doi:10.3969/j.issn.1000-436x.2014.07.019

MIBS 算法的积分攻击

潘志舒[1,3]，郭建胜[2,3]，曹进克[3]，罗伟[3,4]
（1. 西安卫星测控中心，陕西 西安 710043; 2. 信息保障技术重点实验室， 北京 100000；
3. 解放军信息工程大学，河南 郑州 450001; 4. 解放军 78179 部队，四川 都江堰 611830）

摘 要：对分组密码算法 MIBS 在积分攻击下的安全性进行了研究，构造了 MIBS 算法的 5 轮积分区分器，利用 Feistel 结构的等价结构以及 MIBS 密钥扩展算法中主密钥和轮密钥的关系，对 10 轮 MIBS 算法实施了积分攻击，给出了攻击算法。攻击 10 轮 MIBS-64 的数据复杂度和时间复杂度分别为 2^{28} 和 $2^{52.7}$，攻击 10 轮 MIBS-80 的数据复杂度和时间复杂度分别为 $2^{28.2}$ 和 $2^{53.2}$。分析结果表明，10 轮 MIBS 算法对积分攻击是不免疫的，该积分攻击的轮数和数据复杂度上都要优于已有的积分攻击。

关键词：分组密码；密码分析；积分攻击；MIBS 算法
中图分类号：TN918.1 **文献标识码**：A **文章编号**：1000-436X(2014)07-0157-07

Integral attack on MIBS block cipher

PAN Zhi-shu[1,3], GUO Jian-sheng[2,3], CAO Jin-ke[3], LUO Wei[3,4]
(1. Xi'an Satellite Control Center, Xi'an 710043, China; 2. Science and Technology on Information Assurance Laboratory, Beijing 100000, China;
3. PLA Information Engineering University, Zhengzhou 450001, China; 4.Unit 78179 of PLA, Dujiangyan 611830, China)

Abstract: The security of the block cipher MIBS against integral attack was analyzed and a 5-round distinguisher of MIBS was founded. Considering the equivalent structure of Feistel structure and the relation of master key and round key in the key expansion algorithm of MIBS, it applied integral attack to 10 rounds of MIBS and gave the attack algorithm. The data and time complexities of 10 round attack on MIBS-64 are 2^{28} and $2^{52.7}$ respectively. The data and time complexities of 10 round attack on MIBS-80 are $2^{28.2}$ and $2^{53.2}$ respectively. These results demonstrate that integral attack on 10-round MIBS is no immunity, both rounds and data complexity of this integral attack are better than the integral attack existing.

Key words: block cipher; cryptanalysis; integral attack; MIBS

1 引言

MIBS 算法是 Izadi 等[1]在 CANS2009 上提出的一种轻量级分组密码算法，适用于电子标签和传感器网络等环境。由于其采用简单的异或等运算，所以非常便于硬件实现。该算法整体采用 Feiste 结构，F 函数采用 S-P 结构。在文献[2]中对 MIBS 算法抵抗差分攻击和线性攻击的能力进行了安全性评估，文献[3]对其抵抗宽度差分故障分析进行了研究。文献[4]首次对 MIBS 进行了积分攻击研究，构造了 4.5 轮积分区分器，给出了对 8 轮 MIBS-64 和 9 轮 MIBS-80 的积分攻击。在攻击过程中，利用密钥扩展方法中主密钥与轮密钥的关系，减少猜测的密钥个数，从而降低了攻击的时间复杂度。文献[5]亦对 MIBS 进行了 8 轮、9 轮、10 轮的积分攻击。

本文对 MIBS 算法进行积分攻击的研究，构造了 4 轮积分区分器，并向前做高阶积分将 4 轮区分器扩展至 5 轮，利用 Feistel 结构的等价结构以及 MIBS 算法密钥扩展算法中主密钥与轮密钥的关系，对 10 轮 MIBS 算法实施了积分攻击，通过验证区分器中第 5 轮的一个 4 bit 字为平衡集给出积分攻击算法，攻击 10 轮 MIBS-64 的数据复杂度和时

收稿日期：2013-03-21；**修回日期**：2014-04-19
基金项目：河南省科技创新杰出青年计划基金资助项目（104100510025）
Foundation Item: The Scientific Innovation Talents Foundation of Henan Province (104100510025)

间复杂度分别为 2^{28} 和 $2^{52.7}$，攻击 10 轮 MIBS-80 的数据复杂度和时间复杂度分别为 $2^{28.2}$ 和 $2^{53.2}$。积分攻击的轮数和所需的数据复杂度都要优于文献[4]的结果，数据复杂度明显优于文献[5]的结果。

2 相关知识

2.1 MIBS 算法结构简介

MIBS 算法整体采用 Feistel 结构。分组长度为 64 bit，密钥长度有 64 bit 和 80 bit 这 2 种，加密轮数为 32 轮。每一轮的 F 函数包括轮子密钥加变换，非线性 S 盒变换和线性 P 盒变换。S 盒变换为 8 个相同的 4 bit 进 4 bit 出的小 S 盒并置，P 盒变换为 8 个小 S 盒的输出对位异或加和位置变换。第 i 轮的结构如图 1 所示，F 函数的结构如图 2 所示。

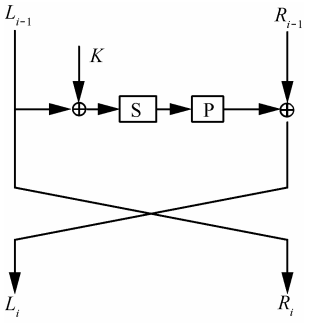


图 1 MBIS 算法第 i 轮结构

设 64 bit 明文为 $L_0 \| R_0$，约定其从左至右为高比特到低比特的排列，则加密得到密文 $L_{32} \| R_{32}$ 过程如下。对 $1 \leqslant i \leqslant 32$，$L_i = F(L_{i-1}, K_i) \oplus R_{i-1}$，$R_i = L_{i-1}$。$F(L_{i-1}, K_i)$ 定义如下。

