Zodiac算法的零相关-积分攻击

马 猛 赵亚群 刘庆聪
(信息工程大学数学工程与先进计算国家重点实验室 郑州 450001)

摘 要 Zodiac算法是一种由一批韩国学者设计的分组密码算法,它是16轮平衡Feistel型的分组密码。首次从零相关-积分分析的角度评价了Zodiac算法的安全性,构造出算法的两类13轮零相关线性逼近,并据此给出了13轮零相关-积分区分器,对全轮Zodiac算法进行了零相关-积分分析,成功恢复出了144bit轮子密钥信息。结果显示:完整16轮Zodiac-128/192/256算法的零相关-积分攻击的数据复杂度为2^{120}个选择明文,时间复杂度大约为2^{82}次16轮Zodiac算法加密,时间复杂度明显优于已有的积分攻击结果。

关键词 分组密码,Zodiac算法,零相关线性逼近,零相关-积分分析
中图法分类号 TP918.1 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2017.02.032

Integral Zero-correlation Cryptanalysis on Zodiac

MA Meng ZHAO Ya-qun LIU Qing-cong
(State Key Lab. of Mathematical Engineering and Advanced Computing, Information Engineering University, Zhengzhou 450001, China)

Abstract Zodiac algorithm, which was designed by a group of Korean scholars, is a 16-round Feistel-type block cipher. In this paper, the security of Zodiac algorithm was evaluated from the point of integral zero-correlation cryptanalysis for the first time. Two groups of 13-round zero-correlation linear approximations for zodiac were constructed, and the 8-round integral zero-correlation distinguisher of zodiac was given, based on which integral zero-correlation cryptanalysis was made on the full-round Zodiac algorithm, and 144bit round-subkey was restored successfully. It shows that the integral zero-correlation cryptanalysis on the full-round Zodiac-128/192/256 algorithm needs 2^{120} pairs of chosen plaintext-ciphertext and about 2^{82} full-round Zodiac encryptions, and its time complexity is obviously better than the existing results of integral attack.

Keywords Block cipher, Zodiac, Zero-correlation linear approximation, Integral zero-correlation cryptanalysis

1 引言

Zodiac算法是韩国学者Lee等人设计的一种分组密码[1],该密码于2000年9月被提交至ISO/IEC JTC1/SC27(信息安全技术标准委员会)。Zodiac算法的整体结构为典型的Feistel型分组迭代结构,分组长度为128bit,支持128bit,192bit,256bit 3种长度的密钥,该算法在加密过程中引入了白化密钥,并对输入明文和输出密文分别进行了初始置换和输出置换。Zodiac算法共迭代16轮,每一轮变换均由密钥加变换、线性变换P以及非线性S盒变换组成。自该算法被提出后,国内外密码学专家从不同攻击方法的角度评价了其安全性。目前主要的攻击方法包括不可能差分攻击、积分攻击和中间相遇攻击。Hong等人[2]在FSE 2001上指出Zodiac算法存在14轮和15轮不可能差分,并利用14轮不可能差分对完整16轮的Zodiac算法实施了不可能差分攻击,时间复杂度为2^{119}次16轮加密运算,Shakiba等人[3]进一步改进了该结果。文献[4]找到了Zodiac算法的16轮不可能差分和9轮积分区分器,据此对不同轮数的Zodiac算法进行了积分攻击。文献[5]找到了9轮和10轮区分器,据此对15轮和16轮Zodiac算法实施了中间相遇攻击。文献[6]分别给出了Zodiac算法的两个8轮和9轮区分器,并对其进行了碰撞攻击,结果显示全轮Zodiac算法对碰撞攻击是不免疫的。

在ASIACRYPT 2012上,Bogdanov等人[7]揭示了在输入掩码和输出掩码相互独立的情况下,零相关线性区分器与积分区分器是等价的,并且给出了两者之间的转化方法,据此给出了零相关-积分分析的密钥恢复攻击方法。与零相关线性分析相比,零相关-积分分析方法同样是利用分组密码算法中广泛存在的相关度为零的线性逼近来区分密码算法与随机函数,由此进行密钥恢复攻击,但是零相关-积分分析的数据量随着零相关线性逼近条数的增多降低得更为显著。

