doi:10.11959/j.issn.1000-436x.2016234

MIBS 密码的零相关—积分攻击

刘庆聪[1]，赵亚群[1]，马猛[1]，刘凤梅[2]
(1. 信息工程大学数学与先进计算国家重点实验室，河南 郑州 450001;
2. 信息保障技术重点实验室，北京 100072)

摘 要：MIBS 算法是一种轻量级分组密码算法，普遍应用于电子标签和传感器网络等环境。首先，分析 MIBS 算法抵抗零相关积分分析的能力，给出一个 8 轮的 MIBS 算法零相关线性区分器。然后，利用零相关线性区分器和积分区分器之间的关系，构造一个 8 轮的 MIBS 算法的积分区分器。最后，利用该区分器结合 MIBS 算法的对称结构，基于部分和技术，分析 10 轮、12 轮的 MIBS-80 算法。得到的攻击时间复杂度分别为 $2^{27.68}$、$2^{48.81}$，数据复杂度为 2^{48}。

关键词：分组密码；密码分析；MIBS 算法；零相关—积分分析
中图分类号： TP918.1 **文献标识码**：A

Zero correlation-integral attack of MIBS block cipher

LIU Qing-cong[1], ZHAO Ya-qun[1], MA Meng[1], LIU Feng-mei[2]
(1. State Key Laboratory of Mathematical Engineering and Advanced Computing, Information Engineering University, Zhengzhou 450001, China;
2. Science and Technology on Information Assurance Laboratory, Beijing 100072, China)

Abstract: MIBS is a lightweight block cipher for extremely constrained environments such as RFID tags and sensor networks. The MIBS algorithm's ability to resist zero correlation-integral analysis was evaluated. An 8-round zero correlation linear distinguisher of MIBS was given. Then, a 8-round distinguisher of MIBS was founded by using relationship between zero-correlation linear distinguisher and integral distinguisher. Finally, considering the symmetrical structure of the MIBS and using the partial-sum technique, it applied integral attack to 10 and 12 rounds of MIBS-80. The time complexities of 10 and 12 round attack on MIBS-80 are $2^{27.68}$and $2^{48.81}$. The data complexity is 2^{48}.
Key words: block cipher, cryptanalysis, MIBS algorithm, zero-correlation integral cryptanalysis

1 引言

随着移动通信技术以及互联网的高速发展，RFID 技术得到了迅速发展。为适应 RFID 技术在便携式计算设备上的应用，一些软硬件易于实现、运算速度较快的轻量级分组密码算法相继被提出。MIBS[1]算法是一种轻量级 Feistel 型分组密码算法，它使用成本低、占用资源少、常应用在微型计算设备上。MIBS 算法的分组长度为 64 bit，共有 32 轮。密钥长度分为 2 种：64 bit 和 80 bit。从 MIBS 提出到现在已有很多分析结果，在文献[2]中，密码设计者利用差分分析和线性分析方法说明了 MIBS 算法在安全性、加密速度和执行成本这 3 个方面实现了很好的平衡。文献[3]给出了 MIBS 算法的 4.5 轮积分区分器，并对其进行了 8 轮、9 轮积分攻击。文献[4]对 MIBS 算法进行了 10 轮积分攻击。文献[5]构造了一个 5 轮积分区分器，使用等效的思想给出了 MIBS 算法 10 轮的积分攻击。

零相关线性分析[6]由 Bogdanov 等首次提出，并在诸多算法中得到了应用，其中，有 XTEA[7]、TEA[7]、LBLOCK[8]、Camellia[9]、CLEIFA[9]、HIGHT[10]和 E2[11]等算法。零相关线性分析所需要的数据量是整个或一半文本空间。为了解决数据复杂度较高的问题，文献[9]给出了多重零相关线性分析模型。但

收稿日期：2015-12-28；**修回日期**：2016-04-06
基金项目：信息安全保障技术国家重点实验室开放基金资助项目（No.KJ-13-009）
Foundation Item: The Foundation of Science and Technology on Information Assurance Laboratory(No.KJ-13-009)

该模型依赖一个强假设条件：线性逼近相互对立。为了消除这个强假设条件，Bogdanov 等[12]给出了多维零相关线性分析模型，并从理论上证明了与积分区分器的关系。与多维零相关线性分析相比，积分零相关的数据复杂度显著降低。但是迄今为止还没有人将零相关—积分攻击用于 MIBS 算法的分析。

本文首次使用零相关—积分分析[12]方法对 MIBS-80 算法进行攻击。根据零相关线性区分器与积分区分器之间的关系，由 MIBS-80 算法的 8 轮零相关区分器得出一个 8 轮积分区分器。最后利用积分分析方法，再结合部分和技术对 10 轮、12 轮的 MIBS-80 算法进行了攻击。攻击结果显示，使用零相关—积分分析方法，优于以往的积分分析方法得出的结果。

