MIBS-80 的 13 轮不可能差分分析

付立仕* 金晨辉
(解放军信息工程大学 郑州 450001)

摘 要：该文首次对 13 轮 MIBS-80 算法进行了不可能差分分析。首先基于 MIBS-80 中 S 盒的不可能差分筛选明文对，其次通过第 1 轮轮密钥与第 2 轮轮密钥、第 1 轮轮密钥与第 13 轮轮密钥之间的制约关系进一步筛选明文对。该文的攻击排除掉的明文对数量是已有的不可能差分攻击排除掉的明文对数量的 $2^{18.2}$ 倍，因而同时降低了攻击的存储复杂度和时间复杂度。此外，该文多次利用查表的方法求出攻击中涉及的密钥，进一步降低了攻击所需的时间复杂度和存储复杂度。最后，该文利用独立的 80 bit 轮密钥来恢复主密钥，确保得到正确密钥。该文的攻击需要 $2^{60.1}$ 个选择明文，$2^{69.5}$ 次 13 轮加密，存储量为 $2^{71.2}$ 个 64 bit，该结果优于已有的不可能差分攻击。

关键词：轻量级分组密码；MIBS-80 算法；不可能差分分析；密钥制约关系

中图分类号：TN918.1 **文献标识码**：A **文章编号**：1009-5896(2016)04-0848-08

DOI: 10.11999/JEIT150673

Impossible Differential Cryptanalysis on 13-round MIBS-80

FU Lishi JIN Chenhui
(*The Information Engineering University of PLA*, *Zhengzhou* 450001, *China*)

Abstract: This paper presents the 13-round impossible differential cryptanalysis on MIBS-80 for the first time. Firstly, this paper filters the plaintexts based on the impossible differentia of S-box in MIBS-80. Secondly, by taking advantage of the restrict relation between key in the first round and in the second round, the restrict relation between key in the first round and in the 13th round, the number of plaintexts is further reduced. To sum up, $2^{18.2}$ times can be eliminated as big as the number of plaintexts eliminated in former impossible attacks, therefore both the time complexity and memory complexity are saved. Besides, by looking up various tables to get the needed key bits in the attack, the time complexity and memory complexity are thereafter reduced. Finally, 80 independent key bit are used to recover the main key, which ensures that only the right key is kept. The presented attack needs $2^{60.1}$ chosen plaintexts, $2^{69.5}$ 13-round encryptions and $2^{71.2}$ 64 bit blocks, which is the best result of impossible differential attack on MIBS so far.

Key words: Lightweight block cipher; MIBS-80 algorithm; Impossible differential cryptanalysis; Restrict relation between keys

1 引言

近年来，随着微型计算设备如 RFID、无线传感等技术的广泛应用，轻量级分组密码成为了密码学的一个研究热点。许多轻量级分组密码算法也被研制出来，如 PRESENT, LED, KLEIN, LBlock 和 MIBS 等。2009 年，文献[1]在 CANS 会议上首次提出了 MIBS 算法，MIBS 占用资源少，适合应用于计算能力受限的微型计算设备上。自 MIBS 算法被提出以来，其安全性受到广泛重视，目前已有基于不可能差分分析[2,3]、差分分析[2,4]、线性分析[2]、积分攻击[5]、多维线性攻击[6]、中间相遇攻击[7]、多维零相关线性分析[8]、相关密钥不可能差分分析[9]的分析结果。

不可能差分攻击是于 1999 年在文献[10]和文献[11]中分别提出来的。它的攻击原理是利用差分转移概率为 0 的差分对应排除错误的密钥，进而恢复出正确的密钥。若密钥 Key 使得密钥中存在不可能差分对应，则该密钥 Key 为错误的密钥。2010 年，文献[12]基于快速排序给出了明文对的筛选方法，降低了筛选明文对所占的时间复杂度。在 2014 年的亚密会上，文献[13]提出了状态检测技术来进一步降低不可能差分攻击过程中所要猜测的密钥数，进而降低了不可能攻击的时间复杂度。目前，不可能差分攻击已是攻击密码算法的有效方法之一，其中不可能差分攻击对 AES[14,15]，FOX[16,17]，ARIA[18]，

收稿日期：2015-06-04；改回日期：2015-11-25；网络出版：2016-01-14
*通信作者：付立仕 15036018167@163.com
基金项目：国家自然科学基金(61272488, 61402523)
Foundation Items: The National Natural Science Foundation of China (61272488, 61402523)

Camellia[18−21], 3D[22]已取得了显著效果。

本文主要研究不可能差分分析对 MIBS 算法的攻击效果。2010 年 CANS 会议上文献[2]首次给出了 MIBS 算法中存在的 8 轮不可能差分对应，并对 MIBS-80 进行了 12 轮的不可能差分攻击。2012 年，文献[3]指出了文献中[2]不可能差分分析的错误，并进一步改进了对 12 轮 MIBS-80 算法的不可能差分攻击。2014 年，文献[6]修正了文献[2]中不可能差分的攻击结果，但并没有给出具体的攻击算法。需要指出的是，文献[3]利用连续的 80 bit 轮子密钥进而恢复出主密钥，但连续的 80 bit 轮密钥之间有至少 13 bit 的冗余信息，因此在文献[3]给出的时间复杂度之内并不能得出正确密钥。本文利用独立的 80 bit 子密钥恢复出主密钥，确保能够得到正确的密钥。

为了降低时间复杂度和存储复杂度，本文在对 13 轮 MIBS-80 算法进行攻击时尽可能早和尽可能多地排除明文对，并结合查表方法穷举尽可能少的密钥。首先，基于 MIBS 算法中 S 盒的不可能差分对应，本文比文献[2,3]中的不可能差分攻击多过滤 $2^{7.2}$ 倍的明文对，降低了明文对的数量。在攻击过程中，基于第 1 轮密钥与第 2 轮密钥，第 13 轮密钥和第 1 轮密钥之间的密钥制约关系，本文进一步对明文对进行过滤。通过以上过滤，本文过滤掉的明文对数量是文献[2,3]中过滤掉的明文对数量的 $2^{18.2}$ 倍，因而降低了攻击所需要的时间复杂度和存储复杂度。本文多次利用查表技术给出攻击过程中所涉及的密钥，进一步降低了攻击的时间复杂度和存储复杂度。此外，为了降低存储复杂度，本文在具体攻击时，依次对每个明文结构中的明文对进行过滤，故只需存储当前结构中保留的明文对，而在对下一个结构进行攻击时，释放上一个结构所占用的存储空间，由此降低了存储复杂度。本文还给出了 MIBS-80 算法第 $1, 2, 12, 13$ 轮的轮密钥与主密钥之间的关系，在攻击过程中利用密钥之间的制约关系进一步降低了攻击的时间复杂度。基于此本文首次提出了对 13 轮 MIBS-80 的不可能差分攻击，该文的结果优于文献[2,3]中对 MIBS-80 的不可能差分攻击。

