文章编号:1673-0291(2017)02-0028-08 DOI:10.11860/j.issn.1673－0291.2017.02.005

六轮 DES 截断差分攻击算法的改进与实现

刘 伟,何永忠,赵 佳,黎 琳
(北京交通大学 计算机与信息技术学院,北京 100044)

摘 要:对分组密码进行截断差分攻击时,部分 S 盒会产生很多组子密码候选值,导致暴力攻击剩余密钥位时消耗大量时间.本文详细分析了截断差分算法中出现多组密钥候选值的原因,并分析了其出现的概率,提出两种改进截断差分攻击方案,减少候选子密码的数量并提高了攻击效率.第 1 种方法基于各轮 S 盒子密钥的非独立性,利用轮密钥在初始密钥中的重复位得到最终的候选值,最终筛选出只有一组候选值的概率达到 40%左右.第 2 种方法将计算得到的 8 个 S 盒的所有 6 比特候选子密钥进行计数,选取出现频率最高的密钥,最终使 48 比特的候选密码个数缩减为一个.通过对六轮 DES 密码算法攻击的实验数据分析得知:第 2 种方法能够恢复出唯一的 48 比特子密码.

关键词:差分分析;数据加密标准;截断差分;S 盒;分组密码
中图分类号:TP393.4 **文献标志码**:A

Rapid realization of truncated differential attack on 6-round DES

LIU Wei, HE Yongzhong, ZHAO Jia, LI Lin
(School of Computer and Information Technology, Beijing Jiaotong University, Beijing 100044, China)

Abstract: In the process of the truncated differential attack to block cipher, some substitution-boxes(S-boxes) will have a great deal of cipher candidate values, which will use a lot of time when the remaining key is attacked by violence. This paper mainly analyzes the reasons and the related probability of the emergence of multi sets of recommended values, and then puts forward two improvement schemes to reduce the number of the candidate key and improve the efficiency of the attack. The first method uses the incomplete dependence among round keys, and makes full use of the identical key that is in the first and in the final round. But the probability of one set of candidate value is about 40%. The second method uses the whole 6 bits candidate key in 8 S－boxes, and obtains the final key by counting the numbers of values. Using this method can reduce the number of 48 bits candidate to 1 with the probability close to one. Through the 6－round DES attack experimental results, the second method can recover the initial key with the probability close to one.

Keywords: differential cryptanalysis; data encryption standard; truncated differential; S-boxes; block cipher

收稿日期:2016-03-02
基金项目:国家自然科学基金青年科学基金(61502030,61402035);中央高校基本科研业务费专项基金(2016JBM020)
Foundation item: National Natural Science Foundation of China(61502030;61402035); Fundamental Research Funds for the Central Universities(2016JBM020)
第一作者:刘伟(1991—),女,河北唐山人,硕士.研究方向为信息安全.email:14120405@bjtu.edu.cn.
引用格式:刘伟,何永忠,赵佳,等.六轮 DES 截断差分攻击算法的改进与实现[J].北京交通大学学报,2017,41(2):28－35.
LIU Wei, HE Yongzhong, ZHAO Jia, et al. Rapid realization of truncated differential attack on 6－round DES[J]. Journal of Beijing Jiaotong University, 2017, 41(2): 28－35.(in Chinese)

数据加密标准(Data Encryption Standard, DES)由美国国家标准局于 1977 年颁布,具有加解密速度快、易于标准化等特点[1].DES 是典型分组密码算法之一,早期对分组密码的研究基本都是围绕 DES 进行.到了 20 世纪 90 年代,对 DES 类密码的分析研究更加深入[2],并取得了丰硕的研究成果.具有重大意义的成果之一便是差分密码分析(Differential Cryptanalysis)[3]和线性密码分析(Linear Cryptanalysis)[4]的提出,这两种分析方法也可用于当前的迭代密码.同时,人们也在差分密码分析和线性密码分析的基础上,提出了很多其他的分析方法.如对差分密码分析推广的高阶差分密码分析、不可能差分密码分析和矩阵分析等[5];而非线性密码分析、多重线性密码分析和差分-线性密码分析等都是线性密码分析的推广和扩充.

差分密码分析和线性密码分析被认为是迄今已知攻击迭代密码最有效的方法之一[6].线性密码分析方法与差分密码分析方法的结合也被认为是一种非常有效的方案[7-8].差分密码分析在 1990 年的 CRYpto 会议上被发表[9-10],它由文献[10]针对 DES 算法提出,本质上属于选择明文攻击.其分析过程如下:分析者寻找具有某些特定差分的明文,同时获得相应的密文对,比较这些带有某种特性的明文对和密文对,计算密钥的概率值,取概率最高的密钥作为最可能的加密密钥[11-12].

但是差分攻击方法并不是对所有分组密码都有用,因为对于某些分组密码,几乎不可能找到高概率的差分特征[13].差分密码分析也会受到分组密码轮数的影响.如当轮数为 17 时,差分密码分析需要花费的时间与穷尽密钥搜索相同.另一方面,差分密码分析需要大量具有某些特定差分的明文对及其相应的密文对作为支持.

