低轮 FOX64 算法的零相关-积分分析

郭 瑞* 金晨辉
(解放军信息工程大学三院 郑州 450001)

摘 要：FOX 系列算法是一类基于 Lai-Massey 模型设计的分组密码算法。该文首先评估低轮 FOX64 算法抵抗零相关线性分析的能力，给出 4 轮 FOX64 算法的零相关线性区分器。然后，利用零相关线性区分器与积分区分器的关系，首次得到 4 轮 FOX64 算法的积分区分器。最后，利用积分区分器分析 5, 6, 7, 8 轮 FOX64 算法，攻击的时间复杂度分别约为 $2^{52.7}$, $2^{116.7}$, $2^{180.7}$, $2^{244.7}$ 次加密，数据复杂度为 2^{50} 个选择明文。该文首次给出攻击 8 轮 FOX64/256 时间复杂度小于穷举攻击的有效攻击。

关键词：密码学；分组密码；密码分析；FOX64 算法；零相关-积分分析
中图分类号：TN918 **文献标识码**：A **文章编号**：1009-5896(2015)02-0417-06
DOI: 10.11999/JEIT140373

Integral Cryptanalysis of Reduced Round FOX64

Guo Rui Jin Chen-hui
(*The Third Institute*, *PLA Information Engineering University*, *Zhengzhou* 450001, *China*)

Abstract: FOX family block ciphers are based on Lai-Massey scheme. Firstly, the evaluation is performed on the ability of the reduced round FOX64 to resist zero-correlation linear cryptanalysis, and some 4-round zero-correlation linear distinguishers are presented. Then, by using the relation between the integral distinguishers and zero-correlation distinguishers, the 4-round integral distinguishers of FOX64 are found. Finally, the 4-round integral distinguishers are used to attack 5, 6, 7 and 8 rounds FOX64 with the time complexity of $2^{52.7}$, $2^{116.7}$, $2^{180.7}$ and $2^{244.7}$ encryptions respectively, and the data complexity is 2^{50} chosen plaintexts. This is the first paper pointing out that 8-round FOX64/256 is vulnerable against the statistical attack.

Key words: Cryptography; Block cipher; Cryptanalysis; FOX 64 algorithm; Zero-correlation integral cryptanalysis

1 引言

目前，对分组密码算法的攻击方法主要分为：差分密码分析[1]及其推广、线性密码分析[2]及其推广、积分攻击、密钥相关攻击、中间相遇攻击、插值攻击等。其中，差分密码分析和线性密码分析是目前对分组密码算法安全性分析的最重要和最有效的工具。最近，文献[3]提出了零相关线性分析，该分析方法基于相关系数为 0 的线性逼近，并通常被看作与不可能差分分析相对应的一类推广的线性密码分析方法。

文献[3]提出零相关线性分析方法时，给出了 AES 算法、Skipjack 算法、CAST256 算法、CLEFIA 算法相关系数为 0 的线性逼近，并成功攻击了低轮 AES-192, AES-256 以及 CLEFIA-256。但是，为了判断选取的线性逼近的相关系数是否为 0，零相关线性分析需要选取明文规模至少为分组规模一半。因此，攻击所需数据复杂度较高是零相关线性分析最大的缺陷。随后，文献[4]证明了使用多个独立的零相关线性逼近可以降低数据复杂度。但是，多个线性逼近相互独立的假设难以满足。为此，文献[5]指出可以使用不同的已知明文来消除线性逼近互相独立的假设，从而降低攻击所需的数据复杂度，并给出了零相关线性区分器与积分区分器、多维线性区分器的关系。证明了由积分区分器可以得到零相关线性逼近区分器、由零相关线性逼近区分器在一定条件下同样可以得到积分区分器，证明了零相关线性区分器是多维线性区分器的特例。同时，首次给出了变形的 31 轮 Skipjack 算法的零相关-积分攻击。此外，文献[6]还给出了 LBlock 算法的多维-零相关线性分析，且攻击结果的时间复杂度优于已有攻击结果。

本文分析 FOX 系列分组密码算法抵抗零相关线性分析的能力。FOX 分组密码算法是文献[7]为了满足 Mediacrypt 公司的需求而设计，包括分组规模

2014-03-19 收到，2014-07-07 改回
国家自然科学基金(61272488)资助课题
*通信作者：郭瑞 guorui201@sohu.com

为 64 bit 和 128 bit 两类算法，通常称为 FOX64 和 FOX128。FOX 系列分组密码算法的安全性基于 Lai-Massey 模型[8,9]的可证明安全结论，其圈函数采用嵌套 SPS 结构的 Lai-Massey 模型，密钥规模 k 满足 $0 \le k \le 256$，且是 8 的倍数。特别地，FOX 算法使用了复杂的密钥编排算法，使得其由若干子密钥无法获取种子密钥或其它子密钥。已有对 FOX 算法有效的攻击包括碰撞-积分攻击、不可能差分分析、差分碰撞攻击等。文献[10]利用 FOX 算法的 3 轮区分器及碰撞技术对 4, 5, 6, 7 轮 FOX64 分析的时间复杂度分别为 $2^{45.4}$, $2^{109.4}$, $2^{173.4}$, $2^{237.4}$，数据复杂度为 2^9 个选择明文。文献[11]和文献[12]独立地找到了 4 轮 FOX 算法的不可能差分对应，并指出不可能差分攻击对 5, 6, 7 轮 FOX64 的时间复杂度分别为 2^{69}, 2^{133}, 2^{197}，攻击的数据复杂度大约为 2^{39} 个选择明文。此外，文献[13]给出了 FOX 算法的差分-碰撞攻击，攻击需要的数据复杂度很小，但预处理复杂度较高。文献[14]给出了 FOX 算法的差错故障分析结果。

本文首先给出了FOX64算法大量4轮零相关线性逼近，然后利用零相关线性逼近区分器与积分区分器的关系，首次得到了 FOX64 算法 4 轮积分区分器。最后，利用积分分析方法对 5,6,7,8 轮 FOX64 进行了攻击。

2 基础知识

本节首先简单介绍 FOX 算法及其圈函数线性逼近的一般规律，然后介绍零相关线性分析。

2.1 FOX 分组密码算法[7]简述

FOX 算法使用的圈函数是嵌套 SPS 结构的 Lai-Massey 模型。限于篇幅，只对 FOX64 进行详细介绍，FOX128 可看作两个 FOX64 的并置。FOX64/k 中的 k 是密钥长度。