本文首次研究了Zodiac算法抵抗零相关-积分攻击的能力,构造了零相关线性逼近,据此给出了零相关-积分区分器,对全轮Zodiac算法进行了零相关-积分攻击,并成功恢复出了144bit轮子密钥信息,该攻击对3种密钥类型128/192/256

到稿日期:2016-01-21 返修日期:2016-06-20 本文受信息安全保障技术国家重点实验室开放基金(KJ-13-009)资助。
马 猛(1986—),男,硕士生,主要研究方向为密码学,E-mail:173122881@qq.com;赵亚群(1961—),女,博士,教授,主要研究方向为密码基础理论、概率统计应用;刘庆聪(1990—),男,硕士生,主要研究方向为密码学。

的算法都有效，时间复杂度明显优于已有的积分攻击结果。

本文第 2 节描述了 Zodiac 算法的加解密过程以及零相关-积分分析的一般原理；第 3 节描述了 Zodiac 算法的零相关-积分区分器的构造以及基于零相关-积分区分器的密钥恢复攻击；第 4 节分析了复杂度；最后总结全文。

2　预备知识

2.1　一些记号

$A|B$：向量 A 和 B 的连接；

$A\cdot B$：向量 A 和 B 的内积；

V^i：向量 V 的第 i 个字节；

$b,c,d,e,f,g,h,i,j,k,*$：非零字节；

?：不确定的字节；

$\circ$：复合运算。

2.2　Zodiac 算法描述

Zodiac 算法采用 16 轮 Feistel 型结构，在第 1 轮之前和最后 1 轮之后分别有初始置换和输出置换，如图 1 所示。其算法结构包括 Π 置换、白化层和轮变换。轮变换分别由密钥加 K、轮函数 F 构成。Zodiac 算法采用了具有两个分支的 Feistel 结构，设 Zodiac 算法的输入明文为 p，输出密文为 c，第 i 轮的输入、输出分别记为 $(L_{i-1},R_{i-1})\in(F_2^{64})^2$ 和 $(L_i,R_i)\in(F_2^{64})^2$，$k_i\in F_2^{64}(1\leqslant i\leqslant 16)$ 表示轮密钥，$WK_i\in F_2^{64}(i=0,1)$ 表示白化密钥。

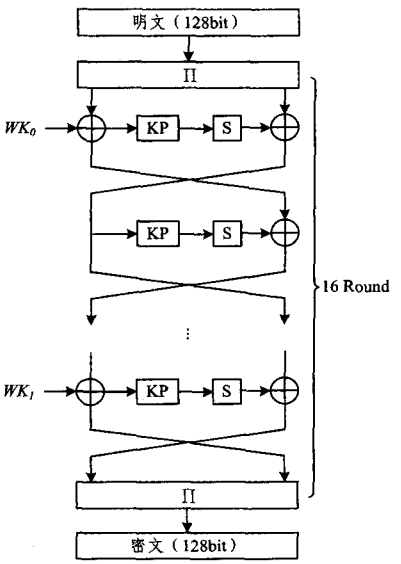

图 1　Zodiac 算法结构

Zodiac 算法的加密流程如下所示。

①初始 Π 置换：$(L,R)=\Pi(p)$，为初始白化层的输入。

②初始白化层：$(L_0,R_0)=(L\oplus WK_0,R)$，为第 1 轮轮变换的输入。

③16 轮轮变换：$(L_i,R_i)=(F(L_{i-1}\oplus k_i)\oplus R_{i-1},L_{i-1})$ $(1\leqslant i\leqslant 16)$，为末尾白化层的输入。

④末尾白化层：$(CL_0,CR_0)=(R_{16}\oplus WK_1,L_{16})$，为输出变换的输入。

⑤输出 Π 置换：$c=\Pi(CL_0,CR_0)$，为最终的输出密文。

轮函数 $F(\cdot)=S(L(\cdot))$ 由线性变换 L 和非线性变换 S 构成。设 $Y=L(X)$，其中 $X=(x_0,x_1,\cdots,x_7)\in(F_2^8)^8$，$Y=(y_0,y_1,\cdots,y_7)\in(F_2^8)^8$，则有：

$$Y=L(X)\begin{cases}y_0=x_2\oplus x_3\oplus x_4\\ y_1=x_0\oplus x_1\\ y_2=x_1\oplus x_2\\ y_3=x_2\oplus x_3\\ y_4=x_0\oplus x_6\oplus x_7\\ y_5=x_4\oplus x_5\\ y_6=x_5\oplus x_6\\ y_7=x_6\oplus x_7\end{cases}$$