1) 密钥加变换：$X = L_{i-1} \oplus K_i$。

2) 非线性 S 盒变换：令 $X = x_8 \| x_7 \| x_6 \| x_5 \| x_4 \| x_3 \| x_2 \| x_1$，$y_i = S(x_i)(i = 1, 2, \cdots, 8)$。

3) 线性 P 盒变换

$$y_1' = y_1 \oplus y_2 \oplus y_4 \oplus y_5 \oplus y_7 \oplus y_8$$
$$y_2' = y_2 \oplus y_3 \oplus y_4 \oplus y_5 \oplus y_6 \oplus y_7$$
$$y_3' = y_1 \oplus y_2 \oplus y_3 \oplus y_5 \oplus y_6 \oplus y_8$$
$$y_4' = y_2 \oplus y_3 \oplus y_4 \oplus y_7 \oplus y_8$$
$$y_5' = y_1 \oplus y_3 \oplus y_4 \oplus y_5 \oplus y_8$$
$$y_6' = y_1 \oplus y_2 \oplus y_4 \oplus y_5 \oplus y_6$$
$$y_7' = y_1 \oplus y_2 \oplus y_3 \oplus y_6 \oplus y_7$$
$$y_8' = y_1 \oplus y_3 \oplus y_4 \oplus y_6 \oplus y_7 \oplus y_8$$

$F(L_{i-1}, K_i)$ 的输出即为 $y_8' \| y_7' \| y_6' \| y_5' \| y_4' \| y_3' \| y_2' \| y_1'$。

MIBS 算法的密钥扩展算法如下描述。

算法 1 （MIBS-64 的密钥扩展算法）

设 64 bit 主密钥为 $\hat{K} = (\hat{K}_{63}, \hat{K}_{62}, \cdots, \hat{K}_0)$，$state^0 \leftarrow \hat{K}$，$[a \sim b]$ 表示从高比特 a 到低比特 b 之间的 $a-b+1$ bit。由主密钥生成 32 个长度为 32 bit 的轮密钥 $K_i (1 \leqslant i \leqslant 32)$ 的过程如下。

Step1 $state^i \leftarrow state^{i-1} >>> 15$；

Step2 $state^i \leftarrow S(state^i_{[63\sim60]}) \| state^i_{[59\sim0]}$；

Step3 $state^i \leftarrow state^i_{[63\sim16]} \| state^i_{[15\sim11]} \oplus Round-Counter \| state^i_{[10\sim0]}$；

Step4 $K_i \leftarrow state^i_{[63\sim32]}$。

其中，$>>>15$ 表示循环右移 15 位，S 盒与加密算法中的 S 盒一样，*Round-Counter* 表示轮数。

算法 2 （MIBS-80 的密钥扩展算法）

设 80 bit 的密钥为 $\hat{K} = (\hat{K}_{79}, \hat{K}_{78}, \cdots, \hat{K}_0)$，$state^0 \leftarrow \hat{K}$，$[a \sim b]$ 表示从高位比特 a 到低位比特 b 之间的 $i-j+1$ bit。由主密钥生成 32 个长度为 32

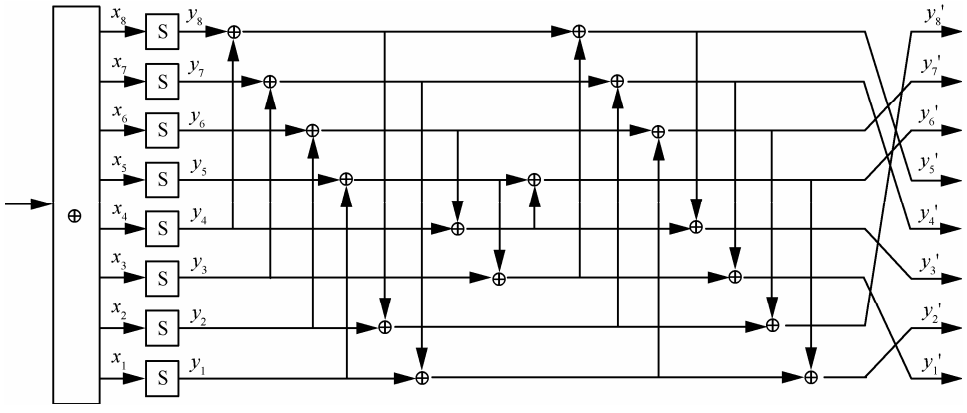


图 2 MBIS 算法 F 函数结构

bit 的轮密钥 $K_i(1 \leqslant i \leqslant 32)$ 的过程如下。

Step1　$state^i \leftarrow state^{i-1} >>> 19$；

Step2　$state^i \leftarrow S(state^i_{[79\sim76]}) \| S(state^i_{[75\sim72]}) \| state^i_{[71\sim0]}$；

Step3　$state^i \leftarrow state^i_{[79\sim19]} \| state^i_{[18\sim14]} \oplus Round-Counter \| state^i_{[13\sim0]}$；

Step4　$K_i \leftarrow state^i_{[79\sim48]}$。

其中 >>>19 表示循环右移 19 位，S 盒与加密算法中的 S 盒一样，*Round-Counter* 表示轮数。

2.2　积分攻击

积分攻击是 Knudsen 等[6]总结提出的一种分组密码选择明文攻击方法，自提出以来，得到越来越广泛的关注，用该攻击方法对许多算法进行了安全性分析，例如 AES[7]、ARIA [8]、Camellia[9]、CLEFIA[10]等。

