软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2011,22(8):1911−1917 [doi: 10.3724/SP.J.1001.2011.03875]

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

Zodiac 算法的不可能差分和积分攻击*

孙 兵[1+], 张 鹏[1], 李 超[1,2]

[1](国防科学技术大学 理学院 数学与系统科学系,湖南 长沙 410073)

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

Impossible Differential and Integral Cryptanalysis of Zodiac

SUN Bing[1+], ZHANG Peng[1], LI Chao[1,2]

[1](Department of Mathematics and Systems Science, College of Science, National University of Defense Technology, Changsha 410073, China)

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

+ Corresponding author: E-mail: happy_come@163.com

Sun B, Zhang P, Li C. Impossible differential and integral cryptanalysis of Zodiac. *Journal of Software*, 2011,22(8):1911−1917. http://www.jos.org.cn/1000-9825/3875.htm

Abstract: This paper reevaluates the security of Zodiac against impossible differential and integral attacks. In the past, results have shown that there are 15-round impossible differentials and 8-round integral distinguishers of Zodiac. Based on an 8-round truncated differential, with probability being 1, full 16-round impossible differentials and 9-round integral distinguishers are constructed. Integral attacks are applied to 12/13/14/15/16-round Zodiac with time complexities being 2^{34}, 2^{59}, 2^{93}, 2^{133} and 2^{190}, respectively. Both the numbers of chosen plaintexts are no more than 2^{16}, which shows that the full 16-round Zodiac is not immune to integral attack.

Key words: Zodiac; impossible differential; truncated differential; integral attack

摘 要: 重新评估了 Zodiac 算法抗不可能差分攻击和积分攻击的能力.已有结果显示,Zodiac 算法存在 15 轮不可能差分和 8 轮积分区分器.首先得到了算法概率为 1 的 8 轮截断差分,以此构造了 Zodiac 算法完整 16 轮不可能差分和 9 轮积分区分器.利用 9 轮积分区分器,对不同轮数 Zodiac 算法实施了积分攻击,对 12 轮、13 轮、14 轮、15 轮和 16 轮 Zodiac 的攻击复杂度分别为 2^{34},2^{59},2^{93},2^{133} 和 2^{190} 次加密运算,选择明文数均不超过 2^{16}.结果表明,完整 16 轮 192 比特密钥的 Zodiac 算法也是不抗积分攻击的.

关键词: Zodiac;不可能差分;截断差分;积分攻击

中图法分类号: TP309 **文献标识码**: A

积分攻击[1]是继差分密码分析[2]和线性密码分析[3]后,密码学界公认的一种比较有效的密码分析方法.1997 年,Daemen 等人针对 Square 密码提出了一种新的攻击方法,后来被命名为 Square 攻击.这种攻击方法主要利用了 S 盒是满射的性质,与算法部件的具体取值几乎无关.作为主要分析针对面向字节运算算法安全性的密码分析方法,Square 从其出现就受到密码学界的广泛关注[4,5].2001 年,Lucks 在分析 Twofish 算法的安全性时,首次将

* 基金项目: 国家自然科学基金(60803156, 61070215); 信息安全国家重点实验室开放基金(01-07, 01-02-5)
收稿时间: 2009-07-06; 修改时间: 2010-03-04; 定稿时间: 2010-04-22

Square 攻击的方法用于 Feistel 密码,提出了 Saturation 攻击[6].同年,Biryukov 等人在分析 SPN 结构安全性时提出了 Multiset 攻击,并指出,对于一个 4 轮 SPN 密码而言,即使算法采用的 S 盒和线性变换都不公开,利用 Multiset 攻击的思想仍然可以恢复出一个与原算法等价的算法[7].在总结 Square 攻击、Saturation 攻击和 Multiset 攻击的基础上,Knudsen 在 FSE2002 上提出了积分攻击的思想,并给出了积分攻击和高阶积分攻击的一般原理和方法[1].

