改进的减轮MIBS-80密码的中间相遇攻击

任炯炯* 侯泽洲 李曼曼 林东东 陈少真
(战略支援部队信息工程大学 郑州 450001)

摘 要：MIBS密码算法是一个Feistel结构的轻量级分组密码，广泛适用于资源严格受限的环境。该文利用多重集和有效的差分枚举方法，构造了8轮MIBS中间相遇区分器，并在新区分器的基础上，实现了12轮和13轮MIBS-80密码的中间相遇攻击。攻击过程利用差分传递的性质筛选明文对，利用MIBS-80密钥扩展算法中主密钥和轮密钥的关系减少密钥的猜测量，攻击12轮MIBS-80的时间复杂度为$2^{53.2}$，攻击13轮MIBS-80的时间复杂度为2^{62}。与已有中间相遇攻击的结果相比，该文对MIBS-80中间相遇攻击的轮数提高了2轮。

关键词：分组密码；MIBS算法；中间相遇攻击；截断差分；差分枚举
中图分类号：TN918.1 **文献标识码**：A **文章编号**：1009-5896(2022)08-2914-10
DOI: 10.11999/JEIT210441

Improved Meet-in-the-middle Attacks on Reduced-round MIBS-80 Cipher

REN Jiongjiong HOU Zezhou LI Manman LIN Dongdong CHEN Shaozhen
(*Strategic Support Force Information Engineering University*, *Zhengzhou* 450001, *China*)

Abstract: MIBS is a Feistel structured lightweight block cipher aimed at extremely constrained resources environment. In this paper, an 8-round meet-in-the-middle distinguisher of MIBS is constructed by utilizing multiset and effective differential enumeration technique. Then, the meet-in-the-middle attacks on 12-round and 13-round MIBS-80 are proposed based on the new distinguisher. In the attack process, the plaintexts are filtered utilizing the differential properties and the guessed keys are reduced using the relation of master key and round key in the key expansion algorithm of MIBS-80. The time complexity of attacking 12-round and 13-round MIBS-80 is $2^{53.2}$ and 2^{62}, respectively. Compared with the known results of the meet-in-the-middle attack, the number of rounds of meet-in-the-middle attack on MIBS-80 is increased by 2-round.

Key words: Block cipher; MIBS algorithm; Meet-in-the-middle attack; Truncated differential; Differential enumeration

1 引言

随着物联网新技术的突破式发展，万物联网的需求使得无线传感器、智能卡和射频识别(Radio Frequency IDentification, RFID)标签等受限设备的应用越来越广泛。轻量级分组密码广泛应用于这类资源受限环境下的数据安全和隐私保护，成为密码学研究的热点。MIBS密码算法是Izadi等人[1]在2009年提出的一个整体采用Feistel型，轮函数为代换置换网络(Substitution-Permutation Network, SPN)型结构的轻量级分组密码。其分组长度为64 bit，密钥长度有64 bit和80 bit两种，迭代轮数均为32轮。由于MIBS算法涉及的运算便于硬件实现，占用资源少，MIBS算法广泛适用于物联网和传感器网络等环境，对MIBS密码的分析已备受关注。

对MIBS密码的安全性分析主要集中在传统的差分与线性分析、不可能差分攻击、积分攻击、相关密钥攻击和故障分析等。杨林等人[2]首先以0.99的成功概率给出了13轮MIBS差分分析的结果。Bay等人[3]对MIBS抗差分和线性攻击的能力进行了新的评估。但是，杜承航等人[4]发现文献[3]不可能差分分析的错误并重新给出了12轮不可能差分分析的结果。文献[5]首次利用积分攻击分析了8轮MIBS-64和9轮MIBS-80，随后文献[6,7]给出了10轮MIBS-80积分攻击的结果。刘超等人[8]利用MIBS算法Feistel结构的等价性，构造出6轮中间相遇区分器，并结

收稿日期：2021-05-19；改回日期：2021-10-31；网络出版：2021-11-07
*通信作者： 任炯炯 jiongjiong_fun@163.com
基金项目：数学工程与先进计算国家重点实验室开放基金(2019A08)
Foundation Item: The Open Fund Project of the State Key Laboratory of Mathematical Engineering and Advanced Computing (2019A08)

合轮子密钥与主密钥的关系，首次给出11轮MIBS-80算法的中间相遇攻击。付立仕等人[9]基于MIBS-80中S盒不可能差分和密钥间的制约关系筛选明文对，并利用独立的80-bit轮密钥来恢复主密钥，对13轮MIBS-80进行了不可能差分分析。文献[10,11]从侧信道的角度，分别对MIBS密码进行故障分析和旁路立方攻击。

中间相遇攻击是一种时空折中的攻击方法，首先由Diffie等人[12]在1977年分析双重DES(TWO-DES)时提出，广泛应用于很多主流分组密码的分析[13–15]。其主要思想是将密码算法分解成两部分，首先建立选择明文经过前半部分加密对应的筛选集合，接着猜测相关的密钥，正向加密和逆向解密明密文对的若干字节和比特，判断是否构成中间数据的碰撞，进而形成有效的攻击。中间相遇攻击需要大量的预计算和时间复杂度，虽然预计算只需要计算1次，但如果涉及的猜测密钥太多，就会超过穷举复杂度。因此如何减少预计算的参数个数，减少需要猜测的密钥量，降低时间复杂度，是亟需解决的问题。