非线性变换 S 由两个不同的 S 盒交替并置而成，设 $Z=S(Y)$，其中 $Z=(z_0,z_1,\cdots,z_7)\in(F_2^8)^8$，$z_0=S_1(y_0)$，$z_1=S_2(y_1)$，$z_2=S_1(y_2)$，$z_3=S_2(y_3)$，$z_4=S_1(y_4)$，$z_5=S_2(y_5)$，$z_6=S_1(y_6)$，$z_7=S_2(y_7)$。$S_1,S_2$ 均是 $F_2^8\to F_2^8$ 上的 S 盒，具体可参考文献[1]。本文不考虑轮密钥之间的关系，因此这里不再介绍 Zodiac 的密钥扩展算法；Π 置换和白化密钥不影响本文的分析，不作考虑，具体可参考文献[1]。

2.3　零相关-积分分析

对于传统的线性密码分析，人们往往关注相关度较大的线性逼近，线性逼近的相关度越大，越有利于线性密码分析。分组密码算法中广泛存在着相关度为零的线性逼近，而零相关-积分分析就是利用相关度为零的线性逼近作为区分器来区分分组密码算法和随机函数，由此进行密钥恢复攻击。因此，零相关-积分分析方法的必要条件是构造相关度为零的线性逼近。

2.3.1　零相关线性逼近

定义 1[8]　对于给定的函数 $f:F_2^n\to F_2^n$，设 α 和 β 分别表示 $n$bit 的输入掩码和输出掩码，称 $\beta\cdot f(x)\oplus\alpha\cdot x$ 为 f 的线性逼近表达式，(α,β) 为 f 的一个线性逼近。$n$bit 迭代型分组密码算法 E 可表示为 $f_r\circ f_{r-1}\circ\cdots\circ f_2\circ f_1$，其中 $f_i:F_2^n\to F_2^n$ $(i=1,2,\cdots,r)$ 是第 i 轮的轮函数，r 个一轮线性逼近的级联 $U=(u_0,u_1,\cdots,u_{r-1},u_r)$ 称为 E 的一个线性特征，其中 (u_{i-1},u_i) 是轮函数 $f_i(i=1,2,\cdots,r)$ 的线性逼近。设 $n$bit 明文掩码为 Γ_P，密文掩码为 Γ_C，则称 $(\Gamma_P,\Gamma_C)=\{U|u_0=\Gamma_P,u_r=\Gamma_C\}$ 为分组密码 E 的线性逼近。

定义 2[9]　若线性逼近 $\Gamma_P\to\Gamma_C$ 成立的概率为 p_{Γ_P,Γ_C}，则 Γ_P 和 Γ_C 的相关度为 $c(\Gamma_P\cdot P,\Gamma_C\cdot C)=2p_{\Gamma_P,\Gamma_C}-1$，其中 $p_{\Gamma_P,\Gamma_C}=\underset{P\in F_2^n}{Pr}\{\Gamma_P^{\mathrm{T}}P\oplus\Gamma_C^{\mathrm{T}}C=0\}$，$\Gamma_A^{\mathrm{T}}A$ 表示域 F_2 上 $n$bit 向量的乘积。

设 α 是输入掩码，β 是输出掩码，线性逼近的相关度在分组密码组件中的传播具有如下的性质。

引理 1[10]（异或运算）　如果 $h(x_1,x_2)=x_1\oplus x_2$，那么 $c(\beta\cdot h(x_1,x_2),\alpha_1\cdot x_1\oplus\alpha_2\cdot x_2)\neq 0$ 当且仅当 $\beta=\alpha_1=\alpha_2$。