截断差分密码分析是差分分析的变种,它是由 Knudsen 首先提出来的[8].与经典差分不同的是,截断差分仅仅考虑差分的部分性质,如,常用的字节差分只考虑差分的有无而不考虑差分的具体值,这种方法对基于字节构造的分组算法十分有效,因此对此类密码而言,截断差分是主要的潜在安全威胁.不可能差分密码分析是差分密码分析的另一个变种,这个概念由 Biham 和 Knudsen 分别独立提出[9,10].通常的差分分析方法通过寻找高概率差分来恢复密钥,不可能差分与之相反,寻找的是不可能出现的差分.若某个猜测密钥能使不可能差分出现,则一定是错误密钥,从而淘汰.利用不可能差分攻击的思想,我们可以证明轮函数为满射的 5 轮 Feistel 密码是不安全的.利用不可能差分攻击的方法并结合轮密钥之间的关系,可以得到目前对 AES 和 Camellia 算法的最好攻击结果[11−13].

Zodiac 是由韩国学者 Lee 等人提出的一种 Feistel 型迭代分组密码算法,其分组长度为 128 比特,算法支持 128 比特、192 比特和 256 比特密钥长度(以下简记为 Zodiac-128,Zodiac-192 和 Zodiac-256).与 DES 算法类似,算法对输入明文和输出密文采用了相应的初始置换和输出变换.Zodiac 算法迭代轮数为 16,每一轮变换均由密钥加变换、线性 P 变换以及非线性 S 盒变换组成.算法提出后,密码学界对 Zodiac 抗已知攻击的能力做了评估,主要是抗不可能差分攻击和抗积分攻击的能力.在 FSE2001 上,Hong 等人指出,Zodiac 算法存在 14 轮和 15 轮不可能差分.同时,他们利用 14 轮差分对完整 16 轮 Zodiac 算法成功实施了不可能差分攻击.攻击的时间复杂度为 2^{119} 次加密运算.因此,该攻击对 Zodiac-128,Zodiac-192 和 Zodiac-256 均有效[14].在 ISPEC2008 上,Ji 等人指出,Zodiac 算法存在 8 轮积分区分器,利用该区分器可以对 13 轮 Zodiac-128、15 轮 Zodiac-192 以及完整 16 轮的 Zodiac-256 算法实施积分攻击,攻击的复杂度分别为 $2^{124.8}$,$2^{189.5}$ 和 $2^{221.7}$ 次加密运算[15].

本文进一步研究了 Zodiac 算法抗不可能差分攻击和积分攻击的能力.我们得到了一条概率为 1 的 8 轮截断差分,利用中间相遇法找到了 Zodiac 算法的 16 轮不可能差分,这个结果进一步说明了 Zodiac 算法对不可能差分攻击是很脆弱的.在 8 轮截断差分的基础上,根据积分攻击与截断差分攻击的关系,我们进一步找到了算法的 9 轮截断差分,并指出,该截断差分对应了 Zodiac 算法 9 轮积分区分器,利用 9 轮积分区分器可以成功地对 14 轮 Zodiac-128 以及完整轮数的 Zodiac-192 和 Zodiac-256 实施积分攻击,攻击复杂度分别为 2^{133} 和 2^{190} 次加密运算.这说明 Zodiac-192 和 Zodiac-256 对积分攻击都是不免疫的.

1 Zodiac 算法介绍

1.1 符号说明

$L=(l_0,l_1,l_2,l_3,l_4,l_5,l_6,l_7)\in(\mathbb{F}_2^8)^8$:输入明文的左半部分.

$R=(r_0,r_1,r_2,r_3,r_4,r_5,r_6,r_7)\in(\mathbb{F}_2^8)^8$:输入明文的右半部分.

$L_i=(l_{i,0},l_{i,1},l_{i,2},l_{i,3},l_{i,4},l_{i,5},l_{i,6},l_{i,7})\in(\mathbb{F}_2^8)^8$:第 i 轮输入的左半部分.

$R_i=(r_{i,0},r_{i,1},r_{i,2},r_{i,3},r_{i,4},r_{i,5},r_{i,6},r_{i,7})\in(\mathbb{F}_2^8)^8$:第 i 轮输入的右半部分.