Dunkelman等人 [16]在亚密会(ASIACRYPT) 2010年分析高级加密标准(Advanced Encryption Standard, AES)时，引入多重集并利用有效的差分枚举手段，大大降低了中间相遇攻击预计算阶段涉及的参数数量。此外还发现存储差分筛选集合的有效方法，降低了存储复杂度。总的来说，文献[16]对AES中间相遇攻击的思想具有里程碑式的进步。2013年欧密会，Derbez等人[17]在Dunkelman基础上，借鉴“rebound-like”思想，证明了文献[16]预计算阶段满足截断差分路径的多重集参数不会全部取遍，进而再次降低了区分器涉及的参数，给出了7轮AES-128和8轮AES-192中间相遇攻击的最好结果。随后，文献[18]利用有效的密钥桥和差分枚举技术，给出了对10轮AES-256的中间相遇攻击，是目前为止针对AES-256攻击轮数最长的单密钥攻击。近年来，随着自动化搜索技术的发展，文献[19,20]给出了中间相遇攻击一般化的搜索模型，可以快速有效地给出典型结构分组密码最优中间相遇区分器。

本文主要研究了针对MIBS密码的中间相遇攻击，首先利用MIBS算法Feistel结构的特点，构造了8轮多重集，多重集的相关位置比特由28个半字节决定，超过穷举的计算复杂度。接着通过研究MIBS算法S盒和截断差分的性质，利用有效的枚举技术，剔除中间重复计算的变量，将预计算的参数由28个减少到15个，降低预计算复杂度，构造了8轮中间相遇区分器。最后给出MIBS算法差分传递的性质，结合轮密钥与主密钥的关系，首次实现了13轮MIBS-80算法的中间相遇攻击，需要的数据复杂度为2^{53}个选择明文，时间复杂度为2^{62}次13轮加密运算。此外，利用8轮中间相遇区分器，结合MIBS算法的部分差分传递性质，攻击了12轮MIBS-80算法，所需时间复杂度为$2^{53.2}$次12轮加密运算。表1列出了针对MIBS-80算法单密钥攻击的主要结果。

本文的结构安排如下：第2节简要介绍MIBS密码算法；第3节给出2个定理，构造8轮中间相遇区分器；第4节给出差分传递和密钥扩展算法的相关性质，具体描述13轮MIBS-80密码中间相遇攻击的过程；第5节利用第3节和第4节的部分结果，简要介绍12轮MIBS-80密码中间相遇攻击的结果；第6节总结全文。

2　MIBS密码算法

2.1　MIBS加密算法

分组密码MIBS算法[1]是Feistel结构的密码体制，分组长度为64 bit，支持的密钥长度有64 bit和80 bit两种，加密轮数均为32轮。MIBS中间状态的

表 1　MIBS-80算法单密钥攻击结果比较

攻击方法	攻击轮数	选择明文量	时间复杂度	预计算复杂度	文献
积分攻击	9	$2^{39.6}$	$O(2^{68.4})$	–	文献[5]
积分攻击	10	$2^{61.6}$	$O(2^{40})$	–	文献[6]
积分攻击	10	$2^{28.2}$	$O(2^{53.2})$	–	文献[7]
不可能差分	12	2^{59}	$O(2^{63})$	--	文献[4]
不可能差分	13	$2^{60.1}$	$O(2^{69.5})$	$O(2^{71.2})$	文献[9]
差分分析*	13	2^{62}	$O(2^{25})$	–	文献[2]
中间相遇	9	25	$O(2^{46.28})$	$O(2^{51.06})$	文献[8]
中间相遇	10	$2^{8.7}$	$O(2^{50.2})$	$O(2^{50.96})$	文献[8]
中间相遇	11	$2^{24.9}$	$O(2^{66.25})$	$O(2^{51.03})$	文献[8]
中间相遇	12	2^{53}	$O(2^{53.2})$	$O(2^{63.4})$	本文
中间相遇	13	2^{53}	$O(2^{62})$	$O(2^{63.3})$	本文

注：差分分析攻击成功的概率为99%

操作以4 bit为1个单位，称为半字节。轮函数F函数为SPN型，包括密钥加、S盒变换以及线性P置换。

设64 bit的明文为$L_0||R_0$，加密得到密文$L_{32}||R_{32}$。对于$1 \le i \le 32$，加密过程为$L_i = F(L_{i-1}, K_i) \oplus R_{i-1}$，$R_i = L_{i-1}$，其中$F(L_{i-1}, K_i)$定义如下：

(1) 轮密钥加变换：将每轮左边的输入状态与32 bit的轮密钥K_i相异或，轮子密钥由密钥扩展算法产生，即$X_i = L_{i-1} \oplus K_i$。

(2) 非线性S盒变换：将密钥加后X_i的每1个半字节进行相同的4 bit进4 bit出的S盒操作，即$Y_i = S(X_i) = (S(x_1), S(x_2), S(x_3), S(x_4), S(x_5), S(x_6), S(x_7), S(x_8))$。

(3) 线性P置换：设S盒变换后$Y_i = (y_1, y_2, y_3, y_4, y_5, y_6, y_7, y_8)$，则经过线性P置换后，$Z_i = P(Y_i) = (z_1, z_2, z_3, z_4, z_5, z_6, z_7, z_8)$，其线性关系为

$$\left.\begin{aligned} z_1 &= y_1 \oplus y_2 \oplus y_4 \oplus y_5 \oplus y_7 \oplus y_8,\\ z_2 &= y_2 \oplus y_3 \oplus y_4 \oplus y_5 \oplus y_6 \oplus y_7,\\ z_3 &= y_1 \oplus y_2 \oplus y_3 \oplus y_5 \oplus y_6 \oplus y_8,\\ z_4 &= y_2 \oplus y_3 \oplus y_4 \oplus y_7 \oplus y_8,\\ z_5 &= y_1 \oplus y_3 \oplus y_4 \oplus y_5 \oplus y_8,\\ z_6 &= y_1 \oplus y_2 \oplus y_4 \oplus y_5 \oplus y_6,\\ z_7 &= y_1 \oplus y_2 \oplus y_3 \oplus y_6 \oplus y_7,\\ z_8 &= y_1 \oplus y_3 \oplus y_4 \oplus y_6 \oplus y_7 \oplus y_8 \end{aligned}\right\} \tag{1}$$