2　MIBS 算法简介

MIBS 算法是嵌套 SP 网络的 Feistel 结构的分组密码算法，其消息分组长度为 64 bit，加密轮数为 32 轮。MIBS 算法的密钥规模有 64 bit 和 80 bit 两种，分别记为 MIBS-64 和 MIBS-80，本文针对 MIBS-80 进行了 13 轮的不可能差分攻击。

在本文中，64 bit 的消息分组被分成左右两部分 L_0 和 R_0，各占 32 bit。记初始输入为 L_0, R_0，第 i 轮的输入为 L_{i-1}, R_{i-1}，k_i 是 32 bit 轮密钥，第 i 轮的迭代公式为 $L_i = F(K_i, L_{i-1}) \oplus R_{i-1}, R_i = L_{i-1}$。其中 MIBS 算法中 F 函数由轮密钥加、S 盒变换、扩散层 P 组成。记 L_{i-1} 经过第 i 轮的 S 盒变换后为 y_i，经过第 i 轮的扩散层 P 变换后为 $y_i^{'}$。记 $y_{i,j}$ 代表 y_i 的第 j 个 4-bit 块，$y_{i,j}^{'}$ 代表 $y_i^{'}$ 的第 j 个 4-bit 块。

MIBS 算法中的混合层 P：该层为线性变换，由下列线性关系式构成：

$$
\begin{aligned}
y_1^{'} &= y_1 \oplus y_2 \oplus y_4 \oplus y_5 \oplus y_7 \oplus y_8\\
y_2^{'} &= y_2 \oplus y_3 \oplus y_4 \oplus y_5 \oplus y_6 \oplus y_7\\
y_3^{'} &= y_1 \oplus y_2 \oplus y_3 \oplus y_5 \oplus y_6 \oplus y_8\\
y_4^{'} &= y_2 \oplus y_3 \oplus y_4 \oplus y_7 \oplus y_8\\
y_5^{'} &= y_1 \oplus y_3 \oplus y_4 \oplus y_5 \oplus y_8\\
y_6^{'} &= y_1 \oplus y_2 \oplus y_4 \oplus y_5 \oplus y_6\\
y_7^{'} &= y_1 \oplus y_2 \oplus y_3 \oplus y_6 \oplus y_7\\
y_8^{'} &= y_1 \oplus y_3 \oplus y_4 \oplus y_6 \oplus y_7 \oplus y_8
\end{aligned}
$$

本文记加密的轮数为 $r = 1,2,\cdots,32$，每轮的轮密钥为 k_r，$k_{r,i}$ 代表 k_r 的第 i 个 4-bit 块，$k_{r,i}[j_1, j_2, \cdots, j_n]$ 代表 $k_{r,i}$ 的第 $j_1, j_2, \cdots, j_n$ bit，$k_{r,[i_1,i_2,\cdots,i_m]}$ 代表 k_r 的 $i_1, i_2, \cdots, i_m$ 个 4-bit 块，其中 $j_1, j_2, \cdots, j_n \in \{1,2,3,4\}$，$i_1, i_2, \cdots, i_m \in \{1,2,\cdots,8\}$。记 $k_r[1 \sim 32] = k_{r,[1,2,\cdots,8]}$，即 32 bit 轮密钥 k_r 从左至右依次被划分为 $k_{r,[1]}, k_{r,[2]}, \cdots, k_{r,[8]}$。

由于本文分析的是 MIBS-80 算法，因此本文只介绍 MIBS-80 的密钥生成算法，MIBS-64 算法的密钥生成算法详见文献[1]，MIBS-80 的密钥生成算法如下所示。

设长度为 80-bit 的主密钥为 $K = (K_{79}, K_{78}, \cdots, K_0)$，由主密钥 K 生成 32 个 32 bit 的轮密钥 $k_i (1 \le i \le 32)$ 的过程如下：

$\text{state}^i \leftarrow K$，对 $i = 1,2,\cdots,32$

(1) $\text{state}^i = \text{state}^{i-1} >>> 19$;

(2) $\text{state}^i = S\left(\text{state}^i_{[79\sim76]}\right) \cdot \left\| S\left(\text{state}^i_{[75\sim72]}\right) \right\| \text{state}^i_{[75\sim0]}$;

(3) $\text{state}^i = \left(\text{state}^i_{[79\sim19]}\right) \left\| \left(\left(\text{state}^i_{[18\sim14]}\right) \oplus \text{Round\_counter}\right) \right\| \text{state}^i_{[73\sim0]}$;

(4) $k_i[1 \sim 32] = \text{state}^i_{[79\sim48]}$。

备注：由于 Round_counter 是与轮数 r 有关的常数，而与主密钥 $K = (K_{79}, K_{78}, \cdots, K_0)$ 无关，因此本文在考虑轮密钥与主密钥 K 的相关性时，忽略 Round_counter 的影响，但这不影响本文结论的正确性。此外，由于每轮的轮密钥与主密钥之间相差

若干个 S 盒的运算，又 S 盒为双射运算，则在攻击时只需获取独立的 80 bit 轮密钥即可恢复出主密钥。

3 约减至 13 轮的不可能差分攻击

3.1 预备知识

引理 1 (S盒的差分性质) 对于 F_2^n 至 F_2^n 的字节替换变换 S 盒，有以下性质：

(1)若已知 S 盒的输入差分 α，输出差分 β，则平均有一个输入 x 满足 $S(x\oplus\alpha)\oplus S(x)=\beta$；

(2)对于给定的 $(\Delta,\nabla,\beta_1,\beta_2)$，其中 $\Delta,\nabla,\beta_1,\beta_2,\alpha,x\in F_2^n$，当 β_1,β_2 从 F_2^n 中随机选取时，下述两个方程 $S(x\oplus\alpha)\oplus S(x)=\beta_1, S(x\oplus\alpha\oplus\Delta)\oplus S(x\oplus\nabla)=\beta_2$ 平均有一个解 (α,x)。

证明 性质(1)在在文献[14]中已有证明。下面我们来证明性质(2)。令

$$\begin{aligned}&\mathrm{set}((\Delta,\nabla)\to(\beta_1,\beta_2))\\&=\#\Big\{x,\alpha\in\{0,1\}^n: S(x\oplus\alpha)\oplus S(x)\\&\quad=\beta_1 \text{且} S(x\oplus\alpha\oplus\Delta)\oplus S(x\oplus\nabla)=\beta_2\Big\}\end{aligned}$$

则集合 $\mathrm{set}((\Delta,\nabla)\to(\beta_1,\beta_2))$ 中元素的平均个数为

$$\begin{aligned}&2^{-2n}\sum_{\beta_1,\beta_2\in F_2^n}\mathrm{set}((\Delta,\nabla)\to(\beta_1,\beta_2))\\&=2^{-2n}\sum_{\beta_1,\beta_2\in F_2^n}2^{2n}\Pr((\Delta,\nabla)\to(\beta_1,\beta_2))=1\end{aligned}$$

故性质 2 得证。

引理 2 对于 32 bit X,X^*，若存在 s 使得 $P^{-1}(X\oplus X^*\oplus 000000s0)$ 具有形式 ??0?00??，则 s 是唯一的，其中 $s\in F_2^4\big/\{0\}$，且 $s=P^{-1}(X\oplus X^*)_5$。

