减轮 Deoxys-BC 和 RAIN 算法的积分攻击

杜小妮[1,2]，关雪莹[1]，余恬[1]，梁丽芳[1]
（1. 西北师范大学数学与统计学院，甘肃 兰州 730070；2. 西北师范大学密码技术与数据分析重点实验室，甘肃 兰州 730070）

摘 要：考虑调柄对可调分组密码算法的影响，将零相关线性分析与积分攻击结合，利用部分和技术，对 Deoxys-BC 和 RAIN 算法进行积分攻击。通过研究调柄的掩码传播规律，构造 Deoxys-BC-256 的 176 类 5.5 轮零相关线性区分器以及 Deoxys-BC-384 的 176 类 6.5 轮零相关线性区分器。基于零相关线性区分器与积分区分器的联系，结合等价密钥技术，分别实现 Deoxys-BC 算法两个版本的 10 轮和 12 轮积分攻击。另外，构造 RAIN 算法的 48 类 6 轮零相关线性区分器，并将其转换为 6 轮积分区分器。在不考虑白化密钥的情况下，对 RAIN 算法的两个版本进行 10 轮积分攻击。结果表明，与已有研究结果相比，所提攻击方案所需复杂度显著降低。

关键词：可调分组密码；Deoxys-BC；RAIN；积分攻击
中图分类号：TP309.7
文献标志码：A
DOI：10.11959/j.issn.1000–436x.2026028

Integral attacks on reduced-round Deoxys-BC and RAIN algorithms

Du Xiaoni[1,2], Guan Xueying[1], Yu Tian[1], Liang Lifang[1]
1. College of Mathematics and Statistics, Northwest Normal University, Lanzhou 730070, China
2. Key Laboratory of Cryptography and Data Analytics, Northwest Normal University, Lanzhou 730070, China

Abstract: Considering the impact of tweakeys on tweakable block cipher algorithms, achieved integral attacks on Deoxys-BC and RAIN algorithms by combining zero-correlation linear cryptanalysis with integral attacks and utilizing partial-sum technique. 176 types of 5.5-round zero-correlation linear distinguishers for Deoxys-BC-256 and 176 types of 6.5-round zero-correlation linear distinguishers for Deoxys-BC-384 were constructed by taking the mask propagation rules of tweakeys into consideration. Based on the relationship between zero-correlation linear distinguishers and integral distinguishers, achieved 10-round and 12-round integral attacks on the two versions of Deoxys-BC respectively by combining equivalent key technique. Then, 48 types of 6-round zero-correlation linear distinguishers for RAIN algorithm were constructed, and converted them into 6-round integral distinguishers. Without considering the whitening key, 10-round integral attacks were achieved on both versions of RAIN algorithm. The results show that the complexities of the proposed attack scheme are significantly reduced compared with those of the existing ones.

Keywords: tweakable block ciphers, Deoxys-BC, RAIN, integral attack

收稿日期：2025–08–16；**修回日期：**2026–01–29
通信作者：关雪莹，gggxyggg@126.com
基金项目：国家自然科学基金资助项目（No.62172337, No.62562055）；甘肃省自然科学基金重点资助项目（No.23JRRA685）；甘肃省基础研究创新群体基金资助项目（No.23JRRA684）
Foundation Items： The National Natural Science Foundation of China (No.62172337, No.62562055), The Key Project of Gansu Natural Science Foundation (No.23JRRA685), The Funds for Innovative Fundamental Research Group Project of Gansu Province (No.23JRRA684)

0 引言

随着传感器技术、物联网和分布式系统的快速发展，智能硬件已经深入智能家居、工业控制、医疗监测等领域。这些设备数量多、分布广且复杂性高，传统密码算法已无法满足其安全性需求。为了保证智能硬件在资源受限环境下安全通信，轻量级分组密码算法应运而生。其中，存在额外输入调柄的密码算法被称为轻量级可调分组密码算法，如Deoxys-BC[1]和RAIN[2]等，它们的出现为分组密码算法的设计提供了灵活性和安全性。

Deoxys-BC算法是Jean等[1]设计的轻量级可调分组密码算法，分组长度为128 bit，可调密钥支持256 bit和384 bit，迭代轮数分别为14轮和16轮。轻量级可调分组密码算法RAIN由曹梅春等[2]提出，支持64 bit和128 bit两种分组长度，对应的迭代轮数分别为30轮和36轮，且密钥长度、调柄长度和分组长度均相同。目前对这两种算法的安全性分析主要包括差分分析[2]、不可能差分分析[3-4]、零相关线性分析[5]、中间相遇攻击[6]、Boomerang攻击[7]、不可能Boomerang攻击[8]和Rectangle攻击[9]等。

零相关线性分析的概念由Bogdanov等[10]提出，其主要思想是根据线性掩码的传播规律，构造相关度为0的线性逼近来区分分组密码算法与随机置换，随后被广泛应用于分组密码算法的安全性分析[11-12]。Leander等[13]的研究结果表明，添加由线性扩展得到的调柄并不会影响掩码的传播规律，但在考虑调柄时，搜索到的零相关线性逼近的轮数更多。Knudsen等[14]提出了积分攻击，其原理是固定算法输入的某些比特，其余比特活跃，从而使输出的特定比特保持平衡。近年来，积分攻击受到了学者的广泛关注[15]。值得一提的是，Ankele等[16]将零相关线性分析与积分攻击相结合，对具有线性扩展方案的高通认证随机消息认证码（qualcomm authenticated random message authentication code, QA-RMA）算法进行了密钥恢复攻击。

通过对文献[3-9]的研究发现，当前针对Deoxys-BC与RAIN算法的安全性分析虽已涵盖多种分析方法，但积分攻击这一重要分析方法尚未得到应用。另外，通过调柄的掩码传播规律来构造这两个算法区分器的研究也尚属空白。鉴于此，本文在考虑调柄对可调分组密码算法影响的情形下，将零相关线性分析与积分攻击相结合，并利用部分和技术[17]，首次对Deoxys-BC和RAIN算法进行（选择调柄）积分攻击，结果如表1所示。本文主要贡献如下。

1) 根据调柄的掩码传播规律，构造Deoxys-BC-256的176类5.5轮零相关线性区分器以及Deoxys-BC-384的176类6.5轮零相关线性区分器，并得到对应的积分区分器。

2) 对1) 中的积分区分器分别向前扩展1轮、向

表1 算法分析结果

算法	轮数	复杂度			攻击方法	参考文献
		时间	数据	存储		
Deoxys-BC-256	9	2^{118}	2^{118}	2^{117}	不可能差分分析	文献[3]
	9	$2^{61.02}$	2^{58}	2^{40}	积分攻击	2.3节
	10	$2^{177.42}$	$2^{132.9}$	$2^{101.79}$	不可能Boomerang攻击	文献[8]
	10	$2^{191.02}$	$2^{60.3}$	2^{168}	积分攻击	2.3节
Deoxys-BC-384	12	$2^{329.7}$	$2^{135.3}$	2^{312}	不可能差分分析	文献[4]
	12	$2^{321.91}$	$2^{69.2}$	2^{296}	积分攻击	2.3节
RAIN-64	10	$2^{74.3}$	2^{62}	2^{66}	零相关线性分析	文献[5]
	10	$2^{119.19}$	$2^{52.8}$	2^{112}	积分攻击	3.3节
RAIN-128	8	2^{109}	2^{72}	2^{75}	中间相遇攻击	文献[6]
	8	$2^{97.58}$	$2^{97.6}$	2^{32}	积分攻击	3.3节
	10	2^{214}	2^{72}	2^{219}	中间相遇攻击	文献[6]
	10	$2^{239.02}$	$2^{100.8}$	2^{224}	积分攻击	3.3节

后扩展3.5轮和4.5轮，利用等价密钥技术，分别实现Deoxys-BC算法两个版本的10轮和12轮积分攻击。结果表明，Deoxys-BC-256的9轮积分攻击较文献[3]中的不可能差分分析时间复杂度显著降低，10轮积分攻击的数据复杂度远远低于文献[8]中的不可能Boomerang攻击，Deoxys-BC-384的12轮积分攻击的时间复杂度低于文献[4]中的不可能差分分析。

3) 根据算法的结构特性，构造RAIN算法的48类6轮零相关线性逼近，将其作为零相关线性区分器，结合零相关线性区分器与积分区分器的联系，得到RAIN算法的6轮积分区分器。

4) 在不考虑白化密钥的情况下，将3) 中的积分区分器分别向前扩展1轮和向后扩展3轮，对RAIN算法的两个版本进行10轮积分攻击。结果表明，RAIN-64的10轮积分攻击的数据复杂度较文献[5]中的零相关线性分析有所降低，且RAIN-128的8轮积分攻击的时间复杂度低于文献[6]中的中间相遇攻击。