针对这些缺点,1995 年,文献[14]提出了针对 DES 的截断差分密码分析方法.截断差分密码分析只需要知道部分比特上的差分特征,相对于传统的差分特征,它可以完成更多轮数的攻击,或是以更低的复杂度攻击相同的轮数.因此截断差分的思想在分组密码中得到了广泛的应用,如文献[15]使用截断差分的方法成功的攻击了 13 轮的 3D 分组密码.文献[16]应用了截断差分的思想攻击了 5 轮 Salsa 算法.文献[17]使用截断差分攻击方法成功的攻击了 12 轮 Camellia-128 算法,恢复了所有的密钥.文献[18]则将截断差分的思想与线性密码分析方法结合,分析了对 9 轮和 11 轮 DES 算法的攻击过程.

尽管截断差分攻击算法相对于传统的差分攻击算法具有一定的优点,但是其密钥恢复算法存在缺陷.比如,截断差分攻击在最终使用穷举方法前得到的 45 比特密钥候选值有很多组.所有的这些 45 比特密钥候选值剩余的 11 比特使用暴力攻击方法,这将浪费很多资源.

本文作者针对上述问题,提出了两种改进方案.实验结果表明:这两种方案都能减少候选密钥的个数,特别是第 2 种方法能够以很大的概率获得唯一的候选密钥,大大提高了密钥攻击时的效率.

1　预备知识

1.1　记号

本文所用记号及其含义分别如下:"|"代表 4 比特的级联;"||"代表 32 比特的级联;$K_{i,j}$ 代表第 i 轮中第 j 个 S 盒的 6 比特输入值;P 是 DES 算法中轮函数的最后置换函数.

1.2　数据加密标准 DES

DES 加密算法是一种对称加密算法,它使用 56 比特的密钥,明文和密文的长度均为 64 比特,加密算法和解密算法基本相同.算法中的 S 盒的结构对算法的安全性有较大的影响.

1.3　六轮 DES 截断差分密码分析算法

截断差分密码分析是差分密码分析的推广,它只要求知道某些比特的差分,甚至某些情况下,仅仅知道 1 比特的差分就能够成功的攻击一个分组密码或其低轮变形.

六轮 DES 截断差分攻击方法基于一个四轮的截断差分特征,如图 1 所示.由于 DES 的初始置换和末尾置换函数均为公开函数,不影响攻击方法分析,本文作者在分析过程中将忽略初始和末尾置换,以及 DES 加密最后一轮得到密文也不再做交换.

在 DES 加密算法中,由于扩展函数 E 和置换 P 的影响,一个 S 盒的 4 比特输出最多只能够影响下一轮 6 个 S 盒的输入.经过一些简单的计算,就可以得到上一轮 S 盒输出与下一轮 S 盒输入的比特关系,如表 1 所示.例如第 1 个 S 盒的输出不会影响下一轮中第 1 个和第 7 个 S 盒的输入.本文实现的截断差分密码分析方法正是利用了 DES 的这个特性.

用 R 表示扩展函数 E 的 32 比特输入,K 表示扩展函数 E 的轮密钥,它的长度为 48 比特.表 2 为 DES 算法的比特选择表.

根据表 2 可知,扩展函数 E 的作用是将 32 比特的输入 R 扩充为 48 比特.而这 48 比特根据 DES 算法的设计,将分为长度为 6 的 8 组二进制串,这 8 组数据将分别与轮密钥进行异或操作后,作为 8 个

S盒的输入.因此在轮密钥不发生变化的前提下,如果只改变 R 的第2比特和第3比特(从0开始计数),则只影响第1个S盒的输出,而不会影响其他7个S盒的输出.

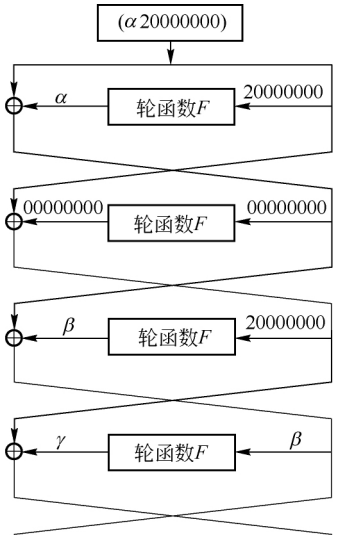

图1 DES的四轮差分特征

Fig.1 Differential characteristics of 4-round DES

表1 S盒输出的比特流向

Tab. 1 Flow of the S-box output bits

k_{i_j}	k_{i+1_k}	k_{i_j}	k_{i+1_k}
1	1,7	5	5,8
2	2,6	6	6,4
3	3,1	7	7,5
4	4,2	8	8,3