引理 2[10]（分支操作）　如果 $h(x)=(x,x)$，那么 $c((\beta_1,\beta_2)\cdot h(x),\alpha\cdot x)\neq 0$ 当且仅当 $\alpha=\beta_1\oplus\beta_2$。

引理 3[11]（可逆 F 函数）　设 $h(x)$ 是可逆函数，若 $c(\beta\cdot h(x),\alpha\cdot x)\neq 0$，则 α 和 β 同时为 0 或者同时不为 0，反之不成立。

引理 4 给出了零相关线性逼近存在的充分条件。

引理 4[8]　对于一个迭代型分组密码算法，若与其线性逼近相对应的每个线性特征中都至少存在一对矛盾的相邻线性掩码，则该线性逼近的相关度为零。

2.3.2 零相关-积分区分器

引理 5[12] 设 ξ,η 均是二元随机变量，且 ξ 服从等概分布，则 $\xi\oplus\eta$ 服从等概分布的充分必要条件是 ξ 与 η 独立。

引理 6[12] 设 $\xi_1,\xi_2,\cdots,\xi_m$ 和 $\eta_1,\eta_2,\cdots,\eta_n$ 都是二元随机变量，则 $\xi_1,\xi_2,\cdots,\xi_m$ 和 $\eta_1,\eta_2,\cdots,\eta_n$ 独立等价于对于所有二元非零向量 $(a_1,a_2,\cdots,a_m)$ 和 $(b_1,b_2,\cdots,b_m)$，$a_1\xi_1\oplus a_2\xi_2\oplus\cdots\oplus a_m\xi_m$ 与 $b_1\eta_1\oplus\cdots\oplus b_n\eta_n$ 均独立。

引理 7 对于算法 $f:(F_2^8)^8\to(F_2^8)^8$，设其输入和输出分别为 $x=(x_0|x_1|\cdots|x_7,x_8|x_9|\cdots|x_{15})$ 和 $y=(y_0|y_1|\cdots|y_7,y_8|y_9|\cdots|y_{15})$。对所有非零向量 $a,b\in F_2^8$，当 $\alpha=(0|0|a|a|0|0|0|0,0|0|0|0|0|0|0|0)$ 和 $\beta=(0|0|0|0|0|0|0|0,0|0|0|b|0|0|0|0)$ 都满足 $\alpha\cdot x\oplus\beta\cdot f(x)$ 的相关系数为零时，则有 $x_2\oplus x_3$ 与 y_{11} 独立，即加密形如 $(x_0x_1x_2x_2x_3x_4x_5x_6,x_7x_8\cdots x_{14})$ 的所有可能的输入值，y_{11} 每个可能值出现的次数是相同的。

证明：由于对任意的非零向量 $a,b\in F_2^8$，都有 $\alpha\cdot x\oplus\beta\cdot f(x)$ 的相关系数为零，即 $a\cdot(x_2\oplus x_3)\oplus b\cdot y_{11}$ 为平衡函数，因此由引理 5 可知 $a\cdot(x_2\oplus x_3)$ 与 $b\cdot y_{11}$ 相互独立，再由引理 6 可知 $x_2\oplus x_3$ 与 y_{11} 相互独立。

3 Zodiac 算法的零相关-积分分析

3.1 Zodiac 算法的 13 轮零相关线性逼近

命题 1 $(0|0|\alpha|\alpha|0|0|0|0,0|0|0|0|0|0|0|0)\to(0|0|0|0|0|0|0|0,0|0|0|\beta|0|0|0|0)$ 是 Zodiac 算法的 13 轮零相关线性逼近。其中 $\alpha,\beta\in F_2^8$，$\alpha\neq0$，$\beta\neq0$。

证明：输入掩码是 $(0|0|\alpha|\alpha|0|0|0|0,0|0|0|0|0|0|0|0)$，根据 Zodiac 算法结构和引理 1－引理 3，向下迭代 6 轮，可以确定线性掩码在第 1－6 轮的传播轨迹，如图 2 所示。输入掩码是 $(0|0|0|0|0|0|0|0,0|0|0|\beta|0|0|0|0)$，向上迭代 7 轮，可以确定线性掩码在第 7－13 轮的传播轨迹，如图 3 所示，虚线内，$k=0$，这与上述矛盾，根据引理 4，结论得证。