1　基础知识

本节给出本文所需的符号，并介绍可调分组密码算法，以及零相关线性分析与积分攻击的相关理论。

1.1　符号说明

在本文中，除非另有说明，否则采用以下符号。

$\mathbb{N}^+$：正整数集；

$P(C)$：明（密）文；

$\mathbb{F}_2$：二元有限域；

$\mathbb{F}_2^n$：二元有限域$\mathbb{F}_2$上的n维向量空间，其中$n \in \mathbb{N}^+$；

$\langle a,b \rangle$：向量a与b的内积；

$a \| b$：向量a与b的级联；

T：主调柄；

K：主密钥；

$\#A$：集合A的基数；

$\mathbb{Z}_n$：集合$\{0,1,\cdots,n-1\}$。

1.2　可调分组密码算法

本节给出可调分组密码算法的定义与结构。Liskov等[18]提出了可调分组密码算法的概念，相比于传统分组密码算法$E: P \times K \to C$，$\mathbb{F}_2^n \times \mathbb{F}_2^k \to \mathbb{F}_2^n$，可调分组密码算法拥有一个额外的输入调柄$T \in \mathbb{F}_2^t$，记为$\overline{E}: P \times K \times T \to C$，$\mathbb{F}_2^n \times \mathbb{F}_2^k \times \mathbb{F}_2^t \to \mathbb{F}_2^n$，其中$n, k, t \in \mathbb{N}^+$。

可调密钥结构[19]可用来构造一个分组长度为n bit，密钥长度为k bit和调柄长度为t bit的可调分组密码算法，其中$n, k, t \in \mathbb{N}^+$。如图1所示，若把密钥K和调柄T看成一个整体TK，则可调密钥结构有两部分输入，分别为明文$P \in \mathbb{F}_2^n$和可调密钥$\mathrm{TK} \in \mathbb{F}_2^{t+k}$，并且可在轮函数、可调密钥更新函数和提取函数的协同作用下，输出密文$C \in \mathbb{F}_2^n$。其中，轮函数$f: \mathbb{F}_2^n \to \mathbb{F}_2^n$对密码状态进行迭代更新，可调密钥更新函数$h: \mathbb{F}_2^{t+k} \to \mathbb{F}_2^{t+k}$由主调柄生成轮调柄，提取函数$g: \mathbb{F}_2^{t+k} \to \mathbb{F}_2^n$提取轮调柄并将其合并到内部状态。

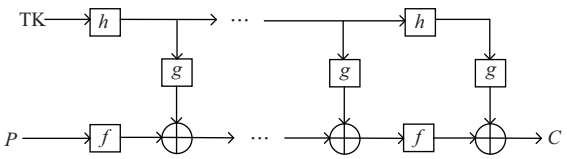

图1　可调密钥结构

叠加可调密钥结构[19]如图2所示，将可调密钥$\mathrm{TK} \in \mathbb{F}_2^{t+k}$分为$p = \dfrac{t+k}{n}$个$n$ bit的字符串，与明文$P \in \mathbb{F}_2^n$共同作为算法的输入。叠加可调密钥结构的函数h包括两个步骤，首先对由可调密钥TK得到的p个字符串进行相同的置换h'，其次分别进行线性变换α_i（当$1 \leqslant i \neq j \leqslant p$时有$\alpha_i \neq \alpha_j$）。函数$g$将每一轮函数$h$输出的$p$个字符串以及轮常数$C_i$与内部状态进行异或。

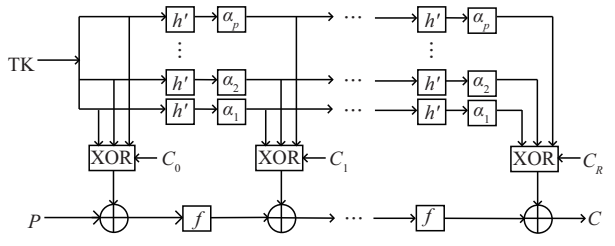

图2　叠加可调密钥结构（以TK-P为例）

1.3　可调分组密码算法的零相关线性逼近

本节介绍利用调柄的掩码传播规律构造可调分组密码算法的零相关线性逼近方法。

为了方便叙述，将线性掩码$\Gamma = \Gamma^0 \| \Gamma^1 \| \cdots \| \Gamma^{15} \in \mathbb{F}_2^n$记为如式(1)所示的$4 \times 4$矩阵。

$$\boldsymbol{\Gamma}=\begin{pmatrix}\Gamma^0 & \Gamma^1 & \Gamma^2 & \Gamma^3\\ \Gamma^4 & \Gamma^5 & \Gamma^6 & \Gamma^7\\ \Gamma^8 & \Gamma^9 & \Gamma^{10} & \Gamma^{11}\\ \Gamma^{12} & \Gamma^{13} & \Gamma^{14} & \Gamma^{15}\end{pmatrix} \tag{1}$$

其中，$\Gamma^i\in\mathbb{F}_2^{\frac{n}{16}}$，$0\leqslant i\leqslant 15$。

定义1　Γ序列[16]。对于一个$R\in\mathbb{N}^+$轮算法，若给定一对输入、输出掩码(Γ_0,Γ_R)，穷举所有可能的线性迹$(\Gamma_0,\Gamma_1,\cdots,\Gamma_R)$，那么每一个线性迹中都可提取出相应的序列$\left(\Gamma_1^{h(i)},\Gamma_2^{h^2(i)},\cdots,\Gamma_R^{h^R(i)}\right)\in\mathbb{F}_2^{\frac{n}{16}\times R}$，$0\leqslant i\leqslant 15$，该序列被称为$\Gamma$序列。

对于一个$R\in\mathbb{N}^+$轮算法，给定一对输入、输出掩码(Γ_0,Γ_R)，穷举线性迹$(\Gamma_0,\Gamma_1,\cdots,\Gamma_R)$的所有可能性，计算相应的异或值，可得到式(2)所示集合。

$$S^i=\left\{\bigoplus_{r=1}^{R}\Gamma_r^{h^r(i)}:\left(\Gamma_1^{h(i)},\Gamma_2^{h^2(i)},\cdots,\Gamma_R^{h^R(i)}\right)\in\mathbb{F}_2^{\frac{n}{16}\times R}\right\} \tag{2}$$

其中，Γ_r^i表示第r轮输出掩码的第i个单元格，h^r表示调用r次可调密钥更新函数h，且$1\leqslant r\leqslant R$，$0\leqslant i\leqslant 15$。若存在某个$0\leqslant i_0\leqslant 15$，使主调柄掩码$\Lambda^{i_0}\notin S^{i_0}$，则$(\Gamma_0,\Gamma_R)$为一个零相关线性逼近，如图3所示。

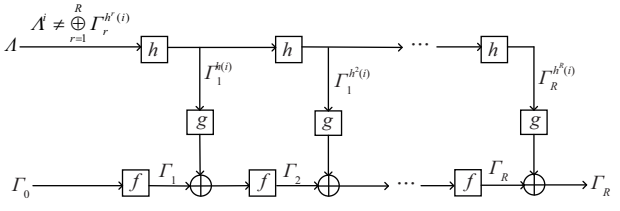

图3　R轮零相关线性逼近

为了更直观地判断输入、输出掩码(Γ_0,Γ_R)是否为一个零相关线性逼近，引入以下命题。

命题1[16]　如图3所示，给定一对输入、输出掩码(Γ_0,Γ_R)，通过观察主调柄掩码$\Lambda^i(0\leqslant i\leqslant 15)$与$(\Gamma_0,\Gamma_R)$所提取$\Gamma$序列的线性关系，若存在以下情形之一，则$(\Gamma_0,\Gamma_R)$为一个零相关线性逼近。

1) 存在一个$0\leqslant i_0\leqslant 15$，使$\Lambda^{i_0}\neq 0$，且对任意$1\leqslant r\leqslant R$，都有$\Gamma_r^{h^r(i_0)}=0$；

2) 存在一个$0\leqslant i_0\leqslant 15$，使$\Lambda^{i_0}=0$，且存在唯一的$1\leqslant r_0\leqslant R$，满足$\Gamma_r^{h^{r_0}(i_0)}\neq 0$。

由命题1可推广至叠加可调密钥结构（以TK-P为例），结论如下。

命题2[16]　如果存在一对输入、输出掩码(Γ_0,Γ_R)，通过观察$p\geqslant 2$个主调柄掩码$\Lambda_j^i(0\leqslant i\leqslant 15,1\leqslant j\leqslant p)$与$(\Gamma_0,\Gamma_R)$所提取$\Gamma$序列的线性关系，若存在以下情形之一，则$(\Gamma_0,\Gamma_R)$为一个零相关线性逼近。

1) 存在一个$(0\leqslant i_0\leqslant 15,1\leqslant j_0\leqslant p)$，使$\Lambda_{j_0}^{i_0}\neq 0$，且对任意$1\leqslant r\leqslant R$，都有$\Gamma_r^{h^r(i_0)}=0$；

