ISSN 1000-9825, CODEN RUXUEW
Journal of Software, Vol.19, No.10, October 2008, pp.2659−2666
DOI: 10.3724/SP.J.1001.2008.02659

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel/Fax: +86-10-62562563

对 DES 的 Rectangle 攻击和 Boomerang 攻击*

张 蕾[1,2+], 吴文玲[1,2]

[1](中国科学院 软件研究所 信息安全国家重点实验室,北京 100190)

[2](中国科学院 研究生院 信息安全国家重点实验室,北京 100049)

Rectangle and Boomerang Attacks on DES

ZHANG Lei[1,2+], WU Wen-Ling[1,2]

[1](State Key Laboratory of Information Security, Institute of Software, The Chinese Academy of Sciences, Beijing 100190, China)

[2](State Key Laboratory of Information Security, Graduate University, The Chinese Academy of Sciences, Beijing 100049, China)

+ Corresponding author: E-mail: zhanglei1015@is.iscas.ac.cn

Zhang L, Wu WL. Rectangle and Boomerang attacks on DES. *Journal of Software*, 2008,19(10):2659−2666.
http://www.jos.org.cn/1000-9825/19/2659.htm

Abstract: In spite of being replaced by AES (advanced encryption standard), DES (data encryption standard) still plays an important role as encryption standard. DES and the triple DES are still widely used in many areas, especially in the financial sector. Recently, some new cryptanalytic techniques are introduced and of which the Rectangle attack and the Boomerang attack had proved to be very powerful. Therefore, it is necessary to re-evaluate the effects that these new cryptanalytic techniques may have on DES. This paper examines the strength of DES against the Rectangle attack and the Boomerang attack. By using the best differential characteristic of DES, the paper gets an attack against up to 12-round DES using the Rectangle attack and an attack against 11-round DES using the Boomerang attack respectively. The Rectangle attack on 12-round DES requires 2^{62} chosen plaintexts and the time complexity is equivalent to 2^{42} 12-round encryptions, while the Boomerang attack on 11-round DES requires 2^{58} adaptive chosen plaintexts and ciphertexts and the time complexity is equivalent to 2^{38} 11-round encryptions. Because the differential characteristics used in the attacks are all the best ones, it is believed that the attacks are the best results that the Rectangle attack and the Boomerang attack can get on DES.

Key words: DES (data encryption standard); Rectangle attack; Boomerang attack; differential characteristic; distinguisher

摘 要: 作为加密标准,DES(data encryption standard)算法虽然已被 AES(advanced encryption standard)算法所取代,但其仍有着不可忽视的重要作用.在一些领域,尤其是金融领域,DES 和 Triple DES 仍被广泛使用着.而近年来又提出了一些新的密码分析方法,其中,Rectangle 攻击和 Boomerang 攻击已被证明是非常强大而有效的.因此,有必要重新评估 DES 算法抵抗这些新分析方法的能力.研究了 DES 算法针对 Rectangle 攻击和 Boomerang 攻击的安全性.

* Supported by the National Natural Science Foundation of China under Grant No.90604036 (国家自然科学基金); the National Basic Research Program of China under Grant No.2004CB318004 (国家重点基础研究发展计划(973)); the National High-Tech Research and Development Plan of China under Grant No.2007AA01Z470 (国家高技术研究发展计划(863))

Received 2007-03-23; Accepted 2007-06-07

利用 DES 各轮最优差分路径及其概率,分别得到了对 12 轮 DES 的 Rectangle 攻击和对 11 轮 DES 的 Boomerang 攻击.攻击结果分别为:利用 Rectangle 攻击可以攻击到 12 轮 DES,数据复杂度为 2^{62} 个选择明文,时间复杂度为 2^{42} 次 12 轮加密;利用 Boomerang 攻击可以攻击到 11 轮 DES,数据复杂度为 2^{58} 个适应性选择明密文,时间复杂度为 2^{38} 次 11 轮加密.由于使用的都是 DES 各轮的最优差分路径,所以可以相信,该结果是 Rectangle 攻击和 Boomerang 攻击对 DES 所能达到的最好结果.

关键词: DES(data encryption standard)算法;Rectangle 攻击;Boomerang 攻击;差分路径;区分器

中图法分类号: TP309 **文献标识码**: A

DES 加密算法[1]是由 IBM 公司开发的一种 Feistel 分组密码,是 LUCIFER 密码算法的改进版本,于 1977 年被美国标准局采用为数据加密标准,之后得到了广泛使用.1994 年,NIST 把 DES 的有效期延长了 5 年,并建议将其用于政府或军事机密信息防护以外的其他应用.虽然 DES 已被 2000 年由 NIST 公布的高级加密标准(AES)所取代,但其仍有着不可忽视的重要作用.在一些领域,尤其是金融领域,DES 和 Triple DES 仍被广泛使用着.在 DES 的使用过程中,最主要的担心就是它较短的密钥长度(56 bit),这使得穷举式密钥搜索攻击的复杂度仅为 2^{55}.除此之外,对 DES 最有效的攻击就是由 Biham,Shamir 于 1992 年提出的对 16 轮 DES 的差分分析[2]和由 Matsui 于 1994 年提出的优化后的对 16 轮 DES 的线性分析[3],其复杂度分别为 2^{47} 个选择明文和 2^{43} 个已知明文.