轮函数 f: $\{0,1\}^{32}\times\{0,1\}^{64}\to\{0,1\}^{32}$ 由字节代替变换 sigma4、线性置换 mu4 和密钥异或加构成，其使用的子密钥 $K=k_0\|k_1$ 是 64 bit，表达式为 $f(x,K)=\text{sigma4}(\text{mu4}(\text{sigma4}(x\oplus k_0))\oplus k_1)\oplus k_0$。其中 sigma4: $\{0,1\}^{32}\to\{0,1\}^{32}$ 由 4 个相同的 8 进 8 出的 s 盒并置而成，扩散层 mu4: $[\text{GF}(256)]^4\to[\text{GF}(256)]^4$ 使用一个分支数为 5 的 MDS 矩阵，其定义为

$$\begin{pmatrix}y_1\\y_2\\y_3\\y_4\end{pmatrix}=\begin{pmatrix}1&1&Z&\alpha\\1&Z&\alpha&1\\Z&\alpha&1&1\\\alpha&1&Z&1\end{pmatrix}\begin{pmatrix}x_1\\x_2\\x_3\\x_4\end{pmatrix}$$

$Z=\alpha^{-1}\oplus 1$，α 是不可约多项式 $m(x)=x^8\oplus x^7\oplus x^6\oplus x^5\oplus x^4\oplus x^3\oplus 1$ 的一个根。

FOX64 算法圈函数迭代 16 次，64 bit 明文 P 经加密后得到的 64 bit 密文为

$$C=\text{Imid64}\big(\text{Imor64}\big(\cdots(\text{Imor64}(P,K_1),\cdots,K_2\big),K_r\big)$$

其中圈函数 $\text{Imor64}(x_l\,\|\,x_r)=\text{or}(x_l\oplus f_{32}(x_l\oplus x_r,k))\,\|\,(y_r\oplus f_{32}(x_l\oplus x_r,k)),K_1,K_2,\cdots,K_r$ 是各圈使用的 64 bit 子密钥，$\text{or}(x,y)=(y,x\oplus y)$ 是圈函数使用的线性正形置换，最后一轮圈函数 Imid64 无正形置换。

设 FOX 算法中使用的正形置换 or 对应矩阵为 $\boldsymbol{M}$。给出 FOX64 算法圈函数线性逼近对应的一般规律。

引理 1 FOX64 算法圈函数 Q_k 的线性逼近 $(\boldsymbol{\alpha},\boldsymbol{\beta})\to(\boldsymbol{A},\boldsymbol{B})$ 的相关系数为非零 ρ 的充分必要条件是 $\boldsymbol{\alpha}\oplus\boldsymbol{\beta}\oplus\boldsymbol{B}\oplus\boldsymbol{MA}=\boldsymbol{0}$。此时，F 函数对应的线性逼近为 $\boldsymbol{\beta}\oplus\boldsymbol{B}\to\boldsymbol{\alpha}\oplus\boldsymbol{\beta}$ 且满足相关系数也是 ρ。

证明 设 $(\boldsymbol{x}_1,\boldsymbol{x}_2)$ 为 Q_k 的输入，令 $\boldsymbol{x}=\boldsymbol{x}_1$，$\boldsymbol{y}=\boldsymbol{x}_1\oplus\boldsymbol{x}_2$，将 $\boldsymbol{x}$，$\boldsymbol{y}$ 看作列向量，则有

$$\begin{aligned}&(\boldsymbol{A},\boldsymbol{B})\cdot Q_k(\boldsymbol{x}_1,\boldsymbol{x}_2)\oplus(\boldsymbol{\alpha},\boldsymbol{\beta})\cdot(\boldsymbol{x}_1,\boldsymbol{x}_2)\\&\quad=\boldsymbol{A}\cdot\text{or}(F(\boldsymbol{x}_1\oplus\boldsymbol{x}_2)\oplus\boldsymbol{x}_1)\oplus\boldsymbol{B}\\&\qquad\cdot(F(\boldsymbol{x}_1\oplus\boldsymbol{x}_2)\oplus\boldsymbol{x}_2)\oplus\boldsymbol{\alpha}\cdot\boldsymbol{x}_1\oplus\boldsymbol{\beta}\cdot\boldsymbol{x}_2\\&\quad=(\boldsymbol{\alpha}\oplus\boldsymbol{\beta}\oplus\boldsymbol{B})\cdot\boldsymbol{x}\oplus\boldsymbol{A}\cdot\text{or}(\boldsymbol{x})\oplus(\boldsymbol{\beta}\oplus\boldsymbol{B})\\&\qquad\cdot\boldsymbol{y}\oplus\boldsymbol{A}\cdot\text{or}(F(\boldsymbol{y}))\oplus\boldsymbol{B}\cdot F(\boldsymbol{y})\\&\quad=(\boldsymbol{\alpha}\oplus\boldsymbol{\beta}\oplus\boldsymbol{B})^{\mathrm{T}}\boldsymbol{x}\oplus\boldsymbol{A}^{\mathrm{T}}\boldsymbol{Mx}\oplus(\boldsymbol{\beta}\oplus\boldsymbol{B})^{\mathrm{T}}\boldsymbol{y}\\&\qquad\oplus\boldsymbol{A}^{\mathrm{T}}\boldsymbol{M}F(\boldsymbol{y})\oplus\boldsymbol{B}^{\mathrm{T}}F(\boldsymbol{y})\\&\quad=(\boldsymbol{\alpha}\oplus\boldsymbol{\beta}\oplus\boldsymbol{B}\oplus\boldsymbol{M}^{\mathrm{T}}\boldsymbol{A})\cdot\boldsymbol{x}\oplus(\boldsymbol{M}^{\mathrm{T}}\boldsymbol{A}\oplus\boldsymbol{B})\\&\qquad\cdot F(\boldsymbol{y})\oplus(\boldsymbol{\beta}\oplus\boldsymbol{B})\cdot\boldsymbol{y}\end{aligned}$$

本文记 $\boldsymbol{\Delta}=\boldsymbol{\alpha}\oplus\boldsymbol{\beta}\oplus\boldsymbol{B}\oplus\boldsymbol{M}^{\mathrm{T}}\boldsymbol{A}$，$\Gamma(\boldsymbol{y})=(\boldsymbol{M}^{\mathrm{T}}\boldsymbol{A}\oplus\boldsymbol{B})\cdot F(\boldsymbol{y})\oplus(\boldsymbol{\beta}\oplus\boldsymbol{B})\cdot\boldsymbol{y}$。则有

$$\sum_{\boldsymbol{x}_1,\boldsymbol{x}_2}(-1)^{(\boldsymbol{A},\boldsymbol{B})\cdot Q_k(\boldsymbol{x}_1,\boldsymbol{x}_2)\oplus(\alpha,\beta)\cdot(\boldsymbol{x}_1,\boldsymbol{x}_2)}=\sum_{\boldsymbol{x},\boldsymbol{y}}(-1)^{\boldsymbol{\Delta}\cdot\boldsymbol{x}\oplus\Gamma(\boldsymbol{y})}=\left[\sum_{\boldsymbol{x}}(-1)^{\boldsymbol{\Delta}\cdot\boldsymbol{x}}\right]\left[\sum_{\boldsymbol{y}}(-1)^{\Gamma(\boldsymbol{y})}\right]$$

