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

阻止差分密码攻击的有效方法*

唐朝京
（电子技术系）

摘 要 差分密码分析方法是1990年由E. Biham和A. Shamir提出的，这种方法对DES算法及DES类体制构成了威胁。本文在剖析了差分密码分析方法工作原理的基础上，提出了改进DES算法的7种方法，从而可以有效地阻止差分密码分析法的攻击。

关键词 密码体制，密码分析，数据加密标准
分类号 TN918.4

1977年DES算法被美国NBS定为数据加密标准。十多年来，尽管DES的安全性受到了来自各方面的挑战和争论，但这些争论并未能从根本上否定DES的安全性，相反还提高了它的声誉，使DES被公认为分组密码体制设计的成功范例。但是E. Biham和A. Shamir在1991年国际密码学年会（CRYPTO90）发表的论文："对DES类密码体制的差分密码分析"[1]动摇了这种看法，在该文中，两位作者创造性地提出了一种"差分密码分析"的新方法，从而对DES构成了现实的威胁。据作者称，利用差分密码分析法在个人计算机上破译6圈DES只需不到0.3秒，破译8圈DES的时间也不超过2分钟。尽管目前这种新的破译方法对付16圈DES仍显得有点不够（计算量略超过穷尽攻击的计算量），但它的问世确实开辟了密码分析的一条新途径，因此研究防范它的具体措施是十分必要的。本文正是在剖析差分密码分析法的工作原理的基础上，针对DES算法的薄弱环节，提出了七种方法用以改进DES算法，从而可以有效地阻止差分密码分析法的攻击。

1 差分密码分析法原理简析

差分密码分析属于选择明文攻击。它利用具有特定差分值的若干对明文以及与之相对应的密文对的值，对DES实施攻击。这种攻击法首先分析特定明文差分对相应密文差分的影响，并利用这种影响给出各种可能密钥的概率，进而找出真正的密钥，达到破译的目的。

差分密码分析法赖以生效的首要前提是DES的8个S盒输出差分关于输入差分的

* 1992年2月22日收稿

分布是不均匀的。这就为它提供了利用选择明文攻击的可能。

首先让我们考察一下 S 盒的特性。十多年来的大量研究表明[2]：DES 的 8 个 S 盒关于其输入比特具有良好的非线性特性，这保证了 DES 能经受解析法攻击。但这只是问题的一个方面。当我们不再考虑输入数据的值进入 S 盒的结果，转而考虑 S 盒的一对输入数据的差分值对于相应的一对输出数据的差分值所产生的影响时，情况就发生了很大的变化。

表 1　S1 盒的数据结构

14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

表 1 是 DES 的 S1 盒的数据结构。表 2 描述了在 S1 盒的所有输入状态上迭加了 64 种差分值 D_{in}后导致的相应输出的差分值 D_{out}之分布情况，表中数据表示在特定的 D_{in}下各相应的 D_{out}值取到的次数，因此各 D_{out}出现次数与总的可能次数之比可视作 S1 盒输入差分与输出差分的条件转移概率 $P(D_{out}/D_{in})$。

表 2　S1 盒输入差分与输出差分的分布情况

D_{in}	D_{out}															
	0	1	2	3	4	5	6	7	8	9	*A*	*B*	*C*	*D*	*E*	*F*
00	64	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
01	0	0	0	6	0	2	4	4	0	10	12	4	10	6	2	4
02	0	0	0	8	0	4	4	4	0	6	8	6	12	6	4	2
03	14	4	2	2	10	6	4	2	6	4	4	0	2	2	2	0
04	0	0	0	6	0	10	10	6	0	4	6	4	2	8	6	2
05	4	8	6	2	2	4	4	2	0	4	4	0	12	2	4	6
06	0	4	2	4	8	2	6	2	8	4	4	2	4	2	0	12
07	2	4	10	4	0	4	8	4	2	4	4	2	2	2	4	4
08	0	0	0	12	0	8	8	4	0	6	2	8	8	2	2	4
09	10	2	4	0	2	4	6	0	2	2	8	0	10	0	2	12
0*A*	0	8	6	2	2	8	6	0	6	4	6	0	4	0	2	10
0*B*	2	4	0	10	2	2	4	0	2	6	2	6	6	4	2	12
0*C*	0	0	0	8	0	6	6	0	0	6	6	4	6	6	14	2
0*D*	6	6	4	8	4	8	2	6	0	6	4	6	0	2	0	2
0*E*	0	4	8	8	6	6	4	0	6	6	4	0	0	4	0	8
0*F*	2	0	2	4	4	6	4	2	4	8	2	2	2	6	8	8
⋮				⋮				⋮					⋮			
3*E*	4	8	2	2	2	4	4	14	4	2	0	2	0	8	4	4
3*F*	4	8	4	2	4	0	2	4	4	2	4	8	8	6	2	2