证明 s 的唯一性在文献[2]中已有说明，在此不再证明。下面给出 s 的具体表达式。由于 $P^{-1}(X\oplus X^*\oplus 000000s0)=P^{-1}(X\oplus X^*)\oplus ss0ss0ss$ 具有形式 ??0?00??，则有 $P^{-1}(X\oplus X^*)_5\oplus s=0$，得证。

引理 3[2] 在 MIBS-80 算法中，相邻两轮的轮密钥之间具有线性关系 $k_i[1\sim 13]=k_{i+1}[20\sim 32]$，即 $k_{i,1}\|k_{i,2}\|k_{i,3}\|k_{i,4}[1]=k_{i+1,5}[4]\|k_{i+1,6}\|k_{i+1,7}\|k_{i+1,8}$。

引理 4 在 MIBS-80 算法中，$k_1,k_{2,[1,2,3,4]},k_{13,[1,2,3,4,5,6,8]},k_{12,5}$ 与主密钥 K 之间有如下关系：

$$\begin{aligned}k_1&=\big(S(K(18\sim 15)),S(K(14\sim 11)),\\&\quad K(10\sim 0),K(79\sim 67)\big)\\k_{2,[1,2,3,4]}&=\big(S(K(37\sim 34)),S\big(K(33\sim 30)\big),\\&\quad K(29\sim 26),K(25\sim 22)\big)\\k_{13,[1,2,3,4,5,6,8]}&=(SS(K(6\sim 3)),S(K(2\sim 0,79)),\\&\quad K(78\sim 76),S(K(75\sim 72)),\\&\quad SS(K(71\sim 68)),SS(K(67\sim 64)),\\&\quad S(K(63\sim 60))[1],K(58,57),\\&\quad S(K(56\sim 53))[1,2])\\k_{12,5}&=(SS(K(52\sim 49))[2,3,4],SS(K(48\sim 45))[1])\end{aligned}$$

引理 4 可由 MIBS-80 算法的密钥扩展算法直接得到，在此不再证明。在已知 $(k_1,k_{2,[1,2,3,4]},k_{13,[1,2,3,4,5,6,8]},k_{12,5})$ 时，可直接通过 S 盒的逆运算求出 $K(18\sim 0),K(79\sim 64),K(37\sim 22),K(58,57)$ 共 53 bit 密钥。

推论 MIBS-80 算法中第 13 轮密钥与第 1 轮密钥之间有如下关系：

$$\begin{aligned}&k_{13,1}=S\big(S(k_{1,4})\big),\ k_{13,2}=S(k_{1,5}),\\&k_{13}[9,10,11]\ =k_1[21,22,23],\\&\big(k_{13,3}[4],k_{13,4}[1,2,3]\big)=S\big(k_{1,6}[4],k_{1,7}[1,2,3]\big)\big),\\&\big(k_{13,4}[4],k_{13,5}[1,2,3]\big)=S\big(k_{1,7}[4],k_{1,8}[1,2,3]\big)\big)\end{aligned}$$

3.2 对 13 轮 MIBS-80 的不可能差分攻击

在对 MIBS-80 算法的不可能差分攻击中，本文主要利用文献[2]给出的 8 轮不可能差分，并在该 8 轮不可能差分的基础上向前扩展 3 轮，向后扩展 2 轮，由此攻击了 13 轮 MIBS-80 算法(如图 1)。由文献[2]知，若输入差分对应为 $(00000000,000000s0)$，输出差分对应为 $(0000h000,00000000)$，当 $s\neq 0$, $h\neq 0$, $s,h\in F_2^4$ 时，差分对应 $(00000000,000000s0)\to(0000h000,00000000)$ 的转移概率为零。

预计算：构建预计算表 H。该表用于在给定的输入差分 α 与输出差分 β 下，给出满足 $S(x\oplus\alpha)\oplus S(x)=\beta$ 的 $(x,S(x))$，其中 $\alpha,\beta,x\in F_2^4$。

预计算：构建预计算表 T。该表用于在给定的 $(\Delta,\nabla,\beta_1,\beta_2)$ 下，给出满足 $S(x\oplus\alpha)\oplus S(x)=\beta_1$, $S(x\oplus\nabla)\ \oplus S(x\oplus\alpha\oplus\Delta)=\beta_2$ 的 $(\alpha,x,S(x))$，其中 $\Delta,\nabla,\beta_1,\beta_2\in F_2^4$。

本节我们首先给出对 13 轮 MIBS-80 进行不可能差分的攻击流程图，如图 2 所示。接下来给出具体攻击过程如下：

步骤 1 选择由满足下面形式的明文组成的结构：

$$\begin{aligned}L_0&=P(x_1,x_2,a_3,x_4,a_5,a_6,x_7,x_8)\\&\quad\oplus(b_1,b_2,b_3,b_4,b_5,b_6,x,b_8)\\R_0&=(y_1,y_2,y_3,y_4,y_5,y_6,y_7,y_8)\end{aligned}$$

其中 $x_i(i=1,2,4,7,8),y_i(1\le i\le 8)$ 与 x 均有 2^4 种取值，a_i,b_i 是 4 bit 的常数。故一个结构含有 $2^{(6+8)\times 4}=2^{56}$ 个明文，这些明文可构成 $2^{56\times 2-1}=2^{111}$ 个明文对。取 2^m 个结构，则共有 2^{m+111} 个明文对。

步骤 2 对每个结构中的明文对，选择密文差分满足如下形式的明文对：即

$$\begin{aligned}\Delta L_{13}&=P(q_1,q_2,q_3,0,q_5,q_6,0,0)\oplus(0,0,0,0,h,0,0,0)\\\Delta R_{13}&=(g,g,g,0,g,g,0,0)\end{aligned}$$

其中，$h,q_i(i=1,2,3,5,6)\in F_2^4$。由于 $h\to g$，$g\to q_i$ $(i=1,2,3,5,6)$ 为 MIBS 算法中 S 盒的差分转移概率

非零的差分对应。由 MIBS 算法 S 盒的差分分布性质知，对非零 g，h，$q_i(i=1,2,3,5,6)$ 均有 7 种取值，故满足过滤条件的密文差分有 $15\times7\times7^5=2^{20.8}$ 种取值，所以一个明文对通过过滤的概率为 $2^{20.8}/2^{64}=2^{-43.2}$，则一个结构中有 $2^{111}\times2^{-43.2}=2^{67.8}$ 明文对被保留下来，将 $2^{67.8}$ 个明文对存储在表 H_1 中，并将明文对依次编号为 $j=0,1,\cdots,2^{67.8}-1$，存储内容为 $(j,L_0\|R_0,L_0^*\|R_0^*,L_{13}\|R_{13},L_{13}^*\|R_{13}^*)$，为 j 分配 68 bit 的地址空间即可。