如若 $\boldsymbol{\Delta}\neq 0$，则有 $\sum_x(-1)^{\boldsymbol{\Delta}\cdot\boldsymbol{x}}=0$，与 $\rho\neq 0$ 矛盾，所以 $\boldsymbol{\alpha}\oplus\boldsymbol{\beta}\oplus\boldsymbol{B}\oplus\boldsymbol{M}^{\mathrm{T}}\boldsymbol{A}=\boldsymbol{0}$。此时，$\rho_{Q_k}((\boldsymbol{\alpha},\boldsymbol{\beta})\to(\boldsymbol{A},\boldsymbol{B}))=\rho_F(\boldsymbol{\beta}\oplus\boldsymbol{B}\to\boldsymbol{M}^{\mathrm{T}}\boldsymbol{A}\oplus\boldsymbol{B})=\rho_F(\boldsymbol{\beta}\oplus\boldsymbol{B}\to\boldsymbol{\alpha}\oplus\boldsymbol{\beta})$。特别地，由于正形置换 or 满足 $\boldsymbol{M}^{\mathrm{T}}=\boldsymbol{M}$，可得 $\boldsymbol{\alpha}\oplus\boldsymbol{\beta}\oplus\boldsymbol{B}\oplus\boldsymbol{MA}=\boldsymbol{0}$。充分条件显然。 证毕

此外，FOX 算法使用的正形置换 $\text{or}(x,y)=(y,x\oplus y)$ 及逆置换 $\text{io}(x,y)=(x\oplus y,x)$ 具有的性质为：

性质 1[7] (1) $\text{or}^2(x,y)=\text{io}(x,y)$，$\text{io}^2(x,y)=\text{or}(x,y)$；(2) $\text{io}(x,y)\oplus\text{or}(x,y)\oplus(x,y)=(0,0)$；(3)

$\mathrm{or}(x,y)=(x,y)$ 当且仅当 $(x,y)=(0,0)$；(4) $\mathrm{or}^3(x,y)=(x,y)$。

2.2 零相关线性逼近[15]

对于 n 维向量 $\boldsymbol{\alpha}=(\alpha_1,\alpha_2,\cdots,\alpha_n)$ 和 $\boldsymbol{x}=(x_1,x_2,\cdots,x_n)$，令 $\boldsymbol{\alpha}\cdot\boldsymbol{x}=\overset{n}{\underset{i=1}{\oplus}}\alpha_i x_i$。设 $f:\mathbb{F}_2^n\to\mathbb{F}_2^n$，给定输入选择模式 $\boldsymbol{\alpha}$ 和输出选择模式 $\boldsymbol{\beta}$，令 $p_f(\boldsymbol{\alpha},\boldsymbol{\beta})=\Pr\{\boldsymbol{\alpha}\cdot\boldsymbol{x}\oplus\boldsymbol{\beta}\cdot f(\boldsymbol{x})=0\}$ 表示线性逼近 $\boldsymbol{\alpha}\to\boldsymbol{\beta}$ 的概率，则其对应的相关系数 $C_f(\boldsymbol{\alpha},\boldsymbol{\beta})=2p_f(\boldsymbol{\alpha},\boldsymbol{\beta})-1$。此外，令 $F=f_{r-1}\circ f_{r-2}\circ\cdots\circ f_0$，$f_i:\mathbb{F}_2^n\to\mathbb{F}_2^n$，$0\le i\le r-1$，对于每个 f_i 对应的线性逼近 $\boldsymbol{\alpha}_i\to\boldsymbol{\alpha}_{i+1}$，记 $C_{f_i}(\boldsymbol{\alpha}_i,\boldsymbol{\alpha}_{i+1})=2p_{f_i}(\boldsymbol{\alpha}_i,\boldsymbol{\alpha}_{i+1})-1$。

定义 1[2]　给定函数 $F=f_{r-1}\circ\cdots\circ f_0$ 的一个线性堆 $\boldsymbol{\alpha}\to\boldsymbol{\beta}$，称 $\boldsymbol{\Gamma}=(\boldsymbol{\alpha}_0,\boldsymbol{\alpha}_1,\cdots,\boldsymbol{\alpha}_r)$ 为 F 函数的一个起点为 $\boldsymbol{\alpha}=\boldsymbol{\alpha}_0$，终点为 $\boldsymbol{\beta}=\boldsymbol{\alpha}_r$ 的组合传递链。设线性堆 $\boldsymbol{\alpha}\to\boldsymbol{\beta}$ 的相关系数为 $C_F(\boldsymbol{\alpha},\boldsymbol{\beta})$，$f_i$ 的线性特征 $(\boldsymbol{\alpha}_{i-1},\boldsymbol{\alpha}_i)$ 的相关系数为 $C_{f_i}(\boldsymbol{\alpha}_{i-1},\boldsymbol{\alpha}_i)$，则有 $C_F(\boldsymbol{\alpha},\boldsymbol{\beta})=C_{f_1}(\boldsymbol{\alpha}_0,\boldsymbol{\alpha}_1)C_{f_2}(\boldsymbol{\alpha}_1,\boldsymbol{\alpha}_2)\cdots C_{f_r}(\boldsymbol{\alpha}_{r-1},\boldsymbol{\alpha}_r)$。

定义 2[2]　给定函数 $F=f_{r-1}\circ f_{r-2}\circ\cdots\circ f_0$，设 $\boldsymbol{\Gamma}=(\boldsymbol{\alpha}_0,\boldsymbol{\alpha}_1,\cdots,\boldsymbol{\alpha}_r)$ 为 F 函数的一条组合传递链，如果圈函数 f_i 的线性逼近 $\boldsymbol{\alpha}_i\to\boldsymbol{\alpha}_{i+1}$ 的相关系数 $C_{f_i}(\boldsymbol{\alpha}_i,\boldsymbol{\alpha}_{i+1})=0$，则称线性选择模式对 $(\boldsymbol{\alpha}_i,\boldsymbol{\alpha}_{i+1})$ 是不相容的。

由此，文献[3]给出了零相关线性逼近存在的充分条件为：

引理 2[3]　给定函数 $F=f_{r-1}\circ f_{r-2}\circ\cdots\circ f_0$，设 $\boldsymbol{\alpha}\to\boldsymbol{\beta}$ 为 F 函数的一个线性堆对应，如果该线性堆的任意一条组合传递链 $\boldsymbol{\Gamma}=(\boldsymbol{\alpha},\boldsymbol{\alpha}_1,\boldsymbol{L},\boldsymbol{\alpha}_{r-2},\boldsymbol{\beta})$ 至少存在一对不相容的选择模式对，则 $C_F(\boldsymbol{\alpha},\boldsymbol{\beta})=0$。