2 基础知识

2.1 相关符号

$\boldsymbol{a}\|\boldsymbol{b}$：向量 $\boldsymbol{a}$、$\boldsymbol{b}$ 的连接。

F_i^j：第 i 轮的轮函数输出的第 j 个半字节。

$L_i\|R_i$：第 $i+1$ 轮的输入，同时也是第 i 轮的输出。

$L_i(j)$：L_i 的第 j 个半字节。

$R_i(j)$：R_i 的第 j 个半字节。

$k_i(j)$：第 i 轮函数子密钥的第 j 个半字节。

$M_i(j)$：第 i 轮 S 盒输出的第 j 个半字节。

2.2 MIBS 算法简介

本节首先介绍 MIBS 算法的加密过程及其密钥扩展算法，然后介绍了零相关线性分析和积分分析之间的关系。

2.2.1 加密过程

MIBS 算法是轻量级 Feistel 型分组密码算法，分组长度是 64 bit，共 32 轮。密钥长度有 64 bit 和 80 bit 这 2 种。64 bit 的明文分成左右 2 部分：L_0 和 R_0。MIBS-80 以 4 bit 为一个单位（称为半字节或半位元）。MIBS 的轮函数由密钥加操作、S 盒变换、P 盒变换构成。S 盒变换为 8 个相同的 4×4 的小 S 盒的并置，P 盒变换为 8 个小 S 盒输出的对位异或加以及位置变换。设 L_{i-1}、R_{i-1} 是第 i 轮的输入，k_i 是第 i 轮的轮密钥，长度为 32 bit。第 i 轮的输出为：$L_i = F(k_i, L_{i-1}) \oplus R_{i-1}$，$R_i = L_{i-1}$。

轮密钥加操作：每一轮左侧的 32 bit 消息与 32 bit 轮子密钥进行异或加。

S 盒变换：$S = \{4,15,3,8,13,10,12,0,11,5,7,14,2,6,1,9\}$，$S: F_2^4 \to F_2^4 : y_i = S(x_i), 1 \leqslant i \leqslant 8$。

P 盒变换：P 盒变换包括混合层和置换层，可以看为线性变换 $\boldsymbol{L}$，由如下线性关系构成。

$$y_1 = x_1 \oplus x_2 \oplus x_4 \oplus x_5 \oplus x_7 \oplus x_8$$

$$y_2 = x_2 \oplus x_3 \oplus x_4 \oplus x_5 \oplus x_6 \oplus x_7$$

$$y_3 = x_1 \oplus x_2 \oplus x_3 \oplus x_5 \oplus x_6 \oplus x_8$$

$$y_4 = x_2 \oplus x_3 \oplus x_4 \oplus x_7 \oplus x_8$$

$$y_5 = x_1 \oplus x_3 \oplus x_4 \oplus x_5 \oplus x_8$$

$$y_6 = x_1 \oplus x_2 \oplus x_4 \oplus x_5 \oplus x_6$$

$$y_7 = x_1 \oplus x_2 \oplus x_3 \oplus x_6 \oplus x_7$$

$$y_8 = x_1 \oplus x_3 \oplus x_4 \oplus x_6 \oplus x_7 \oplus x_8$$

这个线性变换是可逆的，其逆记为 $\boldsymbol{L}^{-1}$，表示为 $(x_1, x_2, \cdots, x_8) = \boldsymbol{L}^{-1}(y_1, y_2, \cdots, y_8)$，由如下线性关系构成。

$$x_1 = y_2 \oplus y_4 \oplus y_6 \oplus y_7 \oplus y_8$$

$$x_2 = y_1 \oplus y_4 \oplus y_5 \oplus y_7 \oplus y_8$$

$$x_3 = y_1 \oplus y_3 \oplus y_5 \oplus y_6 \oplus y_7$$

$$x_4 = y_2 \oplus y_3 \oplus y_5 \oplus y_6 \oplus y_7$$

$$x_5 = y_1 \oplus y_3 \oplus y_4 \oplus y_5 \oplus y_7 \oplus y_8$$

$$x_6 = y_1 \oplus y_2 \oplus y_4 \oplus y_5 \oplus y_6 \oplus y_8$$

$$x_7 = y_1 \oplus y_3 \oplus y_5 \oplus y_6 \oplus y_7 \oplus y_8$$

$$x_8 = y_1 \oplus y_2 \oplus y_3 \oplus y_4 \oplus y_6 \oplus y_7$$

2.2.2 MIBS 的密钥扩展算法

设主密钥 $K = (K_{79}, K_{78}, \cdots, K_0)$，其长度为 80 bit，由主密钥生成 32 个 32 bit 的轮子密钥 k_i $(1 \leqslant i \leqslant 32)$ 的过程如下。