步骤 3　求 H_1 中的每个明文对对应的 32 bit k_1，并进一步对 $2^{67.8}$ 个明文对进行过滤。

由于明文对 $(L_0\|R_0,L_0^*\|R_0^*)$ 经过第 1 轮 S 盒变换后的输出差分为 $S(L_{0,i}\oplus k_{1,i})\oplus S(L_{0,i}^*\oplus k_{1,i})$，其中 $i\in\{1,2,\cdots,8\}$。又该输出差分为 $P^{-1}(\Delta R_0\oplus\Delta L_1)=P^{-1}(\Delta R_0)\oplus(000000u0)$，由该表达式知明文对经过第 1 轮 S 盒变换后，其输出差分的 8 个 4-bit 中仅有第 7 个 4-bit 不确定，其它 7 个 4-bit 均可由输入差分 ΔR_0 得到。以 $L_{0,i}\oplus L_{0,i}^*$ 和 $P^{-1}(\Delta R_0)_i$ 为索引查表 H，可平均得到 1 个 $L_{0,i}\oplus k_{1,i}$ 及 $S(L_{0,i}\oplus k_{1,i})$（即 $y_{1,i}$），进而结合 L_0 得到 $k_{1,i}$，其中 $i=1,2,3,4,6,8$。

由 MIBS 算法扩散层 P 可知：

$$L_{1,7}=y_{1,1}\oplus y_{1,2}\oplus y_{1,3}\oplus y_{1,6}\oplus y_{1,7}\oplus R_{0,7}$$

$$L_{1,8}=y_{1,1}\oplus y_{1,3}\oplus y_{1,4}\oplus y_{1,6}\oplus y_{1,7}\oplus y_{1,8}\oplus R_{0,8}$$

$$L_{1,7}^*=y_{1,1}^*\oplus y_{1,2}^*\oplus y_{1,3}^*\oplus y_{1,6}^*\oplus y_{1,7}^*\oplus R_{0,7}^*$$

$$L_{1,8}^*=y_{1,1}^*\oplus y_{1,3}^*\oplus y_{1,4}^*\oplus y_{1,6}^*\oplus y_{1,7}^*\oplus y_{1,8}^*\oplus R_{0,8}^*$$

则有

$$L_{1,7}\oplus L_{1,8}=y_{1,2}\oplus y_{1,4}\oplus y_{1,8}\oplus R_{0,7}\oplus R_{0,8}$$

$$L_{1,7}^*\oplus L_{1,8}^*=y_{1,2}^*\oplus y_{1,4}^*\oplus y_{1,8}^*\oplus R_{0,7}^*\oplus R_{0,8}^*$$

又 $y_{1,i}$ 已知，结合 $P^{-1}(\Delta R_0)$ 可求出 $y_{1,i}^*$（$i=1,2,3,4,6,8$），由此可得 $L_{1,7}\oplus L_{1,8}$ 和 $L_{1,7}^*\oplus L_{1,8}^*$。又由引理 3 知 $k_{2,7}=(k_{1,2}[2,3,4],k_{1,3}[1]),k_{2,8}=(k_{1,3}[2,3,4],k_{1,4}[1])$，且有

$$\begin{cases}\Delta y_{2,7}=S(L_{1,7}\oplus k_{2,7})\oplus S(L_{1,7}^*\oplus k_{2,7})\\ \qquad\quad=P^{-1}(\Delta L_0)_7\oplus P^{-1}(\Delta L_0)_5\\ \Delta y_{2,8}=S(L_{1,8}\oplus k_{2,8})\oplus S(L_{1,8}^*\oplus k_{2,8})\\ \qquad\quad=P^{-1}(\Delta L_0)_8\oplus P^{-1}(\Delta L_0)_5\end{cases}$$

以 $(L_{1,7}^*\oplus L_{1,8}^*\oplus k_{2,7}\oplus k_{2,8},L_{1,7}\oplus L_{1,8}\oplus k_{2,7}\oplus k_{2,8},\Delta y_{2,7},\Delta y_{2,8})$ 为索引查表 T 得到对应的存储值，若以 $(L_{1,7}\oplus k_{2,7},L_{1,7}\oplus L_{1,7}^*)$ 为上述方程组的未知变量，则该存储值即为 $(L_{1,7}\oplus k_{2,7},L_{1,7}\oplus L_{1,7}^*,y_{2,7})$，结合 $k_{2,7}$ 可得 $L_{1,7}$，进而可得 $L_{1,7},L_{1,7}^*,y_{2,7}$。若以 $(L_{1,8}\oplus k_{2,8},L_{1,8}\oplus L_{1,8}^*)$ 为上述方程组的变量，则查表 T 所得到的存储值即为 $(L_{1,8}\oplus k_{2,8},L_{1,8}\oplus L_{1,8}^*,y_{2,8})$，结合 $k_{2,8}$ 可得 $L_{1,8}$，进而可得 $L_{1,8},L_{1,8}^*,y_{2,8}$。

又由 MIBS 算法中 P 盒的表达式知，$y_{1,7}$ 同时满足两个方程：$y_{1,7}=y_{1,1}\oplus y_{1,2}\oplus y_{1,3}\oplus y_{1,6}\oplus R_{0,7}\oplus L_{1,7}$，$y_{1,7}=y_{1,1}\oplus y_{1,3}\oplus y_{1,4}\oplus y_{1,6}\oplus y_{1,8}\oplus R_{0,8}\oplus L_{1,8}$。因此，当由明文对求出的 $k_{1,[1,2,3,4,6,8]}$ 正确时，由两个方程求出的 $y_{1,7}$ 一定相等；当由明文对求出的 $k_{1,[1,2,3,4,6,8]}$ 错误时，由两个方程求出的 $y_{1,7}$ 以 1/16 的概率相等；据此可筛选掉错误的 $k_{1,[1,2,3,4,6,8]}$ 及其对应的明文对，故经过此步骤后每个结构保留的明文对个数为 $2^{67.8}\times2^{-4}=2^{63.8}$。