2) 存在一个$0\leqslant i_0\leqslant 15$，使所有$\Lambda_j^{i_0}=0$，且至多存在$p$个$1\leqslant r_0\leqslant R$，满足$\Gamma_r^{h^{r_0}(i_0)}\neq 0$。

1.4　零相关线性区分器与积分区分器的联系

引理1[20]　设A为$\mathbb{F}_2^n$的子空间，A的对偶空间为$A^\perp=\{x\in\mathbb{F}_2^n|\langle\alpha,x\rangle=0,\forall\alpha\in A\}$。定义函数$F$:$\mathbb{F}_2^n\to\mathbb{F}_2^n$和$T_\lambda$:$A^\perp\to\mathbb{F}_2^n$，$T_\lambda(x)=F(x\oplus\lambda)$，$\lambda\in\mathbb{F}_2^n$，则对任意$\beta\in\mathbb{F}_2^n$，有$\sum_{\alpha\in A}(-1)^{\alpha\lambda}c_F(\alpha,\beta)=c_{T_\lambda}(0,\beta)$。

由引理1可知，对所有$\alpha\in A$，当$c_F(\alpha,\beta)=0$，即(α,β)为一对零相关线性掩码时，有$c_{T_\lambda}(0,\beta)=0$，从而得到定理1。

定理1[20]　设A为$\mathbb{F}_2^n$的子空间，定义函数F:$\mathbb{F}_2^n\to\mathbb{F}_2^n$。若存在$\beta\in\mathbb{F}_2^n\backslash\{\mathbf{0}\}$，对所有$\alpha\in A$，使$(\alpha,\beta)$是函数$F$的零相关线性逼近，则对所有$\lambda\in\mathbb{F}_2^n$，当$x$取遍$A^\perp$时，$\beta T_\lambda(x)$是平衡的，其中$\mathbf{0}$表示长度为$n$的全0比特串。

定理1表明，当$\beta\in\mathbb{F}_2^n\backslash\{\mathbf{0}\}$时，对所有$\alpha\in A$，若$(\alpha,\beta)$是函数$F$的零相关线性逼近，将其作为零相关线性区分器，则可获得相应的积分区分器。为了便于描述零相关线性区分器与积分区分器的联系，对任意向量$v=(v_0,v_1,\cdots,v_{n-1})\in\mathbb{F}_2^n$，本文定义集合$\mathrm{Supp}\,v=\{i|v_i\neq 0,0\leqslant i\leqslant n-1\}$。积分区分器的输入空间为$A^\perp$，由于当$\beta^j=0$时，$\beta^jT_\lambda(x)^j=0$，不影响输出的平衡性，所以输出在集合$\mathrm{Supp}\,\beta$对应比特位置处平衡，即$\oplus_{x\in A^\perp,j\in\mathrm{Supp}\,\beta}T_\lambda(x)^j=0$。由此可将零相关线性分析与积分攻击相结合，对分组密码算法进行密钥恢复攻击。

2　Deoxys-BC算法的积分攻击

本节首先介绍Deoxys-BC算法；其次，根据命题2构造Deoxys-BC-256的176类5.5轮零相关线性区分器以及Deoxys-BC-384的176类6.5轮零相关线

性区分器；最后，对Deoxys-BC算法的两个版本分别进行10轮和12轮积分攻击。

2.1　Deoxys-BC算法描述

Deoxys-BC算法由Jean等[1]提出，其分组长度为128 bit，可调密钥TK支持256 bit和384 bit，分别记为Deoxys-BC-256和Deoxys-BC-384，对应的迭代轮数R分别为14轮和16轮。每轮加密包含轮调柄加（add round tweakey, ART）和轮函数f两个步骤，其中轮函数由字节替换（sub cells, SC）、行移位（shift row, SR）和列混合（mix columns，MC）构成。

Deoxys-BC算法的加密流程如下。将第i轮的输入状态$X_i = x_i^0 \| x_i^1 \| \cdots \| x_i^{15} \in \mathbb{F}_2^{8\times 16}$记为

$$\boldsymbol{X}_i = \begin{pmatrix} x_i^0 & x_i^1 & x_i^2 & x_i^3 \\ x_i^4 & x_i^5 & x_i^6 & x_i^7 \\ x_i^8 & x_i^9 & x_i^{10} & x_i^{11} \\ x_i^{12} & x_i^{13} & x_i^{14} & x_i^{15} \end{pmatrix} \tag{3}$$

其中，$x_i^j \in \mathbb{F}_2^8$，$0 \leqslant i < R$，$R \in \{14,16\}$，$0 \leqslant j \leqslant 15$。

1) 轮调柄加（ART）：将轮调柄$T_i \in \mathbb{F}_2^{128}$与$X_i$进行异或得到$Y_i \in \mathbb{F}_2^{128}$，$0 \leqslant i < R$。

2) 字节替换（SC）：对于Y_i的每个字节，应用与高级加密标准（advanced encryption standard, AES）算法相同的8 bit S盒，得到状态$Z_i = z_i^0 \| z_i^1 \| \cdots \| z_i^{15} \in \mathbb{F}_2^{128}$，其中$z_i^j = \mathrm{SC}(y_i^j) \in \mathbb{F}_2^8$，$0 \leqslant i < R$，$0 \leqslant j \leqslant 15$。

3) 行移位（SR）：将Z_i的第l行向左循环移位l个字节得到状态$W_i \in \mathbb{F}_2^{128}$，$0 \leqslant i < R$，$l = 0,1,2,3$。

4) 列混合（MC）：W_i左乘可逆矩阵$\boldsymbol{M}$得到第i轮的输出状态$X_{i+1} \in \mathbb{F}_2^{128}$，即$X_{i+1} = \boldsymbol{M} \cdot W_i$，$0 \leqslant i < R$。特别地，算法最后一轮省略列混合操作。

$$\boldsymbol{M} = \begin{pmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{pmatrix}, \boldsymbol{M}^{-1} = \begin{pmatrix} E & B & D & 9 \\ 9 & E & B & D \\ D & 9 & E & B \\ B & D & 9 & E \end{pmatrix} \tag{4}$$

Deoxys-BC算法的调柄扩展算法如下。对于Deoxys-BC-256算法，将可调密钥记为$\mathrm{TK} = \mathrm{TK}_0^1 \| \mathrm{TK}_0^2 \in \mathbb{F}_2^{256}$，可得轮调柄$T_i = \mathrm{TK}_i^1 \oplus \mathrm{TK}_i^2 \oplus C_i$。对于Deoxys-BC-384算法，将可调密钥记为$\mathrm{TK} = \mathrm{TK}_0^1 \| \mathrm{TK}_0^2 \| \mathrm{TK}_0^3 \in \mathbb{F}_2^{384}$，可得轮调柄$T_i = \mathrm{TK}_i^1 \oplus \mathrm{TK}_i^2 \oplus \mathrm{TK}_i^3 \oplus C_i$。其中$\mathrm{TK}_{i+1}^1 = h(\mathrm{TK}_i^1)$，$\mathrm{TK}_{i+1}^2 = \mathrm{LFSR}_2(h(\mathrm{TK}_i^2))$，$\mathrm{TK}_{i+1}^3 = \mathrm{LFSR}_3(h(\mathrm{TK}_i^3))$，且LFSR表示线性反馈移位寄存器（linear feedback shift register）。

1) 置换h：$(0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15) \rightarrow (4,5,6,7,9,10,11,8,14,15,12,13,3,0,1,2)$。

2) LFSR_2：$(x_7 \| x_6 \| \cdots \| x_0) \rightarrow (x_6 \| x_5 \| \cdots \| x_0 \| x_7 \oplus x_5)$。类似地，有$\mathrm{LFSR}_3$：$(x_7 \| x_6 \| \cdots \| x_0) \rightarrow (x_0 \oplus x_6 \| x_7 \| x_6 \| \cdots x_5 \| x_1)$。

由于LFSR_2、LFSR_3和轮常数加操作均不影响线性掩码的传播规律，故在后文中，本文只考虑置换h。由此可得，Deoxys-BC算法结构符合命题2的条件。

以Deoxys-BC-256为例，算法的整体结构如图4所示。

2.2　Deoxys-BC算法的零相关线性区分器

本节根据命题2构造Deoxys-BC算法的零相关线性逼近，并将其作为零相关线性区分器。

命题3　设输入掩码$\alpha = \alpha^0 \| \alpha^1 \| \cdots \| \alpha^{15} \in \mathbb{F}_2^{8\times 16}$与输出掩码$\beta = \beta^0 \| \beta^1 \| \cdots \| \beta^{15} \in \mathbb{F}_2^{8\times 16}$分别满足某一组$\left(\alpha^{i_1}, \alpha^{i_2}, \alpha^{i_3}, \alpha^{i_4}, \alpha^{i_5}\right)$为0，其余字节活跃，某个$\beta^j$非零，其余字节为0，$j \in O$，$\#O = 11$，其中$i_1, i_2, i_3, i_4, i_5, O$的具体取值如表2所示，且$(i_1, i_2, i_3, i_4)$的4种取值分别代表$\alpha$的4条正对角线上的字节，则可得到：1) Deoxys-BC-256的176类5.5轮零相关线性逼近；2) Deoxys-BC-384的176类6.5轮零相关线性逼近。