积分攻击就是选择特定形式的明文进行加密，再对所得密文求和（积分），通过积分值的不随机性将密码算法与随机置换区分开。在构造积分区分器时，需要定义一些符号。

定义 1[6,11]　一些特殊形式的集合

1) 活跃集：若对任意的 $0 \leqslant i < j \leqslant 2^n - 1$，都有 $x_i \neq x_j$，则集合 $\{x_i \mid x_i \in F_{2^n}, 0 \leqslant i \leqslant 2^n - 1\}$ 是活跃集，记为 A。

2) 稳定集：若对任意的 $0 < i \leqslant 2^n - 1$，都有 $x_i = x_0$，则集合 $\{x_i \mid x_i \in F_{2^n}, 0 \leqslant i \leqslant 2^n - 1\}$ 是稳定集，记为 C。

3) 平衡集：若 $\oplus_{i=0}^{2^n-1} x_i = 0$，则集合 $\{x_i \mid x_i \in F_{2^n}, 0 \leqslant i \leqslant 2^n - 1\}$ 是平衡集，记为 B。

这些集合之间的运算遵循一些基本原则。

性质 1[6,11]　不同集合之间满足如下性质。

1) A 集合通过双射（如 S 盒，密钥加）后，仍是 A 集合；C 集合通过双射后，仍是 C 集合。

2) 2 个 A 集合的和不一定为 A 集合，但一定是 B 集合；A 集合与 C 集合的和仍是 A 集合；2 个 B 集合的和仍为 B 集合。

3) B 集合通过非线性双射（如 S 盒），将无法确定其平衡性。

本文讨论的 MBIS 算法以 4 bit 字为操作单位，即定义 1 中的 n 取 4。

2.3　Feistel 结构的等价结构

Feistel 结构分组密码在加密时，每一轮总有一半数据保持不变，因此可以对其结构进行适当变形，变形后的结构不影响算法加解密结果，但结构的不同有时可以便利攻击方法的实施。

一轮 Feistel 结构如图 1 所示，可用式(1)定义。

$$\begin{cases} L_i = P \circ S(L_{i-1} \oplus K_i) \\ R_i = L_{i-1} \end{cases} \tag{1}$$

定义密文为 $C = (L_r, R_r)$。

Feistel 结构有若干种等价结构，这里介绍本文利用的一种等价结构，如图 3 所示，可用式(2)定义。

$$\begin{cases} L_i = S(L_{i-1} \oplus K_i) \oplus R_{i-1} \\ R_i = L_{i-1} \end{cases}, \quad \text{若}i\text{为奇数}$$
$$\begin{cases} L_i = P \circ S \circ P(L_{i-1} \oplus K_i) \oplus R_{i-1} \\ R_i = L_{i-1} \end{cases}, \quad \text{若}i\text{为偶数} \tag{2}$$

定义密文为 $C = (L_r, P(R_r))$。

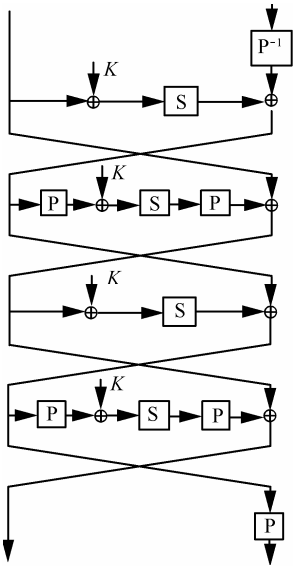


图 3　一种 4 轮 Feistel 结构的等价结构

3　密钥扩展算法的相关性质

利用 MIBS 算法的密钥扩展算法生成的轮密钥，其实就是主密钥经过循环移位，S 盒变换和异或运算后，再截断选取 32 bit 生成的，所以 MIBS 算法不同轮的轮密钥某些比特是由主密钥中相同的比特生成。在进行攻击时，如果需要猜测这些轮密钥比特，可以将猜测轮密钥改为猜测主密钥的相关比特，从而减少所猜的轮密钥个数，达到降低计算复杂度和攻击更多轮数的目的。而在猜测密钥时，只要确定需要猜测的轮密钥比特与主密钥哪些比特有关即可。

设第 i 轮密钥为 $K_i = K_{i,8} \| K_{i,7} \| \cdots \| K_{i,1}$，其中，是第 i 轮密钥的第 j 个 4 bit 字。根据密钥扩展算法，可以很容易得到如下性质。

性质 2 对 MIBS-64，如果需要猜测轮密钥 $K_{i,j}$，只需要猜测主密钥 $\hat{K}_{[a\sim a-3]}$（$a=0,1,2$ 时，$\hat{K}_{[a\sim a-3]}$ 为 $\hat{K}_a$，$\hat{K}_{(a-1)\bmod 64}$，$\hat{K}_{(a-2)\bmod 64}$，$\hat{K}_{(a-3)\bmod 64}$ 这 4 个比特），其中 $a=(4j+31+15i)\bmod 64$。

证明 轮密钥是由主密钥经过循环移位，S 盒变换和异或运算后所得，其中循环移位改变密钥各比特的位置，S 盒只是 Step1 后前 4 bit 之间的混乱，异或运算不改变密钥比特位置。所以轮密钥中 4 比特字由主密钥中哪 4 bit 确定，只需考虑循环移位的影响。由算法 1 可知，生成 K_1 时，轮密钥中第 j 个 4 bit 字是主密钥经过了右循环移位 15 bit 及其他不影响比特位置的变换，最后截取高 32 bit 所得，所以 $a=(4j+31+15)\bmod 64$；生成 $K_i(i=2,\cdots,32)$ 时，可只看作上一步生成的密钥经过右循环移位 15 bit 及其他不影响比特位置的变换所得，所以有 $a=(4j+31+15i)\bmod 64$。

