Zodiac 算法新的 Square 攻击

张 鹏[①] 李瑞林[①] 李 超[①②]
[①](国防科技大学理学院数学与系统科学系 长沙 410073)
[②](中国科学院软件所信息安全国家重点实验室 北京 100190)

摘 要：该文重新评估了 Zodiac 算法抗 Square 攻击的能力。Zodiac 算法存在 8 轮 Square 区分器，该文首先根据算法的结构特性，给出了 Zodiac 的 4 个等价结构，而后利用等价结构得到了两个新的 9 轮 Square 区分器。利用新的区分器，对不同轮数的 Zodiac 算法实施了 Square 攻击，对 12 轮，13 轮，14 轮，15 轮和 16 轮 Zodiac 的攻击复杂度分别为 $2^{37.3}$，$2^{62.9}$，$2^{96.1}$，$2^{137.1}$ 和 $2^{189.5}$ 次加密运算，选择明文数分别为 $2^{10.3}$，2^{11}，$2^{11.6}$，$2^{12.1}$ 和 $2^{12.6}$。结果表明：完整 16 轮 192 bit 密钥的 Zodiac 算法是不抗 Square 攻击的。

关键词：密码学；Zodiac；等价结构；区分器；Square 攻击
中图分类号：TN918 **文献标识码**： A **文章编号**：1009-5896(2010)11-2790-05
DOI: 10.3724/SP.J.1146.2010.00388

New Square Attack on Zodiac

Zhang Peng[①] Li Rui-lin[①] Li Chao[①②]
[①](*Department of Mathematics and System Science*, *Science College*, *National University of Defense Technology*, *Changsha* 410073, *China*)
[②](*State Key Laboratory of Information Security*, *Institute of Software*, *Chinese Academy of Sciences*, *Beijing* 100190, *China*)

Abstract: This paper re-evaluates the security of Zodiac against Square attacks. There are 8-round Square distinguishers of Zodiac. In this paper, four equivalent structures of Zodiac are given, based on which two new 9-round distinguishers are proposed. Then by using the 9-round Square distinguishers, Square attacks are applied to 12/13/14/15/16-round Zodiac with time complexities being $2^{37.3}$, $2^{62.9}$, $2^{96.1}$, $2^{137.1}$, $2^{189.5}$, and data complexities being $2^{10.3}$, 2^{11}, $2^{11.6}$, $2^{12.1}$, $2^{12.6}$, respectively. Additionally, these attacks show that full 16-round Zodiac-192 is not immune to Square attack.

Key words: Cryptography; Zodiac; Equivalent structures; Distinguisher; Square attack

1 引言

Square 攻击是继差分密码分析和线性密码分析后，密码学界公认的一种比较有效的密码分析方法[1]，它是 Daemen 等人[1]在 FSE 1997 针对 Square 密码提出的一种新的攻击方法，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 攻击从其出现就受到了密码学界的广泛关注。近几年，利用该攻击思想，学术界对 Camellia，CLEFIA，HIGHT 和 3D 等分组密码算法的安全性进行了评估，取得了较好的分析结果[2−5]。

Zodiac 密码是由韩国学者 Lee 等人[6]提出的一个 Feistel 型迭代分组密码算法，其分组长度为 128 bit，算法支持 128 bit，192 bit，和 256 bit 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 Square 攻击的能力[7,8]，其中，Ji 等人[8]指出：Zodiac 算法存在 8 轮 Square 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 Square 攻击。

本文进一步研究了 Zodiac 算法抗 Square 攻击的能力。文章首先给出了 Zodiac 的 4 个等价结构，进而利用等价结构得到了两个新的 9 轮 Square 区分器，利用得到的 9 轮区分器可以成功对 14 轮 Zodiac-128，以及完整轮数的 Zodiac-192 和 Zodiac-256 实施 Square 攻击，这说明 Zodiac-192 和 Zodiac-256 对 Square 攻击都是不免疫的。

2010-04-16 收到，2010-07-09 改回
国家自然科学基金(60803156)和信息安全国家重点实验室开放基金(01-07)资助课题
通信作者：张鹏 cheetahzhp@gmail.com