证明　1) 对于Deoxys-BC-256，为不失一般性，仅以$i_1 = 0, i_2 = 5, i_3 = 10, i_4 = 15, i_5 = 4, j = 0$

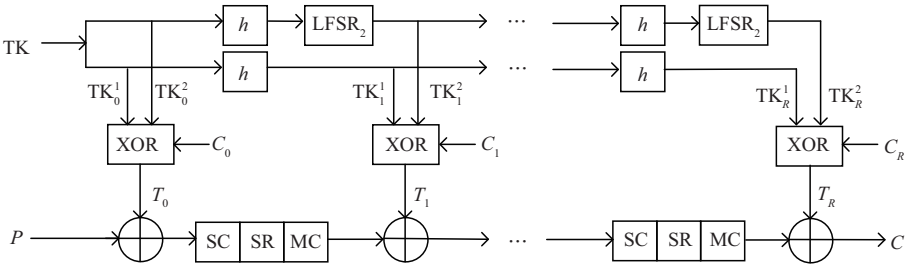

图4　Deoxys-BC-256算法的整体结构

表 2 **Deoxys-BC-256(Deoxys-BC-384)的 176 类 5.5(6.5)轮零相关线性逼近**

(i_1,i_2,i_3,i_4)	i_5	O	(i_1,i_2,i_3,i_4)	i_5	O
(0,5,10,15)	3	$\mathbb{Z}_{16}\setminus\{3,7,8,11,15\}$	(2,7,8,13)	1	$\mathbb{Z}_{16}\setminus\{1,5,9,10,13\}$
	4	$\mathbb{Z}_{16}\setminus\{2,6,10,14,15\}$		6	$\mathbb{Z}_{16}\setminus\{0,4,8,12,13\}$
	9	$\mathbb{Z}_{16}\setminus\{1,2,5,9,13\}$		11	$\mathbb{Z}_{16}\setminus\{0,3,7,11,15\}$
	14	$\mathbb{Z}_{16}\setminus\{0,4,5,8,12\}$		12	$\mathbb{Z}_{16}\setminus\{2,6,7,10,14\}$
(1,6,11,12)	0	$\mathbb{Z}_{16}\setminus\{0,4,8,9,12\}$	(3,4,9,14)	2	$\mathbb{Z}_{16}\setminus\{2,6,10,11,14\}$
	5	$\mathbb{Z}_{16}\setminus\{3,7,11,12,15\}$		7	$\mathbb{Z}_{16}\setminus\{1,5,9,13,14\}$
	10	$\mathbb{Z}_{16}\setminus\{2,3,6,10,14\}$		8	$\mathbb{Z}_{16}\setminus\{0,1,4,8,12\}$
	15	$\mathbb{Z}_{16}\setminus\{1,5,6,9,13\}$		13	$\mathbb{Z}_{16}\setminus\{3,4,7,11,15\}$

为例进行证明，其他 175 类的证明过程与之类似，故不再赘述。证明分为以下 3 个步骤，如图 5 所示。

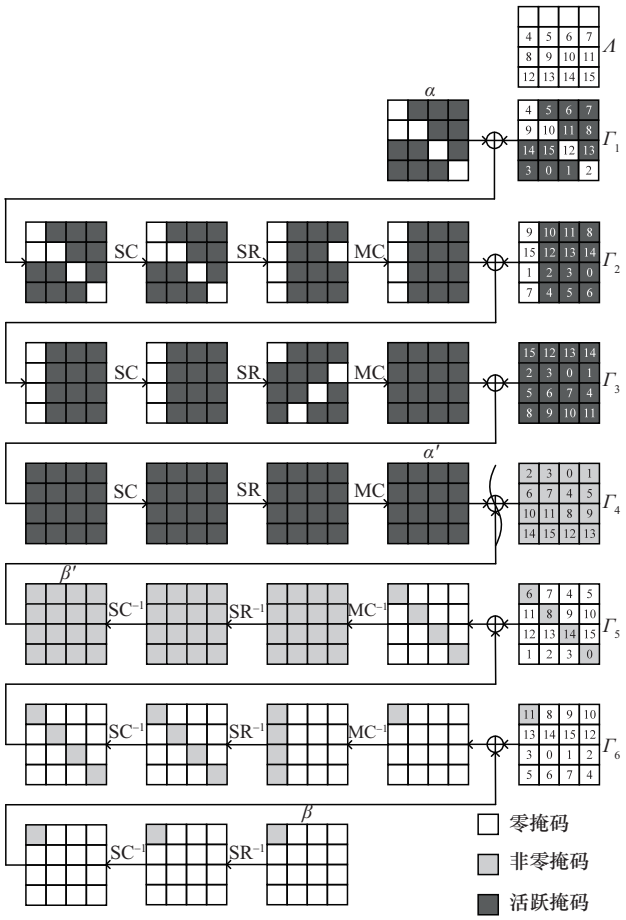

图 5 Deoxys-BC-256 的 5.5 轮零相关线性区分器

① 从加密方向考虑，令输入掩码 $\alpha=\alpha^0\|\alpha^1\|\cdots\|\alpha^{15}\in\mathbb{F}_2^{8\times 16}$，其中 $\alpha^0,\alpha^4,\alpha^5,\alpha^{10},\alpha^{15}$ 为 0，其余字节活跃，对 α 进行 3 轮加密，得到一条概率为 1 的 3 轮线性迹。将输入掩码 α 加密 3 轮后的结果记为 $\alpha'\in\mathbb{F}_2^{128}$。

② 从解密方向考虑，令输出掩码 $\beta=(\beta^0\mathbf{000\ 0000\ 0000\ 0000})\in\mathbb{F}_2^{8\times 16}$，其中 β^0 非零，与步骤① 类似，得到一条概率为 1 的 2.5 轮线性迹。将输出掩码 β 解密 2.5 轮后的结果记为 $\beta'\in\mathbb{F}_2^{128}$，其中区分器最后一轮不考虑列混合操作。

③ 由步骤① 和步骤② 可得 α' 的所有字节均活跃，而 β' 的所有字节均非零，故 α' 与 β' 可能存在矛盾。此外，观察图 5 中主调柄掩码 $\Lambda\in\mathbb{F}_2^{128}$ 第 9 个字节的传播情况，可以得到 Γ 序列 $(\Gamma_1^{h(9)},\Gamma_2^{h^2(9)},\cdots,\Gamma_6^{h^6(9)})\in\mathbb{F}_2^{8\times 6}$，发现只有 $\Gamma_3^{h^3(9)}$ 和 $\Gamma_4^{h^4(9)}$ 非零。当 $\Lambda^9=0$ 时，(α,β) 满足命题 2 中的条件 2)，因而 (α,β) 为一条 5.5 轮零相关线性逼近，由此得到 Deoxys-BC-256 的一条 5.5 轮零相关线性逼近。

2) 证明过程与 1) 类似，故不再赘述。证毕。

2.3 Deoxys-BC 算法的密钥恢复攻击

本节首先提出了 Deoxys-BC-256 的 5.5 轮积分区分器；其次，基于此积分区分器实现算法的 10 轮积分攻击；最后，对 Deoxys-BC-384 进行 12 轮积分攻击。

事实上，命题 3 中包含 Deoxys-BC-256 的 176 类 5.5 轮零相关线性区分器，根据定理 1，这些区分器均可转换为相应的积分区分器。为不失一般性，以图 5 所示的零相关线性区分器为例，可得到命题 4，证明显然。

命题 4 令 Deoxys-BC-256 输入的第 0,4,5,10,15 个字节活跃，其余字节为 0，对所有可能的输入进行 5.5 轮算法加密后，输出的第 0 个字节平衡，即所有可能的值异或为 0。由此可得 Deoxys-BC-256 的一个 5.5 轮积分区分器。

定理 2　设积分区分器如命题 4 所示，则可对 Deoxys-BC-256 进行 10 轮积分攻击，如图 6 所示。其时间复杂度为 $2^{191.02}$ 次 10 轮算法加密，数据复杂度为 $2^{60.3}$ 个选择密文，存储复杂度为 2^{168} bit。

证明　首先，利用等价密钥与部分和技术恢复正确轮调柄，如表 3 所示，具体步骤如下。

表 3　Deoxys-BC-256 的 10 轮积分攻击

步骤	猜测的轮调柄	存储的状态	存储复杂度	时间复杂度
1)	—	$\overline{W_8}$	2^{128}	2^{56}
2)	eT_9	$\overline{W_7^{0,7,10,13}}$	$2^{32+128}=2^{160}$	$2^{184-3.32}$
3)	$eT_8^{0,7,10,13}$	$\overline{W_6^0}$	$2^{8+160}=2^{168}$	$2^{190-3.32}$