证毕

根据性质 2 的证明和算法 2 可得性质 3。

性质 3 对 MIBS-80，如果需要猜测轮密钥 $K_{i,j}$ 只需要猜测主密钥 $\hat{K}_{[a\sim a-3]}$（$a=0,1,2$ 时，$\hat{K}_{[a\sim a-3]}$ 为 $\hat{K}_a$，$\hat{K}_{(a-1)\bmod 64}$，$\hat{K}_{(a-2)\bmod 64}$，$\hat{K}_{(a-3)\bmod 64}$ 这 4 个比特），其中 $a=(4j+47+19i)\bmod 80$。

4 5 轮 MIBS 算法积分区分器的构造

根据定义 1 和性质 1，选择特定形式的明文，构造 MIBS 算法的积分区分器。在构造之前，约定 MIBS 算法第 i 轮输入为 $L_{i-1} \| R_{i-1}$（L_{i-1} 和 R_{i-1} 分别为 32 bit 字），其中，$L_{i-1} = L_{i-1,8} \| L_{i-1,7} \| \cdots \| L_{i-1,0}, R_{i-1} = R_{i-1,8} \| R_{i-1,7} \| \cdots \| R_{i-1,0}$（$L_{i,j}$ 和 $R_{i,j}$ 分别为 4 bit 字）。

定理 1（4 轮积分区分器） 选择 2^4 个明文，满足条件：$R_{0,8}$ 遍历所有 2^4 个取值，即为集合 A；$R_{0,j}(j=1,2,\cdots,7)$ 和 L_0 均为常数，即集合 C。则经过 4 轮 MIBS 后，输出的 $R_{4,j}(j=1,2,\cdots,8)$ 均为平衡集 B。

证明 首先说明的是，每一轮的密钥加相当于加上一个常量，并不改变集合模式，可以不予考虑。此外 MIBS 算法 Feistel 结构第 i 轮输出的 R_i 为上一轮的 L_{i-1}，证明过程将不再赘述。

第 1 轮 L_0 为稳定集合 C，经过 F 函数变换后，仍为 C，再与 R_0 异或加后仍为 R_0，成为第 1 轮的输出 L_1，所以第 1 轮的输出为 $L_1 \| R_1 = (ACCCCCCC \| CCCCCCCC)$。

第 2 轮 L_1 进入 F 函数，经过 S 盒变换后，仍为 $(ACCCCCCC)$，再经过 P 盒变换，A 所在的 4 bit 字将影响到输出的 5 个 4 bit 字，得到 $(ACCAAACA)$，再与 R_1 异或加后仍为 $(ACCAAACA)$，为第 2 轮的输出 L_2，所以第 2 轮的输出为 $L_2 \| R_2 = (ACCAAACA \| ACCCCCCC)$。

第 3 轮 L_2 进入 F 函数，经过 S 盒变换后，仍为 $(ACCAAACA)$，再进行 P 盒变换，P 盒输出的 8 个 4 bit 字都至少是输入中 5 个 4 bit 字的异或加，而输入中有 5 个 4 bit 字为 A，所以由 P 盒结构，输出的每个 4 bit 字都有 2 个 A 相加，由性质 1 的 2），P 盒输出的每个 4 bit 字均为 B；再与 R_2 异或加后仍为，为第 3 轮的输出 L_3，所以第 3 轮的输出为 $L_3 \| R_3 = (BBBBBBBB \| ACCAAACA)$。

第 4 轮 L_3 进入 F 函数，经过 S 盒变换后，由性质 1 的 3），每一个 4 bit 字将不能确定其是否平衡，再经过 P 盒变换，F 函数的输出亦不能确定其是否平衡，记为“？”，所以与 R_3 异或后，第 4 轮的输出 L_4 不能确定其是否平衡，第 4 轮的输出为 $L_4 \| R_4 = (? \| BBBBBBBB)$，定理得证。证毕。

定理 1 构造的积分区分器如图 4 所示。

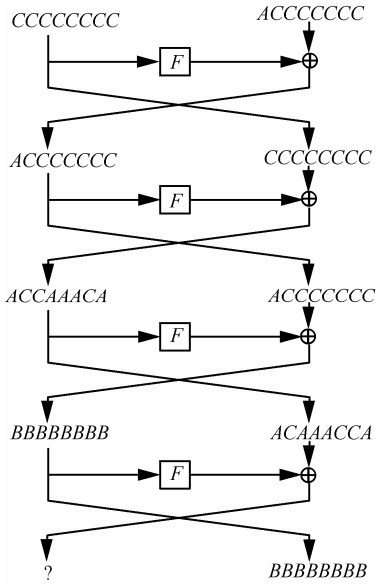


图 4 4 轮 MIBS 算法的积分区分器

进一步，将定理 1 构造的 4 轮区分器向前做高

阶积分扩展，得到 5 轮积分区分器。

定理 2　（5 轮积分区分器）选择 2^{24} 个明文，满足条件：$L_{0,8},R_{0,8},R_{0,5},R_{0,4},R_{0,3},R_{0,1}$ 分别遍历所有 2^4 个取值，其余 4 bit 字均为常数，即为集合 C。则经过 5 轮 MIBS 后，输出的 $R_{5,j}(j=1,2,\cdots,8)$ 均为平衡集 B。

证明　第 1 轮：$L_0=(ACCCCCCC)$ 进入 F 函数，由定理 1 证明中第 2 轮可知，F 函数输出为 $(ACCAAACA)$，再与 $R_0=(ACCAAACA)$ 异或加为 $(BCCBBBCB)$，所以第 1 轮输出为 $L_1\|R_1=(BCCBBBCB\|ACCCCCCC)$。其中 $L_1=(BCCBBBCB)$ 遍历所有 2^{20} 个取值，取 $L_{1,8},L_{1,5},L_{1,4},L_{1,3},L_{1,1}$ 的任意一组值，则 $L_1\|R_1$ 可看作 $(CCCCCCCC\|ACCCCCCC)$。其正好是定理 1 所构造的 4 轮积分区分器的输入，由定理 1，再经过 4 轮 MIBS 算法，输出的 $R_{5,j}(j=1,2,\cdots,8)$ 均为平衡集 B。