$K_i=(k_{i,0},k_{i,1},k_{i,2},k_{i,3},k_{i,4},k_{i,5},k_{i,6},k_{i,7})\in(\mathbb{F}_2^8)^8$:第 i 轮的轮密钥.

K_{in}:初始白化密钥.

K_{out}:输出白化密钥.

1.2 算法描述

由于初始置换不影响本文的分析,因此本文的分析都不考虑初始置换的影响.设 Zodiac 算法的输入为

$P=(L,R)\in(\mathbb{F}_2^{64})^2$,定义 $L_0=L\oplus K_{in}$,$R_0=R$,则 Zodiac 算法第 1 轮~第 15 轮变换定义如下:

$$\begin{cases}L_i=F(L_{i-1}\oplus K_i)\oplus R_{i-1}\\ R_i=L_{i-1}\end{cases},\ 1\leqslant i\leqslant 15.$$

第 16 轮变换定义为

$$\begin{cases}R_{16}=F(L_{15}\oplus K_{15})\oplus R_{15}\\ L_{16}=L_{15}\oplus K_{out}\end{cases}.$$

(L_{16},R_{16})即为明文 P 对应的密文.轮函数定义为 $F(X)=S(P(X))$,其中,P 将 $X=(x_0,x_1,x_2,x_3,x_4,x_5,x_6,x_7)$变换为 $Y=(y_0,y_1,y_2,y_3,y_4,y_5,y_6,y_7)$:

$$y_0=x_2\oplus x_3\oplus x_4,\quad y_1=x_0\oplus x_1,\quad y_2=x_1\oplus x_2,\quad y_3=x_2\oplus x_3,$$
$$y_4=x_6\oplus x_7\oplus x_0,\quad y_5=x_4\oplus x_5,\quad y_6=x_5\oplus x_6,\quad y_7=x_6\oplus x_7.$$

S 将 $Y=(y_0,y_1,y_2,y_3,y_4,y_5,y_6,y_7)$变换为 $Z=(z_0,z_1,z_2,z_3,z_4,z_5,z_6,z_7)$:

$$z_0=S_1(y_0),\quad z_1=S_2(y_1),\quad z_2=S_1(y_2),\quad z_3=S_2(y_3),$$
$$z_4=S_1(y_4),\quad z_5=S_2(y_5),\quad z_6=S_1(y_6),\quad z_7=S_2(y_7).$$

其中,S_1 和 S_2 均是 $\mathbb{F}_2^8\to\mathbb{F}_2^8$ 的非线性变换(S 盒).

由于本文不考虑轮密钥之间的影响,因此我们不详细介绍密钥扩展算法.

2 Zodiac 算法 16 轮不可能差分

本节我们考虑 Zodiac 算法的不可能差分.

算法的输入差分为

$$(\Delta_L^{(0)},\Delta_R^{(0)})=(00000000,00000aaa),$$

其中,$a\neq 0$,

根据算法流程可知,第 1 轮的输出差分为

$$(\Delta_L^{(1)},\Delta_R^{(1)})=(00000aaa,00000000).$$

第 2 轮~第 8 轮的输出差分依次为

$$(\Delta_L^{(2)},\Delta_R^{(2)})=(00000b00,00000aaa),$$
$$(\Delta_L^{(3)},\Delta_R^{(3)})=(00000\ a\oplus c\ a\oplus d\ a,00000b00),$$
$$(\Delta_L^{(4)},\Delta_R^{(4)})=(0000eABf,00000a\oplus ca\oplus da),$$
$$(\Delta_L^{(5)},\Delta_R^{(5)})=(g000CDEF,0000eABf),$$
$$(\Delta_L^{(6)},\Delta_R^{(6)})=(Gh00IJKL,g000CDEF),$$
$$(\Delta_L^{(7)},\Delta_R^{(7)})=(MNi0OPQR,Gh00IJKL),$$
$$(\Delta_L^{(8)},\Delta_R^{(8)})=(STUjVWXY,MNi0OPQR).$$

