1000-9825/2003/14(03)0569 ©2003 Journal of Software 软 件 学 报 Vol.14, No.3

AC 分组密码的差分和线性密码分析*

吴文玲+, 马恒太, 卿斯汉

(中国科学院 软件研究所,北京 100080)
(中国科学院 信息安全技术工程研究中心,北京 100080)

Differential and Linear Cryptanalysis of AC Block Cipher

WU Wen-Ling+, MA Heng-Tai, QING Si-Han

(Institute of Software, The Chinese Academy of Sciences, Beijing 100080, China)
(Engineering Research Center for Information Security Technology, The Chinese Academy of Sciences, Beijing 100080, China)
+ Corresponding author: Phn: 86-10- 62561197 ext 8004, E-mail: wwl@ercist.iscas.ac.cn
http://www.ercist.iscas.ac.cn
Received 2001-11-13; Accepted 2002-06-12

Wu WL, Ma HT, Qing SH. Differential and linear cryptanalysis of AC block cipher. *Journal of Software*, 2003,14(3):569~574.

Abstract: The security of AC against differential and linear cryptanalysis is discussed in this paper. It is shown that 12-round AC has no differential characteristic with probability higher than 2-128 and no linear approximations with approximation bias larger than 2-67 by estimating the lower bound of the number of active-boxes in 3-round differential characteristic and 12-round linear approximation. Hence, AC is secure to differential and linear cryptanalysis.
Key words: differential cryptanalysis; linear cryptanalysis; differential characteristic; linear approximation; S-box

摘 要: 讨论 AC 分组密码对差分和线性密码分析的安全性,通过估计 3 轮 AC 的差分活动盒子的个数下界和 12 轮 AC 的线性活动盒子的个数下界,本文得到 AC 的 12 轮差分特征概率不大于 2-128 和线性逼近优势不大于 2-67.因此,AC 分组密码对差分和线性密码分析是安全的.
关键词: 差分密码分析;线性密码分析;差分特征;线性逼近;S-盒
中图法分类号: TP309 **文献标识码**: A

在世纪交替之际,AES[1]的征集和 NESSIE[2]项目的启动引起了世人的广泛关注,推出了 Rijndael,RC6, Serpent,NOEKEON 和 NUSH 等分组密码.这些分组密码各有特色,有的采用“Bit-Slice”技术,有的基于“宽轨迹原理”,还有的采用数据相依循环等.在对这些分组密码进行深入分析和研究之后,我们结合“宽轨迹原理”和“Bit-Slice”技术设计了 AC[3]分组密码.本文讨论 AC 分组密码针对差分[4]和线性[5]密码分析的安全性,结果显示 AC 分组密码对差分和线性密码分析是安全的.

---

* Supported by the National Natural Science Foundation of China under Grant Nos.60103023, 60083007 (国家自然科学基金)
第一作者简介: 吴文玲(1966-),女,陕西蒲城人,博士,副研究员,主要研究领域为分组密码的设计与分析.

1 AC 的差分密码分析

AC 中的θ相当于 32 个 4×4 S-盒的并置,且 S-盒的差分均匀性和最佳线性逼近优势均为 2^{-2}.

定义 1. 对 $X=(X_3X_2X_1X_0)\in(F_2^{32})^4$,我们称 $U(X)=W_H(X_3\,|\,X_2\,|\,X_1\,|\,X_0)$ 为 X 的并汉明重量.

对 $P:(F_2^{32})^4\to(F_2^{32})^4$ $X=(X_3,X_2,X_1,X_0)\to(Y_3,Y_2,Y_1,Y_0)=Y$,我们令

$$D(i,j)=\{X\in(F_2^{32})^4\,|\,U(X)=i,U(P(X))=j\},\ V(i,j)=\{Y\in(F_2^{32})^4\,|\,U(P^{-1}(Y))=i,U(Y)=j\}.$$