此外，本文给出如下几个引理和定义：

引理 3[3]　对于置换 P，其相关系数非零的充分条件是输入、输出选择模式都为零或者都不为零。

定义 3[2]　如果 $\boldsymbol{X}=(x_0,x_1,\cdots,x_{n-1})\in(Z_2^l)^n$，则称 $\mathrm{wt}(\boldsymbol{X})=\#\{0\le i\le n-1:x_i\ne 0\}$ 为 $\boldsymbol{X}$ 的重量。

定义 4[2]　设线性变换 $L(\boldsymbol{x})=\boldsymbol{A}\boldsymbol{x}$，则线性分支数定义为 $B_l=\min\{\mathrm{wt}(\boldsymbol{A}^{\mathrm{T}}\boldsymbol{\Gamma}\boldsymbol{y})+\mathrm{wt}(\boldsymbol{\Gamma}\boldsymbol{y}):\boldsymbol{\Gamma}\boldsymbol{y}\ne 0\}$，其中 $\boldsymbol{A}^{\mathrm{T}}$ 表示矩阵 A 的转置。

2.3 零相关-积分分析

文献[5]研究了零相关线性区分器与积分区分器的关系，并将由零相关线性区分器得到积分区分器，然后利用积分区分器攻击分组密码算法的分析方法称为零相关-积分分析。本文进一步研究两类区分器的关系：

引理 4[16]　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 5[16]　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 $(\xi_1,\xi_2,\cdots,\xi_m)$ 与 $(\eta_1,\eta_2,\cdots,\eta_n)$ 独立等价于对所有二元非零向量 $(a_1,a_2,\cdots,a_m)$ 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 $b_1\eta_1\oplus b_2\eta_2\oplus\cdots\oplus b_n\eta_n$ 均独立。

引理 6　对于算法 $f:(F_{2^8})^4\to(F_{2^8})^4$，设其输入和输出分别为 $\boldsymbol{x}=(x_1\,x_2\,x_3\,x_4,\ x_5\,x_6\,x_7\,x_8)$ 和 $\boldsymbol{y}=(y_1\,y_2\,y_3\,y_4,\ y_5\,y_6\,y_7\,y_8)$。对所有非零的 $a,b,c,d\in F_{2^8}$，当 $\boldsymbol{\alpha}=(abab,0000)$ 和 $\boldsymbol{\beta}=(cdcd,0000)$ 都满足 $\boldsymbol{\alpha}\cdot\boldsymbol{x}\oplus\boldsymbol{\beta}\cdot f(\boldsymbol{x})$ 的相关系数为零时，则有 $(x_1\oplus x_3,x_2\oplus x_4)$ 与 $(y_1\oplus y_3,y_2\oplus y_4)$ 独立，即对任意给定的常值 λ_1,λ_2，加密形如 $(x_1,x_2,x_1\oplus\lambda_1,x_2\oplus\lambda_2,x_3x_4x_5x_6)$ 的所有可能输入，$(y_1\oplus y_3,y_2\oplus y_4)$ 每个可能值出现的次数是相同的。

证明　由于任意非零的 $a,b,c,d\in F_{2^8}$，有 $\boldsymbol{\alpha}\cdot\boldsymbol{x}\oplus\boldsymbol{\beta}\cdot f(\boldsymbol{x})$ 的相关系数为零，即 $[a\cdot(x_1\oplus x_3)\oplus b\cdot(x_2\oplus x_4)]\oplus[c\cdot(y_1\oplus y_3)\oplus d\cdot(y_2\oplus y_4)]$ 为平衡函数，所以 $(x_1\oplus x_3,x_2\oplus x_4)$ 是平衡函数，故由引理 4 知上式等价于 $a\cdot(x_1\oplus x_3)\oplus b\cdot(x_2\oplus x_4)$ 与 $c\cdot(y_1\oplus y_3)\oplus d\cdot(y_2\oplus y_4)$ 独立，再由引理 5 可知 $(x_1\oplus x_3,x_2\oplus x_4)$ 与 $(y_1\oplus y_3,y_2\oplus y_4)$ 独立。所以对任意给定的常值 λ_1,λ_2，加密形如 $(x_1,x_2,x_1\oplus\lambda_1,x_2\oplus\lambda_2,x_3x_4x_5x_6)$ 的所有可能输入，$(y_1\oplus y_3,y_2\oplus y_4)$ 每个可能值出现的次数是相同的。　证毕

其中 $\boldsymbol{\alpha}=(abab,0000)$ 和 $\boldsymbol{\beta}=(cdcd,0000)$ 最后位置都为 0，只是为了形式简单而为之。

3　低轮 FOX64 算法的零相关线性分析

3.1 4 轮 FOX 算法零相关线性区分器

定理 1　如果 $\boldsymbol{\alpha}\in\{0,1\}^{32}\setminus\{0\}$ 且 $\mathrm{wt}(\boldsymbol{\alpha})+\mathrm{wt}(\boldsymbol{\alpha}\oplus\boldsymbol{\beta})\le 4$，则 $(\mathrm{io}(\boldsymbol{\alpha}),\mathrm{io}(\boldsymbol{\alpha}))\to(\mathrm{io}(\boldsymbol{\beta}),\mathrm{io}(\boldsymbol{\beta}))$ 是 4 轮 FOX64(最后一轮无正形置换)的零相关线性区分器。

证明　如图 1 所示，当输入选择模式为 $(\mathrm{io}(\boldsymbol{\alpha}),\mathrm{io}(\boldsymbol{\alpha}))$ 时，设第 1 轮圈函数的输出选择模式为 $(\boldsymbol{A},\boldsymbol{B})$，由引理 1 可知 $\mathrm{io}(\boldsymbol{\alpha})\oplus\mathrm{io}(\boldsymbol{\alpha})\oplus\boldsymbol{B}\oplus\boldsymbol{M}\boldsymbol{A}=0$，即 $\boldsymbol{A}=\boldsymbol{M}^{-1}\boldsymbol{B}$，且 f_1 的输入选择模式和输出选择模式分别为 $\mathrm{io}(\boldsymbol{\alpha})\oplus\boldsymbol{B}$ 和 $\mathrm{io}(\boldsymbol{\alpha})\oplus\mathrm{io}(\boldsymbol{\alpha})=0$。再由引理 3 可知，$f_1$ 输出选择模式为 0，相关系数非零的输入选择模式必为 0，即 $\mathrm{io}(\boldsymbol{\alpha})\oplus\boldsymbol{B}=0$，得 $\boldsymbol{B}=\mathrm{io}(\boldsymbol{\alpha})$，由此可得 $\boldsymbol{A}=\mathrm{or}(\boldsymbol{\alpha})$，即第 2 圈的输入选择模式为 $(\mathrm{or}(\boldsymbol{\alpha}),\mathrm{io}(\boldsymbol{\alpha}))$。对第 2 轮圈函数使用引理 1，得 f_2 的输出选择模式为 $\mathrm{or}(\boldsymbol{\alpha})\oplus\mathrm{io}(\boldsymbol{\alpha})=\boldsymbol{\alpha}$。假设 f_2 的输入选择模式为 $\boldsymbol{b}$，由引理 1 可得第 2 圈的输出选择模式为 $(\boldsymbol{\alpha}\oplus\mathrm{io}(\boldsymbol{b}),\mathrm{io}(\boldsymbol{\alpha})\oplus\boldsymbol{b})$。