1) $state^i \leftarrow K$，对 $i = 1,2,\cdots,32$

2) $state^i \leftarrow state^i >>> 19$

3) $state^i \leftarrow S(state^i_{[79:76]}) \| S(state^i_{[75:72]}) \| state^i_{[71:0]}$

4) $state^i \leftarrow (state^i_{[79:19]}) \| (state^i_{[18:14]}) \oplus Round\_counter \| state^i_{[13:0]}$

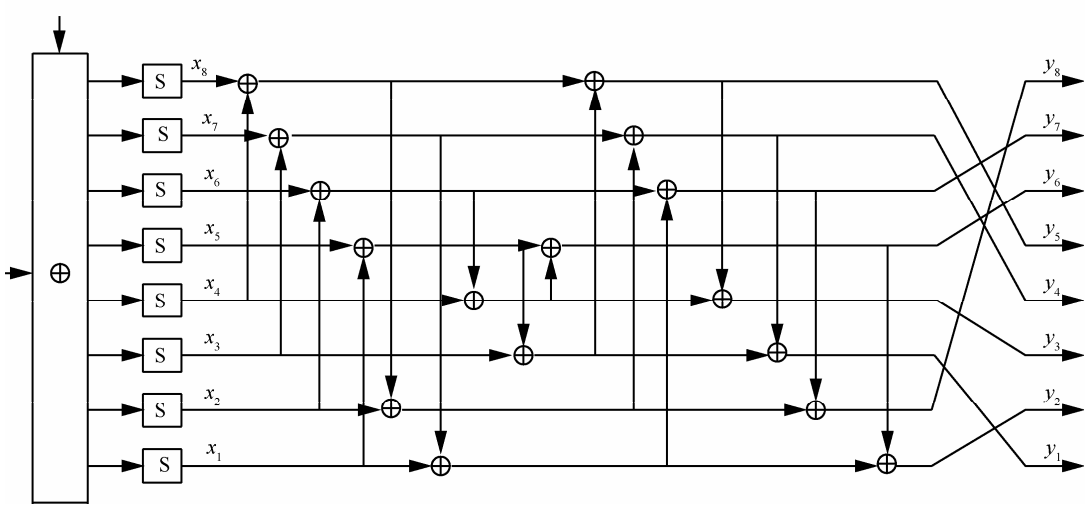


图 1　MIBS 的 F 函数

5)　$k_i \leftarrow state^i_{[79:48]}$

2.3　零相关—积分分析

文献[5]给出了积分区分器与零相关区分器之间的相互关系，零相关线性区分器可以和积分区分器相互转化，并使用积分区分器攻击对分组密码算法进行分析，这种方法被称为零相关—积分分析。

引理 1[13]　设 ξ、η 均是二元随机变量，且 ξ 服从等概率分布，则 $\xi \oplus \eta$ 服从等概率分布的充分必要条件是 ξ 与 η 独立。

引理 2[13]　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 $\eta_1,\eta_2,\cdots,\eta_n$ 独立等价于对所有二元非零向量 $(a_1,a_2,\cdots,a_m)$ 和 $(b_1,b_2,\cdots,b_n)$，$a_1\xi_1 \oplus a_2\xi_2 \oplus \cdots \oplus a_m\xi_m$ 与 $b_1\eta_1 \oplus \cdots \oplus b_n\eta_n$ 均独立。

引理 3[14]　对于算法 $f:(F_{2^8})^4 \to (F_{2^8})^4$，设其输入和输出分别为 $\boldsymbol{x}=(x_1x_2x_3x_4,x_5x_6x_7x_8)$ 和 $\boldsymbol{y}=(y_1y_2y_3y_4,y_5y_6y_7y_8)$。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 $\boldsymbol{\alpha}\cdot\boldsymbol{x} \oplus \boldsymbol{\beta}\cdot\boldsymbol{y}$ 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 $(x_1,x_2,x_1 \oplus \lambda_1, x_2 \oplus \lambda_2, x_3x_4x_5x_6)$ 的全部可能输入，$(y_1 \oplus y_3, y_2 \oplus y_4)$ 每个可能值出现的次数是相同的。