证毕。

这样，就构造了 MIBS 算法的 5 轮积分区分器：$L_0\|R_0=(ACCCCCCC\|CCCCCCCC)\xrightarrow{5轮}L_5\|R_5=(?\|BBBBBBBB)$。

5　对 MIBS 算法的积分攻击

利用第 3 节给出的 5 轮积分区分器以及 Feistel 结构的等价结构，对 MIBS 算法进行积分攻击。选取构造 5 轮区分器时需要的明文，得到加密的密文，通过猜测相关密钥，从密文恢复出第 5 轮的结果，验证其中右半边数据每个 4 bit 字是否平衡。本文以验证 $R_{5,7}$ 为平衡字为例进行说明。

5.1　对 10 轮 MIBS 算法的积分攻击

将 MIBS 算法进行等价结构改造，将第 2 轮到第 9 轮用图 3 所示结构进行代替。由等价结构可知，此时算法中第 5 轮右半边数据是原算法第 5 轮右半边数据经过 P^{-1} 变换后所得，在积分区分器中，第 5 轮右半边数据各 4 bit 字保持平衡，经过线性变换 P^{-1} 后仍保持平衡，所以算法中的 $R_{5,7}$ 仍为平衡字。

算法 3　（10 轮 MIBS 算法的积分攻击）

Step1　选择构造 5 轮积分区分器时的明文（2^{24} 个），进行 10 轮加密得到 2^{24} 个密文 $L_{10}\|R_{10}$。

Step2　猜测密钥 K_{10}，对 2^{24} 个密文进行第 10 轮解密，计算得到 $R_9=P\circ S(R_{10}\oplus K_{10})\oplus L_{10}$，同时有 $L_9=R_{10}$，得到 $L_9\|R_9$。

Step3　由等价结构可知，第 9 轮在输出前右半边数据作 P 变换，在攻击时，需要将 R_9 先作 P^{-1} 变换。然后再作第 9 轮的相关变换。猜测密钥 K_9，计算 $R_8=P\circ S(R_9\oplus K_9)\oplus L_9$，同时有 $L_8=P^{-1}(R_9)$，得到 $L_8\|R_8$。

Step4　猜测密钥 K_8，计算 $R_7=S(R_8\oplus K_8)\oplus L_8$，同时有 $L_7=R_8$，得到 $L_7\|R_7$。

Step5　设 $P(R_7)_i(i=1,2,\cdots,8)$ 为 R_7 经过 P 盒线性变换后所得数据的第 i 个 4 bit 字。猜测密钥 $K_{7,1},K_{7,2},K_{7,3},K_{7,6},K_{7,7}$，计算 $R_{6,7}=S(P(R_7)_1\oplus K_{7,1})\oplus S(P(R_7)_2\oplus K_{7,2})\oplus S(P(R_7)_3\oplus K_{7,3})\oplus S(P(R_7)_6\oplus K_{7,6})\oplus S(P(R_7)_7\oplus K_{7,7})$；同时有 $L_{6,7}=R_{7,7}$。

Step6　猜测密钥 $K_{6,7}$，计算 $R_{5,7}=S(R_{6,7}\oplus K_{6,7})\oplus L_{6,7}$。

Step7　验证所得到的 2^{24} 个 $R_{5,7}$ 的和是否为 0，若是，说明 $R_{5,7}$ 平衡，所猜测的密钥保留为候选密钥；否则，说明 $R_{5,7}$ 不平衡，所猜测的密钥为错误密钥，删除之。

Step8　选择另一组构造 5 轮区分器时的明文，重复 Step1~Step7，直至密钥唯一确定。

攻击流程如图 5 所示。

5.2　对 10 轮 MIBS-64 积分攻击算法的分析

基于 MIBS-64 的密钥扩展算法对算法 3 进行分析，得到定理 3。

定理 3　利用算法 3 对 MIBS-64 进行积分攻击，攻击的数据复杂度为 2^{28}，时间复杂度约为 $2^{52.7}$ 次 10 轮加密。

证明　算法 3 需要猜测 32 bit 密钥 K_{10},K_9,K_8，4 bit 密钥 $K_{7,1},K_{7,2},K_{7,3},K_{7,6},K_{7,7}$ 和 $K_{6,7}$。其中，由性质 2 可知，猜测密钥 $K_{6,7}$，只需猜测主密钥 $\hat{K}_{[21\sim18]}$；猜测密钥 $K_{7,1}$、$K_{7,2}$、$K_{7,3}$、$K_{7,6}$、$K_{7,7}$，只需猜测主密钥 $\hat{K}_{[21\sim9]}$ 和 $\hat{K}_{[36\sim29]}$；猜测密钥 K_8，只需猜测主密钥 $\hat{K}_{[55\sim24]}$；猜测密钥 K_9，只需猜测主密钥 $\hat{K}_{[6\sim0]}$ 和 $\hat{K}_{[63\sim39]}$；猜测密钥 K_{10}，只需猜测主密钥 $\hat{K}_{[21\sim0]}$ 和 $\hat{K}_{[63\sim54]}$。这样，在攻击过程中，需要猜测 32 bit 密钥 K_{10}，K_9 的后 15 个比特，K_8 的后 15 个比特，一共 62 bit 密钥。对于正确密钥，一定能保证 $R_{5,7}$ 平衡；对于错误密钥，其使 $R_{5,7}$ 平衡的概率为 2^{-4}，所以经过一组明密文淘汰后，剩余错误密

钥数目为 $(2^{62}-1)\times 2^{-4}\approx 2^{58}$，为了唯一确定正确密钥，需要 16 组明文，可以唯一确定正确密钥，从而攻击的数据复杂度为 16 组($2^{24}\times 16\approx 2^{28}$ 个)明文。