在上述系列表达式中,小写字母诸如 a,b,c 等表示非零差分,大写字母诸如 A,B,C 等表示无法确定或者无须考虑的差分.因此,若(00000000,00000aaa)和$(p_0,p_1,p_2,p_3,p_4,p_5,p_6,p_7,q_0,q_1,q_2,q_3,q_4,q_5,q_6,q_7)$分别为 8 轮 Zodiac 算法的输入与输出差分,则一定有:

$$p_3\neq 0,\ q_2\neq 0,\ q_3=0.$$

我们首先证明如下关于 Feistel 密码普遍成立的命题:

引理 1. 若 Feistel 密码ε存在 m 轮与密钥无关且概率为 1 的截断差分$(a,b)\to(c,d)$(最后一轮考虑交换),且 $c=d$ 不可能成立,则 $(a,b)\to(a,b)$ 是ε的 $2m$ 轮不可能差分(最后一轮不考虑交换).

证明:我们用中间相遇法证明该差分的不可能性,如图 1 所示.

根据已知,考虑加密算法,截断差分(a,b)经过 m 轮后一定变为(c,d).

从解密方向看,如果考虑交换,因为题设中的差分与密钥无关,因此经过 m 轮后,截断差分(a,b)一定变为

(*c*,*d*).由于在 Feistel 密码中两轮之间只有 1 次交换,因此,从解密方向研究差分传播时不应考虑最后一轮的数据交换.这说明,从解密方向看,经过 *m* 轮后,差分(*a*,*b*)一定变为(*d*,*c*).

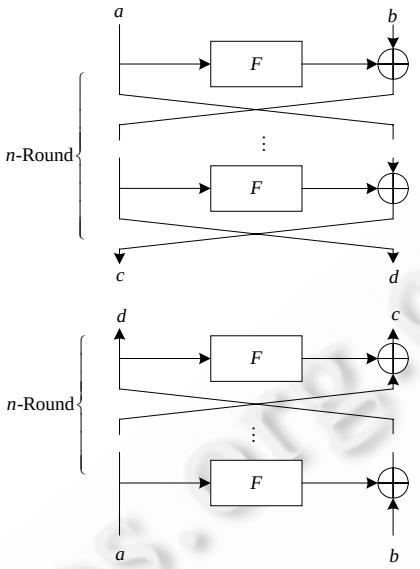

Fig.1 2*m*-Round impossible differential of feistel cipher

图 1 Feistel 密码 2*m* 轮不可能差分

若$(a,b)\rightarrow(a,b)$是一条可能的差分,则$(c,d)=(d,c)$在某些特定的条件下能够成立.显然,这与题设中 $c=d$ 不可能成立矛盾.

综上, $(a,b)\not\rightarrow(a,b)$ 是ε的 2*m* 轮不可能差分. □

注意到,当上述不可能差分 $(a,b)\not\rightarrow(a,b)$ 是具体差分时,输入与输出必须严格相等;当考虑的问题是截断差分时,有时并不一定要严格相等,只要两者的模式相同即可.也就是说,输入差分和输出差分为 0 的字节位置相同.

定理 1. (00000000,00000*aaa*)$\not\rightarrow$(00000000,00000*bbb*) 是 16 轮 Zodiac 算法的不可能差分,其中,*a*,*b* 均为非零差分.

证明:注意到 $q_3=0\neq p_3$,根据上文对 8 轮 Zodiac 算法差分传播的分析和引理 1 可得. □

利用同样的方法可以证明 (00000000,0*aaa*0000)$\not\rightarrow$(00000000,0*bbb*0000) ($a\neq0,b\neq0$)也是 Zodiac 算法 16 轮不可能差分,详细证明从略.

注意到,我们给出的 16 轮不可能差分与文献[14]中给出的 15 轮不可能差分具有相同的形式.之所以能够由 15 轮推到 16 轮,其原因在于,我们把第 3 轮的输出差分表示得更加精确,从而可以确定一个不能确定的差分和一个可确定的差分异或后的差分性质.