1) 如图 6 所示，为满足命题 4 中积分区分器的输入，选取 $X_1 \in \mathbb{F}_2^{8\times 16}$ 的第 0,4,5,10,15 个字节活跃，其余字节为 0，并令可调密钥 $\mathrm{TK}=\mathrm{TK}_0^1\|\mathrm{TK}_0^2 \in \mathbb{F}_2^{256}$ 中 TK_0^1 的第 9 个字节 $\mathrm{TK}_0^{1,9} \in \mathbb{F}_2^8$、$\mathrm{TK}_0^2$ 的第 9 个字节 $\mathrm{TK}_0^{2,9} \in \mathbb{F}_2^8$ 活跃。由 X_1 可计算出明文 P，因此构造一个明文结构包含 $2^{8\times 5}=2^{40}$ 个选择明文，所需相关调柄为 $2^{8\times 2}=2^{16}$ 个，故对应的密文有 $2^{40+16}=2^{56}$ 个。记第 $0 \leqslant r \leqslant 9$ 轮的轮调柄 T_r 的等价调柄为 $eT_r=\mathrm{MC}^{-1}(T_r)$。根据命题 4，积分区分器的输出 $W_6^0 \in \mathbb{F}_2^8$ 是平衡的，由于密钥加操作不改变平衡性质，故 $\overline{W_6^0}$ 也是平衡的。将积分区分器向后扩展 3.5 轮，发现密文中所有字节均受 $\overline{W_6^0}$ 影响。构造列表 A_1 存储 $a_1=C$ 所有可能的值分别出现的次数，当 a_1 出现奇数次时，$A_1=1$，否则 $A_1=0$。基于此，当 $A_1=1$ 时，由密文 C 计算可得所有可能的 W_8。令 $a_2=W_8$，类似地构造列表 A_2 存储 a_2 所有可能的值分别出现的次数。这一步的时间复杂度为 2^{56} 次 10 轮算法加密。

2) 依据式(4)中的矩阵 $\boldsymbol{M}^{-1}$ 和 $\overline{W_7}=\boldsymbol{M}^{-1}\cdot Y_8$，猜测 $eT_9 \in \mathbb{F}_2^{128}$，当 $A_2=1$ 时，由 $\overline{W_8}$ 计算 $\overline{W_7^{0,7,10,13}}$。此步骤的时间复杂度为 $2^{56+128}\times\dfrac{1}{10}=2^{184-3.32}$ 次 10 轮算法加密。令 $a_3=\overline{W_7^{0,7,10,13}}$，类似地构造列表 A_3 存储 a_3 所有可能的值分别出现的次数。

3) 猜测 $eT_8^{0,7,10,13} \in \mathbb{F}_2^{32}$，当 $A_3=1$ 时，由 $\overline{W_7^{0,7,10,13}}$ 计算 $\overline{W_6^0}$。此步骤的时间复杂度为 $2^{32+160}\times\dfrac{4}{16\times 10}=2^{190-3.32}$ 次 10 轮算法加密。

4) 如果 $\oplus\overline{W_6^0}\neq 0$，重复步骤 2) 和步骤 3)，否

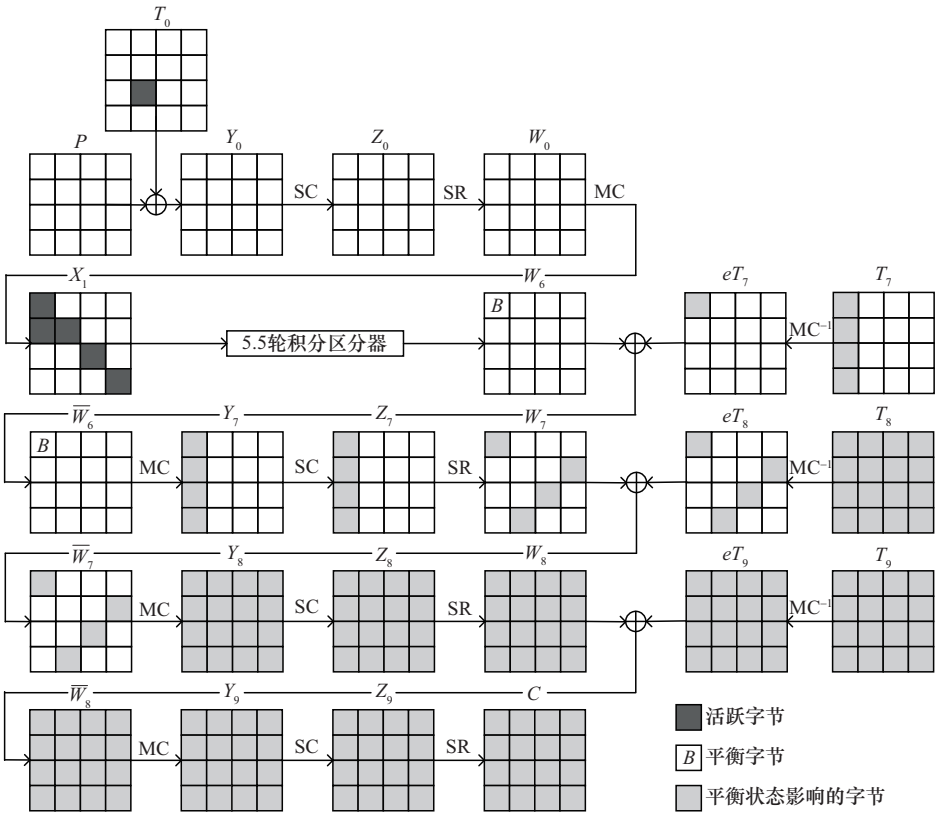

图 6　Deoxys-BC-256 的 10 轮积分攻击

则，所猜测调柄为正确调柄。证毕。

接下来，本文给出复杂度分析。

攻击猜测轮调柄共160 bit，由于一个平衡的字节过滤错误调柄的概率为2^{-8}，故需要$\frac{160}{8}=20$个结构去恢复所涉及的调柄。由表3可知，总的时间复杂度为$(2^{56}+2^{184-3.32}+2^{190-3.32})\times 20\approx 2^{191.02}$次10轮算法加密，数据复杂度为$2^{56}\times 20\approx 2^{60.3}$个选择密文，存储复杂度为$2^{168}$ bit。

注1 由命题3中的条件2)可知，Deoxys-BC-384的6.5轮零相关线性区分器也可得到相应的积分区分器，实现Deoxys-BC-384的12轮积分攻击。其调柄恢复过程与定理2类似，不同的是，首先将积分区分器向后扩展4.5轮。其次，由于Deoxys-BC-256为TP-2结构，而Deoxys-BC-384为TP-3结构，因此攻击Deoxys-BC-384所需要的相关调柄为2^{24}个，故对应的密文有2^{64}个。最后，攻击猜测轮调柄共288 bit，故需要36个结构去恢复所涉及的调柄。Deoxys-BC-384的12轮积分攻击所需时间复杂度为$\left(2^{64}+\frac{\left(2^{192}+2^{320}+2^{320}\times\frac{4}{16}\right)}{12}\right)\times 36\approx 2^{321.91}$次12轮算法加密，数据复杂度为$2^{64}\times 36\approx 2^{69.2}$个选择密文，存储复杂度为$2^{296}$ bit。

注2 应用命题4中的积分区分器也可对Deoxys-BC-256进行9轮积分攻击，其调柄恢复过程与定理2类似，不同的是，只需将积分区分器向后扩展2.5轮。总的时间复杂度为$\left(2^{56}+2^{64}\times\frac{4}{16\times 9}\right)\times 4\approx 2^{61.02}$次9轮算法加密，数据复杂度为$2^{56}\times 4=2^{58}$个选择密文，存储复杂度为$2^{40}$ bit。

3 RAIN算法的积分攻击

本节首先简要介绍RAIN算法；其次，构造RAIN算法的48类6轮零相关线性区分器，进而根据定理1将其转换为积分区分器；最后，对RAIN算法进行10轮积分攻击。

3.1 RAIN算法描述

RAIN算法是由曹梅春等[2]提出的可调分组密码算法，其分组长度支持64 bit和128 bit，分别记为RAIN-64和RAIN-128。RAIN算法两个版本的分组长度、密钥长度和调柄长度均相同，迭代轮数R分别为30轮和36轮。每轮加密包含轮函数f和ART两个步骤，其中轮函数由MC、SC和SR构成。