表2 扩展函数 E

Tab. 2 Diffusion function E

扩展函数 E					
32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

同理,只改变 R 的第6比特和第7比特,只会影响第2个S盒的输出.以此类推,可以得到,只改变表2某一行的第3列和第4列比特,对应的只影响该行所代表的S盒输出.图1是攻击中所用到的四轮截断差分特征,它所用的差分为0x20000000,即改变了第2个比特.仅用1个差分只能得到3个S盒的子密钥,因此还需要其他的差分特征.如仅改变第3个比特得到的差分0x40000000,同时改变第2比特和第3比特得到的差分0x60000000,具体实现过程中从这3个中任意选择两个即可.六轮DES截断差分密码分析的步骤如下:1)由表1可知,第1个S盒的输出不影响下一轮中第1个和第7个S盒的输入,基于该原理,构造概率值为1的四轮DES的截断差分,如图1所示.2)根据所选用的四轮DES截断差分特征,构造相应的明文对,同时遍历DES中 $K_{1,1}$ 的每个候选值,筛选出满足四轮截断差分特征的明文对.3)利用所选用的4组明文对,筛选出第6轮相关S盒的子密钥,筛选方法为只保留所有明文对均建议的密钥.4)利用其他的截断差分特征,恢复出其余的比特密钥.

2 截断差分攻击算法的实现与分析

截断差分密码分析过程中,对于每一个 $K_{1,1}$,均生成4个明文正确对,利用这4个明文正确对来筛选 $K_{6,1}$ 和 $K_{6,7}$.同理,再对 $K_{1,2}$ 的每一个候选值生成4个明文对来筛选 $K_{6,2}$ 和 $K_{6,6}$ 使用 $K_{1,5}$ 得到 $K_{6,5}$ 和 $K_{6,8}$.这样可以得到54比特密钥,因为部分密钥有重叠部分,故实际为45比特.剩余11比特使用暴力攻击.

对每一个 $K_{1,1}$ 的候选值,都有相应的4个正确对与之对应,如果每一个 $K_{1,1}$ 与相对应的4个正确对是一一映射的关系,文献[14]实现攻击的过程将会更加完美,然而这种关系并不是一一映射关系,而是多对多的关系.这种关系的存在使得在密钥恢复的过程中具有多种组合,而且存在这种多对多的关系的密钥和明文对所占百分比为47%.其具体关系如表3所示.由于 $K_{1,1}$ 代表的是二进制000000到111111的所有可能取到的值,可能情况较多且直接表示较为麻烦,因此本文为了方便,将二进制 $K_{1,1}$ 的所有取值使用十进制来表示.例如表中 $K_{1,1}$ 等于10,则实际代表的是6位二进制001010.

表3中,数值063代表的就是 $K_{1,1}$ 可能取到的全部十进制值,与该数值所对应的下一行数据代表的是与 $K_{1,1}$ 对应的4个正确明文对的下标值.第1个明文对是 P_i 和 P_{1_j} 组成的正确对,第2个明文对是 P_{2_j} 和 P_{3_j} 组成的正确对,这两个明文对形成的差分为0x20000000.第3个则为 P_i 和 P_{2_j} 组成的正确对,第4个为 P_{1_j} 和 P_{3_j} 组成的正确对,这两个形成的差分为0x40000000,其中 i 和 j 的取值范围是0~3.举例来说,当 $K_{1,1}$ 的值为0时,4个明文正确对依次为 P_3 与 $P_{1,0}$、P_{2_2} 与 P_{3_1}、P_0 与 P_{2_3}、P_{1_1} 与 P_{3_2},即这4组明文对具有图1所示的四轮截断差分特征,可以用来恢复当 $K_{1,1}$ 为0时第6轮的子密钥 $K_{6,1}$ 和 $K_{6,7}$.但是通过对表3的简单分析,可以发现,有多个密钥对应着相同的4个正确对.如当 $K_{1,1}$

为 35、39、43、47 时,对应的 4 个正确对均为 P_2 与 P_{1_3}、P_{2_3} 与 P_{3_2}、P_1 与 P_{2_1}、P_{1_1} 与 P_{3_1}.换句话说,假设当正确密钥为 43 时,实验在恢复的过程中会得到 35、39、43、47 这 4 个密钥.但是,对于错误组合,仍需要对其余的 11 比特做暴力破解,这就使得很多工作都是无效努力,占用了程序的大部分时间,例如有 4 种组合,那么其中的 3 组均为错误组合,对于这 3 种错误组合,也是需要对其余的 11 比特做暴力破解,也就是,在这段程序中,有 3/4 的工作是白费的.