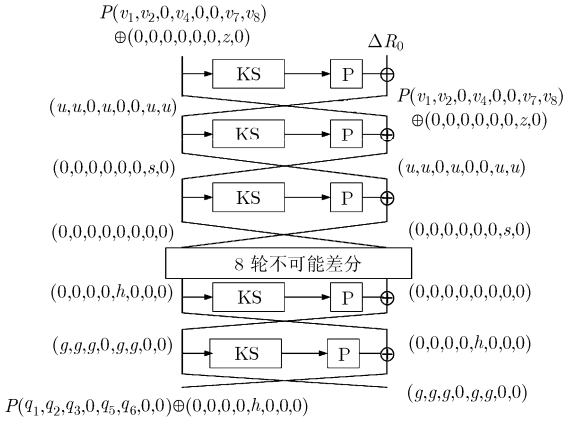

图 1　13 轮 MIBS-80 的不可能差分攻击

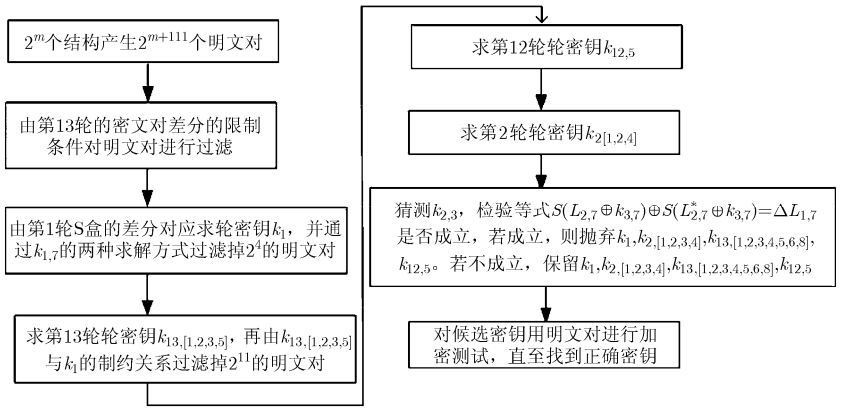

图 2　13 轮 MIBS-80 的不可能差分攻击流程图

又 $k_{1,7}=S^{-1}(y_{1,7})\oplus R_{0,7}$，$P^{-1}(\Delta R_0)_7\oplus u=y_{1,7}\oplus y^*_{1,7}=L_{1,7}\oplus L^*_{1,7}$，由上述等式可求出 $u,k_{1,7}$。以 $L_{0,5}\oplus L^*_{0,5}$ 和 $P^{-1}(\Delta R_0)_5$ 为索引查表 H，可平均得到 1 个 $L_{0,5}\oplus k_{1,5}$ 及 $S(L_{0,5}\oplus k_{1,5})$ (即 $y_{1,5}$)，进而结合 L_0 得到 $k_{1,5}$。

由于明文对 $(L_0\|R_0,L^*_0\|R^*_0)$ 对应的密文对差分具有形式 ΔL_{13}=$P(q_1,q_2,q_3,0,q_5,q_6,0,0)\oplus(0,0,0,0,h,0,0,0)$，建立线性方程组将 q_i 和 h 求出，其中 $i=1,2,3,5,6$，将 $(j,k_{1,[1,2,3,4,5,6,7,8]},L_{1,[1,2,3,4,6,7]},y_{2,7},u,q_1,q_3,q_4,q_5,q_6,h)$ 存入表 H_2 中。

步骤 4　对 H_2 中的 $2^{63.8}$ 个明文对，求出其对应的 $k_{13,[1,2,3,5,6]}$，利用 $k_{1,[1,2,3,4,5,6,8]}$ 和 $k_{13,[1,2,3,5,6]}$ 之间的制约关系对明文对再次筛选。

由于 $\Delta R_{13,3}=g$，$g\to q_3$ 为非零差分对应，以 $(\Delta R_{13,1},q_3)$ 为索引查表 H 可平均得到 $16/7\approx 2^{1.2}$ 个 $L_{12,3}\oplus k_{13,3}$ 及 $S(L_{12,3}\oplus k_{13,3})$ (即 $y_{13,3}$)。又 $L_{12,3}$=$R_{13,3}$，则结合 $R_{13,3}$ 可求出 $2^{1.2}$ 个 $k_{13,3}$，检测等式 $k_{13}[9,10,11]=k_1[21,22,23]$ 是否成立，若成立保留该明文对，否则抛弃该明文对，则一个明文对通过检测的概率为 1/8，保留下来的明文对数量为 $2^{63.8}\times 2^{1.2}\times 1/8=2^{62}$。

由于 $\Delta R_{13,2}=g$，$g\to q_2$ 为非零差分对应，以 $(\Delta R_{13,2},q_2)$ 为索引查表 H 可平均得到 $16/7\approx 2^{1.2}$ 个 $L_{12,2}\oplus k_{13,2}$ 及 $S(L_{12,2}\oplus k_{13,2})$ (即 $y_{13,2}$)。又 $L_{12,2}$=$R_{13,2}$，则结合 $R_{13,2}$ 可求出 $2^{1.2}$ 个 $k_{13,2}$，检测等式 $k_{13,2}=S(k_{1,5})$ 是否成立，若成立保留该明文对，否则抛弃该明文对，则一个明文对通过检测的概率为 1/16，保留下来的明文对数量为 $2^{62}\times 2^{1.2}\times 1/16=2^{59.2}$。

由于 $\Delta R_{13,1}=g$，$g\to q_1$ 为非零差分对应，以 $(\Delta R_{13,1},q_1)$ 为索引查表 H 可平均得到 $16/7\approx 2^{1.2}$ 个 $L_{12,1}\oplus k_{13,1}$ 及 $S(L_{12,1}\oplus k_{13,1})$ (即 $y_{13,1}$)。又 $L_{12,1}=R_{13,1}$，则结合 $R_{13,1}$ 可求出 $2^{1.2}$ 个 $k_{13,1}$，检测等式 $k_{13,1}$=$SS(k_{1,4})$ 是否成立，若成立保留该明文对，否则抛弃该明文对，则一个明文对通过检测的概率为 1/16，保留下来的明文对数量为 $2^{59.2}\times 2^{1.2}\times 1/16$=$2^{56.4}$。

由于 $\Delta R_{13,5}=g$，$g\to q_5$ 为非零差分对应，以 $(\Delta R_{13,5},q_5)$ 为索引查表 H 可平均得到 $16/7\approx 2^{1.2}$ 个 $L_{12,5}\oplus k_{13,5}$ 及 $S(L_{12,5}\oplus k_{13,5})$ (即 $y_{13,5}$)。又 $L_{12,5}$=$R_{13,5}$，则结合 $R_{13,5}$ 可求出 $2^{1.2}$ 个 $k_{13,5}$。同理可求出 $2^{1.2}$ 个 $k_{13,6}$，即有 $2^{56.4}\times 2^{1.2\times 2}$=$2^{58.8}$ 个明文-密钥对，将这些明文-密钥对存储在表 H_3 中，H_3 存储 $(j,k_{13,[1,2,3,5,6]},y_{13,[1,3,5]})$。

对每个 $(k_1,k_{13,[1,2,3,5,6]})$，结合表 H_2 和 H_3，建立表 Ω_1。则每个结构的 Ω_1 有 $2^{58.8}/2^{32+20-11}=2^{17.8}$ 个条目，每个条目存储 $(j,L_{1,[1,2,3,4,6,7]},u,y_{13,[1,3,5]},h)$。

在对当前结构执行完步骤 2~4 后，释放 (H_1,H_2,H_3)，对下个结构执行步骤 2~4。故在对 2^m 个明文结构执行完步骤 2~4 后，Ω_1 的规模为 $2^m\times 2^{17.8}=2^{m+17.8}$。