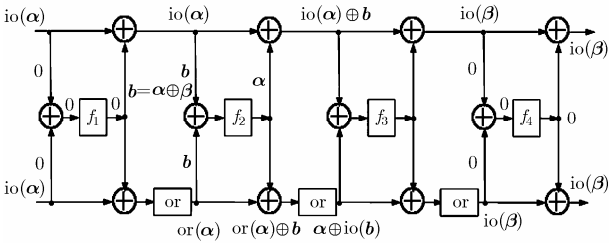

图 1 4 轮 FOX64 的零相关线性区分器

当第 4 圈输出选择模式为 $(\mathrm{io}(\boldsymbol{\beta}),\mathrm{io}(\boldsymbol{\beta}))$ 时，可知第 4 圈的输入选择模式为 $(\mathrm{io}(\boldsymbol{\beta}),\mathrm{io}(\boldsymbol{\beta}))$。此时，对第 3 轮圈函数使用引理 1 有 $\boldsymbol{\alpha}\oplus\mathrm{io}(\boldsymbol{b})\oplus\mathrm{io}(\boldsymbol{\alpha})\oplus\boldsymbol{b}\oplus\mathrm{io}(\boldsymbol{\beta})\oplus\boldsymbol{\beta}=\mathbf{0}$，可得 $\mathrm{or}(\boldsymbol{b})=\mathrm{or}(\boldsymbol{\alpha}\oplus\boldsymbol{\beta})$，即 $\boldsymbol{b}=\boldsymbol{\alpha}\oplus\boldsymbol{\beta}$。因此，$f_2$ 的输入选择模式和输出选择模式分别为 $\boldsymbol{\alpha}\oplus\boldsymbol{\beta}$ 和 $\boldsymbol{\alpha}$。故当 $\mathrm{wt}(\boldsymbol{\alpha})+\mathrm{wt}(\boldsymbol{\alpha}\oplus\boldsymbol{\beta})\le 4$ 时，$\boldsymbol{\alpha}\oplus\boldsymbol{\beta}\to\boldsymbol{\alpha}$ 是不相容的。所以 $(\mathrm{io}(\boldsymbol{\alpha}),\mathrm{io}(\boldsymbol{\alpha}))\to(\mathrm{io}(\boldsymbol{\beta}),\mathrm{io}(\boldsymbol{\beta}))$ 是 4 轮 FOX64 的零相关线性区分器。 证毕

推论 1 对于任意非零字节 a,b,c,d，4 轮 FOX64 算法具有 3 类零相关线性区分器：

$(a0b0,a0b0)\to(c0d0,c0d0)$；$(ab00,ab00)\to(cd00,cd00)$；$(0a0b,0a0b)\to(0c0d,0c0d)$。

证明 当 4 轮 FOX64 算法的输入选择模式和输出选择模式分别为 $(a0b0,a0b0)$ 和 $(c0d0,c0d0)$ 时，有 $\mathrm{wt}(\mathrm{or}(a0b0))+\mathrm{wt}(\mathrm{or}(a0b0)\oplus\mathrm{or}(c0d0))=2+2=4$ 成立，由定理 1 可知 $(a0b0,a0b0)\to(c0d0,c0d0)$ 为 4 轮 FOX64 算法的零相关线性逼近。同理可证另外两种情况。 证毕

3.2 低轮 FOX64 的零相关-积分分析

本节将利用上节给出的 4 轮 FOX 的零相关线性区分器构造 4 轮积分区分器，同时对低轮的 FOX64 算法进行零相关-积分分析。为此，首先给出引理 7。

引理 7 对于 4 轮 FOX64(最后一轮无正形置换)，设 4 轮 FOX64 的输出为 $(w_1w_2w_3w_4,w_5w_6w_7w_8)$，则

(1)加密 2^{48} 个所有可能明文 $(p_1p_2p_3p_4,p_1p_5p_3p_6)$，$w_1\oplus w_5$，$w_3\oplus w_7$ 的 2^8 个可能值各出现 2^{40} 次；

(2)加密 2^{48} 个所有可能明文 $(p_1p_2p_3p_4,p_5p_2p_6p_4)$，$w_2\oplus w_6$，$w_4\oplus w_8$ 的 2^8 个可能值各出现 2^{40} 次；

(3)加密 2^{48} 个所有可能明文 $(p_1p_2p_3p_4,p_1p_2p_5p_6)$，$w_1\oplus w_5$，$w_2\oplus w_6$ 的 2^8 个可能值各出现 2^{40} 次。

证明 (1)由推论 1 可知 $(a0b0,a0b0)\to(c0d0,c0d0)$ 为 4 轮 FOX64 算法的零相关线性逼近，然后取引理 6 中的 $\lambda=0$，即可得此结论。同理可得到引理 7(2)和引理 7(3)。 证毕

下面证明中，令明文结构 $P_1=\{(p_1p_2p_3p_4,p_1p_5p_3p_6)\,|\,p_i\in F_{2^8},i=1,2,\cdots,6\}$，$P_2=\{(p_1\ p_2\ p_3\ p_4,p_5p_2p_6p_4)\,|\,p_i\in F_{2^8},i=1,2,\cdots,6\}$，$P_3=\{(p_1\ p_2\ p_3\ p_4,p_1p_2p_5p_6)\,|\,p_i\in F_{2^8},i=1,2,\ldots,6\}$。

设第 5 轮 64 bit 子密钥为 $\mathrm{RK}_5=K_0^5\,||\,K_1^5=(k_{0,1}^5k_{0,2}^5k_{0,3}^5k_{0,4}^5,k_{1,1}^5k_{1,2}^5k_{1,3}^5k_{1,4}^5)$，5 轮 FOX64(最后一轮无 or 变换)的输出为 $(C_L,C_R)=(u_1u_2u_3u_4,u_5u_6u_7u_8)$。其中，对于第 5 轮的 Imid64 变换，输入块的异或和等于输出块的异或和。所以第 5 轮 F 函数的输入为 $C_L\oplus C_R$。

引理 8 对于 5 轮 FOX64(最后一轮无 or 变换)，第 4 轮的输出 $(w_1w_2w_3w_4,w_5w_6w_7w_8)$ (未经过 or 变换)与密文 $(C_L,C_R)=(u_1u_2u_3u_4,u_5u_6u_7u_8)$ 及 64 bit 密钥 $\mathrm{RK}_5=K_0^5\,||\,K_1^5$ 的关系为：

(1) $w_1\oplus w_5=u_1\oplus u_3\oplus u_5\oplus s_{k_{1,3}^5}(t_3)\oplus k_{0,3}^5$；