其中，P置换是可逆的，其逆变换是P^{-1}，则$Y_i = P^{-1}(Z_i)$，具体地

$$\left.\begin{aligned} y_1 &= z_2 \oplus z_4 \oplus z_6 \oplus z_7 \oplus z_8,\\ y_2 &= z_1 \oplus z_4 \oplus z_5 \oplus z_7 \oplus z_8,\\ y_3 &= z_1 \oplus z_3 \oplus z_4 \oplus z_5 \oplus z_6,\\ y_4 &= z_2 \oplus z_3 \oplus z_5 \oplus z_6 \oplus z_7,\\ y_5 &= z_2 \oplus z_3 \oplus z_4 \oplus z_5 \oplus z_7 \oplus z_8,\\ y_6 &= z_1 \oplus z_2 \oplus z_4 \oplus z_5 \oplus z_6 \oplus z_8,\\ y_7 &= z_1 \oplus z_3 \oplus z_5 \oplus z_6 \oplus z_7 \oplus z_8,\\ y_8 &= z_1 \oplus z_2 \oplus z_3 \oplus z_4 \oplus z_6 \oplus z_7 \end{aligned}\right\} \tag{2}$$

2.2 MIBS-80算法的密钥生成算法

设80 bit的主密钥$K = (k_{79}, k_{78}, \cdots, k_0)$，$\text{state}^0$是初始密钥$K$，$\text{state}^i$表示第$i$轮的密钥扩展状态，$\text{state}^i[a \sim b]$表示$\text{state}^i$从高比特$a$到低比特$b$的$a-b+1$ bit。则由主密钥生成32个32 bit的轮子密钥$K_i (1 \le i \le 32)$的具体过程为

$$\left.\begin{aligned} &\text{state}^i \leftarrow \text{state}^{i-1} >>> 19;\\ &\text{state}^i \leftarrow S(\text{state}^i[79 \sim 76])||\\ &S(\text{state}^i[75 \sim 72])||\text{state}^i[71 \sim 0];\\ &\text{state}^i \leftarrow \text{state}^i[79 \sim 19]\\ &||(\text{state}^i[18 \sim 14] \oplus \text{Round-Counter})||\text{state}^i[13 \sim 0];\\ &K_i \leftarrow \text{state}^i[79 \sim 48] \end{aligned}\right\} \tag{3}$$

其中，$>>> 19$表示循环右移19位，S盒与加密算法所用的相同，Round - Counter表示轮数。

3 MIBS密码算法8轮中间相遇区分器

本文符号及标注(如图1)：M表示明文；C表示密文；K表示主密钥；$K[j]$表示主密钥的第j比特；K_i表示第i轮的轮子密钥；$K_i[j]$表示第i轮子密钥的第j个半字节；A_{i-1}表示Feistel结构左侧第i轮32 bit的输入；B_{i-1}表示Feistel结构右侧第i轮32 bit的输入；$A_i||B_i$表示A_i与B_i的级联；X_i表示第i轮输入A_{i-1}经过轮函数密钥加的值；Y_i表示第i轮X_i经过S盒变换的值；Z_i表示第i轮Y_i经过线性P置换的值；$X_i[j]$, $Y_i[j]$, $Z_i[j]$分别表示X_i, Y_i, Z_i的第j个半字节；A_i^j表示输入状态A_i的8个半字节中某个活动半字节取遍，其得到16个状态值的第$j (0 \le j \le 15)$个取值；B_i^j表示的含义与A_i^j类似；ΔA_i^j, ΔB_i^j分别表示状态差分值$A_i^j \oplus A_i^0$和$B_i^j \oplus B_i^0$。

本节首先针对MIBS中间状态的半字节运算，给出MIBS算法δ-集的定义，再按照其Feistel结构特点构造多重集得到定理1，其相关位置比特由28个半字节决定，超过了穷举的计算复杂度。接着研究MIBS算法S盒的性质，利用有效的差分枚举技术得出定理2，构造了有效的8轮中间相遇区分器。

定义 MIBS算法的δ-集是指中间状态A_m的1个活动半字节遍历2^4个所有可能值，其他半字节取固定值得到的一个集合，表示为$\delta = \{A_m^0, A_m^1, \cdots, A_m^{15}\}$，其中$A_m^i (0 \le i \le 15)$是第$m+1$轮进入轮函数变化前的状态值。