2　Zodiac 算法

2.1 算法符号说明如表 1 所示。

表 1 算法符号及其含义

符号	含义
$L=(l_0,l_1,l_2,l_3,l_4,l_5,l_6,l_7)\in(\mathbb{F}_2^8)^8$	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 轮输出的左半部分
$R_i=(r_{i,0},r_{i,1},r_{i,2},r_{i,3},r_{i,4},r_{i,5},r_{i,6},r_{i,7})\in(\mathbb{F}_2^8)^8$	第 i 轮输出的右半部分
$K_i=(k_{i,0},k_{i,1},k_{i,2},k_{i,3},k_{i,4},k_{i,5},k_{i,6},k_{i,7})\in(\mathbb{F}_2^8)^8$	第 i 轮的轮密钥
$K_i^*=(k_{i,0}^*,k_{i,1}^*,k_{i,2}^*,k_{i,3}^*,k_{i,4}^*,k_{i,5}^*,k_{i,6}^*,k_{i,7}^*)\in(\mathbb{F}_2^8)^8$	第 i 轮的等价轮密钥 ($K_i^*=P(K_i)$)
$CL=(Cl_0,Cl_1,Cl_2,Cl_3,Cl_4,Cl_5,Cl_6,Cl_7)\in(\mathbb{F}_2^8)^8$	输出密文的左半部分
$CR=(Cr_0,Cr_1,Cr_2,Cr_3,Cr_4,Cr_5,Cr_6,Cr_7)\in(\mathbb{F}_2^8)^8$	输出密文的右半部分
$K_0(K_{17})$	初始(输出)白化密钥

2.2 算法描述

由于初始置换不影响本文的分析，因此本文不考虑初始置换的影响。设 Zodiac 算法的明文输入为 $P=(L,R)\in(\mathbb{F}_2^{64})^2$，则有 $L_0=L\oplus K_0$，$R_0=R$，且 Zodiac 算法第 1 到 16 轮的变换表示如下：

$$\begin{cases}L_i=F(L_{i-1}\oplus K_i)\oplus R_{i-1},\\ R_i=L_{i-1},\end{cases}\quad(1\le i\le 16)$$

$C=(CL,CR)=(R_{16}\oplus K_{17},L_{16})$ 即为对应的密文。

算法的轮函数定义为 $F(X)=S(P(X))$，其中 P 将 $X=(x_0,x_1,x_2,x_3,x_4,x_5,x_6,x_7)$ 变换为 $Z=(z_0,z_1,z_2,z_3,z_4,z_5,z_6,z_7)$：

$$z_0=x_2\oplus x_3\oplus x_4,\quad z_1=x_0\oplus x_1,\quad z_2=x_1\oplus x_2,$$
$$z_3=x_2\oplus x_3,\quad z_4=x_6\oplus x_7\oplus x_0,\quad z_5=x_4\oplus x_5,$$
$$z_6=x_5\oplus x_6,\quad z_7=x_6\oplus x_7$$

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

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

其中 S_1 与 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，这里不再介绍密钥扩展算法。

3　Zodiac 算法的等价结构

3.1 等价结构 1($P\to K\to S$)

Zodiac 算法轮函数的具体结构为 $K\to P\to S$，设轮函数的输入为 X，则其输出可表示为

$$S(P(X\oplus K))=S(P(X)\oplus P(K))=S(P(X)\oplus K^*)$$

其中 $K^*=P(K)$，于是利用等价密钥原结构可以等价为 $P\to K^*\to S$。为了叙述的方便，不妨将等价结构 1 记为 $P\to K\to S$(K 为等价密钥)，具体流程见图 1(a)。

3.2 等价结构 2, 3, 4

在 SAC 2005 上，Duo 等人[2]首次提出了 Camellia 算法的等价结构，并且应用等价结构改进了 Camellia 算法的 Square 攻击。下面我们将针对 Zodiac 算法的具体结构特点，给出 Zodiac 算法的几个等价结构，等价结构的具体流程见图 1(b)，1(c)，1(d)。

定理 1　Zodiac 算法的等价结构 1 与结构 2，3，4 均等价。

证明　这里只给出结构 1 与结构 3 等价的证明。

设 L_{i-1}，R_{i-1} 分别表示结构 1 中第 i 轮输入的左右两部分，L_{i-1}^*，R_{i-1}^* 分别表示结构 3 中第 i 轮输入的左右两部分，K_i 表示第 i 轮的密钥。