同理，可以证明 $(0|0|0|0|0|0|0|\alpha|\alpha,0|0|0|0|0|0|0|0)\to(0|0|0|0|0|0|0|0,0|0|0|0|0|0|0|0|\beta)$ 也是其 13 轮零相关线性逼近。

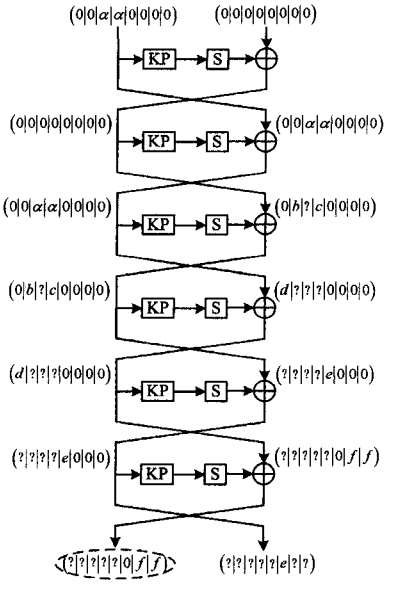

图 2 线性掩码在 6 轮算法结构中的传播轨迹

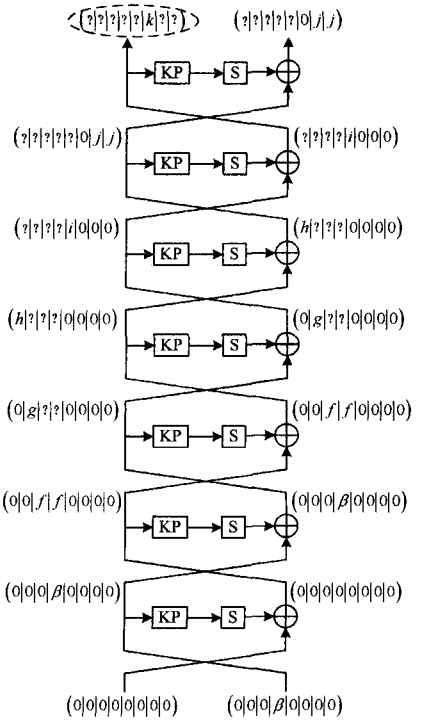

图 3 线性掩码在 7 轮算法结构中的传播轨迹

3.2 全轮 Zodiac 算法的零相关-积分攻击

基于 3.1 节得到的 13 轮零相关线性逼近，由引理 7，加密形如 $(x_0x_1x_2x_2x_3x_4x_5x_6,x_7x_8\cdots x_{14})$ 的所有可能的输入值，y_{11} 每个可能值出现的次数是 2^{112}，将其作为零相关-积分区分器置于算法的第 1－13 轮，以尾部添加 4 轮的方式构成了全轮 Zodiac 算法，如图 4 所示。

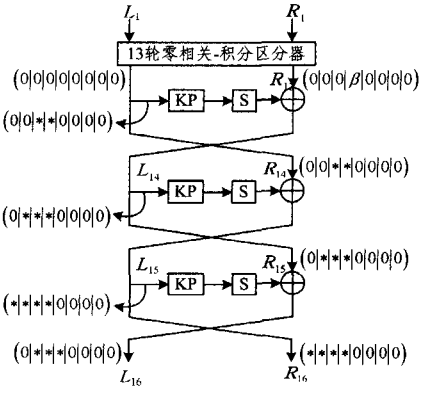

图 4 13 轮零相关-积分区分器

由引理 1－引理 3 可以确定线性掩码在第 14－16 轮的传播轨迹，如图 4 所示。

具体的攻击步骤如下：

1）收集 2^{120} 个选择明密文对 $(L_1|R_1,L_{16}|R_{16})$，其中 $L_1^2=L_1^3$。记 $x_0=(L_{16}^{1,2,3}|R_{16}^{0,1,2,3})$，建立计数器 $V_0[x_0]$ 对 56bit x_0 进行计数。