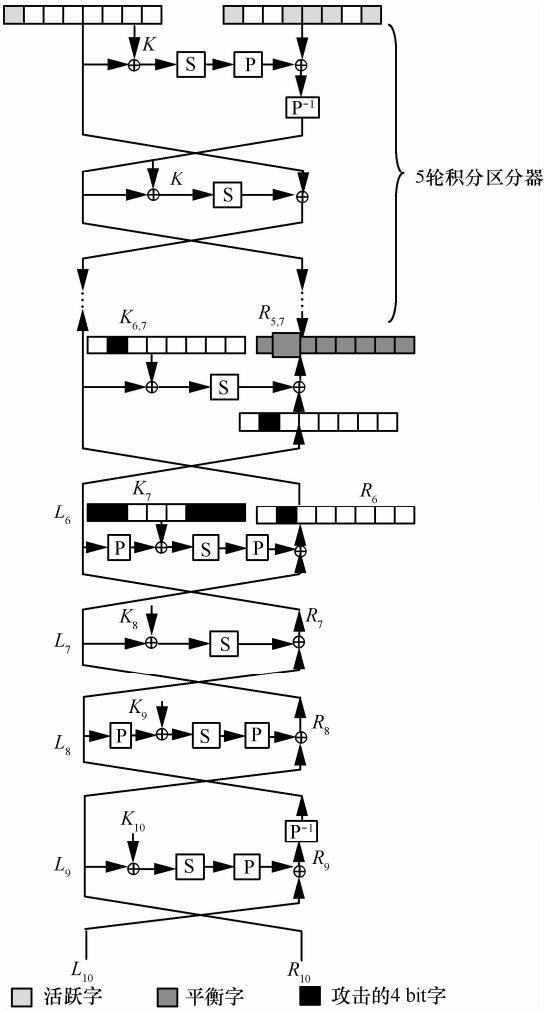


图 5 10 轮 MIBS 算法的积分攻击流程

对第一组明文，Step1 需要 2^{24} 次 10 轮加密，Step2 需要猜测 32 bit 密钥 K_{10}，共 2^{32} 个可能值，又密文至多有 2^{24} 个可能值，所以共约需 $2^{32}\times 2^{24}=2^{56}$ 次 S 盒查表，Step3 需要猜测 K_9 的后 15 个比特，又 $L_9\,\|\,R_9$ 至多有 2^{24} 个可能值，所以共约需 $2^{15}\times 2^{24}=2^{39}$ 次 S 盒查表，Step4 实际需要猜测 K_8 的后 15 个比特，又 $L_8\,\|\,R_8$ 至多有 2^{24} 个可能值，所以共约需 $2^{15}\times 2^{24}=2^{39}$ 次 S 盒查表，Step5 中 $P(R_7)_1,P(R_7)_2,P(R_7)_3,P(R_7)_6,P(R_7)_7$ 至多有 2^{20} 个可能值，所以约需 2^{20} 次 S 盒查表，Step6 中 $R_{6,7},L_{6,7}$ 至多有 2^8 个可能值，所以约需 2^8 次 S 盒查表，而 10 轮 MIBS 算法共需 $8\times 10=80$ 次查表，所以在忽略其他运算所耗时间的情况下，处理第一组明文的时间复杂度约为 $2^{24}+(2^{56}+2^{39}+2^{39}+2^{20}+2^8)/80\approx 2^{49.7}$ 次 10 轮加密；处理完第一组明文后，错误密钥数目还剩 2^{58}。同理处理第二组明文的时间复杂度约为 $2^{49.7}$ 次 10 轮加密；当剩余错误密钥数目小于 2^{32} 时，Step2 进行 S 盒查表次数减小，此时，处理了 8 组明文，处理前 8 组明文的时间复杂度约为 $2^{49.7}$ 次 10 轮加密，处理第 9 组明文时，剩余错误密钥 2^{30} 个，Step2 至多需要 $2^{30}\times 2^{24}=2^{54}$ 次 S 盒查表，于是处理第 9 组明文的时间复杂度约为 $2^{24}+(2^{54}+2^{39}+2^{39}+2^{20}+2^8)/80\approx 2^{47.7}$ 次 10 轮加密；同理，处理第 10、11、12 组明文时，时间复杂度分别约为 $2^{43.7}$、$2^{39.7}$ $2^{39.7}$ 和 2^{36} 次 10 轮加密；处理第 13 组明文时，错误密钥还剩 2^{14} 个，Step2 至多需要 $2^{14}\times 2^{24}=2^{38}$ 次 S 盒查表，Step3 和 Step4 分别至多需要 $2^{14}\times 2^{24}=2^{38}$ 次 S 盒查表，于是处理第 13 组明文的时间复杂度约为 $2^{24}+(2^{38}+2^{38}+2^{38}+2^{20}+2^8)/80\approx 2^{33.3}$ 次 10 轮加密；同理，处理第 14、15、16 组明文的时间复杂度分别约为 $2^{29.3}$、$2^{25.8}$、$2^{24.2}$ 次 10 轮加密。所以整个攻击的时间复杂度约为 $2^{49.7}\times 8+2^{47.7}+2^{43.7}+2^{39.7}+2^{36}+2^{33.3}+2^{29.3}+2^{25.8}+2^{24.2}\approx 2^{52.7}$ 次 10 轮加密。证毕。