近年来又提出了一些新的密码分析方法,Rectangle 攻击[4]和 Boomerang 攻击[5]是其中最杰出的代表.利用这两种攻击方法对现有的大量密码算法给出了非常有效的攻击,如对 COCONUT98[5],AES[6],KASUMI[7]等算法,(related-key) Rectangle 攻击和 Boomerang 攻击得到的结果都是目前已知的最好结果.可见,Rectangle 攻击和 Boomerang 攻击是非常强大而有效的.基于这些观察,我们考虑将这两种攻击方法应用于 DES,看能否得到更好的结果.由于 DES 密钥编排算法的特点,使得几乎每轮密钥都受主密钥差分的影响.如果使用相关密钥攻击,则每轮都将有密钥差分的影响,这将严重降低差分路径的概率.可见,利用相关密钥对 DES 无效.因此,我们的分析中只使用基本的 Rectangle 攻击和 Boomerang 攻击.

本文研究了 DES 算法针对 Rectangle 攻击和 Boomerang 攻击的安全性.利用 DES 各轮最优差分路径及其概率,分别得到了对 12 轮 DES 的 Rectangle 攻击和对 11 轮 DES 的 Boomerang 攻击.攻击结果分别为:利用 Rectangle 攻击可以攻击到 12 轮 DES,数据复杂度为 2^{62} 个选择明文,时间复杂度为 2^{42} 次 12 轮加密;利用 Boomerang 攻击可以攻击到 11 轮 DES,数据复杂度为 2^{58} 个适应性选择明密文,时间复杂度为 2^{38} 次 11 轮加密.由于我们使用的都是 DES 各轮的最优差分路径,所以我们相信,该结果是 Rectangle 攻击和 Boomerang 攻击对 DES 所能达到的最好结果.

本文第 1 节描述 Rectangle 攻击和 Boomerang 攻击的基本思想和方法.第 2 节介绍所使用的 DES 差分路径.第 3 节和第 4 节分别给出对 DES 的 Rectangle 攻击和 Boomerang 攻击,包括攻击过程和复杂度分析.第 5 节总结全文.

1 Boomerang 攻击和 Rectangle 攻击

Boomerang 攻击[5]是由 Wagner 于 1999 年提出来的,它是一种新的差分类型攻击.其主要思想是利用两条短的高概率差分路径来代替一条长的低概率差分路径,这使得对一些加密算法的分析可以进行到更多轮.但是,由于 Boomerang 攻击需要适应性地选择明密文,这使得很多利用区分器恢复密钥的技术无法应用.于是,2000 年,Kelsey 等人提出了 Boomerang 攻击的选择明文变体,称为 Amplified Boomerang 攻击[8].其主要思想是加密大量明文对来寻找符合 Boomerang 区分器要求的四元组.Rectangle 攻击[4]是对 Amplified Boomerang 攻击的改进版本,它通过同时使用多条差分路径来增加区分器的概率,从而降低攻击的复杂度.下面将分别详细介绍 Boomerang 攻击和 Rectangle 攻击.

1.1 Boomerang攻击

Boomerang 攻击的主要思想是连接两条短的高概率差分路径,以便分析到算法的更多轮.假设加密算法表示为两种子算法的连接 $E=E_1\circ E_0$,其中,E_0 存在概率为 p 的差分路径$\alpha\to\beta$,E_1 存在概率为 q 的差分路径$\gamma\to\delta$,则 Boomerang 攻击过程如下:

- 选择明文对(P_1,P_2)满足 $P_1\oplus P_2=\alpha$,记加密后得到的相应密文为(C_1,C_2).
- 计算 $C_3=C_1\oplus\delta$,$C_4=C_2\oplus\delta$,解密密文对记得到的相应明文为(P_3,P_4).
- 检验 $P_3\oplus P_4=\alpha$是否成立.