由定义的δ-集，利用MIBS算法Feistel结构的特点，给出MIBS密码算法8轮多重集，得到以下定理。

定理1 如果δ-集的活动字节定义为左半部分输

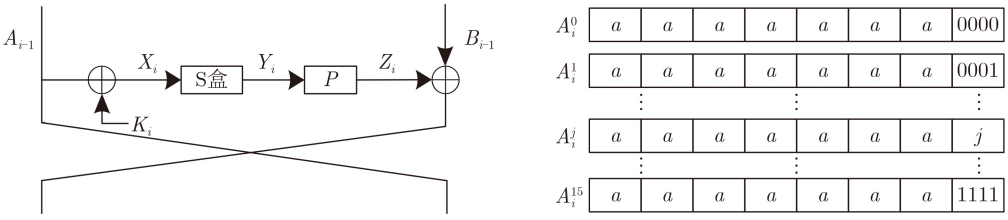

图 1 第i轮符号说明示意图

入A_m的第8个半字节$A_m[8]$，用8轮MIBS算法加密δ集，则多重集序列$\{A^0_{m+6}\oplus A^0_{m+6}, A^1_{m+6}\oplus A^0_{m+6},\cdots, A^{15}_{m+6}\oplus A^0_{m+6}\}$的相关比特$(P^{-1}(\Delta A_{m+6}))[5]$完全由$X_{m+1}[8]$, $X_{m+2}[1,3,4,5,8]$, X_{m+3}, X_{m+4}, X_{m+5} $[1,3,4,5,8]$, $X_{m+6}[5]$这28个半字节变量决定。

证明　由于定义的δ-集的活动半字节为$A_m[8]$，遍历2^4个所有状态，则差分集合$\{\Delta A^0_m, \Delta A^1_m,\cdots,\Delta A^{15}_m\}$也遍历16个无序的状态，经过密钥异或得到$\{\Delta X^0_{m+1}, \Delta X^1_{m+1},\cdots,\Delta X^{15}_{m+1}\}$。对于差分集合的元素$\Delta X_{m+1}[8]$和已知的参数取值$X_{m+1}[8]$，经过S盒变换后得到差分值$\Delta Y_{m+1}[8]=S(X_{m+1}[8])\oplus S(\Delta X_{m+1}[8]\oplus X_{m+1}[8])$，再经过P置换后活动字节扩散到第1,3,4,5,8字节，由Feistel结构的特点，再异或ΔA_{m-1}后得到$\Delta X_{m+2}[1,3,4,5,8]$ 。由于$X_{m+2}[1,3,4,5,8]$的这5个半字节作为参数的一部分给出，则经过S盒后可以得到$\Delta Y_{m+2}[1,3,4,5,8]$的值，经过P置换异或$\Delta A_m$后得到$\Delta X_{m+3}$。同上推导，由于$X_{m+3}$和$X_{m+4}$的值也作为参数的一部分给出，则可得到$\Delta Y_{m+4}$。$\Delta Y_{m+4}$经过P置换并异或$\Delta A_{m+2}$后得到$\Delta A_{m+4}$，经过密钥加得到$\Delta X_{m+5}$。由于$X_{m+5}[1,3,4,5,8]$已知，经过S盒得到$\Delta Y_{m+5}[1,3,4,5,8]$，再根据P置换线性关系

$$\begin{aligned}\Delta Z_{m+5}[5]=&\Delta Y_{m+5}[1]\oplus\Delta Y_{m+5}[3]\oplus\Delta Y_{m+5}[4]\\&\oplus\Delta Y_{m+5}[5]\oplus\Delta Y_{m+5}[8]\end{aligned}\tag{4}$$

可以得到$\Delta Z_{m+5}[5]$的值，异或$\Delta A_{m+3}[5]$得到$\Delta X_{m+6}[5]$；而$X_{m+6}[5]$作为参数给出，则可以得到$\Delta Y_{m+6}[5]$。由MIBS结构特点可知

$$\begin{aligned}(P^{-1}(\Delta A_{m+6}))[5]&=(P^{-1}(\Delta A_{m+4}\oplus\Delta Z_{m+6}))[5]\\&=(P^{-1}(\Delta A_{m+4}))[5]\oplus\Delta Y_{m+6}[5]\end{aligned}\tag{5}$$

所以利用得到的$\Delta Y_{m+6}[5]$和ΔA_{m+4}，可以计算出$(P^{-1}(\Delta A_{m+6}))[5]$。即$(P^{-1}(\Delta A_{m+6}))[5]$由上述28个半字节变量决定。　　证毕

基于MIBS密码结构特点构造的8轮多重集，相关位置比特涉及的参数较多，超过穷举复杂度，不能实现有效的攻击。为了精简参数个数，分析MIBS轮函数的S盒，可得性质1。

性质1　(S盒的性质)对于MIBS算法$F_2^4\to F_2^4$的S盒置换：$(4,15,3,8,13,10,12,0,11,5,7,14,2,6,1,9)$，给定大量S盒的非0输入差分$\Delta_i$和输出差分$\Delta_0$，等式

$$S(x)+S(x+\Delta_i)=\Delta_0\tag{6}$$

平均有一个解。

证明　设式(6)解的个数为$N(\Delta_i,\Delta_0)$，对于所有可能的2^4-1个非0输入差分Δ_i以及给定的输出差分Δ_0，有2^3个输入输出差分使得式(6)解个数$N(\Delta_i,\Delta_0)=0$，有2^3-2个输入输出差分使得式(6)解个数$N(\Delta_i,\Delta_0)=2$，有1个输入输出差分使得式(6)解个数$N(\Delta_i,\Delta_0)=4$。因此总的解个数$\sum_{(\Delta_i,\Delta_0)}N(\Delta_i,\Delta_0)=2^3\times0+(2^3-2)\times2+4\times1=2^4$。所以，式(6)解个数的平均值为$\dfrac{2^4}{2^4-1}\approx1$，即平均有一个解。　　证毕

在图2中MIBS算法8轮截断差分路径的基础上，结合“rebound-like”的思想，利用性质1，通过有效的枚举技术，剔除定理1中间重复计算的参数，构造MIBS算法8轮中间相遇区分器，得到定理2。定理2区分器参数减少到15个半字节，有效降低了预计算复杂度。