引理 4　对于算法 $f:(F_{2^4})^8 \to (F_{2^4})^8$，设其输入为 $\boldsymbol{x}=(x_1x_2\cdots x_8, x_9x_{10}\cdots x_{16})$，输出为 $\boldsymbol{y}=(y_1y_2\cdots y_8,\ y_9y_{10}\cdots y_{16})$。对所有非零的 $a,b \in F_{2^4}$，当 $\boldsymbol{\alpha}=(aaaaa000,00000000)$ 和 $\boldsymbol{\beta}=(bbbbb000,00000000)$ 满足 $\boldsymbol{\alpha}\cdot\boldsymbol{x} \oplus \boldsymbol{\beta}\cdot\boldsymbol{y}$ 的相关系数为零时，则有 $(x_1 \oplus x_2 \oplus x_3 \oplus x_4 \oplus x_5)$ 与 $(y_1 \oplus y_2 \oplus y_3 \oplus y_4 \oplus y_5)$ 独立，即对任意加密形如 $(x_1x_1x_1x_1x_1x_2x_3x_4, x_5x_6\cdots x_{12})$ 的全部可能输入，$(y_1 \oplus y_2 \oplus y_3 \oplus y_4 \oplus y_5)$ 每个可能值出现的次数是相同的。

证明　将引理 3 中的算法 $f:(F_{2^8})^4 \to (F_{2^8})^4$ 改为 $f:(F_{2^4})^8 \to (F_{2^4})^8$，将其中的 λ 设为 0，再由引理 1 和引理 2 即可得证。

3　MIBS 算法的零相关—积分分析

3.1　8 轮 MIBS 算法的零相关线性逼近

将 MIBS 的半字节看成一个整体，考虑 MIBS 算法 P 盒的性质，可以找出一个 8 轮 MIBS 的零相关线性逼近区分器。

定理 1　如果 $a,b \in F_2^4 \setminus \{0\}$，则 $(0aa0aaa0, 00000000) \to (00000000, 0bb0bbb0)$ 是 8 轮 MIBS 算法的零相关线性区分器。证明过程如图 2 所示。

引理 5　设 8 轮 MIBS 算法的输出为 $(w_1w_2\cdots w_8, w_9w_{10}\cdots w_{16})$，则加密 2^{48} 个所有可能明文 $(p_1p_2p_2p_3p_2p_2p_2p_4, p_5p_6p_7p_8p_9p_{10}p_{11}p_{12})$，$w_{10} \oplus w_{11} \oplus w_{13} \oplus w_{14} \oplus w_{15}$ 的 2^4 个可能值各出现 2^{44} 次。

证明　由定理 1 可得 $(0aa0aaa0, 00000000) \to (00000000, 0bb0bbb0)$ 是一个 8 轮的 MIBS 算法的零相关线性逼近，然后由引理 4 可得此结论。

引理 6　对于 10 轮 MIBS-80 第 8 轮的输出

$(w_1w_2\cdots w_8, w_9w_{10}\cdots w_{16})$ 与密文 (L_{10}, R_{10}) 及 64 bit 密钥 $k_{10}\|k_9$ 的关系为

$$w_{10}\oplus w_{11}\oplus w_{13}\oplus w_{14}\oplus w_{15} = R_{10}(2)\oplus R_{10}(3)\oplus R_{10}(5)\oplus R_{10}(6)\oplus R_{10}(7)\oplus M_9(4)$$

为了方便计算，令 $D = R_{10}(2)\oplus R_{10}(3)\oplus R_{10}(5)\oplus R_{10}(6)\oplus R_{10}(7)$，所以其关系可以写为