我们试图搞清 $D(i,j)$ 的分布,但是由于计算能力的限制,仅对 P 计算了 $D(i,j),1\le i\le 6$.这里,把 128 比特 $X=(X_3X_2X_1X_0)\in(F_2^{32})^4$ 看成是 $U(X)$ 个二元向量,每个二元向量的第 1 个分量表示 $X_3|X_2|X_1|X_0$的非 0 位置 t,第 2 个分量表示相应的数据 $X_3[t]2^3+X_2[t]2^2+X_1[t]2+X_0[t]$.例如, $X=(X_3X_2X_1X_0)=(20,100,3,b)$, $U(X)=5$,X 可以表示({0,3},{1,3},{3,1},{5,8},{8,4});把(0,1,3,5,8)称为 X 的位置向量,记为 $T(X)$;(3,3,1,8,4)称为 X 的数据向量,记为 $D(X)$.值得注意的是,$\theta(X)$ 和 X 的位置向量必定相同.如果 $P(X_3X_2X_1X_0)=(Y_3Y_2Y_1Y_0)$,则 $P(X_3<<<n,$ $X_2<<<n,\ X_1<<<n,X_0<<<n)=(Y_3<<<n,Y_2<<<n,Y_1<<<n,Y_0<<<n)$.所以在分析计算时,我们仅考虑循环意义下不相等的 X.

现在证明任意 3 轮 AC 的差分特征至少有 16 个活动盒子.对任意一个 3 轮差分特征: $T\xrightarrow{\theta}X\xrightarrow{P}P(X)\xrightarrow{\theta}Y\xrightarrow{P}P(Y)\xrightarrow{\theta}Z\xrightarrow{P}P(Z)$,因为 $U(P(X))=U(Y)$, $U(P(Y))=U(Z)$, $U(X)=U(T)$,所以它的活动盒子的个数为 $U(X)+U(P(X))+U(P(Y))$.令 $U(X)=i$, $U(P(X))=j$, $U(P(Y))=m$,如果 $i+j+m<16$,我们证明对任意 $\alpha\in V(i,j)$, $\beta\in D(j,m)$,不存在差分 $\alpha\xrightarrow{\theta}\beta$.

对 P 计算的结果显示: $D(i,j)(1\le i\le 6,i+j\le 15)$ 中有如下集合是非空的, $D(1,8)$, $D(1,12)$, $D(2,5)$, $D(2,6)$, $D(2,j)(9\le j\le 13)$, $D(3,j)(3\le j\le 12,j\ne 5)$, $D(4,j)(3\le j\le 11)$, $D(5,j)(2\le j\le 10,j\ne 3)$, $D(6,j)(2\le j\le 9)$.因此,有可能满足 $i+j+m<16$ 的 (i,j,m) 只可能是下列情况:

(1,8,m)(m=1,3,4,5,6);(1,12,m)(m=1,2);(2,5,m)(m=2,4,5,6,7,8);(2,6,m)(m=2,3,4,5,6,7);(2,9,m)(m=2,3,4);(2,10,m)(m=2,3);(2,11,2);(2,12,1);(3,3,m)(m=3,4,6,7,8,9);(3,4,m)(m=3,4,5,6,7,8);(3,6,m)(m=2,3,4,5,6);(3,7,m)(m=3,4,5);(3,8,m)(m=1,3,4);(3,9,m)(m=2,3);(3,10,2);(4,3,m)(m=3,4,6,7,8);(4,4,m)(m=3,4,5,6,7);(4,5,m)(m=2,4,5,6);(4,6,m)(m=2,3,4,5);(4,7,m)(m=3,4);(4,8,m)(m=1,3);(4,9,2);(5,2,m)(m=5,6);(5,4,m)(m=3,4,5,6);(5,5,m)(m=2,4,5);(5,6,m)(m=2,3,4);(5,7,3);(5,8,1);(6,2,m)(m=5,6);(6,3,m)(m=3,4,6);(6,4,m)(m=3,4,5);(6,5,m)(m=2,4);(6,6,m)(m=2,3);(6,8,1);(7,3,m)(m=3,4);(7,4,m)(m=3,4);(7,5,2);(7,6,2);(8,3,m)(m=3,4);(8,4,3);(8,5,2);(9,3,3).

因为 P 和θ都是自反的,所以如果对 (i,j,m) ,任意 $\alpha\in V(i,j)$, $\beta\in D(j,m)$,不存在差分 $\alpha\xrightarrow{\theta}\beta$,则对 (m,j,i) 也有相应的结果.因此,只需证明 (i,j,m) 不可能为下列形式:

(1) (1,8,m)(m=1,3,4,5,6);
(2) (1,12,m)(m=1,2);
(3) (2,5,m)(m=2,4,5,6,7,8);
(4) (2,6,m)(m=2,3,4,5,6,7);
(5) (2,9,m)(m=2,3,4);
(6) (2,10,m)(m=2,3);
(7) (2,11,2);
(8) (3,3,m)(m=3,4,6,7,8,9);
(9) (3,4,m)(m=3,4,5,6,7,8);
(10) (3,6,m)(m=2,3,4,5,6);
(11) (3,7,m)(m=3,4,5);
(12) (3,8,m)(m=1,3,4);
(13) (3,9,3);
(14) (4,3,m)(m=4,6,7,8);

(15) (4,4,m)(m=4,5,6,7);

(16) (4,5,m)(m=4,5,6);

(17) (4,6,m)(m=4,5);

(18) (4,7,4);

(19) (5,2,m)(m=5,6);

(20) (5,4,m)(m=5,6);

(21) (5,5,5);

(22) (6,2,6);

(23) (6,3,6).

