成28bit长的两组数送至移位寄存器C和D。移存器C和D在各轮迭代时同步地按表1给定的移位次数进行循环左移位，其结果分别经过各自的选择置换2后构成24bit的数字序列，将它们连接形成相应轮迭代所需的48bit长的子密钥 $\underline{k}_i$，从表1可知，16轮迭代总的循环左移位次数为28，一组数据加密后，相应密钥也正好回复到初始位置。

表1 移位次数表

i	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
第i轮循环左移位次数	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

Meyer和Matyas[1]曾给出下述弱密钥和半弱密钥的定义。

定义1 若给定的密钥 $\underline{k}$ 有，$\underline{k}_1=\underline{k}_2=\cdots\underline{k}_{16}$，则称 $\underline{k}$ 为弱密钥(Weak-key)。

定义2 若给定的密钥 $\underline{k}$，相应的16个子密钥只有两种取值，且每一种都出现8

①本文是原电子工业部回国留学人员科技活动基金资助的课题，于1989年4月26日收到。

?1994-2016 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

次，则称 $\underline{k}$ 为半弱密钥(semi-weak key)。

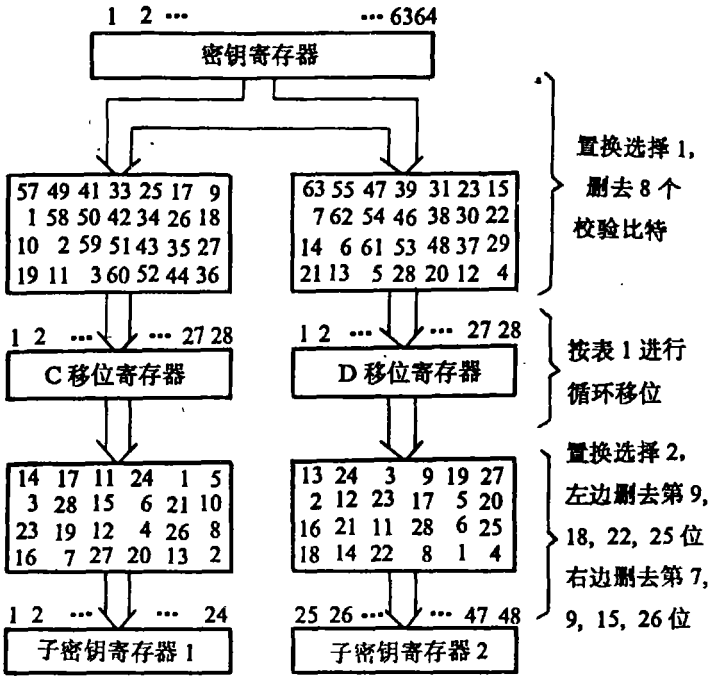

图 1 DES 的密钥产生器

弱密钥的特点是：若 $\underline{k}$ 是弱密钥，$\underline{x}$ 为 64bit 明文，则

$$\mathrm{DES}_{\underline{k}}(\mathrm{DES}_{\underline{k}}(\underline{x}))=\underline{x} \tag{1}$$

$$\mathrm{DES}_{\underline{k}}^{-1}(\mathrm{DES}_{\underline{k}}^{-1}(\underline{x}))=\underline{x} \tag{2}$$

即以 $\underline{k}$ 对 $\underline{x}$ 加密两次或解密两次都可恢复原消息，称这样的密钥 $\underline{k}$ 为对合的(involutory)。对一般密钥只满足

$$\mathrm{DES}_{\underline{k}}^{-1}(\mathrm{DES}_{\underline{k}}(\underline{x}))=\mathrm{DES}_{\underline{k}}(\mathrm{DES}_{\underline{k}}^{-1}(\underline{x}))=\underline{x} \tag{3}$$