在结构 1 与结构 3 的第 i 轮中取相同的输入，即令 $L_{i-1}=L_{i-1}^*$，$R_{i-1}=R_{i-1}^*$，则在结构 1 中，有

$$L_i=R_{i-1}\oplus S(P(L_{i-1})\oplus K_{i-1}),\ R_i=L_{i-1}$$
$$L_{i+1}=R_i\oplus S(P(L_i)\oplus K_i)$$
$$=L_{i-1}\oplus S(P(L_i)\oplus K_i)\quad R_{i+1}=L_i$$

在结构 3 中，有

$$L_i^*=P(R_{i-1}^*)\oplus P(S(P(L_{i-1}^*)\oplus K_{i-1}))$$
$$=P(R_{i-1}\oplus S(P(L_{i-1})\oplus K_{i-1}))=P(L_i)$$
$$R_i^*=L_{i-1}^*=L_{i-1}=R_i$$
$$L_{i+1}^*=R_i^*\oplus S(L_i^*\oplus K_i)=R_i\oplus S(P(L_i)\oplus K_i)=L_{i+1}$$
$$R_{i+1}^*=P^{-1}(L_i^*)=L_i=R_{i+1}$$

因此，对任意相同的输入结构 1 与结构 3 均能得到相同的加密结果，即结构 1 与结构 3 等价，同理可证结构 1 与结构 2，4 等价。　　证毕

4　Zodiac 算法基于等价结构的 Square 攻击

4.1 Zodiac 算法新的 9 轮 Square 区分器

在文献[8]中，作者给出了 Zodiac 算法的如下两个 8 轮 Square 区分器。

(a)　$(C,C,C,C,C,C,C,C\parallel C,A,C,C,C,C,C,C)$
$\xrightarrow{8\text{ round}}(?,?,?,?,?,?,?,?\parallel ?,?,?,?,?,?,?,A)$

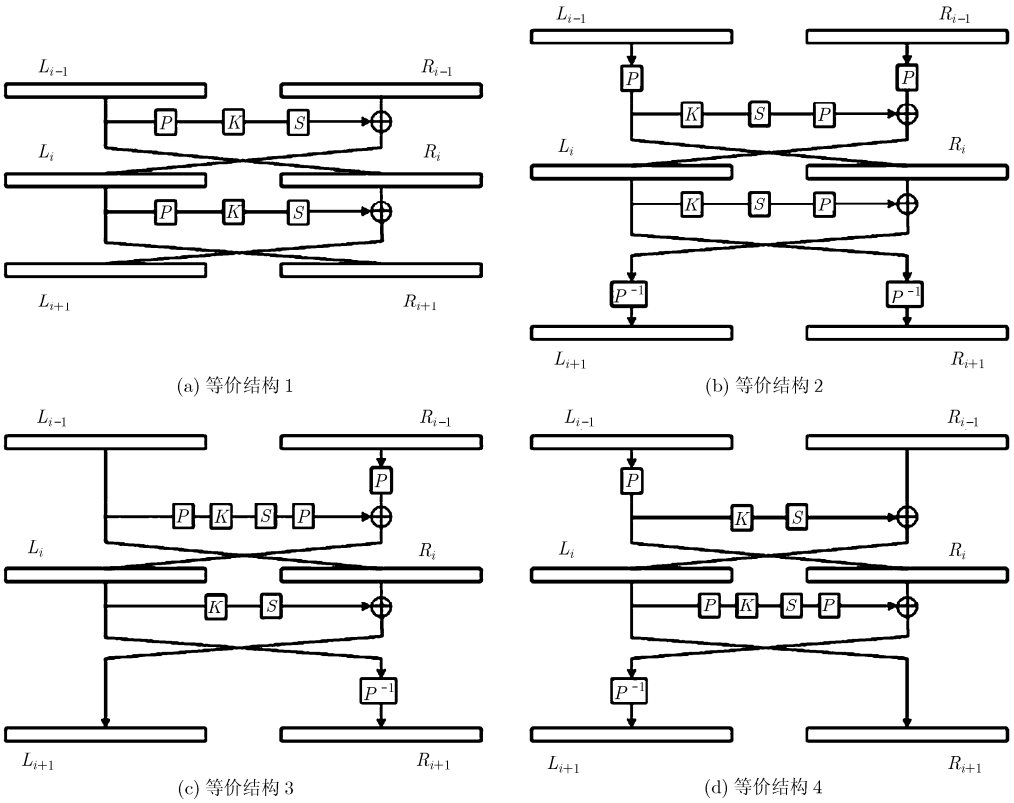
(b) $(C,C,C,C,C,C,C,C \,\|\, C,C,C,C,C,A,C,C) \xrightarrow{8\ \text{round}} (?,?,?,A,?,?,?,? \,\|\, ?,?,?,?,?,?,?,?)$