下面分别证明 (i,j,m) 不可能为上述的 23 种情况,也就是当 $U(X)=i$, $U(P(X))=j$, $U(P(Y))=m$ 时, $X\xrightarrow{P}P(X)\xrightarrow{\theta(?)}Y\xrightarrow{P}P(Y)$ 中的“?”是“NO”.

(1) (**1**,**8**,m)(m=**1**,**3**,**4**,**5**,**6**): 令 $X\in D(1,8)$, $U(P(X))=8$,测试显示 $V(1,8)$ 中元素的位置向量不会和 $\bigcup_{2\le i\le 6}D(8,i)$ 中的某个元素的位置向量等价;因此, $U(P(Y))\ne 2,3,4,5,6$.测试显示 $V(1,8)$ 的两个元素 α_1 和 α_2 的位置向量不等价,所以不存在差分 $\alpha_1\xrightarrow{\theta}\alpha_2$,且不存在差分 $\alpha_1\xrightarrow{\theta}\alpha_1$ 和 $\alpha_2\xrightarrow{\theta}\alpha_2$.因此, $U(P(Y))\ne 1$,这说明 $(i,j,m)\ne$ (1,8,m)(m=1,3,4,5,6).

(2) (**1**,**12**,m)(m=**1**,**2**): 令 $X\in D(1,12)$,则 $U(P(X))=12$,测试显示 $V(1,12)$ 中元素的位置向量不会和 $V(2,12)$ 中的某个元素的位置向量等价.因此, $U(P(Y))\ne 2$.又可以验证 $V(1,12)$ 中的 3 个元素 α_1 , α_2 和 α_3 的位置向量互不等价,因此,当 $l\ne t$ 时,不存在差分 $\alpha_l\xrightarrow{\theta}\alpha_t$.由测试可知:当 t=1,2 或 3 时,不存在差分 $\alpha_t\xrightarrow{\theta}\alpha_t$.因此, $U(P(Y))\ne 1$,这说明 $(i,j,m)\ne$ (1,12,m)(m=1,2).

(3) (**2**,**5**,m)(m=**2**,**4**,**5**,**6**,**7**,**8**): 令 $X\in D(2,5)$,则 $U(P(X))$ =5,对 $V(2,5)$ 中的两个元素 α_1 和 α_2 分别构造集合 $B_5(\alpha_t)=\{X\in(F_2^{32})^4:U(P(X))\le 8,T(X)\equiv T(\alpha_t)\}$.由测试可知: $\forall\beta\in B_5(\alpha_1)$, 不存在差分 $\alpha_1\xrightarrow{\theta}\beta$; $\forall\beta\in B_5(\alpha_2)$, 不存在差分 $\alpha_2\xrightarrow{\theta}\beta$.又经过测试 α_1 和 α_2 的位置向量不等价,所以 $(i,j,m)\ne$(2,5,m)(m=2,4,5,6,7,8).

(4) (**2**,**6**,m)(m=**2**,**3**,**4**,**5**,**6**,**7**): 令 $X\in D(2,6)$,则 $U(P(X))$ =6=j,对 $V(2,6)$ 的惟一元素 α_1 =({0,2},{8,4},{9,1},{15,8},{1c,2},{1d,2})构作集合 $B_6(\alpha_1)=\{X\in(F_2^{32})^4:U(P(X))\le 7,T(X)\equiv T(\alpha_1)\}$.由测试可知: $\forall\beta\in B_6(\alpha_1)$,不存在差分 $\alpha_1\xrightarrow{\theta}\beta$.因此, $(i,j,m)\ne$(2,6,m)(m=2,3,4,5,6,7).