步骤 5　对 Ω_1 中的 $2^{m+17.8}$ 个明文对，执行以下步骤。

先求 $L_{11,5}$，再利用 S 盒的差分性质求 $k_{12,5}$。

由于 $L_{11,5}=L_{13,5}\oplus y'_{13,5}$，又 MIBS 的扩散层中 $y'_{13,5}=y_{13,1}\oplus y_{13,3}\oplus y_{13,4}\oplus y_{13,5}\oplus y_{13,8}$，其中 $y_{13,i}=S[L_{12,i}\oplus k_{13,i}]=S[R_{12,i}\oplus k_{13,i}]$。由于 $k_{13,[1,3,5]}$ 已知，又由引理 4 的推论知，可根据当前 k_1 可求得 $k_{13,4}$，故只需猜测 $k_{13,8}$ 即可求得 $y'_{13,5}$，进而求得 $L_{11,5}$。在当前密钥 $k_{13,8}$ 下，建立表 Ω_2，该表有 $2^{m+17.8}$ 个条目，每个条目存储 $(j,L_{1,[1,2,3,4,6,7]},u,L_{11,5},h)$。

又由于 h,g 已知，且第 1 步在筛选明文对时，已经保证 $h\to g$ 是 S 盒非零的差分对应，故由 $S(L_{11,5}\oplus k_{12,5})\oplus S(L_{11,5}\oplus h\oplus k_{12,5})=g$ 查表 H 可平均求出 $16/7\approx 2^{1.2}$ 个 $L_{11,5}\oplus k_{12,5}$，进而得到 $2^{1.2}$ 个 $k_{12,5}$，即可得到 $2^{m+17.8}\times 2^{1.2}=2^{m+19}$ 个明文-密钥对，将 2^{m+19} 个明文-密钥对存储在表 H_4 中，则表 H_4 一共有 2^{m+19} 个条目，每个条目存储 $(j,k_{12,5})$。结合表 H_4 与 Ω_2，对每个密钥 $k_{12,5}$ 建表 $\Omega_{k_{12,5}}$，则 $\Omega_{k_{12,5}}$ 中有 $2^{m+19}/2^4=2^{m+15}$ 个条目，每个条目存储 $(j,L_{1,[1,2,3,4,6,7]},u)$。

步骤 6　对 $\Omega_{k_{12,5}}$ 中的 2^{m+15} 个明文对，执行以下步骤。

根据 $\Omega_{k_{12,5}}$ 中明文对的序号查表 Ω_1 得到 $(L_{1,[1,2,4]},u)$，其中 $L^*_{1,[1,2,4]}$ 可由 $L_{1,[1,2,4]},u$ 得到。又 $S(L_{1,1}\oplus k_{2,1})\oplus S(L^*_{1,1}\oplus k_{2,1})=P^{-1}(\Delta L_0)_1\oplus P^{-1}(\Delta L_0)_5$ 已知，故可查表 H 得到 $L_{1,1}\oplus k_{2,1}$ 及 $y_{2,1}$，进而求出 $k_{2,1}$，同理可得 $k_{2,[2,4]}$。由于一个 $(L_{1,[1,2,4]},L^*_{1,[1,2,4]})$ 可平均得到一个 $k_{2,[1,2,4]}$，则遍历 $\Omega_{k_{12,5}}$ 中的 2^{m+19} 个明文对可得 2^{m+19} 个明文-密钥对，将 2^{m+19} 个明文-密钥对存储在表 H_4 中，则表 H_4 有 2^{m+19} 个条目，每个条目存储 $(j,k_{2,[1,2,4]})$。根据 $\Omega_{k_{12,5}}$ 和 H_4，将 $k_{2,[1,2,4]}$ 对应的 $(L_{1,[1,2,4]},L^*_{1,[1,2,4]})$ 存储至表 $T_{k_{2,[1,2,4]}}$，则表 $T_{k_{2,[1,2,4]}}$ 有 $2^{m+15}/2^{12}=2^{m+3}$ 个条目，每个条目存储 $(j,y_{2,[1,2]},L_{1,[3,6,7]},u)$。

步骤 7　对 $T_{k_{2,[1,2,4]}}$ 中的 2^{m+3} 个明文对执行以下步骤。

由 MIBS 的扩散矩阵知 $L_{2,7}=y'_{2,7}\oplus L_{0,7}$，其中 $y'_{2,7}=y_{2,1}\oplus y_{2,2}\oplus y_{2,3}\oplus y_{2,6}\oplus y_{2,7}$，其中 $y_{2,i}=S[L_{1,i}\oplus k_{2,i}]$。由于 (L_1,L^*_1) 已知，则若要得出 $L_{2,7}$，需要已知 k_2 的第 1, 2, 3, 6, 7 个 4 bit 值。由于 $y_{2,6}=S(L_{1,6}\oplus k_{2,6})$ 且 $k_{2,6}=(k_{1,1}[2,3,4],k_{1,2}[1])$，故可得 $y_{2,6}$。穷举 $k_{2,3}$，即可得到 $(L_{2,7},L^*_{2,7})$。

又由于 $k_{3,7}$=$(k_{2,2}[2,3,4],k_{2,3}[1])$，计算 $S(L_{2,7}\oplus k_{3,7})\oplus S(L^*_{2,7}\oplus k_{3,7})$。若等式 $S(L_{2,7}\oplus k_{3,7})\oplus S(L^*_{2,7}\oplus$

$k_{3,7})=\Delta L_{1,7}$ 成立，即密钥 $(k_1,k_{2,[1,2,3,4]},k_{13,[1,2,3,4,5,6,8]},k_{12,5})$ 使得该 8 轮不可能差分对应成立，则密钥 $(k_1,k_{2,[1,2,3,4]},k_{13,[1,2,3,4,5,6,8]},k_{12,5})$ 为错误的。若该等式对 2^{m+3} 个明文对均不成立，则保留当前的 60 bit 密钥 $(k_1,k_{2,[1,2,3,4]},k_{13,[1,2,3,4,5,6,8]},k_{12,5})$，故一个错误密钥被保留下来的概率为 $(1-2^{-4})^{2^{m+3}}$，则有 $(2^{60}-1)\times(1-2^{-4})^{2^{m+3}}+1$ 个 $(k_1,k_{2,[1,2,3,4]},k_{13,[1,2,3,4,5,6,8]},k_{12,5})$ 为候选密钥。记候选密钥个数为 N，有

$$\begin{aligned}N&=\left(2^{60}-1\right)\times\left(1-2^{-4}\right)^{2^{m+3}}+1\\&\approx\left(2^{60}-1\right)\times\mathrm{e}^{-2^{m-1}}+1\\&=\left(2^{60}-1\right)\times2^{-2^{m-0.47}}+1\end{aligned}$$

步骤 8　对 N 个候选密钥 $(k_1,k_{2,[1,2,3,4]},k_{13,[1,2,3,4,5,6,8]},k_{12,5})$，通过 S 盒的逆运算求出 $K(18\sim0),K(79\sim64),K(37\sim22),K(58,57)$ 共 53 bit 密钥。对每个候选密钥，穷举 K 剩余的 27 bit 密钥。先穷举 $(K(63\sim60),K(56\sim45))$ 这 16 bit 的密钥，执行如下过滤操作。