从表 2 可以看出，当输入差分为 0 时，相应的 64 次输出差分全部取 0，这是很容易理解的；而当输入差分不为 0 时，理想的输出差分分布应为 16 种状态(0～*F*)中每种取 4 次。但从表 2 可以看出：实际分布具有较大的偏差，最多的取到 14 次(如 $P(0/3)=14/64$)，最少的取 0 次。正是输出差分值分布的这种不均匀性为差分密码分析法提供了攻击的机会。

下面考察差分密码分析法攻击三圈 DES 的情况。图 1 所示为三圈 DES 的结构示意图，此处我们约定以 A、B、C 等表示该处的数据原值，而以 A'、B'、C' 等表示该处相应的特定数据对的差分值。

设明文输入为(L,R)，三圈后密文输出为(l,r)。首先取定所有输入明文对的差分值都为(L',R')，R'的选取应使其经过 F 以后以接近 1/4 的概率转变成 L'，则 $A'_1=B'_0=R'$，$C'_1=L'$，$A'_2=B'_1=L'+C'_1=0$. 由表 2 第一行可知，当 S 盒的输入差分为 0 时，输出差分必为 0，故此时有 $C'_2=0$，$A'_3=B'_2=A'_1+C'_2=R'$，$B'_3=A'_2+C'_3=L'$，即 $l'=R'$，$r'=L'$. 这样就将输入差分与输出差分联系起来了。

图 2 所示为 DES 的非线性 F 函数。输入数据 a 首先经过 E 扩展变成 b，然后与密钥 k 逐位模 2 加，作为 8 个 S 盒的输入，S 盒的输出 c 再经过 P 排列，最后输出为 d。由以上讨论可知，$a'=R'$，$d'=L'$。容易证明：E 扩展、P 排列只是使输入差分的位置有所移动，因此 a 处的差分 R'可认为一直传递至 b，而 c 处的差分值也可看作保留至 d，故 $b'=a'=R'$，$c'=d'=L'$.

考察图 2，由于 $R'\rightarrow L'$的条件转移概率预先选定为 1/4，设 a_1、a_2 为 a 处对应于某一个 S 盒的一对输入，且具有固定的差分 R'，则 a_1、a_2 各加上 64 种密钥组合再经 S 盒输出后，将以 1/4 的概率取到输出差分 L'，但 64 种密钥组合中唯一的正确密钥必定使 S 盒的输入差分取 L'，而大部分不正确的密钥将被淘汰。故当所选择的明文足够多时，必能得到正确的 6 比特密钥，在上述过程中，由于寻找输入各 S 盒的 6 比特密钥的工作是互相独立的，因此总的搜索工作量是相加的关系。

以上即为差分密码分析法破译三圈 DES 的过程。为表达简洁起见，输入差分的转移过程可用表 3 描述。

表 3　三圈 DES 的差分转移过程

迭代次数	差分值	F 的差分变换	转移概率
$i=0$	$\{L',R'\}$	$(R'\rightarrow L')$	$p=1/4$
$i=1$	$\{R',0\}$	$(0\rightarrow 0)$	$p=1$
$i=2$	$\{0,R'\}$	$(R'\rightarrow L')$	$p=1/4$
$i=3$	$\{R'=l',L'=r'\}$		

这一过程的总转移概率约为 1/16.

由文 [1] 可知，若令 $L'=$00808200H，$R'=$60000000H，则这一对 L'、R'即满足上述要求。

为破译 6 圈 DES，文 [1] 作了更深入的讨论。令 $L'=$40040000H，$R'=$04000000H，则其差分转移过程为：

$i=0:\{L',R'\}$　　$(R'\rightarrow L')$　　$p=1/4$

$i=1:\{R',0'\}$　　$(0\rightarrow 0)$　　$p=1$

$i=2:\{0',R'\}$　　$(R'\rightarrow L')$　　$p=1/4$

$i=3:\{R',L'\}$　　$(L'\rightarrow a')$　　以一定概率

$i=4:\{L',R'+a'\}$　　$(R'+a'\rightarrow b')$　　以一定概率

$i=5:\{R'+a',L'+b'\}$　　$(L'+b'\rightarrow c')$　　以一定概率

$i=6:\{L'+b'=l',R'+a'+c'=r'\}$

则 $b'=L'+l'$，$c'=R'+r'+a'$，其中 L'的选取使第 4 圈中有 5 个 S 盒的输入为 0，也即 a'中对应着 5 个 S 盒的全 0 输出。这将为分析第 6 圈的密钥比特提供很大帮助。