$$w_{10}\oplus w_{11}\oplus w_{13}\oplus w_{14}\oplus w_{15} = D\oplus M_9(4)$$

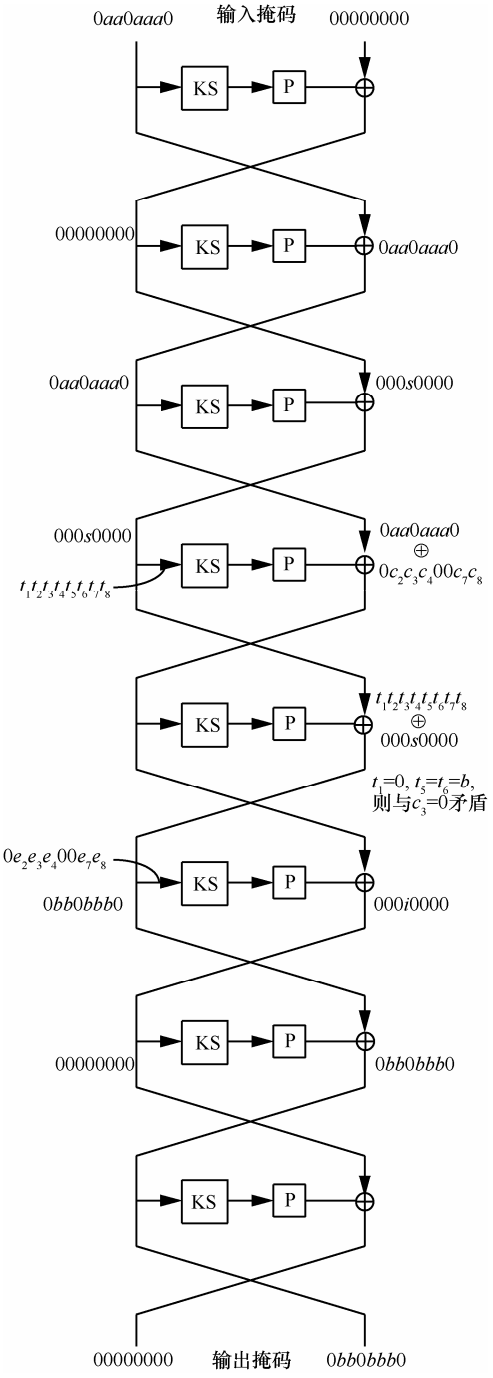


图 2　证明过程

其中，$M_9(4) = S[F_{10}^4(R_{10}(2,3,4,7,8)\oplus k_{10}(2,3,4,7,8))\oplus L_{10}(4)\oplus k_9(4)]$。

证明　由 MIBS-80 算法结构可知

$$w_{10}\oplus w_{11}\oplus w_{13}\oplus w_{14}\oplus w_{15} = R_{10}(2)\oplus R_{10}(3)\oplus R_{10}(5)\oplus R_{10}(6)\oplus R_{10}(7)\oplus F_9^2(R_9)\oplus F_9^3(R_9)\oplus F_9^5(R_9)\oplus F_9^6(R_9)\oplus F_9^7(R_9)$$

由 MIBS 算法的 P 盒变换的逆可知

$$M_9(4) = F_9^2(R_9)\oplus F_9^3(R_9)\oplus F_9^5(R_9)\oplus F_9^6(R_9)\oplus F_9^7(R_9) = S(R_9(4))$$

又　$R_9(4) = L_{10}(4)\oplus F_{10}^4(R_{10}(2,3,4,7,8)\oplus k_{10}(2,3,4,7,8))$，得证。

3.2　对 10 轮 MIBS 算法的零相关—积分分析

利用 3.1 节给出的 8 轮零相关—积分区分器以及 MIBS 算法 Feistel 结构的特点，结合部分和技术对 MIBS 进行积分攻击，如图 3 所示。

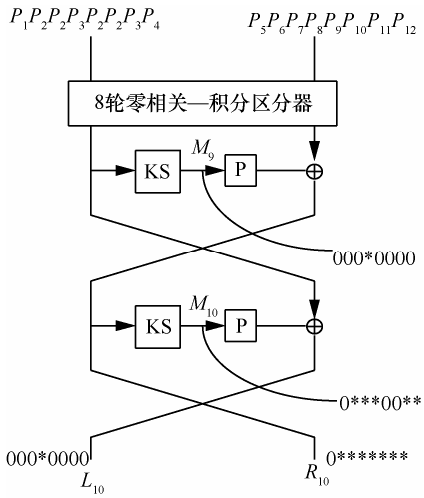


图 3　10 轮 MIBS 算的零相关积分分析

具体的攻击算法如下。

Step1　选择明文 P_1（2^{48} 个）对应的第 10 轮的 2^{48} 个密文为 C_1，记为 $L_{10}\|R_{10}$。

Step2　取 $x_0 = L_{10}(4)\|R_{10}(2,3,4,7,8)\|D$，$x_0$ 共有 2^{28} 种可能取值，并对每一种可能取值建立一个 32 bit 的计数器 $N_0[x_0]$，且全部置为 0。计算 2^{48} 个密文中 x_{10} 的个数，并保存于 $N_0[x_{10}]$ 中。对于 2^{48} 个密文，分配到 2^{28} 个计数器，平均每个计数器的数量为 2^{20}，所以对每一种可能取值建立一个 32 bit 的计数器足够使用。

Step3　猜测半字节密钥 $k_{10}(2)$，对 x_9 的 2^{28} 种可能取值中的每一种建立一个 32 bit 的计数器 $N_1[x_1]$，

其中，$x_1 = M_{10}(2)\|L_{10}(4)\|R_{10}(3,4,7,8)\|D$，将计数器置为 0。对 $R_{10}(2)$ 的全部可能取值进行一次 S 盒变换，得到对应 x_9 的值，更新计数器 $N_1[x_1] += N_0[x_0]$。

Step4　猜测半字节密钥 $k_{10}(3)$，对 x_8 的 2^{28} 种可能取值中的每一种建立一个 32 bit 的计数器 $N_2[x_8]$，其中，$x_8 = M_{10}(2,3)\|L_{10}(4)\|R_{10}(4,7,8)\|D$，将计数器置为 0。对 $R_{10}(2)$ 的全部可能取值进行一次 S 盒变换，得到对应 x_8 的值，更新计数器 $N_2[x_8] += N_1[x_9]$。