(2) $w_3\oplus w_7=u_1\oplus u_7\oplus s_{k_{1,1}^5}(t_1)\oplus s_{k_{1,3}^5}(t_3)\oplus k_{0,1}^5\oplus k_{0,3}^5$；

(3) $w_2\oplus w_6=u_2\oplus u_4\oplus u_6\oplus s_{k_{1,4}^5}(t_4)\oplus k_{0,4}^5$；

(4) $w_4\oplus w_8=u_2\oplus u_8\oplus s_{k_{1,2}^5}(t_2)\oplus s_{k_{1,4}^5}(t_4)\oplus k_{0,2}^5\oplus k_{0,4}^5$。

其中 $(t_1t_2t_3t_4)=\mathrm{mu4}(\mathrm{sigma4}(C_L\oplus C_R\oplus K_0^5))$，$s_{k_{i,j}^5}(t_j)=s[\mathrm{mu4}(\mathrm{sigma4}(\Delta\mathrm{C}\oplus K_0^5)_j\oplus k_{i,j}^5]$。

证明 由于 $f_5(C_L\oplus C_R,\ \mathrm{RK}_5)=\mathrm{sigma4}(\mathrm{mu4}\cdot(\mathrm{sigma4}(C_L\oplus C_R\oplus K_0^5))\oplus K_1^5)\oplus K_0^5$，所以已知 K_0^5 及 $C_L\oplus C_R$ 的值，即可求得 $(t_1t_2t_3t_4)=\mathrm{mu4}(\mathrm{sigma4}\cdot(C_L\oplus C_R\oplus K_0^5))$ 的值。此时，有

$$w_3=u_1\oplus s_{k_{1,1}^5}(t_1)\oplus k_{0,1}^5,\quad w_4=u_2\oplus s_{k_{1,2}^5}(t_2)\oplus k_{0,2}^5$$

$$w_1\oplus w_3=u_3\oplus s_{k_{1,3}^5}(t_3)\oplus k_{0,3}^5$$

$$w_2\oplus w_4=u_4\oplus s_{k_{1,4}^5}(t_4)\oplus k_{0,4}^5$$

$$w_5=u_5\oplus s_{k_{1,1}^5}(t_1)\oplus k_{0,1}^5,\ w_6=u_6\oplus s_{k_{1,2}^5}(t_2)\oplus k_{0,2}^5$$

$$w_7=u_7\oplus s_{k_{1,3}^5}(t_3)\oplus k_{0,3}^5,\ w_8=u_8\oplus s_{k_{1,4}^5}(t_4)\oplus k_{0,4}^5$$

所以 $w_1\oplus w_5=w_1\oplus w_3\oplus w_3\oplus w_5=u_1\oplus u_3\oplus u_5\oplus s_{k_{1,3}^5}(t_3)\oplus k_{0,3}^5$，同理可证其它等式。 证毕

由引理 7(1)可知，对明文结构 P_1 进行加密，有 $\bigoplus_{i=1}^{2^{48}}(w_{i,1}\oplus w_{i,5})=0$ 成立。令 $\Sigma=\bigoplus_{i=1}^{2^{48}}(u_{i,1}\oplus u_{i,3}\oplus u_{i,5})$，则有 $\bigoplus_{i=1}^{2^{48}}(s_{k_{1,3}^5}(t_3))=\Sigma$ 成立，其中 $s_{k_{1,3}^5}(t_3)=s[\mathrm{mu4}\cdot(\mathrm{sigma4}(\Delta\mathrm{C}\oplus K_0^5)_3\oplus k_{1,3}^5]$。因此，对于 2^{48} 个密文以及 2^{40} 个密钥 $(k_{0,1}^5k_{0,2}^5k_{0,3}^5k_{0,4}^5k_{1,3}^5)$，求得 $\bigoplus_{i=1}^{2^{48}}(s_{k_{1,3}^5}(t_3))$ 需要 2^{88} 次查表。这里，利用 $\bigoplus_{i=1}^{2^{48}}(s_{k_{1,3}^5}(t_3))=\bigoplus_{x=0}^{255}x(\#\{i:s_{k_{1,3}^5}(t_3)=x\}\bmod 2)$，给出降低计算 $\bigoplus_{i=1}^{2^{48}}(s_{k_{1,3}^5}(t_3))$ 时间复杂度的方法[17]。此时，令 $T(k_1\,k_2\,k_3\,k_4\,k_5\,x)=\#\{i:\bigoplus_{j=1}^{4}f_j(c_{i,j}\oplus k_j)\oplus k_5=x\}\bmod 2$，并定义 χ 函数为：

$\chi(A)=1$ 如果事件 A 发生，否则 $\chi(A)=0$。给出求得 $\underset{x}{\oplus}[x\cdot T(k_1\,k_2\,k_3\,k_4\,k_5\,x)]$ 快速统计算法，其中 $(k_1\,k_2\,k_3\,k_4\,k_5)=(k_{0,1}^5\,k_{0,2}^5\,k_{0,3}^5\,k_{0,4}^5\,k_{1,3}^5)$：

算法 1　计算 $\underset{x}{\oplus}[x\cdot T(k_1\,k_2\,k_3\,k_4\,k_5\,x)]$ 快速统计算法。

步骤 1　对于 2^{48} 个密文及 k_1 的 2^8 个可能密钥，计算 $T(k_1y_2y_3y_4z_1)=\underset{1\le i\le 2^{48},c_{i,2}=y_2,c_{i,3}=y_3,c_{i,4}=y_4}{\oplus}\chi(f_1(c_{i,1},k_1)=z_1)$；

步骤2　对 (k_1k_2) 的 2^{16} 个可能密钥，遍历 y_2,y_3,y_4,z_1，计算 $T(k_1k_2y_3y_4z_2)=\underset{z_1,y_2}{\oplus}[\chi\{z_1\oplus f_2(y_2,k_2)=z_2\}\times T(k_1y_2y_3y_4z_1)]$；

步骤3　对 $(k_1k_2k_3)$ 的 2^{24} 个可能密钥，遍历 y_3,y_4,z_2，计算 $T(k_1k_2k_3y_4z_3)=\underset{z_2,y_3}{\oplus}[\chi\{z_2\oplus f_3(y_3,k_3)=z_3\}\times T(k_1k_2y_3y_4z_2)]$；

步骤4　对 $(k_1k_2k_3k_4)$ 的 2^{32} 个可能密钥，遍历 y_4,z_3，计算 $T(k_1k_2k_3k_4z_4)=\underset{z_3,y_4}{\oplus}[\chi\{z_3\oplus f_4(y_4,k_4)=z_4\}\times T(k_1k_2k_3y_4z_3)]$；