3 对 Zodiac 的新的积分攻击

本节我们把引理 1 中概率为 1 的 8 轮截断差分区分器扩展成一个概率为 1 的 9 轮截断差分区分器,并证明这条 9 轮截断差分对应于一个 9 轮积分区分器.在此基础上,对不同轮数的 Zodiac 算法实施积分攻击.

3.1 9轮积分区分器

定理 2. Zodiac 算法存在如下概率为 1 的 9 轮截断差分:

$$(00000000,00000aaa)\rightarrow(p_0,p_1,p_2,p_3,p_4,p_5,p_6,p_7,q_0,q_1,q_2,q_3,q_4,q_5,q_6,q_7),$$

其中,$q_3\neq0$.这条 9 轮截断差分对应于如下 9 轮积分区分器:

$$(CCCCCCCC,CCCCCAA_CA_C)\rightarrow(???????,???A????),$$

其中,A 表示该位置上的取值遍历 $\mathbb{F}_2^8$;AA_CA_C 表示存在常数 c_1 和 c_2,使得三元数组$(x,x\oplus c_1,x\oplus c_2)\in AA_CA_C$.

证明:第 9 轮的右半部分等于第 8 轮输出的左半部分,因此概率为 1 的 9 轮截断差分可直接由上文对 8 轮 Zodiac 算法的差分传播性质得到.

若输入为$(CCCCCAA_CA_C)$,则任意明文对的差分均为$(00000000,00000aaa)$;若相应输出位置不遍历,则至少存在两个值相等.这就与差分不为 0 矛盾,因此,定理中的 9 轮积分区分器成立. □

同理可知,$(CCCCCCCC,CAA_CA_CCCCC)\rightarrow(???????,???????A)$也是 Zodiac 算法 9 轮积分区分器.

3.2 对不同轮数Zodiac算法的积分攻击

为方便描述,我们记 $K_i^*=P(K_i)$,即

$$(K_{i,0}^*,K_{i,1}^*,K_{i,2}^*,K_{i,3}^*,K_{i,4}^*,K_{i,5}^*,K_{i,6}^*,K_{i,7}^*)=P(K_{i,0},K_{i,1},K_{i,2},K_{i,3},K_{i,4},K_{i,5},K_{i,6},K_{i,7}).$$

称 K_i^* 为 K_i 的等价密钥,从而原轮函数 $S(P(X\oplus K_i))$等价为 $S(P(X)\oplus K_i^*)$.在下文的攻击过程中,我们不考虑 K_{in} 和 K_{out} 的作用,且恢复的都是等价密钥 K_i^*.下面我们以攻击 12 轮 Zodiac 为例,详细介绍积分攻击的步骤以及相应的复杂度计算方法.

令 $L_0=(c_0c_1c_2c_3c_4xxx)$,猜测 $K_{1,5}^*$,令 $R_0=(c_5c_6c_7c_8c_9S_2(x\oplus c_5\oplus K_{1,5}^*)c_{10}c_{11})$,则选择明文为 $P_x=(L_0,R_0)$,对 P_x 加密,相应的密文记为 $C(x)=(C_L(x),C_R(x))$.根据 Zodiac 算法的加密流程可知,若 $K_{1,5}^*$ 的猜测值正确,则第 2 轮的输入即满足 9 轮积分区分器的输入形式,从而第 10 轮的输出满足 $R_{10,3}$ 为活跃字节.从解密的方向考虑,为了得到 $R_{10,3}$ 的值,我们必须知道 $L_{11,3},R_{11,2},R_{11,3}$ 以及 $K_{11,3}^*$ 的值;为了得到 $L_{11,3},R_{11,2}$ 和 $R_{11,3}$ 的值,由于我们考虑的是对 12 轮 Zodiac 的攻击,因此只需猜测 $K_{12,2}^*$ 和 $K_{12,3}^*$ 的值即可.