Step5　猜测半字节密钥 $k_{10}(4)$，对 x_7 的 2^{28} 种可能取值中的每一种建立一个 32 bit 的计数器 $N_3[x_7]$，其中，$x_7 = M_{10}(2,3,4)\|L_{10}(4)\|R_{10}(7,8)\|D$，将计数器置为 0。对 $R_{10}(4)$ 的全部可能取值进行一次 S 盒变换，得到对应 x_7 的值，更新计数器 $N_3[x_7] += N_2[x_8]$。

Step6　猜测半字节密钥 $k_{10}(7)$，对 x_6 的 2^{28} 种可能取值中的每一种建立一个 32 bit 的计数器 $N_4[x_7]$，其中，$x_7 = M_{10}(2,3,4,7)\|L_{10}(4)\|R_{10}(8)\|D$，将计数器置为 0。对 $R_{10}(7)$ 的全部可能取值进行一次 S 盒变换，得到对应 x_7 的值，更新计数器 $N_4[x_6] += N_3[x_7]$。

Step7　猜测半字节密钥 $k_{10}(8)$，对 x_5 的 2^{12} 种可能取值中的每一种建立一个 50 bit 的计数器 $N_5[x_5]$，其中，$x_5 = R_9(4)\|D$，将计数器置为 0，$R_9(4) = M_{10}(2) \oplus M_{10}(3) \oplus M_{10}(4) \oplus M_{10}(7) \oplus M_{10}(8)$。对 $R_{10}(8)$ 全部可能取值进行一次 S 盒变换，得到对应 x_5 的值，更新计数器 $N_5[x_5] += N_4[x_6]$。

Step8　猜测半字节密钥 $k_9(4)$，对 x_4 的 2^4 种可能取值中的每一种建立一个 50 bit 的计数器 $N_6[x_4]$，其中，$x_8 = M_9(4) \oplus D$，将计数器置为 0。对 $R_9(4)$ 的全部可能取值进行一次 S 盒变换，得到对应 x_4 的值，更新计数器 $N_6[x_4] += N_5[x_5]$。

Step9　$x_4 \in F_2^4$，对于 x_4 的每一个可能取值，如果计数器 $N_6[x_4] \neq 2^{44}$，则为错误密钥，否则是正确密钥。

统计以上攻击过程中的各步骤，时间复杂度主要取决于 Step 3 至 Step 6，并且进行 10 轮 MIBS 算法加密，共需 80 次 S 盒查表，所以时间复杂度为 $2^{28} \times 2^4 \times 4 \times \frac{1}{8} \times \frac{1}{10} \approx 2^{27.68}$，数据复杂度为 2^{48}，存储复杂度为 2^{48}。

3.3　对 12 轮 MIBS 算法的零相关—积分分析

引理 7　对于 12 轮 MIBS-80，第 8 轮输出为 $(w_1 w_2 \cdots w_8, w_9 w_{10} \cdots w_{16})$ 与密文 $L_8\|R_8$，只需求出第 10 轮的密文 $L_{10}(4)\|R_{10}(2,3,4,5,6,7,8)$，就能对 MIBS-80 进行 12 轮的零相关—积分攻击。

证明　由引理 6 可知，第 8 轮的输出 $(w_1 w_2 \cdots w_8, w_9 w_{10} \cdots w_{16})$ 与第 10 轮的密文 $L_{10}\|R_{10}$ 及密钥之间的关系为

$$w_{10} \oplus w_{11} \oplus w_{13} \oplus w_{14} \oplus w_{15} = R_{10}(2) \oplus R_{10}(3) \oplus R_{10}(5) \oplus R_{10}(6) \oplus R_{10}(7) \oplus M_9(4)$$

其中，$M_9(4) = S[P \circ S(R_{10}(2,3,4,7,8) \oplus k_{10}(2,3,4,7,8)) \oplus L_{10}(4) \oplus k_9(4)]$，与其他轮的密文无关，得证。

引理 8　第 10 轮的密文 $L_{10}(4)\|R_{10}(2,3,4,5,6,7,8)$ 与第 12 轮的密文 $L_{12}\|R_{12}$ 以及密钥之间的关系为

$$\begin{cases} L_{11} = R_{12} \\ R_{11} = F_{12}(R_{12} \oplus k_{12}) \oplus L_{12} \\ L_{10}(4) = R_{11}(4) \\ R_{10}(2,3,4,5,6,7,8) = F_{11}^{2,3,4,5,6,7,8}(R_{11}(2,3,4,5,6,7,8) \oplus \\ k_{11}(2,3,4,5,6,7,8)) \oplus L_{11}(2,3,4,5,6,7,8) \end{cases}$$

利用上述 2 个引理，对 MIBS 进行 12 轮的零相关—积分攻击，具体的攻击过程如下。

Step1　选择在构造 8 轮零相关—积分区分器时的明文 $P_1(2^{48})$ 以及对应的第 12 轮密文 $C_1(2^{48})$，记为 $L_{12}\|R_{12}$。

