截断差分-线性密码分析*

贺也平[1,2,3] 吴文玲[1,2,3] 卿斯汉[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 100080)

[2](中国科学院信息安全技术工程研究中心 北京 100080)

[3](中国科学院软件研究所计算机科学开放研究实验室 北京 100080)

E-mail: yphe@ercist.iscas.ac.cn

摘要 对差分-线性密码分析方法进行推广,提出了截断差分-线性密码分析方法.对9-轮和11-轮DES(data encryption standard)密码算法的分析表明,该方法具有更加方便、灵活,适用范围更广的特点.同时,利用截断差分-线性密码分析方法得出,在类似DES结构的算法中,S-盒的摆放顺序对密码的强度有较大的影响.由此,截断差分-线性分析方法给出了优化S-盒排序的一种参考判别准则.

关键词 DES(data encryption standard),密码,S-盒,差分分析,线性分析,截断差分.

中图法分类号 TP393

随着网络信息安全重要性的日益突出,作为信息安全的基础,密码的研究越来越受到广泛的重视.特别是高强度、高效率的分组密码设计与分析,引起了众多研究人员的注意.近些年来,人们通过对密码强度的分析,提出了许多攻击分组密码的方法,在这些方法中,差分密码分析[1]和线性密码分析[2]是最基本和最有效的两种方法.在这两种方法的基础上衍生出了许多密码分析方法,S. K. Langford 和 M. E. Hellmen 提出的差分-线性方法[3]就是其中之一,该方法通过实现差分与线性逼近的套接,恢复部分比特密钥.

本文分析截断差分[4,5]和线性分析[2]两种方法之间的联系,提出了截断差分-线性分析方法,推广了差分-线性方法.由于截断差分只涉及部分比特位的性质,它比相应轮数的差分成立的概率高,更适合于多轮数密码分析.对9-轮DES(data encryption standard)的分析表明,该方法适用范围更广,应用更加方便.利用截断差分-线性分析方法,本文还研究了11-轮DES,证明了S-盒排列顺序对密码强度的影响.因此,截断差分-线性分析方法还给出了优化S盒排序的一个参考判别准则.

1 基本概念与记号

本文采用M. Matsui[2]的记号,$A[i]$表示A的从右数起第i比特位.$A[i,j,\ldots,k]$表示$A[i]\oplus A[j]\oplus\ldots\oplus A[k]$.

1.1 线性分析

M. Matsui[2]提出的线性分析方法是一种对已知明文的攻击方法.通过寻找密码算法的有效线性逼近:

$$P[i_1,i_2,\ldots,i_a]\oplus C[j_1,j_2,\ldots,j_b]=K[k_1,k_2,\ldots,k_c]$$

来恢复部分比特的密钥,其中P,C和K分别表示明文、密文和密钥.如果上式成立的概率不是1/2,利用极大似然方法,可以恢复密钥的部分比特.例如,对于S_5-盒,公式

$$X[4]=S_5[3,2,1,0]$$

---

* 本文研究得到国家重点基础研究发展规划项目(Nos. G1999035802, G1999035810)资助.作者贺也平,1962年生,博士,主要研究领域为分组密码设计与分析,网络信息安全.吴文玲,女,1966年生,博士,副研究员,主要研究领域为分组密码设计与分析.卿斯汉,1939年生,研究员,博士生导师,主要研究领域为信息安全理论和技术.

本文通讯联系人:贺也平,北京 100080,中国科学院信息安全技术工程研究中心

本文2000-05-31收到原稿,2000-06-30收到修改稿

成立的概率为 12/64. 其中 X 表示 S_5-盒的输入,$S_5[\cdot]$表示 S_5-盒输出的相应比特位. 在 DES 中考虑 S_5-盒的这个公式,容易得到 3-轮 DES 的一个线性逼近

$$L_0[7,18,24,29]\oplus L_3[7,18,24,29]\oplus R_0[15]\oplus R_3[15]=K_1[22]\oplus K_2[22]. \tag{1}$$

该等式成立的概率为 0.7.