(5) (**2**,**9**,m)(m=**2**,**3**,**4**): 令 $X\in D(2,9)$,则 $U(P(X))$ =9=j,测试显示 $V(2,9)$ 中元素的位置向量不会和 $\bigcup_{i=3,4}V(i,9)$ 中的某个元素的位置向量等价,因此,m≠3,4. $V(2,9)$ 中的两个元素 α_1 和 α_2 位置向量不等价,由测试可知:不存在差分 $\alpha_1\xrightarrow{\theta}\alpha_2$.所以 m≠1.因此, $(i,j,m)\ne$(2,9,m)(m=2,3,4).

(6) (**2**,**10**,m)(m=**2**,**3**): 令 $X\in D(2,10)$,则 $U(P(X))$ =10=j,测试显示 $V(2,10)$ 中元素的位置向量不会和 $V(3,9)$ 中的某个元素的位置向量等价.因此,m≠3. $V(2,10)$ 中的 5 个元素 γ_t $(t=1,2,3,4,5)$ 位置向量互不等价,由测试可知:不存在差分 $\gamma_t\xrightarrow{\theta}\gamma_t$ $(1\le t\le 5)$;所以 m≠2.因此, $(i,j,m)\ne$(2,10,m)(m=2,3).

(7) (**2**,**11**,**2**): 令 $X\in D(2,11)$,测试显示 $V(2,11)$ 中的 13 个元素 γ_t $(1\le t\le 13)$ 位置向量互不等价,由测试可知:不存在差分 $\gamma_t\xrightarrow{\theta}\gamma_t$ $(1\le t\le 13)$.所以 m≠2.因此, $(i,j,m)\ne$(2,11,2).

(8) (**3**,**3**,m)(m=**3**,**4**,**6**,**7**,**8**,**9**): 对 $V(3,3)$ 中的 3 个元素 α_1 , α_2 和 α_3 分别构作集合 $B_3(\alpha_t)=\{X\in(F_2^{32})^4:U(P(X))\le 9,T(X)\equiv T(\alpha_t)\}$ $(1\le t\le 3)$.由测试可知: $\forall\beta\in B_3(\alpha_1)$, 不存在差分 $\alpha_1\xrightarrow{\theta}\beta$; $\forall\beta\in B_3(\alpha_2)$, 不存在差分 $\alpha_2\xrightarrow{\theta}\beta$; $\forall\beta\in B_3(\alpha_3)$, 不存在差分 $\alpha_3\xrightarrow{\theta}\beta$.又 α_1 , α_2 和 α_3 的位置向量互不等价,所以 $(i,j,m)\ne$(3,3,m)(m=3,4,6,7,8,9).

(9) (**3**,**4**,m)(m=**3**,**4**,**5**,**6**,**7**,**8**): 对 $V(3,4)$ 的惟一元素 α_1 构作集合 $B_4(\alpha_1)=\{X\in(F_2^{32})^4:U(P(X))\le 8,T(X)\equiv T(\alpha_1)\}=$ { α_1 =({0,1},{8,8},{d,2},{f,2})}.由测试可知:不存在差分 $\alpha_1\xrightarrow{\theta}\alpha_1$.所以 $(i,j,m)\ne$ (3,4,m)(m=3,4,5,6,7,8).

(10) (**3**,**6**,m)(m=**2**,**3**,**4**,**5**,**6**): 对 $V(3,6)$ 中的 3 个元素 α_1 , α_2 和 α_3 分别构作集合 $B_6(\alpha_t)=\{X\in(F_2^{32})^4:U(P(X))\le 6,T(X)\equiv T(\alpha_t)\}$ $(1\le t\le 3)$.由测试可知: $\forall\beta\in B_3(\alpha_1)$, 不存在差分 $\alpha_1\xrightarrow{\theta}\beta$; $\forall\beta\in B_3(\alpha_2)$, 不存在差分 $\alpha_2\xrightarrow{\theta}\beta$;

$\forall\beta\in B_3(\alpha_3)$, 不存在差分 $\alpha_3\xrightarrow{\theta}\beta$.又 α_1, α_2 和 α_3 的位置向量互不等价,所以 $(i,j,m)\neq(3,6,m)(m=2,3,4,5,6)$.

(11) (**3**,**7**,m)(m=**3**,**4**,**5**): $V(3,7)$ 中的 5 个元素 γ_t $(t=1,2,3,4,5)$ 的位置向量不会和 $V(4,7)$ 或 $V(5,7)$ 中的某个元素的位置向量等价.因此,$m\neq4,5$.又 γ_t $(t=1,2,3,4,5)$ 的位置向量互不等价,由测试可知:不存在差分 $\gamma_t\xrightarrow{\theta}\gamma_t$ $(1\le t\le5)$.所以 $m\neq3$.因此,$(i,j,m)\neq(3,7,m)(m=3,4,5)$.