定理2　(8轮中间相遇区分器)对定理1中定义的δ-集进行8轮MIBS算法加密，如果δ-集的元素满足图2中的截断差分路径，则多重集序列的相关比特$P^{-1}(\Delta A_{m+6}))[5]$仅由$\Delta X_{m+1}[8]$, $\Delta Y_{m+1}[8]$, $\Delta Y_{m+2}[1,3,4,5,8]$, $\Delta Y_{m+5}[1,3,4,5,8]$, $\Delta X_{m+6}[8]$, $\Delta Y_{m+6}[8]$, $X_{m+6}[5]$这15个半字节变量决定，即$(P^{-1}(\Delta A_{m+6}))[5]$只能取$2^{60}$种可能值。

证明　需证明，由给出$\Delta X_{m+1}[8], \Delta Y_{m+1}[8]$, $\Delta Y_{m+2}[1,3,4,5,8]$, $\Delta Y_{m+5}[1,3,4,5,8]$, $\Delta X_{m+6}[8]$, $\Delta Y_{m+6}[8]$, $X_{m+6}[5]$这15个半字节可以求出定理1中决定$(P^{-1}(\Delta A_{m+6}))[5]$的28个变量。

若δ-集的元素满足图2中的截断差分路径，按照活动字节的传递，由给出的S盒的输入差分$\Delta X_{m+1}[8]$和输出差分$\Delta Y_{m+1}[8]$，利用性质1，可得到一个$X_{m+1}[8]$的值。又由$\Delta Y_{m+1}[8]$的值，经过P置换再异或$\Delta A_{m-1}=(00000000)$得到$\Delta X_{m+2}[1,3,4,5,8]$的值，已知S盒输入差分$\Delta X_{m+2}[1,3,4,5,8]$和输出差分$\Delta Y_{m+2}[1,3,4,5,8]$，可得到一个$X_{m+2}[1,3,4,5,8]$的值。

为了推导X_{m+3}的值，一方面，由$\Delta Y_{m+2}[1,3,4,5,8]$可得$\Delta X_{m+3}$的值；另一方面，由MIBS算法结构可知，从加密和解密方向成立

$$\begin{aligned}\Delta Y_{m+3}&=P^{-1}(\Delta Z_{m+3})=P^{-1}(\Delta A_{m+1}\oplus\Delta A_{m+3})\\&=P^{-1}(\Delta X_{m+2}\oplus(\Delta Z_{m+5}\oplus\Delta A_{m+5}))\end{aligned}\tag{7}$$

其中，ΔZ_{m+5}由$\Delta Y_{m+5}[1,3,4,5,8]$经过P置换得到，$\Delta A_{m+5}$由$\Delta X_{m+6}[8]$得到。现已知S盒输入差分$\Delta X_{m+3}$和输出差分$\Delta Y_{m+3}$，可得$X_{m+3}$的值。

用类似方法可得X_{m+4}，由于$\Delta X_{m+4}=\Delta B_{m+4}=P(\Delta Y_{m+5})\oplus\Delta A_{m+5}$，则$\Delta Y_{m+5}[1,3,4,5,8]$经过P置换再异或$\Delta A_{m+5}$得到$\Delta X_{m+4}$。此外，对于$\Delta Y_{m+4}$成立

$$\begin{aligned}\Delta Y_{m+4}=&P^{-1}(\Delta Z_{m+4})=P^{-1}(\Delta A_{m+2}\oplus\Delta A_{m+4})\\=&P^{-1}((\Delta Z_{m+2}\oplus\Delta X_{m+1})\\&\oplus(\Delta Z_{m+6}\oplus(00000000)))\end{aligned}\tag{8}$$