对于加密算法 E,明文对(P_1,P_2)符合差分路径$\alpha\to\beta$的概率为 p,密文对(C_1,C_3)和(C_2,C_4)均符合差分路径$\gamma\to\delta$的概率为 q^2.当上述各式均成立时,$P_3\oplus P_4=\alpha$成立的概率为 p,即由明密文对组成的四元组通过该区分器的概率为$(pq)^2$.而对于随机置换,四元组通过的概率为 2^{-n}.因此,只要选择好的差分路径使得$(pq)^2>2^{-n}$,即可利用该区分器得到密钥恢复攻击.上述攻击可以改进为对所有可能的差分值β和$\gamma(\beta\neq\gamma)$同时进行分析,此时,四元组通过检验的概率为 $(\hat{p}\hat{q})^2$,其中, $\hat{p}=\sqrt{\sum_{\beta}\Pr^2[\alpha\to\beta]}$, $\hat{q}=\sqrt{\sum_{\gamma}\Pr^2[\gamma\to\delta]}$.对 Boomerang 攻击的完整介绍请参见文献[5].

1.2 Rectangle攻击

鉴于 Boomerang 攻击需要适应性地选择明文和密文,很多密钥恢复技术都无法应用,因此提出了其选择明文变体即 Rectangle 攻击.该变体的主要思想是加密大量输入差分为α的明文对,再从中选出符合区分器要求的四元组.Rectangle 的攻击过程如下:

- 加密大量明文对$(P,P\oplus\alpha)$.
- 选择明文对(P_1,P_2)和(P_3,P_4),使其相应的密文对满足 $C_1\oplus C_3=C_2\oplus C_4=\delta$.

采用与第 1.1 节相似的分析并考虑到 $E_0(P_1)\oplus E_0(P_3)=\gamma$的概率为 2^{-n}可知,对于加密算法 E,四元组通过区分器检验的概率为 $2^{-n}p^2q^2$.当同时分析所有可能的β和$\gamma(\beta\neq\gamma)$时,四元组通过检验的概率增为 $2^{-n}(\hat{p}\hat{q})^2$.而对于随机置换,四元组通过检验的概率为 2^{-2n}.因此,只要选择好的差分路径使得 $2^{-n}(\hat{p}\hat{q})^2>2^{-2n}$, 即可实现密钥恢复攻击.对于 Rectangle 攻击的完整介绍请参见文献[4].

2 DES 差分路径

DES 的分组长度为 64 bit,有效密钥长度为 56 bit,轮数为 16 轮,采用标准的 Feistel 密码结构,轮函数为 $F(K_i,R_{i-1})=P(S(E(R_{i-1})\oplus K_i))$.由于初始置换和逆初始置换对算法的安全性没有影响,所以在后面的分析中均将其省略.关于 DES 算法的完整描述请见参考文献[1].

在对 DES 已有的差分攻击[2,9]中,主要利用了两类基本差分路径,分别是概率为 1/16 的 3 轮差分路径和概率为 1/234 的 2 轮循环差分路径.图 1 和图 2 分别描述了这两条差分路径.

在文献[10]中,Matsui 基于差分和线性分析之间的对偶关系,利用递归算法,通过程序搜索给出了 DES 算法各轮最优差分路径及其概率,结果见表 1.由搜索结果可知,对于 7 轮及以上各轮 DES 算法,由 2 轮循环差分路径迭代得到的差分路径即构成了实际中的最优差分路径[10].

由于在 Rectangle 攻击和 Boomerang 攻击中均要求$(pq)^2>2^{-n}$成立,结合表 1 所示的各轮最优差分路径概率可知,由 7 轮差分路径和 3 轮差分路径连接组成的区分器是符合条件的最优选择.下面分别列出攻击中将使用的这两条差分路径.

第 1 条差分路径是由 2 轮循环差分路径迭代构成的 7 轮差分路径,可以简单表示为

$$(19600000_x,00000000_x)\xrightarrow{p=1}(00000000_x,19600000_x)\xrightarrow{p=1/234}(19600000_x,00000000_x)\xrightarrow{p=1}$$
$$(00000000_x,19600000_x)\xrightarrow{p=1/234}(19600000_x,00000000_x)\xrightarrow{p=1}(00000000_x,19600000_x)\xrightarrow{p=1/234}$$
$$(19600000_x,00000000_x)\xrightarrow{p=1}(00000000_x,19600000_x),$$

其概率为 $p=\left(\frac{1}{234}\right)^3\approx 2^{-23.61}$.

第 2 条差分路径为上述 3 轮差分路径,可以简单表示为

$$(40080000_x,04000000_x)\xrightarrow{p=1/4}(04000000_x,00000000_x)\xrightarrow{p=1}(00000000_x,04000000_x)\xrightarrow{p=1/4}(04000000_x,40080000_x),$$

概率为 1/16,其中,$\gamma=(40080000_x,04000000_x)$.

在第 2 条差分路径中,为了使经过一轮变换后的差分等于$(04000000_x,00000000_x)$,需要γ的左半部分与输入差分 04000000_x 经过轮函数后的输出差分相等.考虑到轮函数的所有可能输出差分及其概率,可以得到γ的全部可能值.当γ同时取遍这些可能值时,第 2 条差分路径的总概率为 $\hat{q}=\sqrt{\sum_{\gamma}p_{\gamma}^{\ 2}}=\frac{3}{32}\approx 2^{-3.42}$.