2）建立计数器 $V_1[x_1]$ 对 56bit x_1 进行计数，其中 $x_1=(R_{15}^{1,2,3}|R_{16}^{0,1,2,3})$，猜测轮子密钥 $k_{16}^{0,1,2,3}$，根据 x_0 计算 x_1，更新计数器 $V_1[x_1]+=V_0[x_0]$，该步骤的时间复杂度为 $2^{56}\cdot2^{32}=2^{88}$。

3）建立计数器 $V_2[x_2]$ 对 24bit x_2 进行计数，其中 $x_2=$

$(R_{14}^{2,3}|R_{15}^{3})$，猜测轮子密钥 $k_{15}^{1,2,3}$，根据 x_1 计算 x_2，更新计数器 $V_2[x_2]+=V_1[x_1]$，该步骤的时间复杂度为 $2^{56}\cdot 2^{24}=2^{80}$。

4)建立计数器 $V_3[x_3]$对 8bit x_3 进行计数，其中 $x_3=R_{13}^{3}$，猜测轮子密钥 $k_{14}^{2,3}$，根据 x_2 计算 x_3，更新计数器 $V_3[x_3]+=V_2[x_2]$，该步骤的时间复杂度为 $2^{24}\cdot 2^{16}=2^{40}$。

5)对于 x_3 的每一个可能取值，如果 $V_3[x_3]\neq 2^{112}$，则猜测密钥$(k_{14}^{2,3}|k_{15}^{1,2,3}|k_{16}^{0,1,2,3})$为错误密钥，否则为正确密钥。

6)根据以上分析，同样地，利用另一条 13 轮零相关线性逼近作为积分区分器对全轮 Zodiac 算法进行密钥恢复攻击，可恢复出轮子密钥$(k_{14}^{6,7}|k_{15}^{5,6,7}|k_{16}^{4,5,6,7})$。

4　复杂度分析

综合以上分析，时间复杂度主要取决于步骤 2)，全轮 Zodiac 算法需要 16×8 次 S 盒查表运算。因此密钥恢复攻击的时间复杂度为 $2\times 2^{88}\times\frac{1}{16}\times\frac{1}{8}=2^{82}$，数据复杂度为 2^{120}，存储复杂度为 2^{56}。表 1 列出了 Zodiac 算法的主要攻击结果对比。与其他积分攻击结果相比，本文的积分攻击的时间复杂度大幅降低，并且对 3 种密钥长度的算法 Zodiac-128/192/256 都有效。

表 1　Zodiac 的主要分析结果

攻击类型	KeyNum	攻击轮数	Data	Time	来源
积分攻击	23	16	$2^{112.6}$ CP	$2^{189.5}$	文献[13]
积分攻击	23	16	2^{112} CP	2^{190}	文献[4]
零相关-积分攻击	18	16	2^{120} CP	2^{82}	本文
不可能差分	9	16	$2^{103.6}$ CP	2^{119}	文献[15]
不可能差分	6	16	$2^{85.6}$ CP	$2^{32.6}$	文献[14]
碰撞攻击	17	16	$2^{63.9}$ CP	$2^{140.1}$	文献[6]

注：KeyNum 表示恢复出的密钥字节数；Data 表示数据复杂度，CP 表示选择明文；Time 表示时间复杂度，单位为 16 轮算法加密次数。

结束语　本文针对已有的积分攻击对 Zodiac 128 算法无效这一结果，衡量了属于积分攻击范畴的零相关-积分攻击的有效性，利用中间相错原理得到了 Zodiac 算法的 13 轮零相关线性逼近，据此构造了算法的零相关-积分区分器，对全轮 Zodiac 算法进行了零相关-积分攻击，攻击结果对 3 种密钥长度 Zodiac-128/192/256 的算法都有效。研究结果表明：零相关-积分攻击在某些条件下比一般的积分攻击更有优势，这对积分攻击的理论、应用及扩展研究有一定的参考价值。Zodiac算法虽然对零相关-积分攻击是不免疫的，时间复杂度明显优于已有的积分攻击结果，但是仍有不足——数据复杂度较高，因此如何取舍、优化分析模型及降低数据复杂度是下一步研究的方向。

参 考 文 献

[1] LEE C, JUN K, JUNG M, et al. Zodiac version 1.0 (revised) architecture and specification [EB/OL]. [2013-3-20]. http://www.kisa.or.kr/seed/index.html.