步骤5　对 $(k_1\,k_2\,k_3\,k_4\,k_5)$ 的 2^{40} 个密钥，遍历 z_4，计算 $T(k_1\,k_2\,k_3\,k_4\,k_5\,z_5)=\underset{z_4}{\oplus}[\chi\{z_4\oplus k_5=z_5\}\times T(k_1\,k_2\cdot k_3\,k_4\,z_4)]$；

步骤 6　求得 $\underset{z_5}{\oplus}[z_5\cdot T(k_1\,k_2\,k_3\,k_4\,k_5\,z_5)]$。

步骤1的时间复杂度为 $2^{48}\times 2^8=2^{56}$，空间复杂度为2^{32}。步骤2到步骤5的时间复杂度均为 2^{48}，空间复杂度分别为2^{24}, 2^{16}, 2^8, 1。故算法1的时间复杂度约为 2^{56}，空间复杂度为2^{32}。

在4轮积分区分器的末尾增加一轮，给出5轮FOX64的积分分析(如图2)，其中用 $(u_1\,u_2\,u_3\,u_4,\,u_5\,u_6\,u_7\,u_8)$ 表示密文，令 $\Delta\mathrm{C}=(u_1\,u_2\,u_3\,u_4)\oplus(u_5\,u_6\,u_7\,u_8)$。本文简记 $\Delta_{j,t}=\overset{2^{48}}{\underset{i=1}{\oplus}}(s(\mathrm{mu4}(\mathrm{sigma4}\cdot(\Delta\mathrm{C}_i\oplus K_0^5))_t\oplus k_{j,t}^5))$，令 $\Gamma_{j,t}$ 表示2^{48}个密文差 $\Delta\mathrm{C}_i$ 及40 bit密钥 $K_0^5\,||\,k_{j,t}^5$ 对应的 $\overset{2^{48}}{\underset{i=1}{\oplus}}(s(\mathrm{mu4}(\mathrm{sigma4}\cdot(\Delta\mathrm{C}_i\oplus K_0^5))_t\oplus k_{j,t}^5))$ 的所有可能值，此时 ΔC 等于 f_5 的输入。攻击5轮FOX64算法的步骤如下：

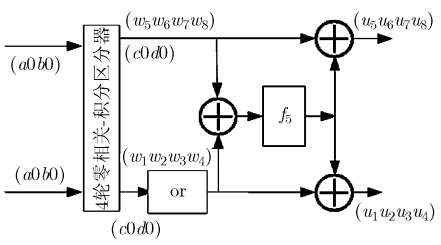

图 2　5轮FOX64的零相关-积分分析

步骤 1　设明文结构 P_1 对应的密文为 C_1，求得 $\Sigma_1=\overset{2^{48}}{\underset{i=1}{\oplus}}(u_{i,1}\oplus u_{i,3}\oplus u_{i,5})$。同时，利用算法 1 求得 $\Gamma_{1,3}$。

猜测40 bit密钥 $K_0^5\,||\,k_{1,3}^5$ 的每个可能值，查表 $\Gamma_{1,3}$ 得到 $\Delta_{1,3}$。如果 $\Delta_{1,3}\oplus\Sigma_1\neq 0$，抛弃 $K_0^5\,||\,k_{1,3}^5$。否则，保留对应密钥 $K_0^5\,||\,k_{1,3}^5$。

步骤 2　设明文结构 P_2 对应的密文为 C_2，求得 $\Sigma_2=\overset{2^{48}}{\underset{i=1}{\oplus}}(u_{i,2}\oplus u_{i,4}\oplus u_{i,6})$。同时，利用算法 1 求得 $\Gamma_{1,4}$。

猜测40比特密钥 $K_0^5\,||\,k_{1,4}^5$ 的每个可能值，查表 $\Gamma_{1,4}$ 得到 $\Delta_{1,4}$。如果 $\Delta_{1,4}\oplus\Sigma_2\neq 0$，抛弃 $K_0^5\,||\,k_{1,4}^5$。否则，保留对应密钥 $K_0^5\,||\,k_{1,4}^5$。

步骤 3　设明文结构 P_3 对应的密文为 C_3，求得 $\Sigma_3=\overset{2^{48}}{\underset{i=1}{\oplus}}(u_{i,1}\oplus u_{i,3}\oplus u_{i,5})$ 及 $\Sigma_4=\overset{2^{48}}{\underset{i=1}{\oplus}}(u_{i,2}\oplus u_{i,4}\oplus u_{i,6})$。同时，分别利用算法 1 求得新的 $\Gamma_{1,3}$ 及 $\Gamma_{1,4}$。

(1) 猜测步骤1保留的每个可能值 $K_0^5\,||\,k_{1,3}^5$，查表 $\Gamma_{1,3}$ 得到 $\Delta_{1,3}$。如果 $\Delta_{1,3}\oplus\Sigma_3\neq 0$，抛弃 $K_0^5\,||\,k_{1,3}^5$。否则，保留对应密钥 $K_0^5\,||\,k_{1,3}^5$。

(2) 猜测步骤2保留的每个可能值 $K_0^5\,||\,k_{1,4}^5$，查表 $\Gamma_{1,4}$ 得到 $\Delta_{1,4}$。如果 $\Delta_{1,4}\oplus\Sigma_4\neq 0$，抛弃 $K_0^5\,||\,k_{1,4}^5$。否则，保留对应密钥 $K_0^5\,||\,k_{1,4}^5$。

步骤 4　对于给定常值 $\lambda\neq 0$，设 $P_\lambda=\{(p_1p_2p_3p_4,\,p_1\oplus\lambda,p_2\oplus\lambda,p_5,p_6)\,|\,p_i\in F_{2^8},i=1,2,\cdots,6\}$　对应密文为 C_4，求得 $\Sigma_5=\overset{2^{48}}{\underset{i=1}{\oplus}}(u_{i,1}\oplus u_{i,3}\oplus u_{i,5})$ 及 $\Sigma_6=\overset{2^{48}}{\underset{i=1}{\oplus}}(u_{i,2}\oplus u_{i,4}\oplus u_{i,6})$。同时，分别利用算法 1 求得新的 $\Gamma_{1,3}$ 及 $\Gamma_{1,4}$。

(1) 猜测步骤3(1)保留的每个可能值 $K_0^5\,||\,k_{1,3}^5$，查表 $\Gamma_{1,3}$ 得到 $\Delta_{1,3}$。如果 $\Delta_{1,3}\oplus\Sigma_5\neq 0$，抛弃 $K_0^5\,||\,k_{1,3}^5$。否则，保留对应密钥 $K_0^5\,||\,k_{1,3}^5$。

(2) 猜测步骤3(2)保留的每个可能值 $K_0^5\,||\,k_{1,4}^5$，查表 $\Gamma_{1,4}$ 得到 $\Delta_{1,4}$。如果 $\Delta_{1,4}\oplus\Sigma_6\neq 0$，抛弃 $K_0^5\,||\,k_{1,4}^5$。否则，保留对应密钥 $K_0^5\,||\,k_{1,4}^5$。