表 3　密钥与正确对的关系

Tab. 3　Relationship of key and a set of plaintexts

0	1	2	3	4	5	6	7
3021	3103	1113	3203	3021	3103	1113	3203
0312	2322	3221	1311	2130	2232	1223	1131
8	9	10	11	12	13	14	15
1203	3013	3111	3023	1203	3013	3111	3023
0312	2322	3221	1311	2130	2232	1223	1131
16	17	18	19	20	21	22	23
1111	2122	2132	1331	1111	2122	2132	1331
2112	3033	3023	3003	2112	3303	3203	3003
24	25	26	27	28	29	30	31
1111	2212	2321	1331	1111	2212	2312	1331
2112	3033	3023	3003	2112	3303	3203	3003
32	33	34	35	36	37	38	39
2233	3111	1231	2332	2233	3111	1231	2332
1230	3221	3103	1111	0321	1223	3013	1111
40	41	42	43	44	45	46	47
3322	1113	1321	2332	3322	1113	1321	2332
1230	3221	3103	1111	0321	1223	3013	1111
48	49	50	51	52	53	54	55
2112	2130	3222	1131	2112	2130	3222	1131
0330	3311	2113	3203	0330	1133	3112	3023
56	57	58	59	60	61	62	63
2112	0312	2223	1311	2112	0312	2223	1311
0330	3311	2113	3203	0330	1133	3112	3023

分析表 3 后可得以下结论,在 $K_{1,1}$ 的 64 个候选值密钥中,能够与 4 个明文对具有一对一关系的有 34 个,即恢复过程中能够唯一确定 6 比特轮密钥.具有多对多关系的有 30 个,恢复过程成功概率为 50%的有 18 个,概率为 25%的密钥值为 12 个.

本文的第 1 种改进方案选择了第 1 轮中第 1 个、第 2 个、第 5 个 S 盒,并相应得到第 6 轮中第 1 个和第 7 个、第 2 个和第 6 个、第 5 个和第 8 个 S 盒的 6 比特子密钥.这样可以得到 54 比特的密钥,但是因为有些轮密钥在初始密钥中所占的位是相同的,所以最终得到的是 45 比特密钥.

同时,充分利用这些恢复的密钥中有重复位这一特点,如果初始密钥中有一位在某一轮密钥中不能确定时,则因为另外一个轮密钥,很有可能使得该位变得唯一而确定.如 $K_{1,1}$ 在初始密钥中所占的位分别为 15、18、12、25、2、6,$K_{6,1}$ 在初始密钥中所占的位分别为 24、27、21、6、11、15,第 6 轮 $K_{6,2}$ 所占位为 13、10、25、16、3、20.当在密钥恢复的过程中,第 1 轮 $K_{1,1}$ 有 4 组候选值,二进制表示分别为 100011 、100111 、101011 、101111.即初始密钥中的第 12 位、第 25 位不能确定.但是 $K_{6,2}$ 只有一组候选值 110100,则可以确定初始密钥中的第 25 位为 0.从而将候选值的个数折半.每个 S 盒出现 4 组候选值的概率为 12/64,但是根据概率论相关知识可知,多个 S 盒同时出现这种情况的概率比较低,这就使得该方法能够达到最初的目的.即 45 比特的密钥候选值个数降低很多,比例也随之降低.但只有一个 45 比特密钥建议值的概率仍然没有超过 50%.

为了进一步提高此阶段只有一个建议值的比例,本文作者第 2 种改进方法对恢复的第 1 轮多个子密钥建议处理措施为直接抛弃,具体措施如下:使用第 1 轮中第 1 个 S 盒,可以获得第 6 轮第 1 个和第 7 个 S 盒子密钥,以此类推,结合表 1,如果第 1 轮的 8 个 S 盒均被使用,恰好能够得到完整的两组第 6 轮 8 个 S 盒的 48 比特密钥,通过对两组 48 比特密钥的筛选,能够得到唯一确定的 48 比特子密钥.

每组轮密钥中,每个 S 盒的 6 比特密钥可能具有多个值.解决方式是构建 8 个具有 64 个计数器的计数矩阵.将长度为 6 的子密钥视为一个 0～63 的整数表示,用 64 个值对应位置 0,1,2,3,…,63.也就是说,位置标号代表着长度为 6 的子密钥.

8 个计数矩阵代表 8 个 S 盒 64 种子密钥的候选值.将获得的两组子密钥按照对应标号对相应的计数矩阵做相应的操作,这样,每一个矩阵中都有相同的值 2,这些计数器的位置确定了 8 个 S 盒的子密钥,最终获得 48 比特的第 6 轮子密钥.

3　改进的截断差分算法

由于第 1 种改进方法前面叙述的较为详细,本节将重点介绍第 2 种改进方法的实现过程.

3.1　构造明文

由于截断差分攻击属于一种选择明文攻击方法,因此构造明文是重中之重.本算法构造明文的方法具体过程如下:

1)选取 4 个明文对,选取的方法如下:

$P_i = A_i \,||\, P_R$.其中:$i = 0,1,2,3$;$A_i = P(a_i \,|\, r_0 \,|\, r_1 \,|\, r_2 \,|\, r_3 \,|\, r_4 \,|\, r_5 \,|\, r_6)$;$a_i = i$($a_i$ 为长度为 4 的二进制串);而 $r_k (k = 0,1,2,3,4,5,6)$ 代表随机

选择的4比特二进制串；P 表示轮函数中的置换；P_R 为随机选择的32比特二进制串.

2) 选取另4个明文，选取方法为：$P_{1,j} = B_j \| P_R \oplus 20000000$.其中：$B_j = P(b_j | r_0 | r_1 | r_2 | r_3 | r_4 | r_5 | r_6)$；$j = 0,1,2,3$；$b_0 = 0x0$；$b_1 = 0x4$；$b_2 = 0x8$；$b_3 = 0xc$($b_j$ 为长度为4的二进制串).