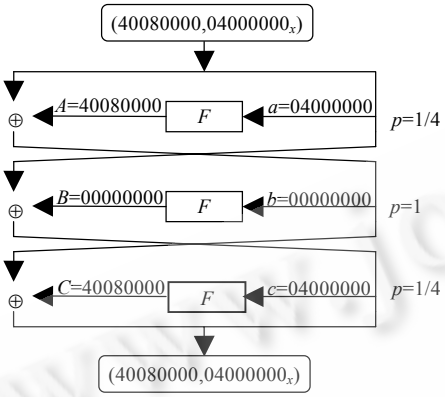

Fig.1 Three-Round differential characteristic of DES

图 1 DES 算法 3 轮差分路径

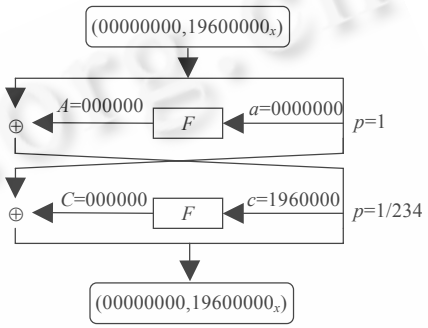

Fig.2 Two-Round iterative differential characteristic of DES

图 2 DES 算法 2 轮循环差分路径

Table 1 The best characteristic probability of DES

表 1 DES 算法各轮最优差分路径的概率

Round	4	5	6	7	8	9	10
Probability	1.31×2^{-10}	1.72×2^{-14}	1.03×2^{-20}	1.31×2^{-24}	1.43×2^{-31}	1.43×2^{-32}	1.57×2^{-39}
Round	11	12	13	14	15	16	
Probability	1.57×2^{-40}	1.71×2^{-47}	1.71×2^{-48}	1.87×2^{-55}	1.87×2^{-56}	1.02×2^{-62}	

3 对 12 轮 DES 的 Rectangle 攻击

将第 2 节给出的两条差分路径连接(分别用于 2 轮~8 轮,9 轮~11 轮)可以构成 10 轮 Rectangle 区分器,其概率为 $\tilde{p}=2^{-n}p^2\hat{q}^2=2^{-118.06}$.由于 $p\hat{q}=2^{-27.03}>2^{-32}=2^{-n/2}$,所以,该区分器可将 DES 算法与随机函数区分开.下面的攻击即利用该 10 轮(第 2 轮~11 轮)区分器来恢复 12 轮 DES 算法的部分密钥信息.

攻击的基本思想为:猜测第 1 轮的部分密钥比特,对明文加密第 1 轮,找到所有满足上述第 1 条差分路径的明文对;猜测最后一轮的部分密钥比特,对密文部分解密最后一轮,找到所有满足第 2 条差分路径的密文对.最后,利用得到的正确四元组的个数将正确的密钥猜测和错误的密钥猜测区分出来,以此恢复部分密钥比特信息.

作为准备工作,先对选择明文的特征进行一下分析.对于轮函数 $F(\cdot)$,当输入差分为 0*x*19600000 时,可能的输出差分形式应为 $P(UVW00000)$,其中,$P(\cdot)$表示轮函数中最后的 32 bit 置换.为满足第 2 轮的输入差分等于$(19600000_x,00000000_x)$,则明文差分的左半部分应等于$P(UVW00000)$.即要求ΔP_L除第 2,6,9,13,16,17,18,23,24,28,30,31 这 12 bit 之外均为 0,而ΔP_R=0*x*19600000.

详细的对 12 轮 DES 的 Rectangle 攻击过程如下:

1. 数据收集:定义 S^a 为由 2^{12} 个明文组成的一个结构,其中每个明文在上述 12 比特处取任意值,其余 52 比特处取一固定值.取 2^{48} 个这样的结构 $S_1^a,S_2^a,...,S_{2^{48}}^a$,分别对其进行 12 轮加密,记得到的密文为 $D_1^a,D_2^a,...,D_{2^{48}}^a$.对每个明文 P_a 在 52 个固定比特处计算 $P_b=P_a\oplus\Delta P$,得到相应的 2^{48} 个结构 $S_1^b,S_2^b,...,S_{2^{48}}^b$,记其密文为 $D_1^b,D_2^b,...,D_{2^{48}}^b$.类似地,取 2^{48} 个结构 $S_1^c,S_2^c,...,S_{2^{48}}^c$,每个结构中明文的上述 12 比特处取任意值,其余 52 比特取一个不重复的固定值.相应地计算 $P_d=P_c\oplus\Delta P$ 得到 2^{48} 个结构 $S_1^d,S_2^d,...,S_{2^{48}}^d$.记密文分别为 $D_1^c,D_2^c,...,D_{2^{48}}^c$ 和 $D_1^d,D_2^d,...,D_{2^{48}}^d$.
2. 数据分析:类似于准备工作中对明文差分的分析,可知密文差分满足 ΔC_L 除第 1,6,9,10,16,17,20,23,24,26,30,31 这 12 bit 之外均为 0,ΔC_R=0*x*40080000.
   a) 对每对结构 D_i^a,D_j^c,将其中的密文对按照除第 1,6,9,10,16,17,20,23,24,26,30,31 这 12 bit 之外的 52 比特进行检查,将不符合相应密文差分 ΔC 的对去掉.
   b) 对相应的结构 D_i^b,D_j^d,检查除上述 12 bit 之外的 52 比特,将不符合相应密文差分 ΔC 的对去掉.此时,由剩余对构成的四元组为候选四元组,记为(P^a,P^b,P^c,P^d).
   c) 此时剩余的四元组个数为 $2^{144}\times2^{-52}\times2^{-52}=2^{40}$,如果同时猜测 18 比特密钥,则复杂度将达到 $2^{40}\times2^{18}\times4\times3/8=6\times2^{56}$ 次一轮加密,相当于穷尽搜索的复杂度.为降低复杂度,将分别猜测进入每个 S 盒的 6 比特密钥,依据相应的差分对候选四元组进行逐步过滤.先猜测轮密钥 K_{12} 进入 S_1 的 6 比特值,对候选四元组部分解密第 12 轮,检查 P^a,P^c 第 11 轮输出差分中的相应 4 比特是否与 0*x*04000000 中的相应比特符合,将不符合该差分的四元组去掉.再检查 P^b,P^d 第 11 轮输出差分中的相应 4 比特是否符合,将不符合该差分的四元组去掉.
   d) 再猜测轮密钥 K_{12} 进入 S_3 的 6 比特值,对剩余的候选四元组部分解密第 12 轮,检查 P^a,P^c 及 P^b,P^d 的相应 4 比特差分是否符合,将不符合该差分的四元组去掉.
   e) 最后猜测轮密钥 K_{12} 进入 S_4 的 6 比特值,检查相应差分并去掉不符合差分的四元组.
   f) 猜测轮密钥 K_1 进入 S_1,S_2,S_3 的 18 比特值,由于其中 10 比特与已猜测的 K_{12} 是共同比特,所以只需再猜测 8 比特值.利用猜测的密钥对剩余的候选四元组部分加密第 1 轮,检查 P^a,P^b 第 2 轮输入差分的右半部分是否为 0*x*00000000,将不符合该差分的四元组去掉.再检查 P^c,P^d 第 2 轮输入差分的右半部分是否为 0*x*00000000,将不符合该差分的四元组去掉.如果此时还有至少 3 个四元组,则输出相应的密钥猜测作为正确密钥;否则重复第(c)~(f)步.

下面给出该攻击的数据复杂度和时间复杂度分析:本攻击共需要 $4\times2^{48}\times2^{12}=2^{62}$ 个选择明文.由这些明文形成了 2^{144} 个四元组,其中,预计将有 $2^{144}\times2^{-12}\times2^{-12}=2^{120}$ 个四元组的第 2 轮输入差分为(19600000_x,00000000_x).将这些四元组应用于上述 10 轮区分器,可知有 $2^{120}\times2^{-118.06}=2^{1.94}\approx3.83$ 个四元组符合该区分器,即预计正确四元组的个数应为 3.

而在攻击过程中,当经过第 2(a),2(b)两步分析后,将剩余 $2^{144}\times2^{-52}\times2^{-52}=2^{40}$ 个候选四元组进入下一步.计算主要集中在下面几步:

第(c)步的时间复杂度为 $2^{40}\times2^6\times4\times1/8=2^{45}$ 次一轮加密,经过第(c)步过滤后,剩余候选四元组个数为 $2^{40}\times2^{-4}\times2^{-4}=2^{32}$;

第(d)步的时间复杂度为 $2^6\times2^{32}\times2^6\times4\times1/8=2^{43}$ 次一轮加密,经过第(d)步过滤后,剩余候选四元组个数为 $2^{32}\times2^{-4}\times2^{-4}=2^{24}$;

第(e)步的时间复杂度为 $2^{12}\times2^{24}\times2^6\times4\times1/8=2^{41}$ 次一轮加密,经过第(e)步过滤后,剩余候选四元组个数为 $2^{24}\times2^{-4}\times2^{-4}=2^{16}$;

第(f)步的时间复杂度为 $2^{18}\times2^{16}\times2^8\times4\times3/8=3\times2^{41}$ 次一轮加密,经过第(f)步过滤后,错误密钥对应的剩余候选四元组个数为 $2^{16}\times2^{-12}\times2^{-12}=2^{-8}$,而正确密钥对应的剩余候选四元组个数至少为 3.