对于 $K(52\sim49)$ 的 16 种取值，检测 $k_{12,5}[1,2,3]=SS(K(52\sim49))[2,3,4]$ 是否成立，若成立，则保留穷举的 $K(52\sim49)$，反之抛弃，经过过滤 $K(52\sim49)$ 剩余 2 种可能取值。

对于 $K(48\sim45)$ 的 16 种取值，检测 $k_{12,5}[4]=SS(K(48\sim45))[1]$ 是否成立，若成立，则保留穷举的 $K(48\sim45)$，反之抛弃，经过过滤 $K(48\sim45)$ 剩余 8 种可能取值。

对于 $K(63\sim60)$ 的 16 种取值，检测 $k_{13,6}[4]=S(K(63\sim60))[1]$ 是否成立，若成立，则保留穷举的 $K(63\sim60)$，反之抛弃，经过过滤 $K(63\sim60)$ 剩余 8 种可能取值。

对于 $K(56\sim53)$ 的 16 种取值，检测 $k_{13,8}[3,4]=S(K(56\sim53))[1,2]$ 是否成立，若成立，则保留穷举的 $K(56\sim53)$，反之抛弃，经过过滤 $K(56\sim53)$ 剩余 4 种可能取值。

经过以上过滤后，$(K(63\sim60),K(56\sim45))$ 共有 $2^{1+3+3+2}=2^9$ 种可能，再穷举剩余的 11 bit 密钥 $(K[59],K(44\sim38),K(21\sim19))$，用明文进行加密测试恢复出正确的密钥。

3.3 攻击复杂度分析

该攻击的算法复杂度主要集中在步骤2~步骤8之中，下面分析每个步骤的时间复杂度。

步骤 2 的时间复杂度主要为两次筛选明文对所占用的时间复杂度，第 1 次筛选所占的时间为 $2^m\times2^{56}\log_2(2^{56})=2^{m+61.8}$ 次比较运算，H_1 所占用的空间为 $2^{67.8}\times(68+64\times4)$ bit。

步骤 3 的时间复杂度为 $2^m\times(2^{67.8}\times(6+1)+2^{63.8}\times1)\approx2^{m+70.6}$ 次查表运算，存储复杂度为 $2^{63.8}\times(64+88)$ bit。

步骤 4 的时间复杂度为 $2^m\times(2^{63.8}+2^{62}\times2+2^{59.2}\times2+2^{56.4}\times2)\approx2^{m+64.4}$ 次查表运算，存储复杂度为 $2^{58.8}\times(59+32)+2^{m+17.8}\times(59+44)$ bit。

步骤 5 的时间复杂度为 $2^{41}\times2^{m+17.8}\times2^4\times(2+1)\approx2^{m+64.4}$ 次查表运算，存储复杂度为 $2^{m+23}\times(l+28)+2^{m+23}\times(l+4)+2^{m+21.8}\times(l+28+8)\approx2^{m+24.3}\times(l+28)$ bit。

步骤 6 的时间复杂度为 $2^{41}\times2^4\times2^4\times2^{m+15}\times3\approx2^{m+65.6}$ 次查表运算，存储复杂度为 $2^{m+19}\times(l+28)$ bit。

步骤 7 的时间复杂度为 $2^{41}\times2^4\times2^4\times2^{12}\times2^{m+3}+2^{41}\times2^4\times2^4\times2^{12}\times2^{m+3}\times2^4\times(1+2)\approx2^{m+69.7}$ 次查表运算。

取 $m=4.1$，则步骤 7 中剩余密钥的个数约为 $2^{47.6}$，且步骤 2 到步骤 7 的时间复杂度约为 $2^{m+71.4}=2^{75.5}$ 次查表运算。该攻击的存储复杂度主要由步骤 2、步骤 3 和步骤 4 的复杂度决定，即为 $2^{67.8}\times(68+64\times4)+2^{63.8}\times(64+88)+2^{58.8}\times(59+32)\times2^{-6}\approx2^{71.2}$ 个 64 bit。又由于对 MIBS 算法，其每轮加密时需要查 8 个 S 盒，13 轮则需要进行 104 次查 S 盒运算，故步骤 2 到步骤 7 的时间复杂度为 $2^{75.5}/104=2^{68.8}$ 次 13 轮加密运算。

步骤 8 的时间复杂度为 $2^{47.6}\times9+2^{47.6}\times(2^{16}\times4/104+2^{20}\times2)\approx2^{68.6}$ 次 13 轮加密运算。这是由于步骤 7 结束后剩余的错误密钥个数为 $2^{47.6}$，步骤 8 中穷举的密钥为 27 bit，又通过已求出的密钥进行制约可得穷举的 27 bit 密钥仅剩余 $2^{11}\times2^9=2^{20}$ 种可能，利用 2 个明文进行加密测试，进而保留正确密钥。此时剩余的错误密钥个数为 $(2^{47.6+20}-1)\times2^{-128}\ll1$，即只有正确密钥被保留下来。

综上所述，整个算法的数据复杂度为 $2^{60.1}$ 个选择明文，时间复杂度为 $2^{69.5}$ 次 13 轮加密运算，存储复杂度为 $2^{71.2}$ 个 64 bit，优于文献[2,3]的结果，如表 1 所示。

4　结束语

本文对 MIBS-80 算法进行了攻击，首次提出了对其 13 轮的不可能差分攻击，得到了目前不可能差分攻击对 MIBS-80 算法最好的分析结果。本文在攻击过程中利用 S 盒的不可能差分对应和轮密钥之间的制约关系尽早地排除错误的明文对，省掉了错误明文对所占用的时间复杂度和存储复杂度。同时，本文多次利用查表技术给出在攻击中所需要猜测的密钥，进一步降低了攻击所需的时间复杂度。此外，我们在攻击中对 2^m 个结构依次执行第 2~4 步骤，因

表 1 MIBS-80 攻击结果比较

攻击方法	轮数	数据复杂度	时间复杂度	存储复杂度	文献
差分攻击	13	2^{62}	2^{25}	—	[2]
不可能差分攻击	12	2^{59}	2^{63}	—	[3]
不可能差分攻击	12	2^{59}	$2^{58.8}$	—	[6]
积分攻击	10	$2^{39.6}$	$2^{68.4}$	—	[5]
中间相遇攻击	11	$2^{24.9}$	$2^{66.25}$	$2^{51.03}$	[7]
多维零相关线性攻击	12	$2^{62.1}$	2^{70}	—	[8]
相关密钥不可能差分攻击	14	2^{54}	2^{56}	—	[9]
不可能差分攻击	13	$2^{60.1}$	$2^{69.5}$	$2^{71.2}$	本文

备注：“—”指参考文献中没有给出相应的存储复杂度

此只需存储当前结构中通过过滤的明文对，在第 4 步骤结束后释放当前结构占用的存储空间，继而对下个结构执行第 2～4 步骤，由此将存储空间降低了 2^m 倍。本文的攻击充分利用 MIBS-80 算法扩散层的性质和各轮的轮密钥之间的制约关系，如何将这些性质和制约关系用到MIBS-80的其它攻击方法上还有待进一步研究。

参 考 文 献

[1] IZADI M, SADEGHIYAN B, and SADEGHIAN S. MIBS: a new light-weight block cipher[C]. CANS 2009, Ishikawa, Japan, 2009: 334–348. doi: 10.1007/978-3-642-10433-6_22.