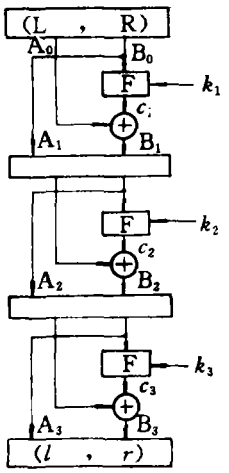

图 1 三圈 DES 结构示意图

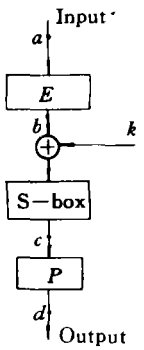

图 2 非线性函数 F 示意图

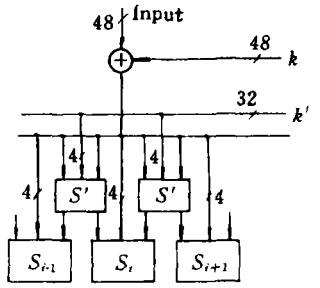

图 3 方法 3 示意图

2 阻止差分密码攻击的方法

综上所述，差分密码攻击法生效的前提有三个：

(1) S 盒的输出差分分布不均匀，最大转移概率为 1/4，而理想值应为 1/16；

(2) 某些输入明文差分能以不太小的概率传递若干圈；

(3) 非线性函数 F 中输入各 S 盒的密钥比特可独立试探。

针对这些前提，本文提出了 7 种方法对 DES 进行改进，可以有效地挫败差分密码攻击。而这些方法均不会破坏 DES 的加密解密可逆性。[4]

方法 1 修改 S 盒的设计

S 盒的输出差分分布不均匀是差分攻击法的首要前提，因此修改 S 盒的设计，以改善 S 盒的差分转移特性，即能从根本上否定差分密码攻击。但这种方法难度比较大，需要做大量艰苦的工作。

方法 2 增加算法迭代圈数

由文 [1] 可知，差分密码分析法攻击 DES 的计算量随 DES 迭代圈数的增加而很快上升，大致规律是 DES 的迭代圈数每增加 2 圈，破译复杂度就增加 100 倍左右。而对于 16 圈的 DES，按差分攻击法目前所达到的水平，其破译复杂度已略超过穷尽攻击，因此适当增加 DES 的迭代圈数，例如圈数取 20、24 或 32，即能有效地阻止差分攻击。

方法 3 密钥的非线性处理

由前面的分析可知，对手在得到最后一圈 F 函数的输入数据对和相应的输出差分值后，即可分别对进入每个 S 盒的 6 比特密钥进行搜索，从而找出真正的密钥，显然这一工作量是很小的。因此方法 3 在 DES 的每一圈增加 32 位密钥 k'，并采用一个 6 进 2 出的非线性替换函数 S'，以增加进入每个 S 盒的密钥比特数，增加对手搜索密钥比特的难度，见图 3.

从图 3 不难看出，这种方法使得进入每个 S 盒的密钥比特数从 6 增加到 16，这就可以大大增加对手搜索密钥的次数以及所需的明文对。

方法 4 双重 S 盒结构

方法 4 也是通过修改 F 函数的结构增加进入每个 S 盒的密钥比特数，详见图 4.

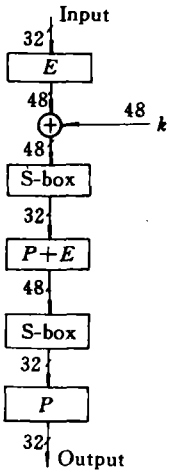

图 4 方法 4 示意图

这种方法使输入数据与密钥的迭加结果两次进入 S 盒，而中间用排列 P 和扩展 E 将数据打乱，使第二次进入各 S 盒的数据中包含更多位密钥的信息。由文 [3] 知：DES 中 P 排列的设计使得下一次迭代时进入每个 S 盒的 6 位数据取自本次迭代的 6 个不同 S 盒的输出，因此方法 4 可使第二层每一个 S 盒的输入中均包含有 36 位密钥的信息。这就使得对手在搜索每个 S 盒的输入密钥时无从下手。方法 4 的另一个突出优点是由于采用了（中间经过交错的）双重 S 盒结构，使本来很明确的 S 盒输出差分分布全部被破坏了，对手面临的是一个等效的 48 进 32 出的巨大 S 盒，而要分析这个大 S 盒的差分分布几乎是不可能的。