步骤 5　输出正确密钥 $K_0^5\,||\,k_{1,3}^5\,||\,k_{1,4}^5$。

上述攻击算法中，数据复杂度为 $4\times 2^{48}=2^{50}$，存储复杂度为 2^{50} 个密文。步骤 1 和步骤 2 的时间复杂度为 2^{56} 次查表运算，步骤 3 和步骤 4 的时间复杂度为 $2\times 2^{56}=2^{57}$ 次查表运算。对于错误密钥，使得 $\overset{2^{48}}{\underset{i=1}{\oplus}}(w_{i,1}\oplus w_{i,5})=0$ 或 $\overset{2^{48}}{\underset{i=1}{\oplus}}(w_{i,2}\oplus w_{i,6})=0$ 成立的概率都为 2^{-8}，则 48 bit 密钥 $K_0^5\,||\,k_{1,3}^5\,||\,k_{1,4}^5$ 经步骤 1 到步骤 4 的过滤，剩余密钥个数为 $2^{48}\times(2^{-8})^6=1$，即正确密钥被唯一确定。

同理，利用引理 7(1)、引理 7(3)，通过统计 $w_3 \oplus w_7$ 和 $w_4 \oplus w_8$ 的 2^8 个可能值是否出现 2^{40} 次，可以分别恢复 $k_{1,1}^5$ 及 $k_{1,2}^5$，时间复杂度都为 2^{56} 次查表。故恢复 RK_5 的数据复杂度为 2^{50} 个选择明文，时间复杂度为 $8\times 2^{56}=2^{59}$ 次查表运算。由于 FOX64 算法圈函数的实现大约需要 2^4 次查表运算。故该攻击的时间复杂度约为 $2^{59}\times 2^{-4}\times 1/5\approx 2^{52.7}$ 次 5 轮 FOX64 加密。获得第 5 轮圈子密钥 RK_5 后，我们可以利用文献[9]给出的 4 轮 FOX64 的积分攻击恢复前 4 轮子密钥，其复杂度约为 $2^{45.4}$ 次 4 轮 FOX64 加密。此外，对于 6 轮 FOX64 的攻击，我们可以通过穷举第 6 轮全部 64 bit 子密钥来实现，其时间复杂度约为 $2^{116.7}$ 次 6 轮 FOX64 加密。同理可知，对 7 轮和 8 轮 FOX64 攻击的时间复杂度约为 $2^{180.7}$ 和 $2^{244.7}$ 次加密。

4 结束语

本文分析了 FOX64 算法抗零相关线性分析的能力，并利用零相关线性分析与积分分析相结合的方法分析了 FOX64 算法的安全性，结果表明零相关-积分分析对低轮 FOX64 算法是一类有效的攻击。攻击的数据复杂度为 2^{50} 个选择明文，攻击 5 轮 FOX64/64 的时间复杂度为 $2^{52.7}$ 次加密，6 轮 FOX64/128 的时间复杂度为 $2^{116.7}$ 次加密，7 轮 FOX64/192 的时间复杂度为 $2^{180.7}$ 次加密，8 轮 FOX64/256 的时间复杂度为 $2^{244.7}$ 次加密。鉴于本文关于低轮 FOX64 的零相关-积分分析结果，要求设计者在设计分组密码算法时，必须评估其抵抗零相关线性分析的能力。

参 考 文 献

[1] Biham E and Shamir A. Differential cryptanalysis of DES-like cryptosystems[C]. Proceedings of the CRYPTO 1990, Santa Barbara, CA, USA, 1990, 537: 2–21.

[2] Matsui M. Linear cryptanalysis method for DES cipher[C]. Proceedings of the EUROCRYPT 1993, Lofthus, Norway, 1993, 765: 386–397.

[3] Bogdanov A and Rijmen V. Linear hulls with correlation zero and linear cryptanalysis of block ciphers[J]. *Designs, Codes and Cryptography*, 2014, 70(3): 369–383.

[4] Bogdanov A and Wang M. Zero correlation linear cryptanalysis with reduced data complexity[C]. Proceedings of the Fast Software Encryption 2012, Washington DC, USA, 2012, 7549: 29–48.

[5] Bogdanov A, Leander G, Nyberg K, *et al*.. Integral and multidimensional linear distinguishers with correlation zero[C]. Proceedings of the ASIACRYPT 2012, Beijing, China, 2012, 7658: 244–261.

[6] Hadi S. Zero correlation linear cryptanalysis of reduced-round LBlock[J]. *Designs, Codes and Cryptography*, 2014, To be published.

[7] Junod P and Vaudenay S. FOX: a new family of block ciphers[C]. Proceedings of the Selected Areas in Cryptography-SAC 2004, Ottawa, Canada, 2004, 2595: 131–146.

[8] Vaudenay S. On the Lai-Massey scheme[C]. Proceedings of the ASIACRYPT 1999, Singapore, 1999, 1716: 8–19.

[9] Aaram Y and Je H. On Lai-Massey and quasi-Feistel ciphers[J]. *Design, Codes and Cryptography*, 2011, 58(1): 45–72.

[10] Wu Wen-ling, Zhang Wen-tao, and Feng Deng-guo. Integral cryptanalysis of reduced FOX block cipher[C]. Proceedings of the Information Security and Cryptology-ICISC 2005, Beijing, China, 2005, 3935: 229–241.

[11] Wu Zhong-ming, Lai Xue-jia, Zhu Bo, *et al*.. Impossible differential cryptanalysis of FOX[C]. Proceedings of the first International Conference on Information Security: Beijing, China, 2010, 6163: 236–249.

[12] 魏悦川, 孙兵, 李超. FOX 密码的不可能差分攻击[J]. 通信学报, 2010, 31(9): 24–29.
Wei Yue-chuan, Sun Bing, and Li Chao. Impossible differential attack on FOX[J]. *Journal on Communications*, 2010, 31(9): 24–29.

[13] Chen jie, Hu Yu-pu, Zhang Yue-yu, *et al*.. Differential collision attack on reduced FOX block cipher[J]. *China Communications*, 2012, 9(7): 71–76.

[14] Li Rui-lin, You Jian-xiong, Sun Bing, *et al*.. Fault analysis study of the block cipher FOX64[J]. *Multimedia Tools and Applications*, 2013, 63(3): 691–708.

[15] Blondeau C and Nyberg K. New links between differential and linear cryptanalysis[C]. Proceedings of the EUROCRYPT 2013, Athens, Greece, 2013, 788: 388–404.

[16] 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.
Jin Chen-hui. 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.

[17] Ferguson N, Kelsey J, Lucks S, *et al*.. Improved cryptanalysis of Rijndael[C]. Proceedings of the Fast Software Encryption 2000, New York, USA, 1978: 213–230.

郭 瑞： 男，1985 年生，博士生，研究方向为密码学.

金晨辉： 男，1965 年生，教授，博士生导师，研究方向为密码学与信息安全.