根据选用的明文 P_i 和 $P_{1,j}$ 可知，每一个 P_i 和每一个 $P_{1,j}$ 可形成具有如下差分的明文对：P (0xh | 0 | 0 | 0 | 0 | 0 | 0 | 0) $\|$ 20000000，h 为1～16的所有可能值. 在8个明文中，一定存在某一个明文对(称为正确对)满足图1所示的四轮截断差分特征.利用类似的原理，可以得到更多的正确对.

3) 同理再选4个明文 $P_{2,j} = B_j \| P_R \oplus 40000000$ 及另外的4个明文 $P_{3,j} = B_j \| P_R \oplus 20000000 \oplus 40000000$，其中 $j = 0,1,2,3$.$P_{2,j}$ 和 $P_{3,j}$ 结合，仍然会得到能够满足图1所示的截断差分特征的明文对.

同理，将 $P_{1,j}$ 和 $P_{2,j}$ 组合，以及 P_i 和 $P_{3,j}$ 组合，将会得到另外两个可利用的明文对.

本文实验在实现的过程中，32比特的 P_R 全部取为0，即 $P_R = 0x00000000$，不再使用随机比特，这种选法便于计算，同时节省程序的运行时间，提高程序的效率，也能够方便人工计算中间结果，进一步理解算法.同理，每一个 $r_k (k = 0,1,2,3,4,5,6)$ 都取值为0，即 $r_k = 0x0$.

3.2 攻击过程

对于 $K_{1,1}$ 的每一个候选值，按照以下方法筛选4个正确对.

1)计算 $c_0 = f(K_1, P_{iR})$，$c_1 = f(K_1, P_{1,jR})$，其中 K_1 的前6比特为 K_{1_1}，剩余42比特全部设为0. P_{iR} 为明文 P_i 的右32比特，P_1，j_R 同理.

2)在 P_i 和 $P_{1,j}$ 中寻找能够使得等式 $c_0 \oplus c_1 = P_{iL} \oplus P_{1,jL}$ 成立的明文对.

3)对 $P_{2,j}$ 和 $P_{3,j}$，$P_{1,j}$ 和 $P_{2,j}$，以及 P_i 和 $P_{3,j}$ 做同样的操作，筛选出4个明文对.

4个正确对选出来之后，过滤第6轮子密钥，过滤方法如下：

1)首先获得DES第3轮函数的32比特输入差分，记为 L'_3.在本实验中，前两组明文对所对应的差分值为0x20000000，后两组明文对的差分值为0x40000000.

2)将明密文对记为(L_0R_0，L_6R_6)和($L_0^*R_0^*$，$L_6^*R_6^*$)，L_0R_0 和 $L_0^*R_0^*$ 为明文对，L_6R_6 和 $L_6^*R_6^*$ 为密文对.则 R_6 的计算公式如下

$$R_6 = L_5 \oplus f(R_5, K_6) = R_4 \oplus f(R_5, K_6) = L_3 \oplus f(R_3, K_4) \oplus f(R_5, K_6) \tag{1}$$

同样的，R_6^* 计算公式为

$$R_6^* = L_5^* \oplus f(R_5^*, K_6) = R_4^* \oplus f(R_5^*, K_6) = L_3^* \oplus f(R_3^*, K_4) \oplus f(R_5^*, K_6) \tag{2}$$

从而有

$$R'_6 = L'_3 \oplus f(R_3, K_4) \oplus f(R_3^*, K_4) \oplus f(R_5, K_6) \oplus f(R_5^*, K_6) \tag{3}$$

式(3)中，R'_6 为 R_6 和 R_6^* 的差分值，其值已知.L'_3 在步骤1)中已经获得.通过图1可知，第4轮轮函数的输出中有8个比特为0，而这8位正是第6轮第1个和第7个S盒的输出差分.在仅考虑这两个S盒的条件下，通过式(3)可得

$$C'_1C'_2C'_3C'_4C'_5C'_6C'_7C'_8 = P^{-1}(R'_6 \oplus 0x40000000) \tag{4}$$

式中，每个 C_i 是长度为4的比特串.那么 C_1 和 C_7 分别是第6轮中 S_1 和 S_7 的输出异或.

3)对于每一个 $K_{6,1}$ 和 $K_{6,7}$ 的候选值，按照下式进行计算

$$C'_1C'_2C'_3C'_4C'_5C'_6C'_7C'_8 = P^{-1}(f(R_5, K_6)) \tag{5}$$

通过上述计算可以得到 S_1 和 S_7 的另一个输出异或.当两个异或相等时，记录 $K_{6,1}$ 和 $K_{6,7}$ 的候选值，即为该组正确对的候选密钥.最终结果选择4组明文对均建议的候选密钥.

经过上述筛选，可以获得 $K_{6,1}$ 和 $K_{6,7}$，可能具有多个建议值.