1.2 截断差分

截断差分是 L. R. Knudson[4,5]在差分分析的基础上提出的一种部分比特的差分分析方法. 如果两个明文块的部分比特位上的差分为 $P'[l_1,\ldots,l_h]$,这两个明文块经过 i-轮加密后部分比特位的差分为 $C'[m_1,\ldots,m_n]$,则称$\langle P'[l_1,\ldots,l_h],C'[m_1,\ldots,m_n]\rangle$为 i-轮截断差分. 通常,当明文的截断差分具有某种特殊性质时,密文的截断差分具有某种规律,通过这些规律可以恢复部分密钥比特.

2 截断差分-线性分析方法

一般来说,差分分析方法对于低轮数的密码十分有效,但是,随着轮数的增加,差分分析的有效性急剧下降,密码分析的复杂性大为增加. 线性分析方法可以比较容易地构造出低轮数密码算法的线性逼近,但是在寻找多轮有效线性逼近方面是比较困难的. S. K. Langford 和 M. E. Hellman 通过差分方法与线性分析方法的套接,提出了差分-线性分析方法. 该方法充分利用两种方法的特点,极大地降低了选择明文对的个数,从而简化了攻击的复杂性. 但是,由于差分本身的复杂性,要寻找与线性逼近匹配的差分是困难的. 而通过前面的介绍可以看出,截断差分和线性分析方法都只涉及明密文的部分比特位,所作用的对象具有相同性. 利用截断差分的概念可以方便地找出与线性逼近相匹配的截断差分,并且由于截断差分只涉及部分比特位,它比相应轮数的差分成立的概率高,因此极大地提高了分析的效率.

下面,我们通过 9-轮 DES 的分析来说明截断差分-线性分析方法. 对于由公式(1)给出的 3-轮最佳线性逼近:

$$L_3[7,18,24,29]\oplus L_6[7,18,24,29]\oplus R_3[15]\oplus R_6[15]=K_1[22]\oplus K_2[22], \tag{2}$$

其等式成立的概率为 0.7. 如图 1 所示.

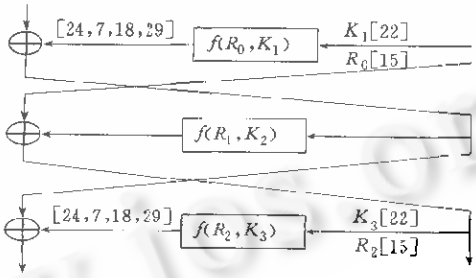


Fig. 1 The best linear approximation of 3-round DES

图1 3-轮DES的最佳线性逼近

为了找到一个 5-轮截断差分与该线性逼近匹配,要求该 5-轮截断差分的左半段的[24,7,29]比特位以及右半段[14]比特位不变. 由于线性逼近仅涉及部分比特位,因此在寻找与其相匹配的差分时,我们只关心这些相应比特位的性质. 注意到这一点,利用截断差分的概念,通过计算可以找到一个与 3-轮 DES 的最佳线性逼近相匹配的 5-轮截断差分. 由于截断差分只涉及部分比特位的性质,故截断差分比一般的差分成立的概率要高. 该截断差分成立的概率为 0.03. 如图 2 所示.