[2] HONG D, SUNG J, MORIAI S, et al. Impossible differential cryptanalysis of Zodiac [C]//FSE 2001. Springer-Verlag, LNCS 2355, 2002: 300-311.

[3] SHAKIBA M, DAKHILALIAN M, MALA H. An improved impossible differential cryptanalysis of Zodiac [J]. The Journal of Systems and Software, 2010, 83(3): 702-709.

[4] SUN B, ZHANG P, LI C. Impossible differential and integral cryptanalysis of Zodiac[J]. Journal of Software, 2011, 22(8): 1911-1917. (in Chinese)
孙兵，张鹏，李超. Zodiac 算法的不可能差分和积分攻击[J]. 软件学报，2011，22(8)：1911-1917.

[5] HAI X, TANG X H, LI C. The meet-in-the-middle attacks on Zodiac[J]. Journal of Electronics & Information Technology, 2012, 34(9): 2259-2262. (in Chinese)
海昕，唐学海，李超. 对 Zodiac 算法的中间相遇攻击[J]. 电子与信息学报，2012，34(9)：2259-2262.

[6] LIU Q, WEI H R, PAN W. Collision attack on Zodiac algorithm [J]. Journal of Computer Applications, 2014, 34(1): 73-77. (in Chinese)
刘青，卫宏儒，潘伟. Zodiac 算法的碰撞攻击[J]. 计算机应用，2014，34(1)：73-77.

[7] BOGDANOV A, LEANDER G, NYBERG K, et al. Integral and multidimensional linear distinguishers with correlation zero[C]// Advances in Cryptology (ASIACRYPT 2012). Springer Berlin Heidelberg, 2012: 244-261.

[8] BOGDANOV A, RIJMEN V. Linear hulls with correlation zero and linear cryptanalysis of block ciphers[J]. Designs, Codes and Cryptography, 2014, 70(3): 369-383.

[9] LUO F, ZHOU X G, OU Q Y. Mutiple Zero-correlation Linear Cryptanalysis[J]. Journal of Xi'an Electronic and Science University, 2014, 41(5): 196-202. (in Chinese)
罗芳，周学广，欧庆于. 对 LBlock 算法的多重零相关线性分析[J]. 西安电子科技大学学报，2014，41(5)：196-202.

[10] WANG M Q, WEN L. Research on zero-correlation linear cryptanalysis[J]. Journal of Cryptologic Research, 2014, 1(3): 296-310. (in Chinese)
王美琴，温隆. 零相关线性分析研究[J]. 密码学报，2014，1(3)：296-310.

[11] YI W T, CHEN S Z. Multidimensional zero-correlation linear attacks on Fox block cipher[J]. Journal of Cryptologic Research, 2015, 2(1): 27-39. (in Chinese)
伊文坛，陈少真. Fox 密码的多维零相关线性分析[J]. 密码学报，2015，2(1)：27-39.

[12] JIN C H. Spectra characterizations of nonsingular feedback polynomials over finite fields and residue class rings[J]. Journal of China Institute of Communications, 2000, 21(1): 74-77. (in Chinese)
金晨辉. 有限域和剩余类环上非奇异反馈多项式的谱刻划[J]. 通信学报，2000，21(1)：74-77.

[13] ZHANG P, LI R L, LI C. New square attack on Zodiac[J]. Journal of Electronics & Information Technology, 2010, 32(11): 2790-2794. (in Chinese)
张鹏，李瑞林，李超. Zodiac 算法新的 Square 攻击[J]. 电子与信息学报，2010，32(11)：2790-2794.

[14] LI C, WEI Y C. New impossible differential cryptanalysis of Zodiac[J]. Journal of National University of Defense Technology, 2012, 34(5): 132-136. (in Chinese)
李超，魏悦川. Zodiac 算法新的不可能差分攻击[J]. 国防科技大学学报，2012，34(5)：132-136.

[15] HONG D, SUNG J, MORIAI S, et al. Impossible differential cryptanalysis of Zodiac[J]. IEICE Transactions on Fundamentals of Electronics, Communications and Computers, 2002, 85(1): 38-43.