若 $\underline{k}$ 为弱密钥，则在选择明文攻击下所需搜索量将减半。

半弱密钥的特点是成对地出现，且具有下述性质：若 $\underline{k}_1$ 和 $\underline{k}_2$ 为一对互逆的半弱密钥，$\underline{x}$ 为明文组，则有

$$\mathrm{DES}_{\underline{k}_2}(\mathrm{DES}_{\underline{k}_1}(\underline{x}))=\mathrm{DES}_{\underline{k}_1}(\mathrm{DES}_{\underline{k}_2}(\underline{x}))=\underline{x} \tag{4}$$

称 $\underline{k}_1$ 和 $\underline{k}_2$ 是互为对合的。

Davies[2]曾指出，若要(1)或(2)式成立，密钥 $\underline{k}$ 的各子密钥 $\underline{k}_i$ 需满足

$$\underline{k}_i=\underline{k}_{17-i} \tag{5}$$

若要(4)式成立，密钥 $\underline{k}_1$ 和 $\underline{k}_2$ 的各子密钥需满足

$$\underline{k}_{1,\,i}=\underline{k}_{2,\,17-i} \tag{6}$$

?1994-2016 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

Moore 和 Simmons[3, 4]给出了满足(5)和(6)式的密钥的生成组，并详细研究了弱密钥和半弱密钥的循环结构和不动点问题. 所谓循环周期是指对给定密钥 $\underline{k}$ 和明文 $\underline{x}$，通过交替使用 $\underline{k}$ 和 $\bar{\underline{k}}$ ($\underline{k}$'的补) 进行加密运算，直到首次恢复明文 $\underline{x}$ 所用的加密运算次数. 若 $DES_{\underline{k}_1}(\underline{x})=\underline{x}$ 或 $DES_{\underline{k}}^{-1}(\underline{x})=\underline{x}$，则称 $\underline{x}$ 为密钥 $\underline{k}$ 的一个不动点. Kaliski 等[5]曾指出 DES 弱密钥的短循环现象，Coppersmith[6]则用密钥的不动点解释了这类现象. Moore 和 Simmons 曾指出，尚未证实 DES 的半弱密钥的明显弱点.

本文将从 DES 的子密钥产生器中循环左移寄存器 C 和 D 的移位次数和存数构造来研究 DES 的弱密钥构造.

2 DES 弱密钥的代数构造

由图 1 可知，如果移位寄存器 C 和 D 中的存数在各轮迭代中保持不变，则得到的各个子密钥 $\underline{k}_i$ 也保持不变. 这是因为 $\underline{k}_i$ 的前半部分是由移存器 C 中存数除去第 9、18、22 和 25 位后再经过一固定置换得到的，$\underline{k}_i$ 的后半部分是由移存器 D 中的存数除去第 7、9、15 和 26 位再经过一固定置换得到的. 仅当 C 和 D 的存数为全"0"或全"1"时才能满足弱密钥的条件. 其可能的组合只有 4 种. 为了方便起见，我们将以 C 和 D 的前 4 位存数所表示的十进制数来表示 C 和 D 中的存数类别和相应的外部密钥. 外部密钥 (即原始的 $\underline{k}$) 是对 C 和 D 中的存数施以置换选择 1 的逆变换得到的. 这 4 个弱密钥所对应的移存器中存数的 16 进制表示为

$$\begin{array}{llllllll}(0,\ 0)\rightleftharpoons & 00 & 00 & 00 & 00 & 00 & 00 & 00\\ (0,\ 15)\rightleftharpoons & 00 & 00 & 00 & 0F & FF & FF & FF\\ (15,\ 0)\rightleftharpoons & FF & FF & FF & F0 & 00 & 00 & 00\\ (15,\ 15)\rightleftharpoons & FF & FF & FF & FF & FF & FF & FF\end{array} \tag{7}$$

相应的外部密钥的 16 进制表示为

$$\begin{array}{llllllll}(0,\ 0)\rightleftharpoons & 01 & 01 & 01 & 01 & 01 & 01 & 01 & 01\\ (0,\ 15)\rightleftharpoons & 1F & 1F & 1F & 1F & 0E & 0E & 0E & 0E\\ (15,\ 0)\rightleftharpoons & E0 & E0 & E0 & E0 & F1 & F1 & F1 & F1\\ (15,\ 15)\rightleftharpoons & FE & FE & FE & FE & FE & FE & FE & FE\end{array} \tag{8}$$

由(7)或(8)式不难看出，DES 的 4 个弱密钥除去奇校验位后构成 GF(2)上 56 维密钥空间中的一个 2 维子空间，以 V_2 表示.