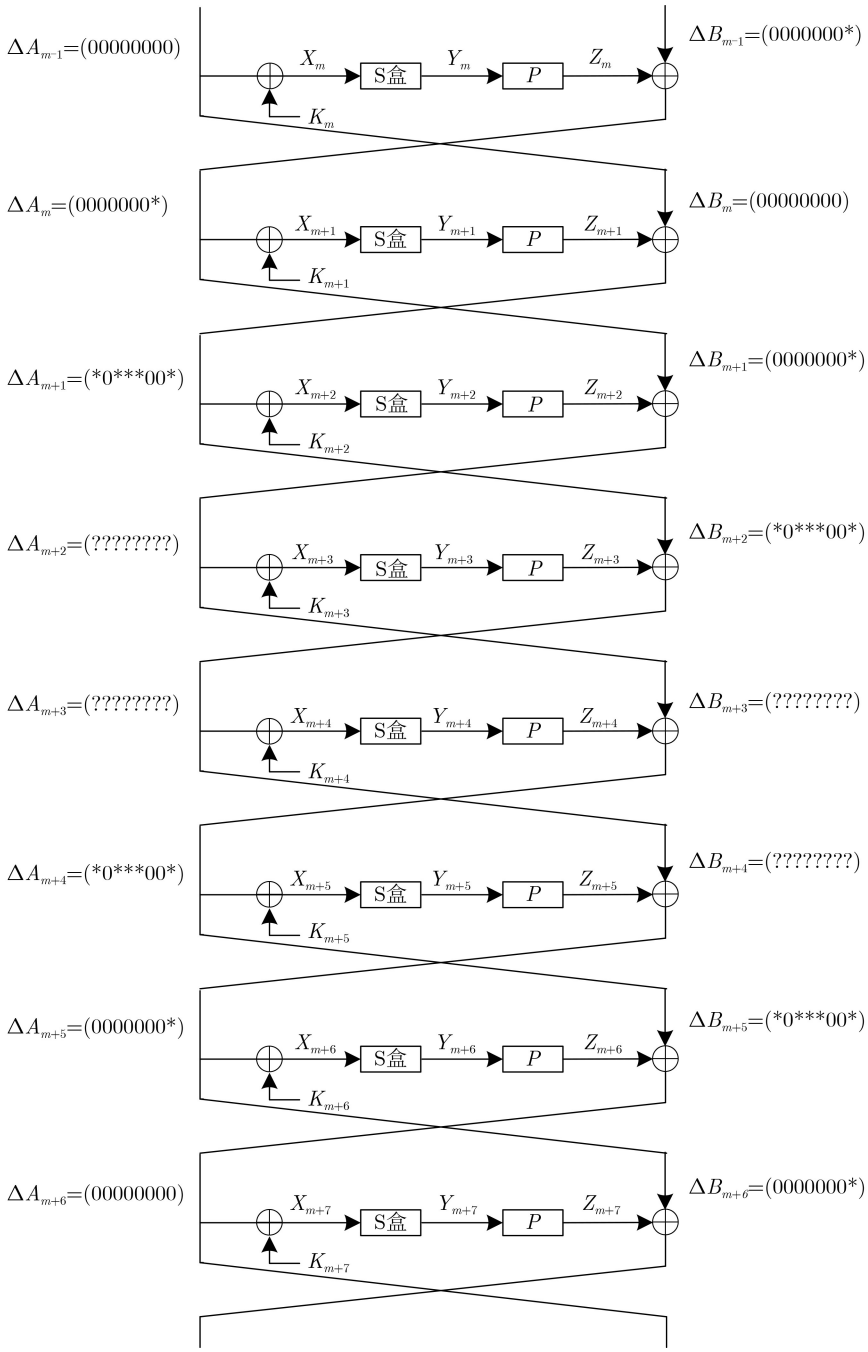

图 2 8轮MIBS算法的截断差分路径

其中，ΔZ_{m+2}由$\Delta Y_{m+2}[1,3,4,5,8]$经过P置换得到，而$\Delta Z_{m+6}$由$\Delta Y_{m+6}[8]$经过P置换得到。现在知道S盒输入差分$\Delta X_{m+4}$和输出差分$\Delta Y_{m+4}$，可得$X_{m+4}$的值。

此外，由$\Delta Y_{m+6}[5]$经过P置换得到$\Delta Z_{m+6}[1,3,4,5,8]$，再异或$\Delta A_{m+6}=(00000000)$得到$\Delta X_{m+5}[1,3,4,5,8]$。由$\Delta Y_{m+5}[1,3,4,5,8]$和$\Delta X_{m+5}[1,3,4,5,8]$，利用性质1可得$X_{m+5}[1,3,4,5,8]$，而$X_{m+6}[5]$的值作为参数值给出。所以决定定理1中$(P^{-1}(\Delta A_{m+6}))[5]$的28个半字节可以由定理2中这15个半字节求出。 证毕

4 13轮MIBS-80密码算法的中间相遇攻击

本节利用第3节构造的8轮中间相遇区分器，前面加2轮，后面加3轮，构成13轮的攻击路径，如图3所示。为了减少复杂度，首先利用MIBS算法的差分传递特征，分别从加密方向和解密方向给出性质2和性质3，筛选满足截断差分的明文；接着利用MIBS-80密钥扩展算法中轮密钥与主密钥的关系，减少密钥的猜测量。

性质2 对MIBS算法，若第$i+1$轮输入差分$\Delta A_i=(0000000\gamma)$, $\Delta B_i=(00000000)$，则第$i+3$轮

的输出差分满足关系式

$$P^{-1}(\Delta B_{i+3})[2]=\gamma \tag{9}$$

$$P^{-1}(\Delta B_{i+3})[j]=\Delta Y_{i+2}[j],\ \ j=3,4,8 \tag{10}$$

$$P^{-1}(\Delta B_{i+3})[j]=\Delta Y_{i+2}[j]\oplus P^{-1}(\Delta B_{i+3})[2],\ \ j=1,5,6,7 \tag{11}$$

证明　当$\gamma=0$时，结论显然；当$\gamma\neq 0$时，由$\Delta A_i=(0000000\gamma)$经过S盒推出$\Delta Y_{i+1}=(0000000\gamma')$，再经过P置换异或$\Delta B_i=(00000000)$得到$\Delta A_{i+1}=(e0eee00e)$，接着经过S盒后得到$\Delta Y_{i+2}[2]=0$。又因为$P^{-1}(\Delta A_i)=(\gamma\gamma00\gamma\gamma\gamma0)$，则$P^{-1}(\Delta A_i)[2]=\gamma$。所以$P^{-1}(\Delta B_{i+3})[2]=P^{-1}(\Delta A_{i+2})[2]=\Delta Y_{i+2}[2]\oplus P^{-1}(\Delta A_i)[2]=\gamma$。

此外，根据Feistel的结构特点可知

$$\begin{aligned}\Delta Y_{i+2}=&P^{-1}(\Delta A_i\oplus\Delta A_{i+2})=P^{-1}(\Delta A_i)\\&\oplus P^{-1}(\Delta B_{i+3})\\=&(\gamma\gamma00\gamma\gamma\gamma0)\oplus P^{-1}(\Delta B_{i+3})\end{aligned} \tag{12}$$

所以成立

$$\begin{aligned}&P^{-1}(\Delta B_{i+3})[j]=\Delta Y_{i+2}[j],\ \ j=3,4,8\\&P^{-1}(\Delta B_{i+3})[j]=\Delta Y_{i+2}[j]\oplus\gamma,\ \ j=1,2,5,6,7\end{aligned} \tag{13}$$