综上所述,对 12 轮 Zodiac 的积分攻击共需猜测 4 个字节的密钥,即 $K_{1,5}^*,K_{11,3}^*,K_{12,2}^*$ 和 $K_{12,3}^*$.对于错误的猜测值, $R_{10,3}$ 遍历 $\mathbb{F}_2^8$ 的概率为 $256!/(256^{256})\approx 2^{-364}$.因此,一个正确的明文结构即可淘汰所有的错误密钥,从而选择明文数为 2^{16}.由于对每个猜测值计算 $R_{10,3}$ 需要 3 次查表运算,因此攻击共需进行 $2^{32}\times 2^8\times 3$ 次查表运算.由于 12 轮 Zodiac 算法共有 8×12=96 次查表运算,因此对 12 轮 Zodiac 积分攻击的时间复杂度为 $2^{32}\times 2^8\times 3/96=2^{35}$ 次加密运算.实际上,判断 $R_{10,3}$ 是否遍历并不需要验证 256 个值,假设选择明文数为 T,则对应的 $R_{10,3}$ 中没有重复元素出现的概率为 $p=256!/(256-T)!\times 256^T$,当 $T=128$ 时,$p=2^{-56}$,这个概率可以保证错误密钥均被淘汰.因此,该攻击的数据复杂度可以降低为 2^{15},时间复杂度降低为 2^{34}(如图 2 所示).

在攻击更多轮 Zodiac 时,攻击方法与 12 轮类似,具体流程不再赘述.表 1 列出了对 12 轮~16 轮 Zodiac 积分攻击所需要猜测的密钥以及攻击的复杂度.由攻击复杂度一栏可知,本文的积分攻击大大优于文献[15]中给出的积分攻击.结果同时显示,完整 16 轮 Zodiac-192 对积分攻击不免疫.

Table 1 Attacks on Zodiac with different rounds

表 1 对不同轮数 Zodiac 的积分攻击

Rounds	Recoverd keys	Time complexity (This paper/Ref.[15])	Chosen plaintexts
12	$K_{1,5}^*,K_{11,3}^*,K_{12,2}^*,K_{12,3}^*$	$2^{34}/2^{92.3}$	2^{15}
13	$K_{1,5}^*,K_{11,3}^*,K_{12,2}^*,K_{12,3}^*,K_{13,1}^*,K_{13,2}^*,K_{13,3}^*$	$2^{59}/2^{124.8}$	2^{15}
14	$K_{1,5}^*,K_{11,3}^*,K_{12,2}^*,K_{12,3}^*,K_{13,1}^*,K_{13,2}^*,K_{13,3}^*,K_{14,0}^*,$ $K_{14,1}^*,K_{14,2}^*,K_{14,3}^*$	$2^{93}/2^{157.2}$	2^{16}
15	$K_{1,5}^*,K_{11,3}^*,K_{12,2}^*,K_{12,3}^*,K_{13,1}^*,K_{13,2}^*,K_{13,3}^*,K_{14,0}^*,$ $K_{14,1}^*,K_{14,2}^*,K_{14,3}^*,K_{15,0}^*,K_{15,1}^*,K_{15,2}^*,K_{15,3}^*,K_{15,4}^*$	$2^{133}/2^{189.5}$	2^{16}
16	$K_{1,5}^*,K_{11,3}^*,K_{12,2}^*,K_{12,3}^*,K_{13,1}^*,K_{13,2}^*,K_{13,3}^*,K_{14,0}^*,$ $K_{14,1}^*,K_{14,2}^*,K_{14,3}^*,K_{15,0}^*,K_{15,1}^*,K_{15,2}^*,K_{15,3}^*,K_{15,4}^*,$ $K_{16,0}^*,K_{16,1}^*,K_{16,2}^*,K_{16,3}^*,K_{16,4}^*,K_{16,6}^*,K_{16,7}^*$	$2^{190}/2^{221.7}$	2^{16}