RAIN算法的加密流程如下。将第i轮的输入状态$X_i=x_i^0\|x_i^1\|\cdots\|x_i^{15}\in\mathbb{F}_2^{n_r}$记为如式(3)所示的矩阵，其中$r\in\{1,2\}$，$n_1=64$，$n_2=128$，且$x_i^j\in\mathbb{F}_2^{\frac{n_r}{16}}$，$0\leqslant i<R$，$R\in\{30,36\}$，$0\leqslant j\leqslant 15$。

1) 列混合（MC）：状态X_i左乘矩阵$\boldsymbol{M}$得到$Y_i\in\mathbb{F}_2^{n_r}$，即$Y_i=\boldsymbol{M}\cdot X_i$，$0\leqslant i<R$。

$$\boldsymbol{M}=\boldsymbol{M}^{-1}=\begin{pmatrix}0&1&1&1\\1&1&0&1\\1&0&1&1\\1&1&1&0\end{pmatrix}\tag{5}$$

2) 字节替换（SC）：对Y_i的每个单元格应用相同的S盒得到$Z_i=z_i^0\|z_i^1\|\cdots\|z_i^{15}\in\mathbb{F}_2^{n_r}$，即$z_i^j=\mathrm{SC}(y_i^j)\in\mathbb{F}_2^{\frac{n_r}{16}}$，$0\leqslant i<R$，$0\leqslant j\leqslant 15$。

3) 行移位（SR）：将Z_i的第l行向左循环移位l个单元格得到状态$W_i\in\mathbb{F}_2^{n_r}$，$0\leqslant i<R$，$l=0,1,2,3$。

4) 轮调柄加（ART）：轮调柄$T_{i+1}\in\mathbb{F}_2^{n_r}$与$W_i$异或得到$X_{i+1}\in\mathbb{F}_2^{n_r}$，$0\leqslant i<R$。

特别地，RAIN算法在第一轮加密前存在初始白化操作，即将明文$P\in\mathbb{F}_2^{n_r}$与主密钥$K\in\mathbb{F}_2^{n_r}$进行异或。

RAIN算法的调柄扩展算法如下。设调柄扩展算法的第i轮输入为$T_i=t_i^0\|t_i^1\|\cdots\|t_i^{15}\in\mathbb{F}_2^{n_r}$，其中$t_i^j\in\mathbb{F}_2^{\frac{n_r}{16}}$，$0\leqslant i<R$，$0\leqslant j\leqslant 15$，且$T_0=T$，$T$为主调柄。

1) 密钥加（AK）：第i轮的输入$T_i\in\mathbb{F}_2^{n_r}$与主密钥$K\in\mathbb{F}_2^{n_r}$异或得到$\mathrm{TK}_i\in\mathbb{F}_2^{n_r}$。

2) 行移位（SR）：对TK_i进行与轮函数相同的行移位操作得到$\mathrm{TK}_{i,1}\in\mathbb{F}_2^{n_r}$。

3) 轮常数加（AC）：将$\mathrm{TK}_{i,1}$与轮常数进行异或得到$\mathrm{TK}_{i,2}\in\mathbb{F}_2^{n_r}$。

4) 比特加（AB）：提取$\mathrm{TK}_{i,2}$中所有16个单元格的第1 bit，并将这16 bit异或得到的1 bit用于替代$\mathrm{TK}_{i,2}$的每个单元格的第1 bit，从而得到$T_{i+1}\in\mathbb{F}_2^{n_r}$。

由于密钥加、轮常数加和比特加操作均不影响线性掩码的传播规律，故在后文中只考虑行移位操作。由此可得RAIN算法结构符合命题1的条件。

PAIN算法的整体结构如图7所示。

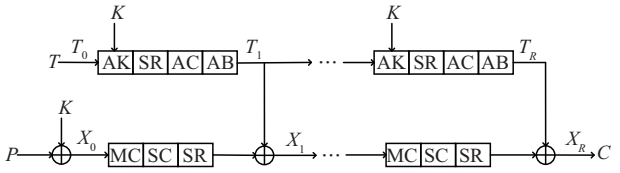

图7　RAIN 算法的整体结构

3.2　RAIN-128 的 6 轮零相关线性区分器

本节构造 RAIN-128 的 48 类 6 轮零相关线性逼近，并将其作为零相关线性区分器。

命题 5　设输入掩码 $\alpha=\alpha^0\|\alpha^1\|\cdots\|\alpha^{15}\in\mathbb{F}_2^{8\times 16}$ 与输出掩码 $\beta=\beta^0\|\beta^1\|\cdots\|\beta^{15}\in\mathbb{F}_2^{8\times 16}$ 分别满足某一组 $\left(\alpha^i,\alpha^{i+4},\alpha^{i+8},\alpha^{i+12}\right)$ 活跃，某个 β^j 非零，其余字节为 0，$0\leqslant i\leqslant 3$，$j\in O$，$\#O=12$，则可得到 RAIN-128 的 48 类 6 轮零相关线性逼近，i 和 O 的取值如表 4 所示。当 $i=0$ 时，α 的第一列字节活跃；当 $i=1$ 时，α 的第二列字节活跃，以此类推。

表 4　RAIN-128 的 48 类 6 轮零相关线性逼近

i	O
0	$\mathbb{Z}_{16}\setminus\{2,4,9,13\}$
1	$\mathbb{Z}_{16}\setminus\{3,5,10,14\}$
2	$\mathbb{Z}_{16}\setminus\{0,6,11,15\}$
3	$\mathbb{Z}_{16}\setminus\{1,7,8,12\}$

证明　为不失一般性，仅以 $i=j=0$ 为例进行证明，其他 47 类的证明与之类似，故不再赘述。证明分为以下 3 个步骤，如图 8 所示。

1) 从加密方向考虑，设输入掩码 $\alpha=(\alpha^0\mathbf{000}\ \alpha^4\mathbf{000}\ \alpha^8\mathbf{000}\ \alpha^{12}\mathbf{000})\in\mathbb{F}_2^{8\times 16}$，其中 $\alpha^0,\alpha^4,\alpha^8,\alpha^{12}$ 活跃，对 α 进行 3 轮加密，得到一条概率为 1 的 3 轮线性迹。记输入掩码 α 加密 3 轮后的结果为 $\alpha'\in\mathbb{F}_2^{128}$。

2) 从解密方向考虑，设输出掩码 $\beta=(\beta^0\mathbf{000\ 0000\ 0000\ 0000})\in\mathbb{F}_2^{8\times 16}$，$\beta^0$ 非零，与步骤 1) 类似，得到一条概率为 1 的 3 轮线性迹。将 β 解密 3 轮后的结果记为 $\beta'\in\mathbb{F}_2^{128}$。

3) 由步骤 1) 和步骤 2) 可得，α' 的所有字节均活跃，而 β' 的第 3 个字节为 0，其余字节非零，故 α' 与 β' 可能存在矛盾。此外，通过观察图 8 主调柄掩码 $\Lambda\in\mathbb{F}_2^{128}$ 中第 9 个字节的传播情况，可以得到 Γ 序列 $\left(\Gamma_1^{\mathrm{SR}(9)},\Gamma_2^{\mathrm{SR}^2(9)},\cdots,\Gamma_6^{\mathrm{SR}^6(9)}\right)\in\mathbb{F}_2^{8\times 6}$，发现只有 $\Gamma_3^{\mathrm{SR}^3(9)}$ 非零。当 $\Lambda^9=0$ 时，(α,β) 满足命题 1 中的条件 2)，因而 (α,β) 为一条 6 轮零相关线性逼近，由此得到 RAIN-128 的一条 6 轮零相关线性区分器。证毕。

3.3　RAIN 算法的密钥恢复攻击

本节提出了 RAIN-128 的 6 轮积分区分器，在不考虑白化密钥的情况下，实现 10 轮积分攻击。类似地，对 RAIN-64 进行 10 轮积分攻击。

事实上，命题 5 中包含 48 类零相关线性区分器，根据定理 1，这些区分器均可转换为相应的积分区分器。为不失一般性，以图 8 所示的零相关线性区分器为例，可得命题 6，证明显然。