进一步，$P^{-1}(\Delta B_{i+3})[j]=\Delta Y_{i+2}[j]\oplus\gamma=\Delta Y_{i+2}[j]\oplus P^{-1}(\Delta B_{i+3})[2]$，$j=1,2,5,6,7$，所以式(9)—式(11)成立。　证毕

性质3　若MIBS算法第$i+2$轮的输出差分$\Delta A_{i+2}=(00000000)$，$\Delta B_{i+2}=(0000000\alpha)$，则第$i+1$轮的输入差分满足关系式

$$P^{-1}(\Delta B_i)[2]=\alpha; \tag{14}$$

$$P^{-1}(\Delta B_i)[j]=\Delta Y_{i+1}[j],\ \ j=3,4,8; \tag{15}$$

$$P^{-1}(\Delta B_i)[j]=\Delta Y_{i+1}[j]\oplus P^{-1}(\Delta B_i)[2],\ \ j=1,5,6,7 \tag{16}$$

证明　与性质2证明类似。因为$P^{-1}(\Delta B_i)=P^{-1}(\Delta A_{i+1})\oplus\Delta Y_{i+1}=(\alpha\alpha00\alpha\alpha0)\oplus\Delta Y_{i+1}$，且$P^{-1}(\Delta B_i)[2]=P^{-1}(\Delta A_{i+1})[2]\oplus\Delta Y_{i+1}[2]=\alpha$，所以式(14)—式(16)成立。　证毕

性质4　(密钥扩展算法的性质)[7]对于MIBS-80，如果需要猜测轮子密钥$K_i[j]$，则只需猜测主密钥$K[\alpha\sim\alpha-3]$，其中$\alpha=(4j+47+19i)\ \bmod 80$。当$\alpha=0,1,2$时，$K[\alpha\sim\alpha-3]$取值为$K[\alpha]$, $K[(\alpha-1)\bmod 80]$, $K[(\alpha-2)\bmod 80]$, $K[(\alpha-3)\bmod 80]$这4 bit。

为了实现13轮MIBS-80的中间相遇攻击，在8轮中间相遇区分器的基础上，前加2轮，后加3轮构成13轮的攻击路径，如图3所示。此时，定理2中$m=3$，即$(P^{-1}(\Delta A_9))[5]$的值由$\Delta X_4[8]$, $\Delta Y_4[8]$, $\Delta Y_5[1,3,4,5,8]$, $\Delta Y_8[1,3,4,5,8]$, $\Delta X_9[8]$, $\Delta Y_9[8]$, $X_9[5]$这15个半字节变量决定，具体攻击步骤分为预计算和在线阶段。

4.1　预计算阶段

穷举定理2构造的中间相遇区分器的15个半字节2^{60}个参数值，建立与8轮多重集相关位置比特$(P^{-1}(\Delta A_9))[5]$的映射关系，并以$(P^{-1}(\Delta A_9))[5]$的取值为索引存储到哈希表中。具体步骤与定理1和定理2的证明类似。

(1) 对于60 bit的$\Delta X_4[8]$, $\Delta Y_4[8]$, $\Delta Y_5[1,3,4,5,8]$, $\Delta Y_8[1,3,4,5,8]$, $\Delta X_9[8]$, $\Delta Y_9[8]$, $X_9[5]$值，利用截断差分和S盒的性质，根据定理2的证明过程计算出$X_4[8]$, $X_5[1,3,4,5,8]$, X_6, X_7, $X_8[1,3,4,5,8]$, $X_9[5]$的值。

(2) 根据定理1的证明，对于其他不同的15个$\Delta^t X_4[8](1\le t\le 15)$的值，利用上述求出的28个半字节参数值，求出$(P^{-1}(\Delta A_9))[5]$的所有可能值。

(3) 在Hash表T中存储2^{60}个$(P^{-1}(\Delta A_9))[5]$的值。

4.2　在线阶段

首先加密选择的明文，筛选满足截断差分路径的明文对，接着利用筛选出的明文对构造对应的δ-集，部分解密δ-集得到其他明文集，并加密明文集得到对应的密文集，最后猜测涉及的轮子密钥进行部分解密求出$(P^{-1}(\Delta A_9))[5]$的值，如果所求得的值在预计算生成的哈希表T中，则猜测的密钥极有可能是正确密钥。具体步骤如下：

步骤1　按照图3选择明文的形式，定义明文空间$M=(A_0||B_0)$，具体地，$A_0=(a||x_1||a+x_2||a+x_3||a+x_4||x_5||x_6||a+x_7)$，其中$x_i(1\le i\le 7)$为常值，$a$取遍所有的值，满足差分在1,3,4,5,8是活动半字节；$B_0=P(b_1||b_2||b_3||b_4||b_5||b_2||b_2||b_6)$，其中$b_i(1\le i\le 6)$取遍所有的值，满足8个差分活动字节的位置且第2与第6, 7半字节的值相同。则明文结构M有$2^{4\times 7}=2^{28}$种可能的取值，约有$2^{28}\times(2^{28}-1)/2\approx 2^{55}$对明文差分。用13轮MIBS加密$2^{21}$种明文结构$M$得到对应的密文结构$C=(A_{13}||B_{13})$，一共有$2^{21}\times 2^{55}=2^{76}$个选择明文对。

步骤2　对于每一个明文对$(A_0||B_0,A_0'||B_0')$和对应的密文对$(A_{13}||B_{13},A_{13}'||B_{13}')$，利用图3路径中密文的形式和性质2与性质3筛选满足截断差分路径的明文对。