Step2　取 $x_0 = L_{12}(2,3,4,7,8)\|R_{12}(1,2,3,4,5,6,7,8)$，最多有 2^{48} 种可能取值，对每一种可能取值建立一个 48 bit 的计数器 $N_0(x_0)$，并置为 0。

Step3　猜测半字节密钥 $k_{12}(1)$，对 x_1 的 2^{48} 种可能取值每一种建立一个 48 bit 的计数器 $N_1(x_1)$，并置为 0。其中，$x_1 = L_{12}(2,3,4,7,8)\|M_{12}(1)\|R_{12}(2,3,4,5,6,7,8)$，将 $R_{12}(1)$ 遍历进行一次 S 盒变换，得到对应 x_1 的值，更新计数器 $N_1[x_1] += N_0[x_0]$。

Step4　同 3.2 节算法，依次猜测半字节密钥 $k_{12}(2)$、$k_{12}(3)$、$k_{12}(4)$、$k_{12}(5)$、$k_{12}(6)$、$k_{12}(7)$、$k_{12}(8)$，对应于 x_2、x_3、x_4、x_5、x_6、x_7、x_8，最终得到相应的 48 bit 计数器 $N_8(x_8)$，其中，$x_8 = L_{12}(1,2,\cdots,8)\|M_{12}(1,2,\cdots,8)$ 最多有 2^{48} 种可能取值。

Step5　根据加密算法，计算得出 x_9，建立 48 bit 的计数器 $N_9[x_9]$，并置为 0，其中，$x_9 = L_{11}(2,3,4,5,6,7,8)\|R_{11}(2,3,4,5,6,7,8)$ 最多有 2^{48} 种可能，相应的计数器进行更新，$N_9[x_9] += N_8[x_8]$。

Step6　根据 MIBS 的密钥扩展算法可知，这次

只需要猜测 k_{11} 的后 15 bit 密钥，即 $k_{11}(5)$ 的后 3 bit 和 $k_{11}(6)$、$k_{11}(7)$、$k_{11}(8)$。同样利用部分和技术，得到相应的 x_{13}，其中，$x_{13}=L_{10}(4)\|R_{10}(2,3,4,5,6,7,8)$，并得到相应的计数器 $N_{13}[x_{13}]$。

Step7 根据 3.2 节的攻击算法，可计算出第 8 轮输出的密文 $z=w_{10}\oplus w_{11}\oplus w_{13}\oplus w_{14}\oplus w_{15}$ 的 2^4 个可能取值的取值次数，记为 $N[z]$，如果 $N[z]=2^{44}$ 则为正确密钥，否则为错误密钥。

3.4 复杂度分析

由上述算法可知，数据复杂度为 2^{48}，时间复杂度主要取决于 Step2 至 Step6，其计算式为 $2^{48}\times 2^4\times 10+2^{48}\times 2^3\approx 2^{55.39}$，而 12 轮 MIBS 算法共需 96 次 S 盒查表，所以在忽略其他运算所耗时间的情况下，处理密文的时间复杂度不超过 $\frac{2^{55.39}}{96}\approx 2^{48.81}$。从攻击过程中可以恢复出 k_{12}、k_{11} 的后 15 bit 密钥以及 3.1 节算法中的 24 bit 密钥，共计 73 bit 密钥，除去重复猜测的 16 bit 密钥，可恢复出 57 bit 主密钥。

本文的方法与以往未与零相关线性分析相结合的方法的积分攻击结果相比较，详细优势如表 1 所示。

从表 1 中可以看出，本文的数据复杂度和时间复杂度要优于文献[5]的方法；虽然在数据复杂度方面比文献[6]的方法差，但时间复杂度要优于文献[6]的方法；对于 12 轮的 MIBS-80 算法的攻击，数据复杂度和时间复杂度也达到了一个很好的平衡，12 轮的 MIBS 算法对零相关—积分攻击是不免疫的。因此，本文方法的分析结果优于以往方法的积分分析结果。

4 结束语

本文对 MIBS 算法的安全性进行了分析。利用零相关线性分析与积分分析相结合的方法对 MIBS-80 算法进行了攻击。结果表明零相关—积分分析对 MIBS-80 算法是有效的。攻击 10 轮 MIBS-80 算法的数据复杂度为 2^{48}，时间复杂度为 $2^{27.68}$，攻击 12 轮 MIBS-80 算法的时间复杂度为 $2^{48.81}$。本文的分析结果表明，对分组密码进行分析时，利用多个分析方法相结合可能会取得更好的结果。

参考文献：

[1] IZADI M, SADEGHIYAN B, SADEGHIAN S S, et al. MIBS: a new lightweight block cipher[C]// 8th International Conference on Cryptology and Network Security. 2009: 334-348.