5.3 对 10 轮 MIBS-80 积分攻击算法的分析

基于 MIBS-80 的密钥扩展算法对算法 3 进行分析，得到定理 4。

定理 4 利用算法 3 对 MIBS-80 进行积分攻击，攻击的数据复杂度为 $2^{28.2}$，时间复杂度约为 $2^{53.2}$ 次 10 轮加密。

证明 算法 3 需要猜测 32 bit 密钥 K_{10}、K_9、K_8，4 比特密钥 $K_{7,1},K_{7,2},K_{7,3},K_{7,6},K_{7,7}$ 和 $K_{6,7}$。其中，由性质 3 可知，猜测密钥 $K_{6,7}$，只需猜测主密钥 $\hat{K}_{[29\sim 26]}$；猜测密钥 $K_{7,1}$、$K_{7,2}$、$K_{7,3}$、$K_{7,6}$、$K_{7,7}$，只需猜测主密钥 $\hat{K}_{[32\sim 21]}$ 和 $\hat{K}_{[48\sim 41]}$；猜测密钥 K_8，只需猜测主密钥 $\hat{K}_{[71\sim 40]}$；猜测密钥 K_9，只需猜测主密钥 $\hat{K}_{[10\sim 0]}$ 和 $\hat{K}_{[79\sim 59]}$；猜测密钥 K_{10}，只需猜测主密钥 $\hat{K}_{[29\sim 0]}$ 和 $\hat{K}_{[79\sim 78]}$。这样，在攻击过程中，需要猜测 32 bit 密钥 K_{10}，K_9 的后 19 个比特，K_8 的后 19 个比特以及 $K_{7,3}$ 的前 3 bit 密钥，一共 73 bit 密钥。对于正确密钥，一定能保证 $R_{5,7}$ 平衡；对于错误密钥，其使 $R_{5,7}$ 平衡的概率为 2^{-4}，所以经过一组明密文淘汰后，剩余错误密钥数目为 $(2^{73}-1)\times 2^{-4}\approx 2^{69}$，为了

唯一确定正确密钥，需要 19 组明文，可以唯一确定正确密钥，从而攻击的数据复杂度为 19 组($2^{24}\times19\approx2^{28.2}$个)明文。

对第一组明文，Step1 需要 2^{24} 次 10 轮加密，Step2 需要猜测 32 bit 密钥 K_{10}，共 2^{32} 个可能值，又密文至多有 2^{24} 个可能值，所以共约需 $2^{32}\times2^{24}=2^{56}$ 次 S 盒查表，Step3 需要猜测 K_9 的后 19 个比特，又 $L_9\|R_9$ 至多有 2^{24} 个可能值，所以共约需 $2^{19}\times2^{24}=2^{43}$ 次 S 盒查表，Step4 需要猜测 K_8 的后 19 个比特，又 $L_8\|R_8$ 至多有 2^{24} 个可能值，所以共约需 $2^{19}\times2^{24}=2^{43}$ 次 S 盒查表，Step5 需要猜测 $K_{7,3}$ 的前 3 bit 密钥，$P(R_7)_1$、$P(R_7)_2$、$P(R_7)_3$、$P(R_7)_6$、$P(R_7)_7$ 至多有 2^{20} 个可能值，所以约需 $2^3\times2^{20}=2^{23}$ 次 S 盒查表，Step6 中 $R_{6,7}$、$L_{6,7}$ 至多有 2^8 个可能值，所以约需 2^8 次 S 盒查表，而 10 轮 MIBS 算法共需 $8\times10=80$ 次查表，所以在忽略其他运算所耗时间的情况下，处理第一组明文的时间复杂度不超过 $2^{24}+(2^{56}+2^{43}+2^{43}+2^{23}+2^8)/80\approx2^{49.7}$ 次 10 轮加密；处理完第一组明文后，错误密钥数目还剩 2^{69}，同理处理第二组明文的时间复杂度不超过 $2^{49.7}$ 次 10 轮加密；当剩余错误密钥数目小于 2^{32} 时，Step2 进行 S 盒查表次数减小，此时，处理了 11 组明文，处理前 11 组明文的时间复杂度约为 $2^{49.7}\times11$ 次 10 轮加密，处理第 12 组明文时，剩余错误密钥 2^{29} 个，Step2 至多需要 $2^{29}\times2^{24}=2^{53}$ 次 S 盒查表，于是处理第 12 组明文的时间复杂度不超过 $2^{24}+(2^{53}+2^{43}+2^{43}+2^{23}+2^8)/80\approx2^{46.7}$ 次 10 轮加密；同理，处理第 13、14 组明文时，时间复杂度分别约为 $2^{42.7}$ 和 $2^{39.3}$ 次 10 轮加密；处理第 15 组明文时，错误密钥还剩 2^{17} 个，Step2 至多需要 $2^{17}\times2^{24}=2^{41}$ 次 S 盒查表，Step3 和 Step4 分别至多需要 $2^{17}\times2^{24}=2^{41}$ 次 S 盒查表，于是处理第 15 组明文的时间复杂度约为 $2^{24}+(2^{41}+2^{41}+2^{41}+2^{23}+2^8)/80\approx2^{36.3}$ 次 10 轮加密；同理，处理第 16、17、18 组明文的时间复杂度分别约为 $2^{32.3}$、$2^{28.3}$、$2^{25.1}$ 次 10 轮加密，处理第 19 组明文时，错误密钥还剩 2 个。Step2~ Step4 至多需要 $2\times2^{24}=2^{25}$ 次 S 盒查表，Step5 约需 $2\times2^{20}=2^{21}$，于是处理第 19 组明文的时间复杂度约为 $2^{24}+(2^{25}+2^{25}+2^{25}+2^{21}+2^8)/80\approx2^{24.1}$。所以整个攻击的时间复杂度约为 $2^{49.7}\times11+2^{46.7}+2^{42.7}+2^{39.3}+2^{36.3}+2^{32.3}+2^{28.3}+2^{25.1}+2^{24.1}\approx2^{53.2}$ 次 10 轮加密。证毕。