如果采用 Zodiac 算法的等价结构 3，并选取合适的输入明文组，则根据每轮输出的具体情况，可以得到两个新的 9 轮 Square 区分器。

定理 2 Zodiac 算法存在如下两个 9 轮 Square 区分器(区分器(a^*)的具体形式见表 2)。

(a*) $(C,C,C,C,C,C,C,C\|C,A,A\oplus C,A\oplus C,C,C,C,C) \xrightarrow{9\ \text{round}} (?,?,?,?,?,?,?,?,? \,\|\, ?,?,?,?,?,?,?,?,A)$

(b*) $(C,C,C,C,C,C,C,C \,\|\, C,C,C,C,C,A,A\oplus C,$



(a) 等价结构 1　(b) 等价结构 2

(c) 等价结构 3　(d) 等价结构 4

图 1 Zodiac 算法的 4 个等价结构(图中 K 均为等价密钥)

表 2 Zodiac 算法的 9 轮 Square 区分器(a^*)

$(L\|\|R)$	$(C,\ C,\ C,\ C,\ C,\ C,\ C,\ C)$	轮函数	$(C,\ A,\ A\oplus C,\ A\oplus C,\ C,\ C,\ C,\ C)$
			P
$(L_0\|\|R_0)$	$(C,\ C,\ C,\ C,\ C,\ C,\ C,\ C)$	$P \to K_1^* \to S \to P$	$(C,\ A,\ C,\ C,\ C,\ C,\ C,\ C)$
$(L_1\|\|R_1)$	$(C,\ A,\ C,\ C,\ C,\ C,\ C,\ C)$	$K_2^* \to S$	$(C,\ C,\ C,\ C,\ C,\ C,\ C,\ C)$
$(L_2\|\|R_2)$	$(C,\ A,\ C,\ C,\ C,\ C,\ C,\ C)$	$P \to K_3^* \to S \to P$	$(C,\ A,\ C,\ C,\ C,\ C,\ C,\ C)$
$(L_3\|\|R_3)$	$(A,\ B,\ B,\ A,\ C,\ C,\ C,\ C)$	$K_4^* \to S$	$(C,\ A,\ C,\ C,\ C,\ C,\ C,\ C)$
$(L_4\|\|R_4)$	$(A,\ ?,\ ?,\ A,\ C,\ C,\ C,\ C)$	$P \to K_5^* \to S \to P$	$(A,\ B,\ B,\ A,\ C,\ C,\ C,\ C)$
$(L_5\|\|R_5)$	$(\ ?,\ ?,\ ?,\ ?,\ ?,\ A,\ C,\ C)$	$K_6^* \to S$	$(A,\ ?,\ ?,\ A,\ C,\ C,\ C,\ C)$
$(L_6\|\|R_6)$	$(\ ?,\ ?,\ ?,\ ?,\ ?,\ A,\ C,\ C)$	$P \to K_7^* \to S \to P$	$(\ ?,\ ?,\ ?,\ ?,\ ?,\ A,\ C,\ C)$
$(L_7\|\|R_7)$	$(\ ?,\ ?,\ ?,\ ?,\ ?,\ ?,\ ?,\ A)$	$K_8^* \to S$	$(\ ?,\ ?,\ ?,\ ?,\ ?,\ A,\ C,\ C)$
$(L_8\|\|R_8)$	$(\ ?,\ ?,\ ?,\ ?,\ ?,\ ?,\ ?,\ A)$	$P \to K_9^* \to S \to P$	$(\ ?,\ ?,\ ?,\ ?,\ ?,\ ?,\ ?,\ A)$
$(L_9\|\|R_9)$	$(\ ?,\ ?,\ ?,\ ?,\ ?,\ ?,\ ?,\ ?)$	$K_{10}^* \to S$	$(\ ?,\ ?,\ ?,\ ?,\ ?,\ ?,\ ?,\ A)$
			P^{-1}
$(L_{10}\|\|R_{10})$	$(\ ?,\ ?,\ ?,\ ?,\ ?,\ ?,\ ?,\ ?)$		$(\ ?,\ ?,\ ?,\ ?,\ ?,\ ?,\ ?,\ ?)$