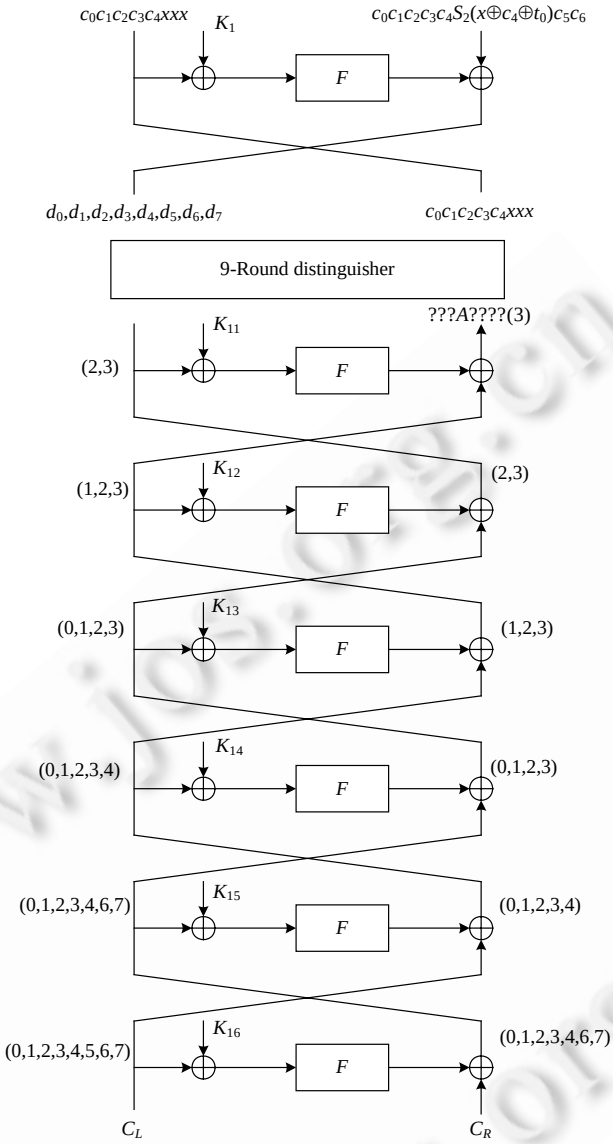

Fig.2 Integral attacks on round-reduced Zodiac

图 2 对简化轮数 Zodiac 的积分攻击

4 结 论

本文对 Zodiac 算法的安全性做了进一步的评估.发现了算法概率为 1 的 8 轮截断差分,在此基础上找到算完整 16 轮算法的不可能差分;同时还找到了算法 9 轮积分区分器,并对不同轮数的 Zodiac 成功实施了积分攻击.结果显示,对 Zodiac-192 而言,16 轮并不足以使算法可以抵抗积分攻击.本文的研究结果说明,在寻找各类区分器时,采用更精确的计算模型可以得到更为精确的结果.比如,文献[14,15]中对第 3 轮输出的刻画都是通过“非确定+确定=非确定”这个模型来计算的;而在本文的计算模型下,由于某些“非确定+确定=确定”,因此得到了更好的结果.如何将引理 2 中寻找不可能差分的方法应用到其他 Feistel 密码,如 Camellia 等算法中,将是下一步研究的主要内容.

References:

[1] Knudsen L, Wagner D. Integral cryptanalysis. In: Daemen J, Rijmen V, eds. Proc. of the Workshop on Fast Software Encryption (FSE 2002). LNCS 2365, Springer-Verlag, 2002. 629−632. [doi: 10.1007/3-540-45661-9_9]

[2] Biham E, Shamir A. Differential cryptanalysis of DES-like cryptosystems. In: Menezes AJ, Vanstone SA, eds. Proc. of the Advances in Cryptology (CRYPTO'90). LNCS 537, Springer-Verlag, 1991. 2−21. [doi: 10.1007/3-540-38424-3_1]

[3] Matsui M. Linear cryptanalysis method for DES cipher. In: Helleseth T, ed. Proc. of the Advances in Cryptology (EuroCrypt'93). LNCS 765, Springer-Verlag, 1993. 386−397. [doi: 10.1007/3-540-48285-7_33]