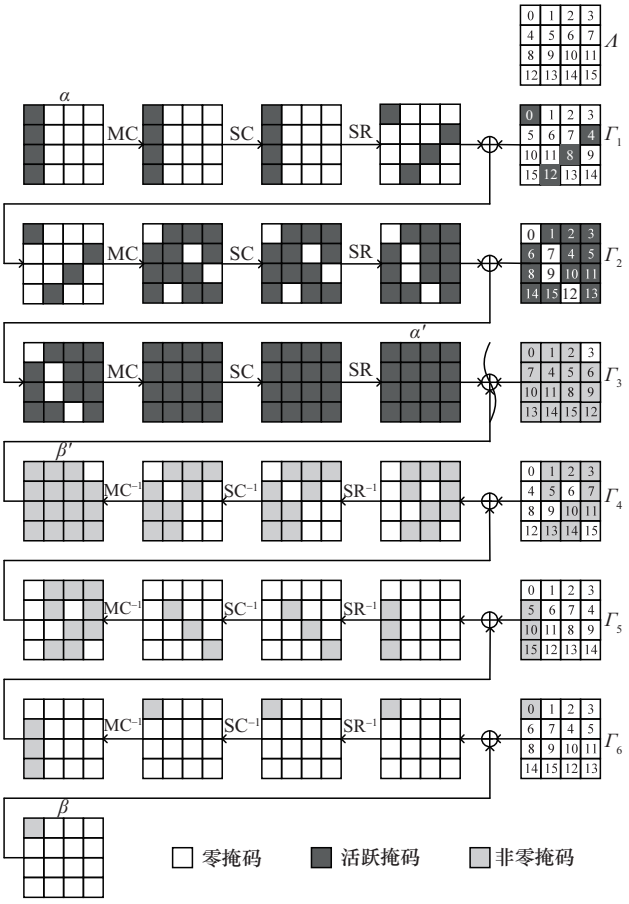

图8　RAIN-128 的 6 轮零相关线性区分器

命题 6　令 RAIN-128 输入的第 0,4,8,12 个字节为 0，其余字节活跃，对所有可能的输入进行 6 轮算法加密后，输出的第 0 个字节平衡，即所有可能的值异或为 0。由此可得 RAIN-128 的一个 6 轮积分区分器。

定理 3　设积分区分器如命题 6 所示，则可对 RAIN-128 进行 10 轮积分攻击，如图 9 所示，其时间复杂度为 $2^{239.02}$ 次 10 轮算法加密，数据复杂度为 $2^{100.8}$ 个选择密文，存储复杂度为 2^{224} bit。

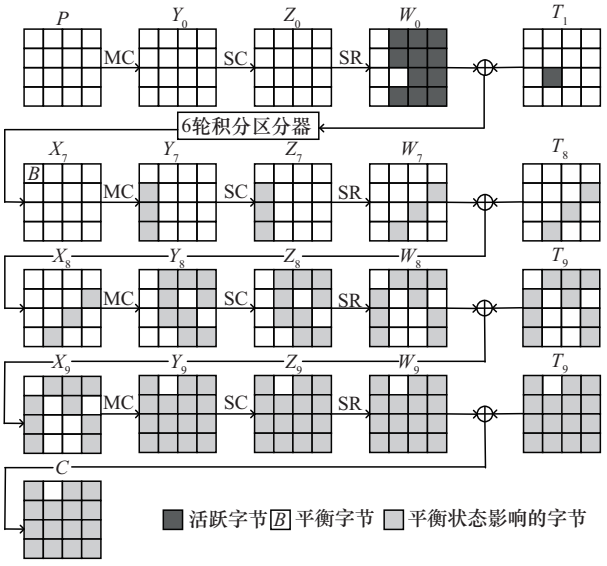

图9　RAIN-128的10轮积分攻击

证明　首先，利用部分和技术恢复正确轮调柄，如表5所示，具体步骤如下。

表5　　RAIN-128的10轮积分攻击

步骤	猜测的轮调柄	存储的状态	存储复杂度	时间复杂度
1)	—	$C^{0,2,\cdots,15}$	2^{120}	2^{96}
2)	$T_{10}^{0,7,10,13}$	$X_9^{4,8,12},C^{2,\cdots,6,8,9,11,12,14,15}$	$2^{112+32}=2^{144}$	$2^{126-3.32}$
3)	$T_{10}^{4,11,14}$	$X_9^{1,4,8,12},C^{2,3,5,6,8,9,12,15}$	$2^{96+56}=2^{152}$	$2^{152-5.74}$
4)	$T_{10}^{2,5,8,15}$	$X_9^{1,2,4,6,8,12},C^{3,6,9,12}$	$2^{80+88}=2^{168}$	$2^{182-3.32}$
5)	$T_{10}^{3,6,9,12}$	$X_9^{1,\cdots,4,6,8,11,12,15}$	$2^{72+120}=2^{192}$	$2^{198-3.32}$
6)	$T_9^{1,4,11}$	$X_8^{13},X_9^{2,3,6,8,12,15}$	$2^{56+144}=2^{200}$	$2^{216-5.74}$
7)	$T_9^{2,8,15}$	$X_8^{10,13},X_9^{3,6,12}$	$2^{40+168}=2^{208}$	$2^{224-5.74}$
8)	$T_9^{3,6,12}$	$X_8^{7,10,13}$	$2^{24+192}=2^{216}$	$2^{232-5.74}$
9)	$T_8^{7,10,13}$	X_7^0	$2^{8+216}=2^{224}$	$2^{240-5.74}$

1) 如图9所示，为满足命题6中积分区分器的输入，令轮调柄T_1^9活跃，其余字节为0，选取$W_0^{0,4,8,9,12}$为0，其余字节活跃，此时积分区分器的输出$X_7^0\in\mathbb{F}_2^8$是平衡的，即$\oplus X_7^0=0$。由W_0可计算出明文P，构造一个明文结构包含$2^{8\times 11}=2^{88}$个选择明文，故选取2^{88}个明文和2^8个调柄，所对应的密文有$2^{88+8}=2^{96}$个。将积分区分器向后扩展3轮，发现密文中受X_7^0影响的字节为$C^{0,2,\cdots,15}$。构造列表A_1存储$a_1=C^{0,2,\cdots,15}$所有可能的值分别出现的次数，当a_1出现奇数次时，$A_1=1$，否则$A_1=0$。这一步骤的时间复杂度为2^{96}次10轮算法加密。

2) 猜测轮调柄$T_{10}^{0,7,10,13}\in\mathbb{F}_2^{32}$，依据式(5)中的矩阵$M=M^{-1}$和$X_9=M^{-1}\cdot Y_9$可得$X_9^4=Y_9^0\oplus Y_9^7\oplus Y_9^{13}$，$X_9^8=Y_9^0\oplus Y_9^{10}\oplus Y_9^{13}$和$X_9^{12}=Y_9^0\oplus Y_9^7\oplus Y_9^{10}$，因此当$A_1=1$时，对密文$C^{0,7,10,13}\in\mathbb{F}_2^{32}$进行1轮部分解密得到$X_9^{4,8,12}$的时间复杂度为$2^{96+32}\times\dfrac{4}{16\times 10}=2^{126-3.32}$次10轮算法加密。令$a_2=\left(X_9^{4,8,12},C^{2,\cdots,6,8,9,11,12,14,15}\right)$，类似地构造列表$A_2$。

3) 猜测$T_{10}^{4,11,14}\in\mathbb{F}_2^{24}$，与步骤2)类似，当$A_2=1$时，对密文$C^{4,11,14}\in\mathbb{F}_2^{24}$进行1轮部分解密得到$X_9^1$的时间复杂度为$2^{96+56}\times\dfrac{3}{16\times 10}=2^{152-5.74}$次10轮算法加密。令$a_3=\left(X_9^{1,4,8,12},C^{2,3,5,6,8,9,12,15}\right)$，类似地构造列表$A_3$。

4) 猜测$T_{10}^{2,5,8,15}\in\mathbb{F}_2^{32}$，当$A_3=1$时，对密文$C^{2,5,8,15}\in\mathbb{F}_2^{32}$进行1轮部分解密得到$X_9^{2,6}$。该步骤的时间复杂度为$2^{96+88}\times\dfrac{4}{16\times 10}=2^{182-3.32}$次10轮算法加密。令$a_4=\left(X_9^{1,2,4,6,8,12},C^{3,6,9,12}\right)$，类似地构造列表$A_4$。

5) 猜测$T_{10}^{3,6,9,12}\in\mathbb{F}_2^{32}$，当$A_4=1$时，对密文$C^{3,6,9,12}\in\mathbb{F}_2^{32}$进行1轮部分解密得到$X_9^{3,11,15}$。该步骤时间复杂度为$2^{80+120}\times\dfrac{4}{16\times 10}=2^{198-3.32}$次10轮算法加密。令$a_5=X_9^{1,\cdots,4,6,8,11,12,15}$，类似地构造列表$A_5$。

6) 猜测$T_9^{1,4,11}\in\mathbb{F}_2^{24}$，当$A_5=1$时，对$X_9^{1,4,11}\in\mathbb{F}_2^{24}$进行1轮部分解密得到$X_8^{13}$。该步骤的时间复杂度为$2^{72+144}\times\dfrac{3}{16\times 10}=2^{216-5.74}$次10轮算法加密。令$a_6=\left(X_8^{13},X_9^{2,3,6,8,12,15}\right)$，类似地构造列表$A_6$。

7) 猜测$T_9^{2,8,15}\in\mathbb{F}_2^{24}$，当$A_6=1$时，对$X_9^{2,8,15}\in\mathbb{F}_2^{24}$进行1轮部分解密得到$X_8^{10}$。该步骤的时间复杂度为$2^{56+168}\times\dfrac{3}{16\times 10}=2^{224-5.74}$次10轮算法加密。令$a_7=\left(X_8^{10,13},X_9^{3,6,12}\right)$，类似地构造列表$A_7$。