(12) (**3**,**8**,m)(m=**1**,**3**,**4**): $V(3,8)$ 中的 8 个元素 γ_t $(1\le t\le8)$ 的位置向量不会和 $V(4,8)$ 或 $V(1,8)$ 中的某个元素的位置向量等价.因此,$m\neq1,4$.又 γ_t $(1\le t\le8)$ 的位置向量互不等价,由测试可知:不存在差分 $\gamma_t\xrightarrow{\theta}\gamma_t$ $(1\le t\le8)$.所以 $m\neq3$.因此,$(i,j,m)\neq(3,8,m)(m=1,3,4)$.

(13) (**3**,**9**,**3**): $V(3,9)$ 中的 25 个元素 γ_t $(1\le t\le25)$ 的位置向量互不等价,由测试可知:不存在差分 $\gamma_t\xrightarrow{\theta}\gamma_t$ $(1\le t\le25)$.所以 $m\neq3$.因此,$(i,j,m)\neq(3,9,3)$.

(14) (**4**,**3**,m)(m=**4**,**6**,**7**,**8**): 对 $V(4,3)$ 中的惟一元素 α_1 构作集合 $B_3(\alpha_1)=\{X\in(F_2^{32})^4:U(P(X))\le8,T(X)\equiv T(\alpha_1)\}=\{\alpha_1\}$,由测试可知:不存在差分 $\alpha_1\xrightarrow{\theta}\alpha_1$.所以 $(i,j,m)\neq(4,3,m)(m=4,6,7,8)$.

(15) (**4**,**4**,m)(m=**4**,**5**,**6**,**7**): 对 $V(4,4)$ 中的惟一元素 α_1 构作集合 $B_4(\alpha_1)=\{X\in(F_2^{32})^4:U(P(X))\le7,T(X)\equiv T(\alpha_1)\}$,由测试可知: $\forall\beta\in B_4(\alpha_1)$, 不存在差分 $\alpha_1\xrightarrow{\theta}\beta$.所以 $(i,j,m)\neq(4,4,m)(m=4,5,6,7)$.

(16) (**4**,**5**,m)(m=**4**,**5**,**6**): 对 $V(4,5)$ 中的 5 个元素 $\alpha_t(1\le t\le5)$ 分别构作集合 $B_5(\alpha_t)=\{X\in(F_2^{32})^4:U(P(X))\le6,$ $T(X)\equiv T(\alpha_{t1})\}(1\le t\le5)$,由测试可知: $\forall\beta\in B_5(\alpha_5)$, 不存在差分 $\alpha_5\xrightarrow{\theta}\beta$ 和 $\alpha_t\xrightarrow{\theta}\alpha_t(t=1,2,3,4)$.所以 $(i,j,m)\neq(4,5,m)$ $(m=4,5,6)$.

(17) (**4**,**6**,m)(m=**4**,**5**): 对 $V(4,6)$ 中的 15 个元素 $\alpha_t(1\le t\le15)$ 分别构作集合 $B_6(\alpha_t)=\{X\in(F_2^{32})^4:U(P(X))=4$ or $5,$ $T(X)\equiv T(\alpha_t)\}$,由测试可知: $\forall t(1\le t\le15)$, $\forall\beta\in B_6(\alpha_t)$, 不存在差分 $\alpha_t\xrightarrow{\theta}\beta$;又 $\alpha_t(1\le t\le15)$ 的位置向量互不相同,所以,$(i,j,m)\neq(4,6,m)(m=4,5)$.

(18) (**4**,**7**,**4**): $V(4,7)$ 中的 28 个元素 γ_t $(1\le t\le28)$ 可以按照位置向量分成 26 个等价类 $C_l(1\le l\le25)$,其中 $C_l(1\le l\le25)$ 中都仅有一个元素,且由测试可知:不存在差分 $\gamma_t\xrightarrow{\theta}\gamma_t$ $(1\le t\le25)$.

$$C_{26}=\{\gamma_{26},\gamma_{27},\gamma_{28}\}=\{(\{0,8\},\{7,2\},\{8,2\},\{10,c\},\{11,1\},\{17,2\},\{18,2\}),(\{0,a\},\{1,2\},\{7,2\},\{8,2\},\{10,4\},\{17,8\},\{18,8\}),(\{0,a\},\{1,2\},\{7,2\},\{8,2\},\{10,c\},\{17,a\},\{18,a\})\}$$

由测试可知:不存在差分 $\gamma_l\xrightarrow{\theta}\gamma_t(26\le l\le t\le28)$.所以 $(i,j,m)\neq(4,7,4)$.