所以,该攻击的总时间复杂度约为 $2^{45}+2^{43}+2^{41}+3\times2^{41}=1.5\times2^{45}$ 次一轮加密,约为 2^{42} 次 12 轮加密.

由此可知,该攻击可成功恢复 18+8=26 bit 密钥,剩余的 30 bit 密钥可使用穷尽搜索完成.综上,该攻击的数据复杂度为 2^{62} 个选择明文,时间复杂度为 2^{42} 次 12 轮加密.

4 对 11 轮 DES 的 Boomerang 攻击

与 Rectangle 攻击类似,将第 2 节的两条差分路径连接(第 2 轮~第 11 轮)构成 10 轮 Boomerang 区分器,其概率为 $\tilde{p}=p^2\hat{q}^2=2^{-54.06}$.下面的攻击即利用该 10 轮(第 2 轮~第 11 轮)区分器来恢复 11 轮 DES 算法的部分密钥信息.

类似于第 3 节准备工作中的分析,可知ΔP_L除第 2,6,9,13,16,17,18,23,24,28,30,31 这 12 bit 之外均为 0,而ΔP_R=0x19600000.密文差分ΔC就是第 2 条差分路径的输出差分δ=(04000000$_x$,40080000$_x$).

详细的对 11 轮 DES 的 Boomerang 攻击过程如下:

1. 数据收集:定义 S^a 为由 2^{12} 个明文组成的一个结构,其中,每个明文在上述 12 比特处取任意值,其余 52 比特处取一个固定值.取 2^{44} 个这样的结构 $S_1^a,S_2^a,...,S_{2^{44}}^a$,分别对其进行 11 轮加密,记得到的密文为 $D_1^a,D_2^a,...,D_{2^{44}}^a$.对每个明文 P_a 在 52 个固定比特处计算 $P_b=P_a\oplus\Delta P$,得到相应的 2^{44} 个结构 $S_1^b,S_2^b,...,S_{2^{44}}^b$,记其密文为 $D_1^b,D_2^b,...,D_{2^{44}}^b$.对密文结构中的每个密文计算 $C^c=C^a\oplus\Delta C,C^d=C^b\oplus\Delta C$,得到相应的密文结构 $D_1^c,D_2^c,...,D_{2^{44}}^c$ 和 $D_1^d,D_2^d,...,D_{2^{44}}^d$.对这些密文分别进行 11 轮解密,得到相应的明文 $S_1^c,S_2^c,...,S_{2^{44}}^c$ 和 $S_1^d,S_2^d,...,S_{2^{44}}^d$.
2. 数据分析:
   a) 对相应的每对结构 S_i^c,S_i^d,将其中每个可能的明文对按照除第 1,6,9,10,16,17,20,23,24,26,30,31 这 12 bit 之外的 52 比特进行检查,将不符合相应明文差分ΔP的对去掉.此时,共剩余 $2^{44}\times2^{12}\times2^{12}\times2^{-52}=2^{16}$ 个候选明文对 P^c,P^d.
   b) 对每个候选明文对,依据密文应符合的差分关系,找到相应的明文 P^a,P^b.由于明文对 P^c,P^d 是取自于下标相同的一对结构,所以,相应的明文对 P^a,P^b 也属于下标相同的一对结构.由结构 S_i^a,S_i^b 中明文的选取方法可知,P^a,P^b 除上述固定 12 bit 外的 52 比特满足相应的明文差分.此时,由这两对明文构成候选四元组,记为(P^a,P^b,P^c,P^d).
   c) 此时,候选四元组共有 2^{16} 个,猜测轮密钥 K_1 进入 S_1 的 6 比特值,对候选四元组部分加密第 1 轮,检查 P^a,P^b 第 2 轮输入差分中相应于 S_1 输出的 4 比特,将不符合所需差分的四元组去掉.再检查 P^c,P^d 第 2 轮输入差分的相应 4 比特,将不符合所需差分的四元组去掉.
   d) 再猜测轮密钥 K_1 进入 S_2 的 6 比特值,对剩余的候选四元组部分加密第 1 轮,检查 P^a,P^b 及 P^c,P^d 的相应 4 比特差分是否符合需要的差分,将不符合该差分的四元组去掉.
   e) 最后猜测轮密钥 K_1 进入 S_3 的 6 比特值,检查相应差分并去掉不符合需要差分的四元组.如果此时还有至少 3 个四元组,则输出相应的密钥猜测作为正确密钥;否则重复第(c)~第(e)步.

该攻击的数据复杂度和时间复杂度分析如下:共需要 $2\times2^{44}\times2^{12}+2\times2^{44}\times2^{12}=2^{58}$ 个适应性的选择明密文.由这些明密文共形成了 $2^{44}\times2^{12}\times2^{12}=2^{68}$ 个四元组,其中,预计将有 $2^{68}\times2^{-12}=2^{56}$ 个四元组的 P^a,P^b 第 2 轮输入差分为 (19600000$_x$,00000000$_x$).将这些四元组应用于上述 10 轮区分器,可知有 $2^{56}\times2^{-54.06}=2^{1.94}\approx3.83$ 个四元组符合该区分器,即正确四元组的个数至少应为 3.