[2] BAY A, NAKAHARA J, and VAUDENAY S. Cryptanalysis of reduced-round MIBS block cipher[C]. CANS 2010, Malaysia, 2010: 1–19. doi: 10.1007/978-3-642-17619-7_1.

[3] 杜承航, 陈佳哲. 轻量级分组密码算法 MIBS 不可能差分分析[J]. 山东大学学报(理学版), 2012, 47(7): 55–58.
DU Chenghang and CHEN Jiazhe. Impossible differential cryptanalysis of reduced-round MIBS[J]. *Journal of Shandong University* (*Natural Science*), 2012, 47(7): 55–58

[4] 杨林, 王美琴. 约简轮的 MIBS 算法的差分分析[J]. 山东大学学报(理学版), 2010, 45(4): 12–15.
YANG Lin and WANG Meiqin. Differential cryptanalysis of reduced-round MIBS[J]. *Journal of Shandong University* (*Natural Science*), 2010, 45(4): 12–15.

[5] 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 Gaoli, and WANG Shaohui. Integral cryptanalysis of reduced-round MIBS block cipher[J]. *Journal of Chinese Computer Systems*, 2012, 33(4): 773–777.

[6] BAY A, HUANG J, and VAUDENAY S. Improved linear cryptanalysis of reduced-round MIBS[C]. The 9th International Workshop on Security, Hirosaki, 2014: 204–220. doi: 10.1007/978-3-319-09843-2_16.

[7] 刘超, 廖福成, 卫宏儒. 对 MIBS 算法的中间相遇攻击[J]. 内蒙古大学学报(自然科学版), 2013, 44(3): 308–315.
LIU Chao, LIAO Fucheng, and WEI Hongru. Meet-in-the-middle attacks on MIBS[J]. *Journal of Inner Mongolia University* (*Natural Science*), 2013, 44(3): 308–315.

[8] 栗许, 关杰. 对轻量级密码算法 MIBS 的零相关线性分析[J]. 信息工程大学学报, 2015, 16(1): 20–24.
LI Xu and GUAN Jie. Zero correlation linear cryptanalysis of lightweight block cipher MIBS[J]. *Journal of Information Engineering University*, 2015, 16(1): 20–24.

[9] 陈平, 廖福成, 卫宏儒. 对轻量级密码算法 MIBS 的相关密钥不可能差分攻击[J]. 通信学报, 2014, 35(2): 190–193.
CHEN Ping, LIAO Fucheng, and Wei Hongru. Related-key impossible differential attack on a lightweight block cipher MIBS[J]. *Journal on Communications*, 2014, 35(2): 190–193.

[10] KNUDSEN L. DEAL — A 128-bit block cipher[R]. Technical Report 151, Department of Informatics, University of Bergen, Bergen, Norway, 1998.

[11] BIHAM E, BIRYUKOV A, and SHAMIR A. Cryptanalysis of Skipjack reduced to 31 rounds using impossible differentials[C]. Advances in Cryptolog — EUROCRYPT'99, Prague, 1999: 2–23. doi: 10.1007/3-540-48910-X_2.

[12] 胡弘坚, 金晨辉, 李信然. 改进的 7 轮 AES-128 的不可能差分攻击[J]. 密码学报, 2015, 2(1): 92–100. doi: 10.13868/j.vcnki.jcr.000063.
HU Hongjian, JIN Chenhui, and LI Xinran. Improved impossible differential attack on 7-round AES-128[J]. *Journal of Cryptologic Research*, 2015, 2(1): 92–100. doi: 10.13868/j.vcnki.jcr.000063.

[13] LI Xinran, FU Fangwei, and GUANG Xi. Multiple impossible differential cryptanalysis on reduced FOX[J]. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, 2015, E98-A(3): 906–911. doi: 10.1587/transfun.E98.A.906.

[14] GUO Rui and JIN Chenhui. Impossible differential cryptanalysis on Lai-Massey scheme[J]. *ETRI Journal*, 2014,

36(6): 1032–1040. doi: 10.4218/etrij.14.0113.1335.

[15] WU Wenling, ZHANG Wentao, and FENG Dengguo. Impossible differential cryptanalysis of reduced-round ARIA and Camellia[J]. *Journal of Computer Science and Technology*, 2007, 22(3): 449–456. doi: 10.1007/s11390-007-9056-0.

[16] WU Wenling, ZHANG Lei, and ZHANG Wentao. Improved impossible differential cryptanalysis of reduced-round Camellia[C]. Selected Areas in Cryptography — 16th Annual International Workshop, SAC 2009, Calgary, Canada, 2009: 442–456. doi: 10.1007/978-3-642-04159-4_29.

[17] MALA H, DAKHILALIAN M, RIJMEN V, *et al*. Improved impossible differential cryptanalysis of 7-round AES-128[C]. The 11th International Conference on Cryptology, Hyderabad, India, 2010: 282–291. doi: 10.1007/978-3-642-17401-8_20.

[18] LIU Ya, GU Dawu, and LIU Zhiqiang. Improved results on impossible differential cryptanalysis of reduced-round Camellia-192/256[J]. *Journal of Systems and Software*, 2012, 85(11): 2451–2458. doi: 10.1016/j.jss.2012.05.051.

[19] BAI Dongxia and LI Leibo. New impossible differential attacks on Camellia[C]. International Conference on Information Security Practice and Experience 2012, Hangzhou, 2012: 80–96. doi: 10.1007/978-3-642-29101-2_6.

[20] 张庆贵. 不可能差分攻击中的明文对筛选方法[J]. 计算机工程, 2010, 36(2): 127–129.
ZHANG Qinggui. Plaintext pair sieve methods in impossible differential attack[J]. *Computer Engineering*, 2010, 36(2): 127–129.

[21] BOURA C, NAYA PLASENCIA M, and SUDER V. Scrutinizing and improving impossible differential attacks: applications to CLEFIA, Camellia, LBlock and Simon (Full Version)[C]. Advances in Cryptology — 20th Annual International Conference on the Theory and Application of Cryptology and Information Security, Kaoshiung, 2014: 179–199. doi: 10.1007/978-3-662-45611-8_10.

[22] 谢作敏, 陈少真, 鲁林真. 11 轮 3D 密码的不可能差分攻击[J]. 电子与信息学报, 2014, 36(5): 1215–1220. doi: 10.3724/SP.J.1146.2013.00948.
XIE Zuomin, CHEN Shaozhen, and LU Linzhen. Impossible differential cryptanalysis of 11-round 3D cipher[J]. *Journal of Electronics & Information Technology*, 2014, 36(5): 1215–1220. doi: 10.3724/SP.J.1146.2013.00948.

付立仕：　女，1989 年生，博士生，研究方向为分组密码.

金晨辉：　男，1965 年生，教授，博士生导师，主要研究方向为密码学.