方法 5 用线性组合网络取代 P 排列

这种方法是以一个线性组合网络 LC 取代 F 函数中的 P 排列，从而使下一圈每个 S 盒的输入中包含有更多位密钥的信息。此 LC 的输入、输出均取 32 位，但其任一位输出都是从每个 S 盒的 4 位输出中至少取一位相加而得。这样，F 函数的每一位输出中均包含了 48 位密钥的信息，在进入下一圈的 F 函数时就能有效地阻止对手搜索密钥。由于线性组合变换 LC 在此处不要求可逆[4]，因此 LC 的结构选取具有很大的自由度。

与方法 4 同理，方法 5 也同时破坏了 S 盒的输出差分分布，从而在很大程度上否定了差分密码攻击法的前提。

方法 6 增加可逆替换函数

由文 [4] 知，由于可逆替换表自身可逆的特点，故可将其附加到迭代可逆型体制的任何部位，因此方法 6 在 DES 的迭代结构中增加一个可逆替换 S 以破坏输入差分的顺利传递，见图 5. S 是一个 n 进 n 出的可逆替换，一般可取 $n=8$. 易知，当 n 较大时，由 S 可获得比较均匀的输出差分分布。这样就可将它的输入差分均匀分散开，从而有效地阻止差分的传递过程。

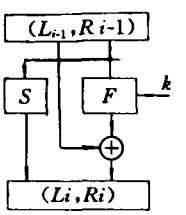

图 5 方法 6 示意图

方法 7 采用广义 Feistel 结构

这种方法主要用来限制差分传递的圈数。

由文 [1] 知，设 DES 的输入，输出差分分别为 $\{L',R'\}$ 和 $\{l',r'\}$，则当中间迭代过程中 F 所产生的新差分均能用 L'、R'、l'、r' 表示时，破译最后一圈的密钥就比较顺利（若再增加一圈，则必然有一个未知的差分值存在，只有当这个未知差分的多数位为 0 时，才便于破译）。因此，若我们能增加每一圈的中间差分个数，便能使对手可破译的圈数减少，以此达到阻止差分密码攻击的目的，而采用广义 Feistel 结构作为迭代结构可以有效地达

此目的。由文 [4] 可知，设迭代结构的分组数为 L，则广义 Feistel 结构中可采用的非线性变换总个数为

$\sum_{n=1}^{L-1}C_n^1+\sum_{n=2}^{L-1}C_n^2+\sum_{n=3}^{L-1}C_n^3+\cdots\cdots+\sum_{n=L-1}^{L-1}C_n^{L-1}=\sum_{n=1}^{L-1}\sum_{m=1}^{n}C_n^m=2^L-L-1$（不考虑非线性项的嵌套），而已知的明、密文差分分量共有 $2L$ 个。即：

当 $L=3$，非线性变换最多有 4 个，已知的明密文差分分量共有 6 个；

当 $L=4$，非线性变换最多有 11 个，已知的明密文差分分量共有 8 个；

当 $L=5$，非线性变换最多有 26 个，已知的明密文差分分量共有 10 个；……

可见只要分组数取到一定的大小，则广义 Feistel 结构一次迭代即有可能产生足够多的中间差分，这样就能有效地减少对手的可破译圈数。

由于广义 Feistel 结构中会出现多个非线性变换的输出相加的情形，这将引起非线性变换的输出差分进一步混乱，因此方法 7 同时还能在一圈迭代中有效地阻止输入差分的顺利传递。

3 结束语

本文以上提出的七种方法分别破坏了差分密码分析法的一个或几个前提，因此可以有效地阻止差分密码攻击。由此可知，差分密码攻击是完全可以防范的。尽管如此，差分密码分析作为一种独创性的攻击方法，其价值将远远超出对 DES 算法的具体分析成果，必将对分组密码体制的发展产生重要的影响，而本文所做工作对于今后分组密码体制的设计和分析将具有较大的参考价值。文中难免有谬误之处，欢迎批评指正。

参 考 文 献

1 Biham E，Shamir A，罗昭武（译）. 对 DES 类密码体制的差分密码分析，通信保密，1991，(3)

2 唐朝京，李情与. S—盒输出表达式的求法及最简化研究，通信保密，1987，(2)

3 唐朝京. DES 算法设计思想分析及新型加密算法的研制，国防科技大学硕士论文，1986

4 唐朝京，王耀勋. 分组密码体制一般结构分析，通信保密，1991，(2)

Effective Methods of Preventing the Attack of Differential Cipher Analysis

Tang Chaojing

(Department of Electronic Technology)

Abstract

The method of differential clpher analysis was presented by E. biham and A. Shamir in 1990. It constitutes a realistic threat to DES and DES—like systems. This paper deeply analyzes its principles and presents seven methods to improve the performance of DES. It is then possible for DES to prevent the attack of differential cipher analysis.

Key words cipher systems; cipher analysis; standard of data encryption