8) 猜测$T_9^{3,6,12}\in\mathbb{F}_2^{24}$，当$A_7=1$时，对$X_9^{3,6,12}\in\mathbb{F}_2^{24}$进行1轮部分解密得到$X_8^7$。该步骤的时间复杂度为$2^{40+192}\times\dfrac{3}{16\times 10}=2^{232-5.74}$次10轮算法加密。令$a_8=X_8^{7,10,13}$，类似地构造列表$A_8$。

9) 猜测$T_8^{7,10,13}\in\mathbb{F}_2^{24}$，当$A_8=1$时，对$X_8^{7,10,13}\in$

$\mathbb{F}_2^{24}$进行1轮部分解密得到X_7^0。该步骤的时间复杂度为$2^{24+216}\times\frac{3}{16\times 10}=2^{240-5.74}$次10轮算法加密。

10) 令 $T^*=T_{10}^{0,2,\cdots,15}\|T_9^{1-4,6,8,11,12,15}\|T_8^{7,10,13}$，若$\oplus X_7^0\neq 0$，则重复步骤2)~步骤9)，否则$T^*$为正确调柄。证毕。

接下来，本文给出复杂度分析。

步骤1)~步骤9)共猜测216 bit轮调柄，故需要$\frac{216}{8}=27$个结构去恢复所涉及的轮调柄。由表5可知，总的时间复杂度为$\left(2^{96}+2^{126-3.32}+2^{152-5.74}+2^{182-3.32}+2^{198-3.32}+2^{216-5.74}+2^{224-5.74}+2^{232-5.74}+2^{240-5.74}\right)\times 27\approx 2^{239.02}$次10轮算法加密，数据复杂度为$2^{96}\times 27\approx 2^{100.8}$个选择密文，存储复杂度为$2^{224}$ bit。

注 3　应用命题6中的积分区分器也可对RAIN-64进行10轮积分攻击，其调柄恢复过程与定理3类似，唯一不同的是，由于RAIN-128的一个单元格为8 bit，而RAIN-64的一个单元格为4 bit，因此每一步的复杂度数量级减半。对RAIN-64的攻击中，总的时间复杂度为$2^{119.19}$次10轮算法加密，数据复杂度为$2^{52.8}$个选择密文，存储复杂度为2^{112} bit。

注 4　应用命题6中的积分区分器也可对RAIN-128进行8轮积分攻击，其调柄恢复过程与定理3类似，不同的是，只需将积分区分器向后扩展1轮。总的时间复杂度为$\left(2^{96}+2^{48}\times\frac{3}{16\times 8}\right)\times 3\approx 2^{97.58}$次8轮算法加密，数据复杂度为$2^{96}\times 3\approx 2^{97.6}$个选择密文，存储复杂度为$2^{32}$ bit。

4　结束语

本文在考虑调柄对可调分组密码算法影响的情形下，将零相关线性分析与积分攻击结合，对轻量级可调分组密码算法Deoxys-BC和RAIN进行了积分攻击。首先，提出了Deoxys-BC-256的5.5轮零相关线性区分器以及Deoxys-BC-384的6.5轮零相关线性区分器。其次，根据零相关线性区分器与积分区分器的联系得到Deoxys-BC算法的积分区分器，分别实现了该算法两个版本的10轮和12轮积分攻击。最后，构造了RAIN算法的6轮积分区分器，并对该算法的两个版本进行了10轮积分攻击。结果表明，本文方案所需复杂度显著降低。

此外，通过寻找更好的零相关线性区分器和积分区分器，改进目前已有的结果或者对算法进行更长轮数的攻击将是下一步工作的重点。

参考文献：

[1] Jean J, Nikolić I, Peyrin T, et al. Deoxys v1.41[S]. CAESAR 124, 2016.

[2] 曹梅春, 张文英, 陈彦琴, 等. RAIN: 一种面向软硬件和门限实现的轻量分组密码算法[J]. 计算机研究与发展, 2021, 58(5): 1045-1055.
Cao M C, Zhang W Y, Chen Y Q, et al. RAIN: a lightweight block cipher towards software, hardware and threshold implementations[J]. Journal of Computer Research and Development, 2021, 58(5): 1045-1055.

[3] Mehrdad A, Moazami F, Soleimany H. Impossible differential cryptanalysis on Deoxys-BC-256[J]. The ISC International Journal of Information Security, 2018, 10(2): 93-105.

[4] Zhang J N, Wang H Y, Tang D. Impossible boomerang attacks revisited: applications to Deoxys-BC, Joltik-BC and SKINNY[J]. IACR Transactions on Symmetric Cryptology, 2024(2): 254-295.

[5] Jia M C, Du X N, Zheng Y N, et al. Multidimensional zero-correlation linear cryptanalysis on uBlock and RAIN[J]. Cryptologia, 2025, 49(5): 443-469.

[6] 杜小妮, 郑亚楠, 梁丽芳, 等. RAIN-128算法的中间相遇攻击[J]. 电子与信息学报, 2024, 46(1): 327-334.
Du X N, Zheng Y N, Liang L F, et al. Meet-in-the-middle attack on RAIN-128[J]. Journal of Electronics & Information Technology, 2024, 46(1): 327-334.

[7] Song L, Zhang N N, Yang Q Q, et al. Optimizing rectangle attacks: a unified and generic framework for key recovery[C]//International Conference on the Theory and Application of Cryptology and Information Security. Berlin: Springer, 2022: 410-440.

[8] Zhang J N, Wang H Y. Optimizing key recovery in impossible cryptanalysis and its automated tool[J]. Cryptology ePrint Archive, 2025.

[9] Song L, Yang Q Q, Chen Y C, et al. Probabilistic extensions: a one-step framework for finding rectangle attacks and beyond[C]//Annual International Conference on the Theory and Applications of Cryptographic Techniques. Berlin: Springer, 2024: 339-367.

[10] 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.

[11] 沈霞民, 熊涛, 李华, 等. CLEFIA动态密码结构的零相关线性区分器构造研究[J]. 信息网络安全, 2024, 24(6): 948-958.
Shen X M, Xiong T, Li H, et al. Research on the construction of zero-correlation linear discriminator for CLEFIA dynamic cipher structure[J]. Netinfo Security, 2024, 24(6): 948-958.

[12] 沈璇, 刘国强, 孙兵, 等. 两类动态密码结构抵抗不可能差分和零相关线性能力评估[J]. 电子学报, 2024, 52(3): 709-718.

Shen X, Liu G Q, Sun B, et al. Security evaluation against impossible differential cryptanalysis and zero correlation linear cryptanalysis for two dynamic cryptographic structures[J]. Acta Electronica Sinica, 2024, 52(3): 709-718.

[13] Leander G, Tezcan C, Wiemer F. Searching for subspace trails and truncated differentials[J]. IACR Transactions on Symmetric Cryptology, 2018: 74-100.

[14] Knudsen L, Wagner D. Integral cryptanalysis[C]//International Workshop on Fast Software Encryption. Berlin: Springer, 2002: 112-127.

[15] Hadipour H, Todo Y. Cryptanalysis of QARMAv2[J]. IACR Transactions on Symmetric Cryptology, 2024, 2024(1): 188-213.

[16] Ankele R, Dobraunig C, Guo J, et al. Zero-correlation attacks on tweakable block ciphers with linear tweakey expansion[J]. IACR Transactions on Symmetric Cryptology, 2019: 192-235.

[17] Dunkelman O, Ghosh S, Keller N, et al. Partial sums meet FFT: improved attack on 6-round AES[C]//Annual International Conference on the Theory and Applications of Cryptographic Techniques. Berlin: Springer, 2024: 128-157.

[18] Liskov M, Rivest R L, Wagner D. Tweakable block ciphers[C]//Annual International Cryptology Conference. Berlin: Springer, 2002: 31-46.

[19] Jean J, Nikolić I, Peyrin T. Tweaks and keys for block ciphers: the TWEAKEY framework[C]//International Conference on the Theory and Application of Cryptology and Information Security. Berlin: Springer, 2014: 274-288.

[20] Sun B, Liu Z Q, Rijmen V, et al. Links among impossible differential, integral and zero correlation linear cryptanalysis[C]//Advances in Cryptology-CRYPTO 2015. Berlin: Springer, 2015: 95-115.

[作者简介]

杜小妮（1972– ），女，甘肃庆阳人，博士，西北师范大学教授、博士生导师，主要研究方向为密码学与信息安全等。

关雪莹（2002– ），女，甘肃平凉人，西北师范大学硕士生，主要研究方向为密码学与信息安全等。

余恬（2001– ），女，安徽安庆人，西北师范大学硕士生，主要研究方向为密码学与信息安全等。

梁丽芳（1995– ），女，甘肃定西人，西北师范大学博士生，主要研究方向为密码学与信息安全等。