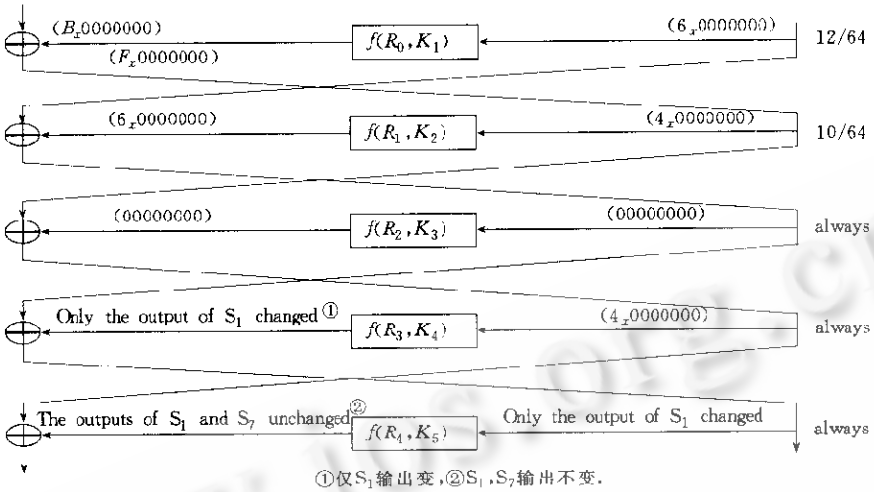
将 5-轮截断差分与 3-轮 DES 的线性逼近套接,得到了一个对 9-轮 DES 的截断差分-线性分析,如图 3 所示.

对于每一个满足截断差分条件的明文对,其密文的截断差分和正确的密钥 K_9 满足

$$R'_9[7,18,24,29]\oplus L'_9[15]\oplus f'(R_8,K_9)[22]=0 \tag{3}$$

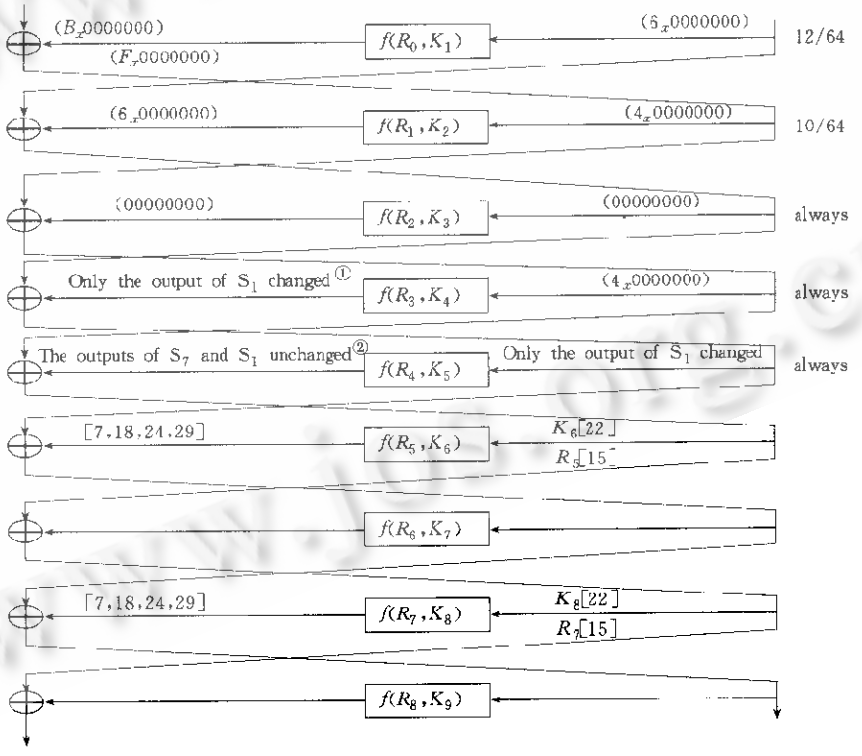
的概率为 0.5024. 利用 Matsui[2]给出的极大似然算法,需选择约 5.76×10^6 个明文对,可以恢复 K_9 中的 6 比特

密钥.对于 K_9 的其他 42 比特密钥,可以通过其他截断差分-线性分析或穷搜索来得到.



①仅S_1输出变,②S_1,S_7输出不变.

Fig. 2　5-Round truncated differential matching linear approximate expression (3)
图2　与线性逼近式(3)匹配的5-轮截断差分



①仅S_1输出变,②S_1,S_7输出不变.

Fig. 3　Truncated differential-linear analyze on 9-round DES
图3　对于9-轮DES的一个截断差分-线性分析

注:在截断差分-线性分析方法中,分析的复杂性取决于线性逼近的有效性和差分成立的概率,它们对分析的复杂性影响很大.