在攻击过程中,当经过第 2(a),2(b)两步分析后,将剩余 2^{16} 个候选四元组进入下一步.计算主要集中在下面几步:

第(c)步的时间复杂度为 $2^{16}\times2^6\times4\times1/8=2^{21}$ 次一轮加密,经过第(c)步过滤后,剩余候选四元组个数为 $2^{16}\times2^{-4}\times2^{-4}=2^8$;

第(d)步时间复杂度为 $2^6\times2^8\times2^6\times4\times1/8=2^{19}$ 次一轮加密,经过第(d)步过滤后,剩余候选四元组个数为 $2^8\times2^{-4}\times2^{-4}=1$;

第(e)步时间复杂度为 $2^{12}\times1\times2^{6}\times4\times1/8=2^{17}$ 次一轮加密,经过第(e)步过滤后,错误密钥对应的剩余候选四元组个数为 $1\times2^{-4}\times2^{-4}=2^{-8}$,而正确密钥对应的剩余候选四元组个数至少为 3.

所以,该攻击的总时间复杂度约为 $2^{21}+2^{19}+2^{17}\approx2^{21.39}$ 次一轮加密,即约为 $2^{17.93}$ 次 11 轮加密.

由此可知,该攻击可成功恢复出 18 比特密钥.即该攻击的数据复杂度为 2^{58} 个适应性的选择明密文,时间复杂度为 $2^{17.93}$ 次 11 轮加密.剩余的 38 比特密钥可使用穷尽搜索完成,所以,恢复全部密钥的时间复杂度为 2^{38} 次 11 轮加密.

除上述工作外,我们还对 8 轮 DES 作了 Rectangle 攻击,主要用于分析和比较.但限于篇幅,这里不再详述具体过程,只将结果列于表 2.同时,表 2 还总结比较了我们所作的攻击结果与已有的差分和线性攻击结果.

Table 2 Summary of our results and previously known results

表 2 本文攻击结果与已有攻击结果的总结

Rounds	Attack	Data complexity	Time complexity	Source
8	Rectangle attack	2^{42} CP	$2^{18.17}$	This paper
8	Differential cryptanalysis	2^{14} CP	2^{9}	Ref.[2]
11	Boomerang attack	2^{58} ACPC	2^{38}	This paper
12	Rectangle attack	2^{62} CP	2^{42}	This paper
16	Differential cryptanalysis	2^{47} CP	2^{37}	Ref.[2]
16	Linear cryptanalysis	2^{43} KP	2^{43}	Ref.[3]

Time complexity is measured in encryption units.
CP—Chosen plaintexts, KP—Known plaintexts
ACPC—Adaptive chosen plaintexts and ciphertexts

5 总 结

由于 DES 算法 4 轮最优差分路径的概率已达到 1.31×2^{-10},而 3 轮最优差分路径的概率只有 2^{-4},我们首先考虑利用概率较大的 3 轮差分路径来构造区分器,再结合 Matsui 搜索到的 DES 各轮最优差分路径及其概率,得到了 10 轮区分器.利用该区分器分别构造了对 12 轮 DES 的 Rectangle 攻击和对 11 轮 DES 的 Boomerang 攻击,结果分别为:Rectangle 攻击的数据复杂度为 2^{62} 个选择明文,时间复杂度为 2^{42} 次 12 轮加密;Boomerang 攻击的数据复杂度为 2^{58} 个适应性的选择明密文,时间复杂度为 2^{38} 次 11 轮加密.由于我们使用的都是最优差分路径,相信我们得到的结果是 Rectangle 攻击和 Boomerang 攻击对 DES 所能达到的最好结果.

将这些结果与已有的对 DES 的攻击结果进行比较,见表 2.可见,对 DES 而言,传统的差分分析和线性分析更加有效.这是因为 DES 中存在较好的循环差分(线性)路径,这样可以容易地构造差分(线性)分析,且数据复杂度和时间复杂度都不高.而对 Rectangle 攻击和 Boomerang 攻击而言,它们适用于那些随着轮数增长概率降低非常大的密码.此时,由两段高概率的低轮差分路径连接得到的特征概率,才会远远大于单一差分路径的概率,从而发挥能够攻击到更多轮的优势.可见,Rectangle 攻击和 Boomerang 攻击更适合于那些不存在较高概率循环差分(线性)路径的算法中.