(19) (**5**,**2**,m)(m=**5**,**6**): 对 $V(5,2)$ 中的 2 个元素 α_1 和 α_2 构作集合 $B_2(\alpha_t)=\{X\in(F_2^{32})^4:U(P(X))=5$ or $6,$ $T(X)\equiv T(\alpha_t)\}$, $B_2(\alpha_1)=\{\alpha_1=(\{0,4\},\{1,1\})\}$, $B_2(\alpha_2)=\{\alpha_2=(\{0,8\},\{7,2\})\}$,由测试可知:不存在差分 $\alpha_1\xrightarrow{\theta}\alpha_1$ 和 $\alpha_2\xrightarrow{\theta}\alpha_2$;又 α_1 和 α_2 的位置向量互不等价,所以,$(i,j,m)\neq(5,2,m)(m=5,6)$.

(20) (**5**,**4**,m)(m=**5**,**6**): 对 $V(5,4)$ 中的 5 个元素 $\alpha_t(1\le t\le5)$ 分别构作集合 $B_2(\alpha_t)=\{X\in(F_2^{32})^4:U(P(X))=$ $5\text{or}6,T(X)\equiv T(\alpha_t)\}$,由测试可知: $\forall t(1\le t\le5)$, $\forall\beta\in B_2(\alpha_t)$, 不存在差分 $\alpha_t\xrightarrow{\theta}\beta$;又 $\alpha_t(1\le t\le5)$ 的位置向量互不相同,所以,$(i,j,m)\neq(5,4,m)(m=5,6)$.

(21) (**5**,**5**,**5**): $V(5,5)$ 的 25 个元素 γ_t $(1\le t\le25)$ 的位置向量互不相同,且由测试可知:不存在差分 $\gamma_t\xrightarrow{\theta}\gamma_t$ $(1\le t\le25)$.所以,$(i,j,m)\neq(5,5,5)$.

(22) (**6**,**2**,**6**): 对 $V(6,2)$ 中的惟一元素 α_1 构作集合 $B_2(\alpha_1)=\{X\in(F_2^{32})^4:U(P(X))=6,T(X)\equiv T(\alpha_1)\}=\{\alpha_1=$ $(\{0,1\},\{d,2\})\}$,由测试可知:不存在差分 $\alpha_1\xrightarrow{\theta}\alpha_1$.所以,$(i,j,m)\neq(6,2,6)$.

(23) (**6**,**3**,**6**): 对 $V(6,3)$ 中的 3 个元素 α_1, α_2 和 α_3 分别构作集合 $B_3(\alpha_t)=\{X\in(F_2^{32})^4:U(P(X))=6,T(X)\equiv$ $T(\alpha_t)\}$ $t=1,2,3$, 由测试可知:不存在差分 $\alpha_t\xrightarrow{\theta}\alpha_t$ $(t=1,2,3)$,又 α_1, α_2 和 α_3 的位置向量互不等价,所以 $(i,j,m)\neq(6,3,6)$.

综上可证任意 3 轮 AC 差分特征至少有 16 个活动盒子,因为 S-盒的差分均匀性为 2^{-2},所以 12 轮 AC 的差分概率不大于 2^{-128}.

2 AC 的线性密码分析

类似差分密码分析,对所有可能的 3 轮线性逼近,检验活动盒子的个数,结果显示仅有如下 4 个特殊的 3 轮线性逼近的活动盒子数小于 16,其他的活动盒子的个数均不小于 16.

(1) (**4**,**6**,**4**): $B_6(\alpha_{10})=\{\alpha_{10}=(\{0,5\},\{1,1\},\{8,9\},\{d,a\},\{f,2\},\{14,2\})\}$, $P(\alpha_{10})=\beta=(\{0,a\},\{7,2\},\{10,1\},\{1d,2\})$. 对$\theta$,存在有效线性逼近 $\alpha_{10}\cdot X=\alpha_{10}\cdot\theta(X)$, $\beta\cdot X=\beta\cdot\theta(X)$,因此对 3 轮 AC:

$$T\xrightarrow{\theta}X\xrightarrow{P}P(X)\xrightarrow{\theta}Y\xrightarrow{P}P(Y)\xrightarrow{\theta}Z\xrightarrow{P}P(Z)$$