DES 加密采用 16 轮迭代，而移存器 C 和 D 的长度为 28，且每轮迭代时的循环左移位次数由表 1 限定，或移 1 次、或移两次，且在 16 轮中的分布是非对称的. 由于移存器长度 $28=1\times2\times2\times7$，所以在移位 16 轮的过程中，要使 C 和 D 中的存数出现重复图样，其长为 28 的初始序列必须是长为 1、2、4、7 或 14 的重复图样. 下面分几种情况进行讨论.

(1) 长为 1 的重复图样

这种图样所给出的序列有二种，即 0，0，…，0 和 1，1，…，1. C 和 D 的存数任

?1994-2016 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

取其中之一就给出了前述的一个子密钥，可能的组合选择有 4 种，它们构成了 V_2。应当指出，这两种图样在循环移位下对其自身是封闭的。

(2) 长为 2 的重复图样

这类图样有两种，即 01，01，…，01 和 10，10，…10，它们对于偶次循环移位具有自封闭性，而对于奇次循环移位具有互封闭性，即对于相应子空间的封闭性。当然，长为 1 的重复图样序列也可看作是长为 2 的重复图样序列。这样移存器 C 和 D 的初值就可有 4 种可能的选择。这 4 种选择构成了 GF(2)上 28 维空间中的一个二维循环子空间，其中元素对于循环左移位的封闭性就决定了相应密钥所产生的子密钥的重复特性。

C 和 D 存数任选这四个图样之一将给出一个半弱密钥，可能的选取有 $4\times4=16$ 个，其中有 4 个为弱密钥。这 16 种组合所决定的 16 个外部密钥构成 GF(2)上 56 维空间中的一个 4 维子空间，以 V_4 表示。显然 V_2 是 V_4 的一个子空间。

V_4-V_2 中的 12 个元素是 DES 的 12 个半弱密钥，其编号列在表 2 中。

表 2 半弱密钥编号

C,D 存数编号	外部密钥								
(10,10)	01	FE	01	FE	01	FE	01	FE	} 互逆对
(5,5)	FE	01	FE	01	FE	01	FE	01	
(10,5)	1F	E0	1F	E0	0E	F1	0E	F1	} 互逆对
(5,10)	E0	1F	E0	1F	F1	0E	F1	0E	
(10,0)	01	E0	01	E0	01	F1	01	F1	} 互逆对
(5,0)	E0	01	E0	01	F1	01	F1	01	
(10,15)	1F	FE	1E	FE	0E	FE	0E	FE	} 互逆对
(5,15)	FE	1F	FE	1F	FE	0E	FE	0E	
(0,10)	01	1F	01	1F	01	0E	01	0E	} 互逆对
(0,5)	1F	01	1F	01	0E	01	0E	01	
(15,10)	E0	FE	E0	FE	F1	FE	F1	FE	} 互逆对
(15,5)	FE	E0	FE	E0	FE	F1	FE	F1	

V_4-V_2 中元素具有下述性质:

(a) 半弱密钥成对地出现，如表 2 所示。各对密钥满足(4)式，互逆对存在条件是，其在移存器 C 和 D 中相应的存数对于左移位运算具有交替的封闭性。

(b) 在 16 轮迭代过程中的 16 个子密钥满足定义 2 的条件。

(3) 长为 4 的重复图样

长为 4 的图样共有 $2^4=16$ 种，即 0000，0001，…，1111。移存器 C 和 D 中的存数可任选其中之一重复 7 次。可能的组合个数为 $16\times16=256$ 种。这 16 种图样可分为 6 组，即