6　结束语

本文对 MIBS 算法进行积分攻击的研究，构造了 4 轮积分区分器，并向前做高阶积分将 4 轮区分器扩展至 5 轮，利用 Feistel 结构的等价结构以及 MIBS 算法密钥扩展算法中主密钥与轮密钥的关系，对 10 轮 MIBS 算法实施了积分攻击。该积分攻击方法的攻击轮数和数据复杂度明显优于文献[4]的结果；在同样对 10 轮 MIBS 算法进行积分攻击的情况下，该攻击方法虽然在时间复杂度上劣于文献[5]，但数据复杂度大大优于文献[5]，因此整体计算复杂度要更优。所以本文结果优于已有的积分攻击方法。

表 1 将本文积分攻击的结果与文献[4]和文献[5]实施积分攻击的结果做了比较。

表 1　　MIBS 算法积分攻击的结果比较

攻击方法来源	攻击轮数	数据复杂度	时间复杂度
文献[4]（64 bit 密钥）	8	$2^{38.6}$	$2^{24.2}$
文献[5]（64 bit 密钥）	10	$2^{61.6}$	2^{40}
本文（64 bit 密钥）	10	2^{28}	$2^{52.7}$
文献[4]（80 bit 密钥）	9	$2^{39.6}$	$2^{68.4}$
文献[5]（80 bit 密钥）	10	$2^{61.6}$	2^{40}
本文（80 bit 密钥）	10	$2^{28.2}$	$2^{53.2}$

参考文献：

[1] IZADI M, SADEGHIYAN B, SADEGHIAN S S, *et al*. MIBS: a new lightweight block cipher[A]. Proceedings of CANS 2009，Lecture Notes in Computer Science 5888[C]. Berlin: Springer, 2009.334-345.

[2] BAY A, NAKAHARA J, VAUDENAY S. Cryptanalysis of reduced-round MIBS block cipher[A]. Proceedings of CANS 2010, Lecture Notes in Computer Science 6467[C]. Berlin: Springer, 2010.1-19.

[3] WANG S Z, ZHAO X J, WANG T, *et al*. Wide differential fault analysis on MIBS[J]. Computer Science, 2011, 38(4): 122-124.

[4] WANG G L, WANG S H. Integral cryptanalysis of reduced-round MIBS block cipher[J]. Journal of Chinese Computer Systems, 2012,33(4):773-777.

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

[6] KNUDSEN L, WAGNER D. Integral cryptanalysis[C]. Springer-Verlag, 2002.112-127

[7] FERGUSON N, KELSEY J, LUCKS S, *et al*. Improved cryptanalysis of Rijndael[C]. Springer-Verlag, 2001/213-230.

[8] LI P, SUN B, LI C. Integral cryptanalysis of ARIA[A]. Proceedings of Information Security and Cryptology-Inscrypt 2009, Lecture Note in Computer Science[C]. Berlin: Springer, 2009.1-14.

[9] LI Y, WU W, ZHANG L. Improved integral attacks on reduced round camellia[EB/OL]. http://eprint.iacr.org/2011/163.pdf, 2011.

（下转第 171 页）

DONG S, WANG G. Research on P2P streaming media identification based on UDP[J]. Journal on Communications, 2012, 33(12): 25-34.

[19] MOORE A W, ZUEV D. Discriminators for Use in Flow-based Classification[R]. Intel Research, Cambridge, 2005.

[20] BERNAILLE L, TEIXEIRA R, AKODKENOU I, *et al*. Traffic classification on the fly[J]. ACM SIGCOMM Computer Communication Review, 2006, 36(2): 23-26.

[21] BERNAILLE L, TEIXEIRA R, SALAMTIAN K. Early application identification[A]. Proceedings of CoNEXT'06[C], Lisboa, Portugal, 2006.

[22] JAIN A K, DUBES R C. Algorithms for clustering data[M]. Prentice-Hall, Inc, 1988.

[23] DUMPSTER A P, PAIRD N M, RUBIN D B. Maximum likelihood from incomplete data via the EM algorithm[J]. Journal of the Royal Statistical Society, 1977, 39(1): 1-38.

[24] ESTER M, KRIEGEL H P, SANDER J, *et al*. A density-based algorithm for discovering clusters in large spatial database with noise[A]. Proceedings of the International Conference on Knowledge Discovery in Databases and Data Mining[C]. Portland, Oregon, 1996.226-231.

[25] GUHA S, RASTOGI R, SHIM K. ROCK: a robust clustering algorithm for categorical attributes[J]. Information System, 2000, 25(5): 345-366.

[26] WEKA[EB/OL]. http://www.cs.waikato.ac.nz/~ml/weka/index.html.

作者简介：

王变琴（1963-），女，陕西蒲城人，博士，中山大学高级工程师，主要研究方向为网络安全与数据挖掘。

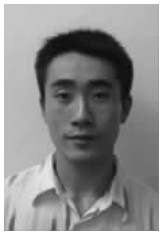
余顺争（1958-），男，江西南昌人，博士，中山大学教授、博士生导师，主要研究方向为计算机网络与网络安全。

（上接第 163 页）

[10] TANG X H, LI C, XIE R Q. Square attack on CLEFIA[J]. Journal of Electronics & Information Technology, 2009, 31(9): 2260-2263.

[11] 李超，孙兵，李瑞林．分组密码的攻击方法与实例分析[M]．北京：科学出版社，2010.
LI C, SUN B, LI R L. Block Cipher Attack Method and Example Analysis[M]. Beijing: Science Press, 2010.

作者简介：



潘志舒（1985-），男，江苏镇江人，解放军信息工程大学硕士生，主要研究方向为分组密码设计与分析。

郭建胜（1972-），男，河南沁阳人，解放军信息工程大学教授、博士生导师，主要研究方向为密码学和信息安全。

曹进克（1964-），男，河南偃师人，硕士，解放军信息工程大学副教授，主要研究方向为信息安全理论与技术。

罗伟（1987-），男，四川双流人，解放军信息工程大学硕士生，主要研究方向为分组密码设计与分析。