存在线性逼近 $\beta\xrightarrow{\theta}\beta\xrightarrow{P}\alpha_{10}\xrightarrow{\theta}\alpha_{10}\xrightarrow{P}\beta\xrightarrow{\theta}\beta\xrightarrow{P}\alpha_{10}$,此逼近的活动盒子的个数为 $2T(\beta)+T(\alpha_{10})$=14<16.由测试和堆积引理可知: $\alpha_{10}\cdot X=\alpha_{10}\cdot\theta(X)$ 的逼近优势为 2^{-10}, $\beta\cdot X=\beta\cdot\theta(X)$ 的逼近优势为 2^{-8},所以此 3 轮逼近的优势不大于 2^{-24},以它为基础构造的 12 轮的线性逼近的优势不大于 2^{-93}.

(2) (**5**,**5**,**5**): $V(5,5)$ 的 25 个中的两个元素 $\gamma_1=(\{0,9\},\{7,2\},\{8,a\},\{d,2\},\{f,2\})$和 $\gamma_2=(\{0,9\},\{7,2\},\{8,2\},\{d,2\},\{10,2\})$, $P(\gamma_1)=(\{0,2\},\{10,9\},\{17,2\},\{18,2\},\{1d,2\})$, $P(\gamma_2)=(\{10,9\},\{17,2\},\{18,a\},\{1d,2\},\{1f,2\})$.对$\theta$存在有效线性逼近: $\gamma_1\cdot X=\gamma_1\cdot\theta(X)$, $P(\gamma_1)\cdot X=P(\gamma_1)\cdot\theta(X)$, $\gamma_2\cdot X=\gamma_2\cdot\theta(X)$, $P(\gamma_2)\cdot X=P(\gamma_2)\cdot\theta(X)$.由测试和堆积引理可知:它们的优势均为 2^{-10},因此,存在如下 3 轮线性逼近:

$$\gamma_1\xrightarrow{\theta}\gamma_1\xrightarrow{P}P(\gamma_1)\xrightarrow{\theta}P(\gamma_1)\xrightarrow{P}\gamma_1\xrightarrow{\theta}\gamma_1\xrightarrow{P}P(\gamma_1),$$

$$P(\gamma_1)\xrightarrow{\theta}P(\gamma_1)\xrightarrow{P}\gamma_1\xrightarrow{\theta}\gamma_1\xrightarrow{P}P(\gamma_1)\xrightarrow{\theta}P(\gamma_1)\xrightarrow{P}\gamma_1,$$

$$\gamma_2\xrightarrow{\theta}\gamma_2\xrightarrow{P}P(\gamma_2)\xrightarrow{\theta}P(\gamma_2)\xrightarrow{P}\gamma_2\xrightarrow{\theta}\gamma_2\xrightarrow{P}P(\gamma_2),$$

$$P(\gamma_2)\xrightarrow{\theta}P(\gamma_2)\xrightarrow{P}\gamma_2\xrightarrow{\theta}\gamma_2\xrightarrow{P}P(\gamma_2)\xrightarrow{\theta}P(\gamma_2)\xrightarrow{P}\gamma_2.$$

这 4 个线性逼近的活动盒子数为 15<16,但是它们的逼近优势为 2^{-28},以它们为基础构造的 12 轮的线性逼近的优势不大于 2^{-109}.

(3) (**6**,**2**,**6**): 对 $V(6,2)$ 中的惟一元素 $\alpha_1=(\{0,1\},\{d,2\})$, $P(\alpha_1)=(\{0,2\},\{8,4\},\{9,1\},\{15,8\},\{1c,2\},\{1d,2\})$,对$\theta$存在有效线性逼近 $\alpha_1\cdot X=\alpha_1\cdot\theta(X)$,不存在有效线性逼近 $P(\alpha_1)\cdot X=P(\alpha_1)\cdot\theta(X)$.假设存在$\beta$,使得 $\beta\cdot X=P(\alpha_1)\cdot\theta(X)$,则活动盒子的个数<16 的 3 轮线性逼近如下:

$$\beta\xrightarrow{\theta}P(\alpha_1)\xrightarrow{P}\alpha_1\xrightarrow{\theta}\alpha_1\xrightarrow{P}P(\alpha_1)\xrightarrow{\theta}\beta\xrightarrow{P}P(\beta).$$