从以上分析可以看出,线性逼近和截断差分都仅涉及明密文的部分比特,它们作用的对象是相同的,其联系更加密切.由于存在着许多不同的线性逼近,对于不同比特位上的差分有着不同的要求,即需要不同的截断差分与之匹配,因此,截断差分-线性分析方法比差分-线性分析方法在应用上更加方便,应用的范围也更加广泛.

3 S-盒的排序对密码强度的影响

本节通过利用截断差分-线性分析方法分析变型的 11-轮 DES 密码,以此来说明 S-盒排序的变化对密码强度的影响.

在 11-轮 DES 密码中,将 S_5 和 S_6 盒互换.即输入的比特位作相应改变,输出比特位保持不变.将变化后的密码记为 DES_m.下面,我们利用截断差分-线性分析方法对 11-轮的 DES_m 密码进行分析.首先构造一个 7-轮的线性逼近.由 Matsui 给出的 7-轮线性逼近的结果,可以得到 DES_m 密码的 7-轮的一个线性逼近.如图 4 所示.

$$L_0[7,18,24]\oplus R_6[12,16]\oplus L_7[7,18,24,29]\oplus R_7[15]=K_1[19,23]\oplus K_3[22]\oplus K_4[44]\oplus K_5[22]K_7[22]. \tag{4}$$

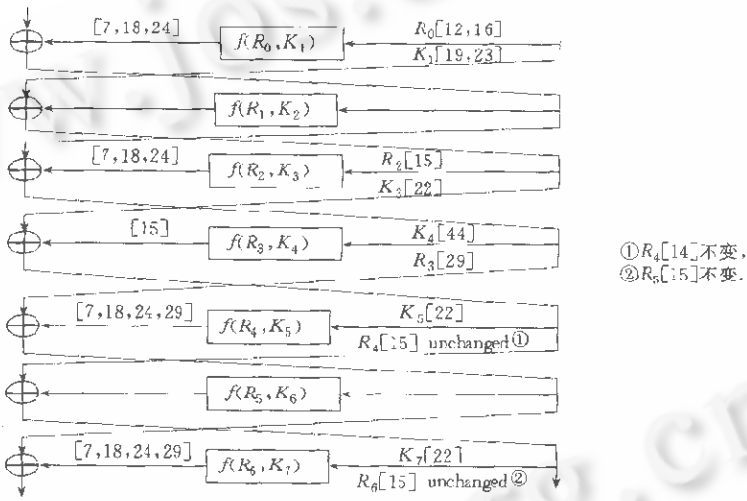
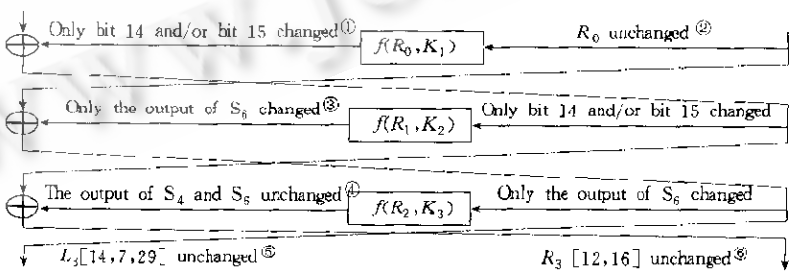


Fig. 4 One of the linear approximations of 7-round DES
图4 7-轮DES的一个线性逼近

同样地,我们需要找一个 3-轮截断差分与该线性逼近匹配,要求该 3-轮截断差分的左半段的[7,18,24]比特位以及右半段[12,16]比特位不变.通过计算得到了这样的一个 3-轮截断差分,如图 5 所示.



①仅第14,15位变,②R_0不变,③仅S_6输出变,④S_4,S_5输出不变,⑤$L_3[14,7,29]$不变,⑥$R_3[12,16]$不变.