[4] Daemen J, Knudsen L, Rijmen V. The block cipher square. In: Biham E, ed. Proc. of the Workshop on Fast Software Encryption (FSE'97). LNCS 1267, Springer-Verlag, 1997. 149−165. [doi: 10.1007/BFb0052343]

[5] Ferguson N, Kelsey J, Lucks S, Schneier B, Stay M, Wagner D, Whiting D. Improved cryptanalysis of Rijndael. In: Schneier B, ed. Proc. of the Workshop on Fast Software Encryption (FSE 2000). LNCS 1978, Springer-Verlag, 2001. 136−141. [doi: 10.1007/3-540-44706-7_15]

[6] Lucks S. The saturation attack—A bait for twofish. In: Matsui M, ed. Proc. of the Fast Software Encryption (FSE 2001). LNCS 2355, Springer-Verlag, 2002. 187−205. [doi: 10.1007/3-540-45473-X_1]

[7] Biryukov A, Shamir A. Structural cryptanalysis of SASAS. In: Pfitzmann B, ed. Proc. of the Advances in Cryptology (EuroCrypt 2001). LNCS 2045, Springer-Verlag, 2001. 394−405. [doi: 10.1007/3-540-44987-6_24]

[8] Knudsen L. Truncated and higher order differentials. In: Hartmanis GG, van Leeuwen J, eds. Proc. of the Fast Software Encryption (FSE'94). LNCS 1008, Springer-Verlag, 1995. 196−211. [doi: 10.1007/3-540-60590-8_16]

[9] Biham E, Biryukov A, Shamir A. Cryptanalysis of skipjack reduced to 31 rounds using impossible differentials. In: Stern J, ed. Proc. of the Advances in Cryptology (EuroCrypt'99). LNCS 1592, Springer-Verlag, 1999. 12−23. [doi: 10.1007/3-540-48910-X_2]

[10] Knudsen L. DEAL—A 128-bit block cipher. Technical Report, 151, Bergen: Department of Informatics, University of Bergen, 1998.

[11] Zhang WT, Wu WL, Feng DG. New results on impossible differential cryptanalysis of reduced AES. In: Proc. of the Int'l Conf. on Information Security and Cryptology (ICISC 2007). LNCS 4817, Springer-Verlag, 2007. 239−250. [doi: 10.1007/978-3-540-76788-6_19]

[12] Lu JQ, Dunkelman O, Keller N, Kim JS. New impossible differential attacks on AES. In: Proc. of the Progress in Cryptology (IndoCrypt 2008). LNCS 5365, Springer-Verlag, 2008. 279−293. [doi: 10.1007/978-3-540-89754-5_22]

[13] Wu WL, Zhang L, Zhang WT. Improved impossible differential cryptanalysis of reduced-round camellia. In: Avanzi R, Keliher L, Sica F, eds. Proc. of the Selected Areas in Cryptography (SAC 2008). LNCS 5381, Springer-Verlag, 2009. 442−456. [doi: 10.1007/978-3-642-04159-4_29]

[14] Hong D, Sung J, Moriai S, Lee S, Lim J. Impossible differential cryptanalysis of Zodiac. In: Matsui M, ed. Proc. of the Workshop on Fast Software Encryption (FSE 2001). LNCS 2355, Springer-Verlag, 2002. 345−348. [doi: 10.1007/3-540-45473-X_25]

[15] Ji W, Hu L. Square attack on reduced-round Zodiac cipher. In: Chen L, Mu Y, Susilo W, eds. Proc. of the Information Security Practice and Experience (ISPEC 2008). LNCS 4991, Springer-Verlag, 2008. 377−391. [doi: 10.1007/978-3-540-79104-1_27]

孙兵(1981－),男,江苏如皋人,博士,讲师,主要研究领域为编码密码理论及其应用.

李超(1966－),男,博士,教授,博士生导师,主要研究领域为编码密码理论及其应用.

张鹏(1984－),男,博士生,主要研究领域为编码密码理论及其应用.