我们把此 3 轮逼近扩充为 4 轮线性逼近:

$$\beta\xrightarrow{\theta}P(\alpha_1)\xrightarrow{P}\alpha_1\xrightarrow{\theta}\alpha_1\xrightarrow{P}P(\alpha_1)\xrightarrow{\theta}\beta\xrightarrow{P}P(\beta)\xrightarrow{\theta}\alpha_2\xrightarrow{P}P(\alpha_2).$$

此 4 轮线性逼近的活动盒子的个数为 $T(P(\alpha_1))+T(\alpha_1)+T(P(\alpha_1))+T(\alpha_2)$,因为 $\alpha_1\xrightarrow{\theta}\alpha_1\xrightarrow{P}P(\alpha_1)\xrightarrow{\theta}\beta\xrightarrow{P}P(\beta)\xrightarrow{\theta}\alpha_2\xrightarrow{P}P(\alpha_2)$ 是$(2,6,m)$的情形,由上述可知, $T(\alpha_1)+T(P(\alpha_1))+T(\alpha_2)\ge 16$,因此 $T(P(\alpha_1))+T(\alpha_1)+T(P(\alpha_1))+T(\alpha_2)\ge$ 6+16=22.这就说明以活动盒子小于 16 的此 3 轮线性逼近构造的 12 轮线性逼近的活动盒子的个数不小于 66.

(4) (**6**,**3**,**6**): 对 $V(6,3)$ 中的 $\alpha_1=(\{0,1\},\{3,1\},\{d,2\})$,由测试可知,存在有效线性逼近 $\alpha_1\cdot X=\alpha_1\cdot\theta(X)$,假设存在$\beta$,使得 $\beta\cdot X=P(\alpha_1)\cdot\theta(X)$,则活动盒子的个数<16 的 3 轮线性逼近如下:

$$\beta\xrightarrow{\theta}P(\alpha_1)\xrightarrow{P}\alpha_1\xrightarrow{\theta}\alpha_1\xrightarrow{P}P(\alpha_1)\xrightarrow{\theta}\beta\xrightarrow{P}P(\beta).$$

我们把此 3 轮逼近扩充为 4 轮线性逼近:

$$\beta\xrightarrow{\theta}P(\alpha_1)\xrightarrow{P}\alpha_1\xrightarrow{\theta}\alpha_1\xrightarrow{P}P(\alpha_1)\xrightarrow{\theta}\beta\xrightarrow{P}P(\beta)\xrightarrow{\theta}\alpha_2\xrightarrow{P}P(\alpha_2).$$

此 3 轮线性逼近的活动盒子的个数为 $T(P(\alpha_1))+T(\alpha_1)+T(P(\alpha_1))+T(\alpha_2)$,因为 $\alpha_1\xrightarrow{\theta}\alpha_1\xrightarrow{P}P(\alpha_1)\xrightarrow{\theta}\beta\xrightarrow{P}P(\beta)\xrightarrow{\theta}\alpha_2\xrightarrow{P}P(\alpha_2)$ 是$(3,6,m)$的情形,由上述可知, $T(\alpha_1)+T(P(\alpha_1))+T(\alpha_2)\ge 16$,因此 $T(P(\alpha_1))+T(\alpha_1)+T(P(\alpha_1))+T(\alpha_2)\ge$ 6+16=22.这就说明以活动盒子小于 16 的此 3 轮线性逼近构造的 12 轮线性逼近的活动盒子的个数不小于 66.

因为 S-盒的最佳逼近优势为 2^{-2},所以综上可证 12 轮 AC 的线性逼近优势不大于 2^{-67}.

3 结束语

本文讨论了 AC 分组密码针对差分和线性密码分析的安全性,结果显示:12 轮 AC 的差分特征概率不大于 2^{-128},12 轮 AC 的线性逼近优势不大于 2^{-67}.又因为 2 轮 AC 的输出依赖于输入的每一比特,所以 AC 分组密码对差分和线性密码分析是安全的.

References:

[1] AES. 1999. http://www.nist.gov/aes/.

[2] NESSIE. 2000. http://www.cryptonessie.org.

[3] Wu WL, Ma HT, Feng DG, Qing SH. The AC block cipher. Journal of China Institute of Communications, 2002,23(5):130~134 (in Chinese with English Abstract).

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

[5] Matsui M. Linear cryptanalysis method for DES cipher. In: Helleseth T, ed. Proceedings of the Advances in Cryptology-EUROCRYPT'93. New York: Springer-Verlag, 1993. 386~397.

附中文参考文献:

[3] 吴文玲,马恒太,冯登国,卿斯汉.AC 分组密码.通信学报,2002,23(5):130~134.