Fig. 5 Truncated differential matching linear approximate expression (4) of 7-round DES
图5 与7-轮DES的线性逼近式(4)匹配的截断差分

与第 2 节完全类似,将得到的匹配 3-轮截断差分与 7-轮线性逼近式(4)套接,得到了对于 11-轮 DES_m 的一

个截断差分-线性分析.对于满足截断差分条件的每一对明文,其密文的差分以及正确的密钥 K_{11} 满足如下等式:

$$L_{11}[15] \oplus R_{11}[7,18,24,29] \oplus f(R_{10},K_{11})[15]=0.$$

其概率大于 0.5.同样地,利用 Matsui[2]给出的极大似然算法,可以恢复 K_{11} 中的 6 比特密钥.

注:在 DES 密码中,7-轮线性逼近式(4)是最佳线性逼近,但是,不存在 3-轮截断差分与之匹配,因此,只能用其他 7-轮线性逼近进行截断差分-线性分析.正如在第 2 节所指出的,由于线性逼近效果差,导致截断差分-线性分析复杂性大为增加.在这个意义下,11-轮 DES 密码比 11-轮 DES_m 密码强度要高.也就是说,对于 11-轮 DES,当 S_3 盒和 S_5 盒交换后,密码的强度下降了.因此,对于类似于 DES 的加密算法,S-盒的排序是非常重要的.

4 结束语

本文通过对截断差分和线性分析的研究,分析了它们存在的内在联系,提出了截断差分-线性分析方法.该方法比差分-线性分析方法的应用范围更广,应用也更加方便、灵活.另一方面,利用截断差分-线性分析方法对 11-轮 DES 的分析表明,S-盒的不同排序影响密码强度.由此,截断差分-线性分析方法为 S-盒排序的优劣提供了一个参考判别准则.

总之,利用截断差分的概念可以方便地寻找与各种线性逼近相匹配的截断差分.而在密码设计中,S-盒的排序要尽量避免截断差分与好的线性逼近相匹配,以达到提高密码强度的目的.

参考文献

1 Biham E, Shamir A. Differential cryptanalysis of DES-like cryptosystems. Journal of Cryptology, 1991,4(1):3~72

2 Matsui M. Linear cryptanalysis method for DES cipher. Advances in Cryptology—— Eurocrypt'93 Proceedings. Lecture Notes in Computer Science 765, Berlin: Springer-Verlag, 1994. 386~397

3 Langford S K, Hellman M E. Differential-Linear cryptanalysis. In: Advances in Cryptology—— Crypto'94 Proceedings. Lecture Notes in Computer Science 863, Berlin: Springer-Verlag, 1994. 17~25

4 Knudson L R. Truncated and higher order differentials. In: Fast Software Encryption, 2nd International Workshop Proceedings. Lecture Notes in Computer Science 1008, Berlin: Springer-Verlag, 1995. 196~211

5 Knudson L R, Berson T A. Truncated differentials of SAFER. In: Fast Software Encryption, 3rd International Workshop Proceedings. Lecture Notes in Computer Science 1039, Berlin: Springer-Verlag, 1996. 15~26

Truncated Differential-Linear Cryptanalysis

HE Ye-ping[1,2,3] WU Wen-ling[1,2,3] QING Si-han[1,2]

[1] (*State Key Laboratory of Information Security Institute of Software The Chinese Academy of Sciences Beijing* 100080)

[2] (*Engineering Research Center for Information Security Technology The Chinese Academy of Sciences Beijing* 100080)

[3] (*Laboratory of Computer Science Institute of Software The Chinese Academy of Sciences Beijing* 100080)

Abstract A truncated differential-linear cryptanalysis method is proposed, which extends differential-linear method. DES (data encryption standard) algorithms of 9-round and 11-round were analyzed. The method was proved more convenient and widely applicable. In DES like cipher algorithms, the fact that the order in which S-boxes were placed would affect the security of cipher was shown by the method. In this way, the truncated differential-linear method gives a criterion for ordering S-boxes optimally.

Key words DES (data encryption standard), cipher, S-box, differential analysis, linear analysis, truncated differential.