注：A 表示活跃字节；C 表示稳定字节，即为常数；B 表示平衡字节；? 表示字节的性质无法预测。区分器输入中的 3 个活跃字节表示同时取相同的值进行遍历。

$A \oplus C) \xrightarrow{9\ \text{round}} (?,?,?,A,?,?,?,? \,\|\, ?,?,?,?,?,?,?,?)$

此外，我们还在个人计算机上对上述两个 9 轮 Square 区分器进行了编程实现，结果进一步验证了上述区分器的正确性。

4.2 对不同轮数 Zodiac 算法的 Square 攻击

利用基于等价结构的 9 轮 Square 区分器，可以对不同轮数的 Zodiac 算法实施 Square 攻击。图 2 给出了 Zodiac 算法基于区分器(a^*)的不同轮数 Square 攻击的具体过程，其中 x 遍历 $\mathbb{F}_2^8$，c_i，d_i，e_i 和 f_i 均为常数。在下文的攻击过程中，不考虑白化密钥的影响，且恢复的都是等价密钥 $K^*(K^*=P(K))$。

由于本文的攻击是基于等价结构做的，而且需要在开始添加一轮，因此在攻击不同轮数时，需要配合使用等价结构 3 和 4，如在对 12，14 和 16 轮的算法实施 Square 攻击时，本文的加密过程采用了等价结构 4，而中间的 9 轮区分器采用的却是等价结构 3；在对 11，13 和 15 轮的算法实施攻击时，从第 2 轮开始可以看做是等价结构 3，即在加密过程中需要对 P 和 P^{-1} 的位置进行适当调整。

下面，我们以基于区分器(a^*)的 12 轮 Square 攻击为例，详细介绍 Square 攻击的具体步骤以及相应的复杂度计算方法：

步骤 1　猜测第 1 轮密钥中的 $k_{1,1}^*$。

步骤 2　选取满足如下条件的明文组进行 12 轮加密：

$$L=(c_0, x\oplus c_1, x\oplus c_2, x\oplus c_3, c_4, c_5, c_6, c_7);$$

$$R=(d_0, S_2((x\oplus c_0\oplus c_1)\oplus k_{1,1}^*)\oplus d_1, d_2, d_3, d_4, d_5, d_6, d_7)$$

其中 x 遍历 $\mathbb{F}_2^8$，c_i 和 d_i 均为常数，相应的密文记为 $L_{12}\,\|\,R_{12}$。若 $k_{1,1}^*$ 的猜测值正确，则第 2 轮的输入即满足 9 轮 Square 区分器(a^*)的输入形式，从而第 10 轮的输出 $r_{10,7}$ 为平衡字节。

步骤 3　猜测密钥 $k_{11,7}^*$，$k_{12,6}^*$ 和 $k_{12,7}^*$，利用步骤 1 中得到的密文组 $L_{12}\,\|\,R_{12}$ 和这些猜测的密钥，求得第 10 轮的输出字节 $r_{10,7}$ 为

$$\begin{aligned} r_{10,7} &= S_2(l_{10,7}\oplus k_{11,7}^*)\oplus l_{11,7} \\ &= S_2(r_{11,7}\oplus k_{11,7}^*)\oplus(r_{12,6}\oplus r_{12,7}) \\ &= S_2(S_2(r_{12,5}\oplus r_{12,7}\oplus k_{12,7}^*)\oplus S_1(r_{12,4}\oplus r_{12,6} \\ &\quad \oplus k_{12,6}^*)\oplus l_{12,7}\oplus k_{11,7}^*)\oplus(r_{12,6}\oplus r_{12,7}) \end{aligned}$$

验证 $r_{10,7}$ 的平衡性，若满足平衡性，则猜测的 $k_{1,1}^*$，$k_{11,7}^*$，$k_{12,6}^*$ 和 $k_{12,7}^*$ 分别为正确密钥的候选值，否则为错误密钥，舍弃。

步骤 4　重复以上 3 个步骤，直到正确密钥唯一确定。

对 12 轮 Zodiac 算法的 Square 攻击共需猜测 4 个字节的密钥，即 $k_{1,1}^*$，$k_{11,7}^*$，$k_{12,6}^*$ 和 $k_{12,7}^*$。对于错