References:

[1] Data Encryption Standard (DES). Federal information processing standards publication (FIPS PUB) 46-3. National Bureau of Standards. 1999. http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf

[2] Biham E, Shamir A. Differential cryptanalysis of the full 16-Round DES. In: Brickell EF, ed. Proc. of the CRYPTO'92. LNCS 740, Berlin: Springer-Verlag, 1993. 487–496.

[3] Matsui M. The first experimental cryptanalysis of the data encryption standard. In: Desmedt YG, ed. Proc. of the CRYPTO'94. LNCS 839, Berlin: Springer-Verlag, 1994. 1–11.

[4] Biham E, Dunkelman O, Keller N. The Rectangle attack—rectangling the serpent. In: Pfitzmann B, ed. Proc. of the EUROCRYPT 2001. LNCS 2045, Berlin: Springer-Verlag, 2001. 340–357.

[5] Wagner D. The Boomerang attack. In: Knudsen L, ed. Proc. of the Fast Software Encryption 1999. LNCS 1636, Berlin: Springer-Verlag, 1999. 156–170.

[6] Biham E, Dunkelman O, Keller N. Related-Key Boomerang and Rectangle attacks. In: Cramer R, ed. Proc. of the EUROCRYPT 2005. LNCS 3494, Berlin: Springer-Verlag, 2005. 507−525.

[7] Biham E, Dunkelman O, Keller N. A related-key Rectangle attack on the full KASUMI. In: Roy B, ed. Proc. of the ASIACRYPT 2005. LNCS 3788, Berlin: Springer-Verlag, 2005. 443−461.

[8] Kelsey J, Kohno T, Schneier B. Amplified Boomerang attacks against reduced-round MARS and serpent. In: Schneier B, ed. Proc. of the Fast Software Encryption 2000. LNCS 1978, Berlin: Springer-Verlag, 2001. 75−93.

[9] Biham E, Shamir A. Differential cryptanalysis of DES-like cryptosystems (extended abstract). In: Menezes AJ, Vanstone SA, eds. Proc. of the CRYPTO'90. LNCS 537, Berlin: Springer-Verlag, 1991. 2−21.

[10] Matsui M. On correlation between the order of *S*-boxes and the strength of DES. In: Santis A, ed. Proc. of the EUROCRYPT'94. LNCS 950, Berlin: Springer-Verlag, 1995. 366−375.

张蕾(1981－),女,吉林通化人,博士生,主要研究领域为分组密码的分析与设计.

吴文玲(1966－),女,博士,研究员,博士生导师,主要研究领域为分组密码,Hash 函数,理论密码学.

敬 告 作 者

《软件学报》创刊以来,蒙国内外学术界厚爱,收到许多高质量的稿件,其中不少在发表后读者反映良好,认为本刊保持了较高的学术水平.但也有一些稿件因不符合本刊的要求而未能通过审稿.为了帮助广大作者尽快地把他们的优秀研究成果发表在我刊上,特此列举一些审稿过程中经常遇到的问题,请作者投稿时尽量予以避免,以利大作的发表.

1. 读书偶有所得,即匆忙成文,未曾注意该领域或该研究课题国内外近年来的发展情况,不引用和不比较最近文献中的同类结果,有的甚至完全不列参考文献.

2. 做了一个软件系统,详尽描述该系统的各个方面,如像工作报告,但采用的基本上是成熟技术,未与国内外同类系统比较,没有指出该系统在技术上哪几点比别人先进,为什么先进.一般来说,技术上没有创新的软件系统是没有发表价值的.

3. 提出一个新的算法,认为该算法优越,但既未从数学上证明比现有的其他算法好(例如降低复杂性),也没有用实验数据来进行对比,难以令人信服.

4. 提出一个大型软件系统的总体设想,但很粗糙,而且还没有(哪怕是部分的)实现,很难证明该设想是现实的、可行的、先进的.

5. 介绍一个现有的软件开发方法,或一个现有软件产品的结构(非作者本人开发,往往是引进的,或公司产品),甚至某一软件的使用方法.本刊不登载高级科普文章,不支持在论文中引进广告色彩.

6. 提出对软件开发或软件产业的某种观点,泛泛而论,技术含量少.本刊目前暂不开办软件论坛,只发表学术文章,但也欢迎材料丰富,反映现代软件理论或技术发展,并含有作者精辟见解的某一领域的综述文章.

7. 介绍作者做的把软件技术应用于某个领域的工作,但其中软件技术含量太少,甚至微不足道,大部分内容是其他专业领域的技术细节,这类文章宜改投其他专业刊物.

8. 其主要内容已经在其他正式学术刊物上或在正式出版物中发表过的文章,一稿多投的文章,经退稿后未作本质修改换名重投的文章.

本刊热情欢迎国内外科技界对《软件学报》踊跃投稿.为了和大家一起办好本刊,特提出以上各点敬告作者.并且欢迎广大作者和读者对本刊的各个方面,尤其是对论文的质量多多提出批评建议.