接下来使用 $K_{1,2}$ 攻击 $K_{6,2}$ 和 $K_{6,6}$.使用类似于图1的四轮截断差分特征，差分在0x20000000，0x40000000 与 0x60000000 中3个任意选择2个，可以这样选择的原因在上面已经描述过，这里不再叙述.

该过程构造的明文为

$P_i = A_i \| P_R$ 其中 $i = 0,1,2,3$，$A_i = P(a_i | r_0 | r_1 | r_2 | r_3 | r_4 | r_5 | r_6)$，$P_R$ 和 r_k 仍全部为0.

$P_{1,j} = B_j \| P_R \oplus 0x02000000$，$P_{2,j} = B_j \| P_R \oplus 0x04000000$，$P_{3,j} = B_j \| P_R \oplus 0x06000000$，其中 $B_j = P(r_0 | b_j | r_1 | r_2 | r_3 | r_4 | r_5 | r_6)$，$j = 0,1,2,3$，$b_0 = 0x0$，$b_1 = 0x4$，$b_2 = 0x8$，$b_3 = 0xc$.

对这十六个明文根据上述攻击第1个和第7个S盒子密钥做同样的操作，即根据第2个S盒的6比特子密钥筛选出需要的4组正确对，使用这些正确对按照筛选第6轮子密钥的算法获得 $K_{6,2}$ 和 $K_{6,6}$.

后面使用第 3、4、5、6、7、8 个第 1 轮 S 盒过程均与第 2 轮相同.明文与差分的选择过程较为方便,只需要将 L_0 按 4 比特为一组,a_i 和 b_j,4 个比特循环赋值给 L_0 的每一组即可.

上述所有过程均实现完成之后,则可以获得两组第 6 轮 8 个 S 盒的子密钥.构造 8 个具有 64 个计数器的计数矩阵.对两组内每个建议的 S 盒子密钥进行计数.例如第 1 组第 1 个 S 盒子密钥为 010100 和 011000,在 J_1 的计数矩阵中的位置 20 和 24 处增加 1.当 8 个计数矩阵均完成后,找到 8 个计数矩阵中数值为 2 的位置,并将这些位置所在的整数转换为相应的二进制,即可获得最终 48 比特密钥值.其余 8 个比特使用暴力破解得到.

4　改进算法评估与分析

通过大量实验测试数据统计,可得到以下结果:使用第 1 种方法时,只有一个密钥候选值的比率在 35%～40%左右.有两组候选值比例在 45%左右.第 2 种方法能够使得只有一组密钥候选值的概率为 1.

两种方法分别举例说明如下:第 1 种方法:当被攻击的密钥为 0x1d1cf6932d3ce51c 时,以攻击 $K_{1,1}$,$K_{6,1}$ 和 $K_{6,7}$ 为例.明文与密文分别如表 4 所示.

表 4　攻击所用明文对与密文对

Tab. 4　Plaintexts and ciphertexts in the attack

明文(十六进制)	密文(十六进制)
0000000200000000	43ffa240eecd6efd
0080800020000000	50b1c23160f52254
0080800040000000	fa5b8f08cd17d6d7
0000000260000000	7419814c8acfad4c
0000020200000000	fd06b7132b7fc179
0000000040000000	650df6598a99f3b8
0000000020000000	fbca3598dfc5bbe9
0000020260000000	7c0a711ca2de145e

根据表 4 中的 4 对明文及其相应的密文攻击得到的第 1 轮第 1 个 S 盒子密钥 $K_{1,1}$ 的候选值与第 6 轮第 1 个与第 7 个 S 盒子密钥 $K_{6,1}$ 与 $K_{6,7}$ 的候选值分别如表 5 所示.

表 5　攻击获得的 $K_{1,1}$、$K_{6,1}$ 与 $K_{6,7}$ 候选值

Tab.5　$K_{1,1}$、$K_{6,1}$ and $K_{6,7}$ suggested by attack

$K_{i,j}$	可能的候选值(二进制)
$K_{1,1}$	010011
	010111
	011011
	011111
$K_{6,1}$	000111
	010100
$K_{6,7}$	100110

由表 5 的数据可知,$K_{1,1}$ 有两位不能确定,$K_{6,1}$ 有两组候选值,$K_{6,7}$ 有一组候选值.利用同样的方法,可以得到其他所需要的子密钥候选值,所有的候选值如表 6 所示.

表 6　攻击得到的所有密钥候选值

Tab. 6　All keys value suggested by attack

$K_{i,j}$	可能的候选值(二进制)
$K_{1,1}$	010011
	010111
	011011
	011111
$K_{6,1}$	000111
	010100
$K_{6,7}$	100110
$K_{1,2}$	000010
	000110
	001010
	001110
$K_{6,2}$	011001
$K_{6,6}$	101110
$K_{1,5}$	110011
	110111
	111011
	111111
$K_{6,5}$	110101
$K_{6,8}$	110011

由表 6 可知,如果不做任何处理,最终得到的 45 比特密钥的候选值将有 $4\times4\times4\times2=128$ 种.如果利用轮密钥在初始密钥中的重复位,可以去掉很多候选值,如表 7 所示.