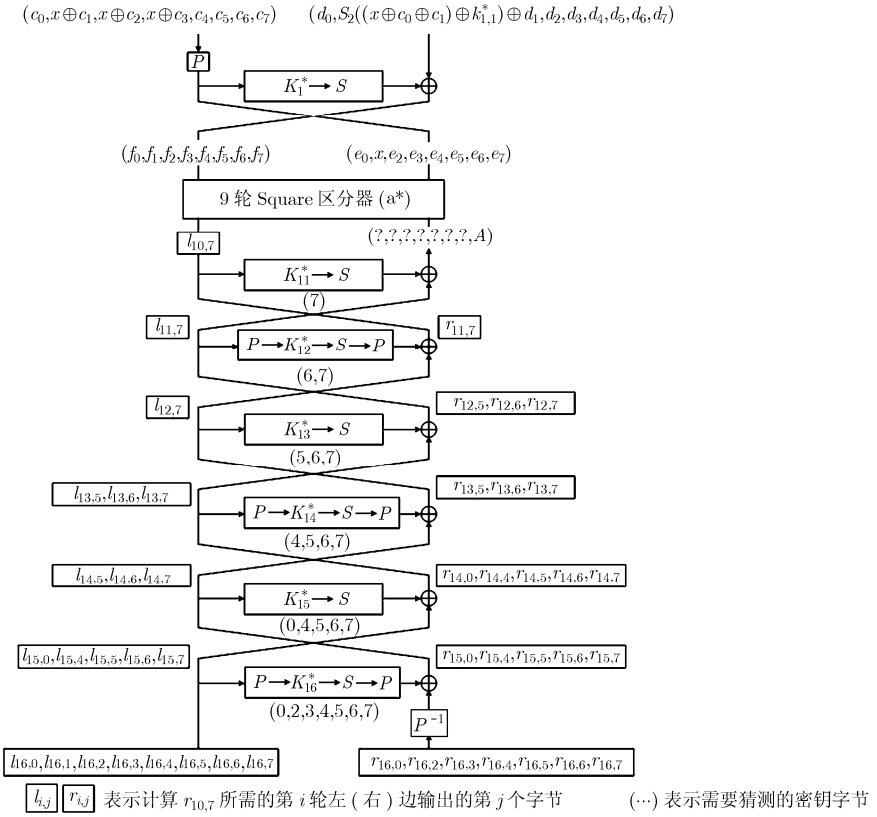


图 2 对不同轮数 Zodiac 算法的 Square 攻击

误的密钥值，满足$r_{10,7}$平衡性的概率为2^{-8}，因此经过一个明文结构淘汰后，剩下的错误密钥的数目为$(2^{32}-1)\times 2^{-8}\approx 2^{24}$。假设选择了$N$个明文结构，则剩余的错误密钥个数为$(2^{32}-1)\times 2^{-8N}$，因此5个正确的明文结构即可淘汰所有的错误密钥($(2^{32}-1)\times 2^{-8N}<1$)，从而选择明文数为$5\times 2^8\approx 2^{10.3}$。对每个猜测值，计算$r_{10,7}$需要3次查表运算，因此攻击共需进行$2^{32}\times 2^{10.3}\times 3$次查表运算，又因为12轮Zodiac算法共有$8\times 12=96$次查表运算，因此对12轮Zodiac算法Square攻击的时间复杂度为$2^{32}\times 2^{10.3}\times 3/96\approx 2^{37.3}$次加密运算。

在12轮Square攻击的基础上，如果在末尾依次增加几轮，可以得到Zodiac算法13–16轮的Square攻击，下面仅给出各轮攻击需要猜测的密钥以及攻击的复杂度(见表3)。由攻击复杂度一栏可知，本文的Square攻击大大优于文献[8]中给出的攻击，结果还表明，完整16轮Zodiac-192对Square攻击是不免疫的。

5 结束语

本文对Zodiac算法的安全性进行了进一步的评估，通过对算法等价结构的研究，首先找到了算法两个新的9轮Square区分器，然后对不同轮数的Zodiac成功实施了Square攻击，结果显示，对Zodiac-192而言，16轮并不足以使得算法可以抵抗Square攻击。另外，本文结果还说明：对轮函数为SP结构的Feistel密码，等价结构可以较好的改进算法的Square攻击，因此，在设计轮函数为SP结构的Feistel密码时，必须充分考虑等价结构对算法抗Square攻击的影响。如何将基于等价结构的分析方法应用到其他SP型Feistel密码中将是下一步研究的主要内容。