[2] BAY A, NAKAHARA J J, VAUDENAY S. Cryptanalysis of reduced-round MIBS block cipher[M]// 9th International Conference on Cryptology and Network Security. 2010: 1-19.

[3] 王高丽, 王少辉. 对 MIBS 算法的 Integral 攻击[J]. 小型微型计算机系统, 2012, 33(4): 773-777.
WANG G L, WANG S H. Intergral cryptanalysis of reduced-round MIBS block cipher[J]. Journal of Chinese Computer Systems, 2012, 33(4): 773-777.

[4] YU X, WU W, LI Y, et al. Integral attack of reduced-round MIBS block cipher[J]. Journal of Computer Research and Development, 2013, 50(10): 2117-2125.

[5] 潘志舒, 郭建胜, 曹进克, 等. MIBS 算法的积分攻击[J]. 通信学报, 2014, 35(7): 157-163.
PAN Z S, GUO J S, CAO J K, et al. Integral attack on MIBS block cipher[J]. Journal on Communications, 2014, 35(7): 157-163.

[6] 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.

表 1 不同方法的 MIBS 算法的积分攻击结果

方法来源	分析方法	攻击轮数	数据复杂度	时间复杂度
文献[4]	积分攻击(64 bit)	8	$2^{38.6}$	$2^{24.2}$
文献[4]	积分攻击(80 bit)	9	$2^{39.6}$	$2^{68.4}$
文献[5]	积分攻击(64 bit)	10	$2^{61.6}$	2^{40}
文献[5]	积分攻击(80 bit)	10	$2^{61.6}$	2^{40}
文献[6]	积分攻击(80 bit)	10	$2^{28.2}$	$2^{53.2}$
文献[15]	积分攻击(80 bit)	11	2^{60}	$2^{56.5}$
本文	积分攻击(80 bit)	10	2^{48}	$2^{27.68}$
本文	积分攻击(80 bit)	12	2^{48}	$2^{48.81}$

[7] BOGDANOV A, WANG M. Zero correlation linear cryptanalysis with reduced data complexity[C]//Fast Software Encryption. 2012: 29-48.

[8] SOLEIMANY H, NYBERG K. Zero-correlation linear cryptanalysis of reduced-round LBlock[J]. Designs, Codes and Cryptography, 2014, 73(2): 683-698.

[9] BOGDANOV A, GENG H, WANG M, et al. Zero-correlation linear cryptanalysis with FFT and improved attacks on ISO standards Camellia and CLEFIA[C]//Selected Areas in Cryptography 2013. 2014: 306-323.

[10] WEN L, WANG M, BOGDANOV A, et al. Multidimensional zero-correlation attacks on lightweight block cipher HIGHT: improved cryptanalysis of an ISO standard[J]. Information Processing Letters, 2014, 114(6): 322-330.

[11] WEN L, WANG M, BOGDANOV A. Multidimensional zero-correlation linear cryptanalysis of E2[C]//Progress in Cryptology–AFRICACRYPT 2014. 2014: 147-164.

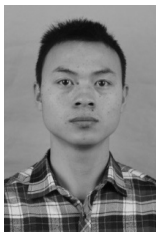
[12] BOGDANOV A, LEANDER G, NYBERG K, et al. Integral and multidimensional linear distinguishers with correlation zero[C]//Advances in Cryptology–ASIACRYPT 2012. 2012: 244-261.

[13] 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 C H. Spectra characterizations of nonsingular feedback polynomials over finite fields and residue class rings[J]. Journal on Communications, 2000, 21(1): 74-77.

[14] 郭瑞, 金晨辉. 低轮 FOX64 算法的零相关—积分分析[J]. 电子与信息学报, 2015, 37(2): 417-422.
GUO R, JIN C H. Integral cryptanalysis of reduced round FOX64[J]. Journal of Electronics & Information Technology, 2015, 37(2): 417-422.

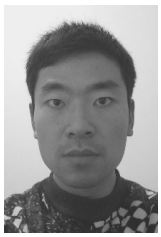
[15] YI W, CHEN S. Improved results on integral and zero-correlation linear cryptanalysis of the block cipher MIBS[J]. Computer Science, 2014.

作者简介：



刘庆聪（1990-），男，山东菏泽人，信息工程大学硕士生，主要研究方向为概率统计应用和密码学。

赵亚群（1961-），女，江苏淮安人，信息工程大学教授、硕士生导师，主要研究方向为密码基础理论及概率统计应用。



马猛（1986-），男，河南南阳人，信息工程大学硕士生，主要研究方向为密码学。

刘凤梅（1974-），女，河南郸城人，信息保障技术重点实验室副研究员，主要研究方向为密码基础理论。