表 7　S 盒子密钥在初始密钥中的位置

Tab. 7　Sub-keys position in the initial key

$K_{i,j}$	在初始密钥中所占的位置(0～63)
$K_{1,1}$	15　18　12　25　2　6
$K_{1,2}$	4　1　16　7　22　11
$K_{1,5}$	42　53　32　38　48　56
$K_{6,1}$	24　27　21　6　11　15
$K_{6,2}$	13　10　25　16　3　20
$K_{6,5}$	51　34　41　47　29　37
$K_{6,6}$	40　50　33　55　43　30
$K_{6,7}$	54　31　49　38　44　35
$K_{6,8}$	56　52　40　46　39　42

可以看到,表 7 中有很多重复位,当 $K_{1,1}$ 不能确定初始密钥的第 25 位时,当 $K_{6,1}$ 有两组候选值时,由于 $K_{1,1}$ 能够确定初始密钥的第 15 位,据此位就可确定 $K_{6,1}$ 两组候选值中正确的那一个.根据同样的道理,可以得到最终的几组密钥候选值,见表 8.

到目前为止,只有初始密钥中的第 12 位、第 7

位、第32位不能确定，对这3位使用穷举方法将得到8组45比特子密钥候选值，达到了降低候选值个数的目的.

表8 最终S盒的密钥候选值

Tab.8 Final keys of $K_{i,j}$

$K_{i,j}$	可能的候选值(二进制)
$K_{1,1}$	010111 011111
$K_{6,1}$	010100
$K_{6,7}$	100110
$K_{1,2}$	000010 000110
$K_{6,2}$	011001
$K_{6,6}$	101110
$K_{1,5}$	110111 111111
$K_{6,5}$	110101
$K_{6,8}$	110011

第2种方法使用了8个S盒，假设初始密钥为0x747b5237ba4e2afd，仍以攻击$K_{1,1}$，$K_{6,1}$和$K_{6,7}$为例.明文与密文分别如表9所示.

表9 明文对和相应的密文对

Tab.9 Plaintexts and the corresponding ciphertexts

明文(十六进制)	密文(十六进制)
0000020000000000	648c1aeafc1eaf32
0000800020000000	37ad1e65bd991140
0000800040000000	8a829eb9f36b8958
0000020060000000	5a6b1fe4d5852886
0000000000000000	5cb77ab4e5611fcc
0080800040000000	7c159096e2cf482d
0080800020000000	322a81d1d187d056
0000000060000000	5666f18d5a570585

利用表9中的4对明文对与相应的密文对，可以得到表10中的$K_{1,1}$、$K_{6,1}$和$K_{6,7}$密钥候选值.其中$K_{1,1}$有4组候选值，$K_{6,1}$和$K_{6,7}$分别各有一组候选值.

表10 $K_{1,1}$、$K_{6,1}$和$K_{6,7}$密钥候选值

Tab.10 $K_{1,1}$、$K_{6,1}$ and $K_{6,7}$ candidate key

$K_{i,j}$	可能的候选值(二进制)
$K_{1,1}$	110000 110100 111000 111100
$K_{6,1}$	101011
$K_{6,7}$	110011

同理，按上述方式，依次用其余7个S盒进行攻击，这里不再列出相应明文对及密文对，可得第1轮其他7个S盒子密钥的候选值及两组第6轮8个S盒子密钥候选值，分别如表11和表12所示.

表11 第1轮8个S盒的密钥候选值

Tab.11 8-S-boxes candidate key in first 1 round

$K_{i,j}$	可能的候选值(二进制)
$K_{1,1}$	110000 110100 111000 111100
$K_{1,2}$	110010 111001
$K_{1,3}$	110001
$K_{1,4}$	100010 100110 101010 101110
$K_{1,5}$	011011
$K_{1,6}$	110110
$K_{1,7}$	100011 100111 101011 101111
$K_{1,8}$	101111

表12 两组第6轮8个S盒的密钥候选值

Tab.12 Two groups of 8-S-boxes in 6 round candidate key

$K_{i,j}$	第1组可能的候选值(二进制)	第2组可能的候选值(二进制)
$K_{6,1}$	101011	101011
$K_{6,2}$	001101	001101
$K_{6,3}$	010101	010101
$K_{6,4}$	011010	011010
$K_{6,5}$	111101	111101
$K_{6,6}$	001101 100100 100110 110110	001101 111111
$K_{6,7}$	110011	110011
$K_{6,8}$	101110	101110

方法2中抛弃了第1轮8个S盒得到的相应候选值，只保留两组第6轮8个S盒的子密钥，将6比特子密钥的二进制形式转换为十进制数，填入计数器中相应的位置.

通过8个计数器中数据可知，每一个计数器中都有一个唯一的位置是2，代表该位置的十进制数正是相应S盒6比特二进制子密钥转换得到，通过8个计数器，可以得到唯一的48比特子密钥候选值.