表 3 Zodiac 算法不同轮数 Square 攻击需猜测的密钥和攻击复杂度

轮数	猜测的密钥	时间复杂度本文/文献[8]	数据复杂度本文/文献[8]
12	$k^*_{1,1}, k^*_{11,7}, k^*_{12,6}, k^*_{12,7}$	$2^{37.3}/2^{92.3}$	$2^{10.3}/2^{12.3}$
13	$k^*_{1,1}, k^*_{11,7}, k^*_{12,6}, k^*_{12,7}, k^*_{13,5}, k^*_{13,6}, k^*_{13,7}$	$2^{62.9}/2^{124.8}$	$2^{11}/2^{15.6}$
14	$k^*_{1,1}, k^*_{11,7}, k^*_{12,6}, k^*_{12,7}, k^*_{13,5}, k^*_{13,6}, k^*_{13,7}, k^*_{14,4}, k^*_{14,5}, k^*_{14,6}, k^*_{14,7}$	$2^{96.1}/2^{157.2}$	$2^{11.6}/2^{16}$
15	$k^*_{1,1}, k^*_{11,7}, k^*_{12,6}, k^*_{12,7}, k^*_{13,5}, k^*_{13,6}, k^*_{13,7}, k^*_{14,4}, k^*_{14,5}, k^*_{14,6}, k^*_{14,7}, k^*_{15,0}, k^*_{15,4}, k^*_{15,5}, k^*_{15,6}, k^*_{15,7}$	$2^{137.1}/2^{189.5}$	$2^{12.1}/2^{16.3}$
16	$k^*_{1,1}, k^*_{11,7}, k^*_{12,6}, k^*_{12,7}, k^*_{13,5}, k^*_{13,6}, k^*_{13,7}, k^*_{14,4}, k^*_{14,5}, k^*_{14,6}, k^*_{14,7}, k^*_{15,0}, k^*_{15,4}, k^*_{15,5}, k^*_{15,6}, k^*_{15,7}, k^*_{16,0}, k^*_{16,2}, k^*_{16,3}, k^*_{16,4}, k^*_{16,5}, k^*_{16,6}, k^*_{16,7}$	$2^{189.5}/2^{221.7}$	$2^{12.6}/2^{16.5}$

参 考 文 献

[1] Daemen J, Knudsen L R, and Rijmen V. The block cipher SQUARE[C]. FSE 1997, Springer-Verlag, 1997, LNCS, 1267: 149–165.

[2] Duo L, Li C, and Feng K. New observation on Camellia[C]. SAC 2005, Springer-Verlag, 2006, LNCS, 3897: 51–64.

[3] 唐学海, 李超, 谢端强. CLEFIA 密码的 Square 攻击[J]. 电子与信息学报, 2009, 31(9): 2260–2263.
Tang X H, Li C, and Xie D Q. Square attack on CLEFIA[J]. *Journal of Electronics & Information Technology*, 2009, 31(9): 2260–2263.

[4] Zhang P, Sun B, and Li C. Saturation attack on the block cipher HIGHT[C]. CANS 2009, Springer-Verlag, 2009, LNCS, 5888: 76–86.

[5] 王美一, 唐学海, 李超等. 3D 密码的 Square 攻击[J]. 电子与信息学报, 2010, 32(1): 157–161.
Wang M Y, Tang X H, and Li C, *et al*.. Square attacks on 3D cipher[J]. *Journal of Electronics & Information Technology*, 2010, 32(1): 157–161.

[6] Lee C, Jun K, and Jung M, *et al*.. Zodiac version 1.0 (revised) architecture and specification. Standardization Workshop on Information Security Technology, Korean Contribution on MP18033, ISO/IEC JTC1/SC27 N2563, 2000. http://www.kisa.or.kr/seed/index.html.

[7] Hong D, Sung J, and Moriai S, *et al*.. Impossible differential cryptanalysis of Zodiac[C]. FSE 2001, Springer-Verlag, 2002, LNCS, 2355: 300–311.

[8] Ji W and Hu L. Square attack on reduced-round Zodiac cipher[C]. ISPEC 2008, Springer- Verlag, 2008, LNCS, 4991: 377–391.

张 鹏： 男，1983 年生，博士生，研究方向为编码密码理论及其应用.

李瑞林： 男，1982 年生，博士生，研究方向为编码密码理论及其应用.

李 超： 男，1966 年生，博士生导师，教授，研究方向为编码密码理论及其应用.