{0000}，{1111}，{0101, 1010}，{0011, 0110, 1100, 1001}，

?1994-2016 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

{0111, 1110, 1101, 1011}, {0001, 0010, 0100, 1000}

各组对于循环左（或右）移位具有封闭性。由它们重复7次所构成的序列在寄存器进行循环左移位时也具有相应的封闭性。这16种重复图样构造成GF(2)上28维空间中的一个4维循环子空间，由这种图样所决定的C和D存数相对应的外部密钥构成的GF(2)上56维空间中的一个8维子空间，以V_8表示。其中每个元素以(i, j)表示，其中i，$j \in [0, 1, \cdots, 15]$。显然V_4是V_8中的一个4维子空间，V_2是V_8中的一个2维子空间。

V_8-V_4中有240个元素，其中每个元素具有下述性质:

(a) 在16轮迭代中的16个子密钥，只有4种图样（循环移位封闭组中元素），而且每种图样将恰好出现4次，各图样出现次序将由初值和表1的移位次数决定。称这种密钥为1/4-弱密钥。Jueneman[7]也曾指出这类弱密钥，称之为demisemi弱密钥而Meyer和Matyas[1]仅给出了48种。他们未考虑长为4重为3和重为1的重复图样。

(b) 由于循环移位次数的非对称配置使这些1/4-弱密钥不具备(4)式给出的条件。

(4) 长为7的重复图样

长为7的二元数字图样有$2^7=128$种。移存器的存数可任选其中之一重复4次得到。由这128种图样可组合出$128\times128=16384$种C、D的存数图样，它们所对应的外部密钥构成了GF(2)上56维空间中的一个14维子空间，以V_{14}表示。其中的每个元素可用(i, j)表示，其中$i, j \in [0, 1, \cdots, 127]$。显然$V_2$是$V_{14}$的一个2维子空间。

$V_{14}-V_2$中每个元素在16轮迭代过程中所产生的16个子密钥中，有两个密钥图样重复出现3次，而有5个密钥图样重复出现2次。

(5) 长为14的重复图样

长为14的重复图样有$2^{14}=16384$种。将这类图样重复两次作为移存器C和D的存数，可能的组合将有$2^{28}=268435456$种。它们所对应的外部密钥构成GF(2)上56维空间中的一个28维子空间，以V_{28}表示。显然V_{14}和V_2都是V_{28}的子空间。$V_{28}-V_{14}$中的元素在16轮迭代所产生的16个子密钥中，只有两个图样出现两次，其它子密钥图样不再有重复出现现象。

3 结 论

由移存器C和D中的存数及表1所决定的移位次数来分析DES的弱密钥和半弱密钥等的构造和性质是比较简便的途径。这一研究可能为研究DES的密钥构造和分类提供方便。至于各类弱密钥的性质及其在分析和破译DES中的作用还有待于进一步深入研究。

参 考 文 献

[1] Meyer C H and Matyas S M. 密码学，计算机数据保密的新领域——保密系统设计和实现指南. 总参第51所，1985

[2] Davies D N. Some regular properties of the DES algorithm. Proc. of the CRYPTO'82, Plenum Press, 1983; 89～96

?1994-2016 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

[3] Moore J H and Simmons G J. Cycle structure of the DES with weak and semi-weak keys. Proc. of the CRYPTO'86, Springer-Verlag, 1987; 9～32

[4] Moore J H and Simmons G J. Cycle structure of the DES for key having palindromic (or antipalindromic) sequences of round keys. IEEE Trans. on 1987; SE-13(2); 262～273

[5] Coppersmith D. The real reason for Rivest's phenomenon. Proc. of the CRYPTO'85, Springer-Verlag, 1986; 535～536

[6] Kaliski B S Jr et al. Is DES a pure cipher (results of more cycling experiment on DES.) in Proc. of the CRYPTO'85, Spring-Verlag, 1986; 212～221

[7] Jueneman R R. Analysis of certain aspect of output feed-back mode. Proc, of the CRYPTO'82, Plenum Press, 1983; 98～128

Algebraic structure of the DES's weak keys

Wang Yumin

Abstract

Algebraic structures of the DES's weak keys, semi-weak keys, and 1 / 4-weak keys are presented, and many more than 48 of the DES's 1 / 4-weak keys are found.

Key Words: DES; weak keys; cryptography

?1994-2016 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net