5 结语

本文首先对截断差分密码攻击的整个过程做了详尽的介绍，并分析了截断差分密码攻击过程中密钥恢复时会产生多组候选值的原因.基于上述不足，

本文作者提供了以下两种解决方案:

1)由于每一轮的轮密钥都是经过初始密钥变换得来的,因此,每轮的轮密钥经过相应的逆变换就可以得到初始密钥.这就导致了不同轮之间的轮密钥中某些位是由初始密钥中的同一位变换而来,基于此性质,本文提出了第 1 种改进方法.该方法能够实现只有一组密钥候选值的概率在 35%～40%左右,而有两组的概率为 45%左右.

2)第 2 种改进方案依次使用了 8 个 S 盒进行攻击,最终能够得到两组第 6 轮轮密钥候选值.由于这两组候选值中均包含正确的密钥值,因此通过对这些候选值进行计数,选出两组均建议的候选值即可.实验结果表明,该方法的效果优于第 1 种,它能够实现只有一组密钥候选值的概率接近为 1.

参考文献(References):

[1] 吴杨, 王韬, 邢萌.基于密文随机性度量值分布特征的分组密码算法识别方案[J]. 通信学报, 2015, 36(4): 146－155.
WU Yang, WANG Tao, XING Meng. Block ciphers identification scheme based on the distribution character of randomness test values of ciphertext[J]. Journal on Communication, 2015, 36(4): 146－155. (in Chinese)

[2] 吴杨, 王韬, 李进东.分组密码算法密文的统计检测新方法研究[J]. 军械工程学院学报, 2015, 27(3): 59－64.
WU Yang, WANG Tao, LI Jindong. Research on new statistical and testing method for ciphertexts of block cipher[J]. Journal of Ordnance Engineering College, 2015, 27(3): 59－64.(in Chinese)

[3] BIHAM E, SHAMIR A. Differential cryptanalysis of the data encryption standard[M]. Springer Verlag, 1993.

[4] MATSUI M. Linear cryptoanalysis method for DES ciper[C]. Advances in Cryptology－EUROCRYPT'93, 1994, 765: 386－397.

[5] MATSUI M. The first experimental cryptanalysis of the data encryption standard[C]. Advances in Cryptology－Crypto'94, 1994, 839: 1－11.

[6] 多磊. 分组密码的设计与分析[D]. 北京:国防科技大学, 2001.
DUO Lei. Analysis and design of block ciphers[D]. Bei－jing: National University of Defense Technology, 2001. (in Chinese)

[7] BLONDENU C, NYBERG K. New Links between differential and linear cryptanalysis[J]. LNCS, 2013, 7881: 388－404.

[8] LANGFORD S K, HELLMAN M E. Differential－linear cryptanalysis[C]. Advances in Cryptology－Crypto'94 Proc, 1994: 17－26.

[9] 冯登国, 吴文玲. 分组密码的设计与分析[M]. 北京:清华大学出版社, 2000.
FENG Dengguo, WU Wenling. Analysis and design of block cipher[M]. Beijing: Tsinghua University Press, 2000. (in Chinese)

[10] BIHAM E, SHAMIR A. Differential cryptanalysis of the full 16－round DES[C]. International Cryptology Conference on Advances in Cryptology, 1992, 740: 487－496.

[11] BIHAM E, SHAMIR A. Differential cryptanalysis of DES－like cryptosystem[J]. Journal of Cryptology, 1991, 4(1): 3－72.

[12] CHAUM D, EVERTSE J H. Cryptanalysis of DES with a reduced number of rounds[C]. Sequences of Linear Factors in Block Ciphers, Advance in Cryptology, Proceeding of Crypto'85, 1985: 192－211.

[13] SHAMIR A. On the security of DES[C]. Advance in Cryptology－Crypto'85, Lecture Notes in Computer Science, 1985, 218: 280－281.

[14] KNUDSON L R. Truncated and higher order differential [J].LNCS,1995:196－211.

[15] KOYAMA T, WANG L, SASAKI Y, et al. New truncated differential cryptanalysis on 3D block ciper [J]. LNCS, 2012, 7232: 109－125.

[16] 关杰, 张中亚. 5 轮 Salsa20 的代数-截断差分攻击[J]. 软件学报, 2013, 24(5): 1111－1126.
GUAN Jie, ZHANG Zongya. Algebraic truncated differential cryptanalysis of 5－round Salsa20[J]. Journal of Software, 2013, 24(5): 1111－1126. (in Chinese)

[17] 李艳俊, 张伟, 欧海文. Camellia－128 的截断差分攻击改进[J]. 计算机应用研究, 2013, 30(7): 2129－2131.
LI Yanjun, ZHANG Wei, OU Haiwen. Improved truncated differential analysis on Camellia－128[J]. Application Research of Computers, 2013, 30(7): 2129－2131. (in Chinese)

[18] 贺也平, 吴文玲, 卿斯汉. 截断差分-线性密码分析[J]. 软件学报, 2000, 11(10): 1294－1298.
HE Yeping, WU Wenling, QING Sihan. Truncated differential－linear cryptanalysis[J]. Journal of Software, 2000, 11(10): 1294－1298. (in Chinese)