(1) 从解密方向来看，由于$\Delta Y_{13}=P^{-1}(\Delta A_{11})\oplus P^{-1}(\Delta A_{13})=(0000000e)\oplus P^{-1}(\Delta A_{13})$，则$\Delta Y_{13}[l]=P^{-1}(\Delta A_{13})[l]$, $l=1,2,3,4,5,6,7$。分别猜测密钥$K_{13}[l]$, $l=1,2,3,4,5,6,7$的值，解密$B_{13}[l]$和$B_{13}'[l]$

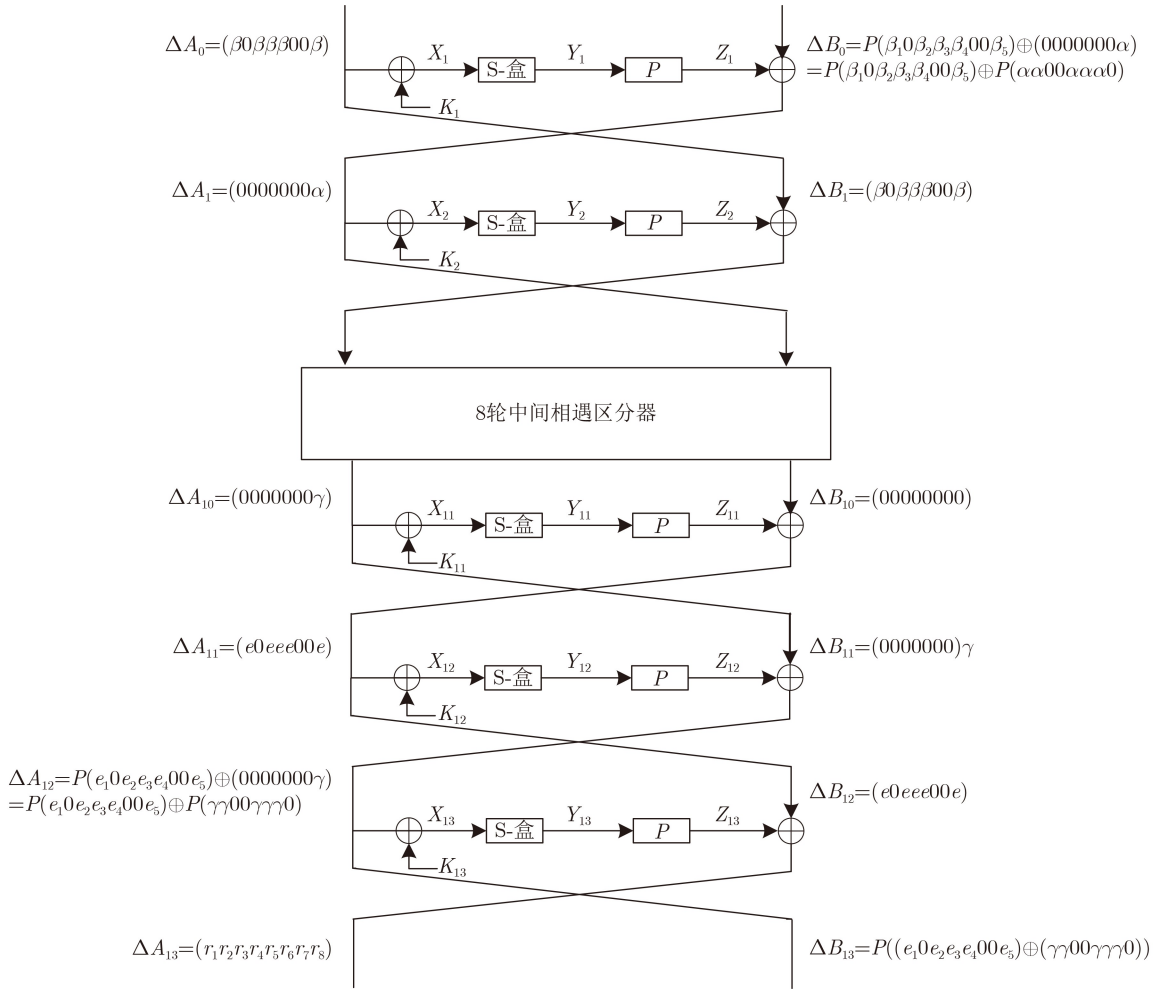

图 3 13轮MIBS-80密码的中间相遇攻击路径

得到$Y_{13}[l]$和$Y'_{13}[l]$，保留满足$\Delta Y_{13}[l]=P^{-1}(\Delta A_{13})[l]$的明文对，则剩余$2^{76}\times 2^{-7\times 4}=2^{48}$个明文对。再猜测密钥$K_{13}[8]$，进而得到$A_{11}$和$A'_{11}$的值。

(2) 猜测$K_{12}[l]$, $l=1,3,4,5,8$，由A_{11}和A'_{11}的值计算中间状态值$Y_{12}[l]$和$Y'_{12}[l]$, $l=1,3,4,5,8$。根据性质2(此时$i=10$)，筛选满足$\Delta Y_{12}[j]=P^{-1}(\Delta B_{13})[j]\oplus P^{-1}(\Delta B_{13})[2]$, $j=1,5$和$\Delta Y_{12}[j]=P^{-1}(\Delta B_{13})[j]$, $j=3,4,8$对应明文对。则剩余明文对的数量为$2^{48}\times 2^{-5\times 4}=2^{28}$个。

(3) 猜测$K_1[l]$, $l=1,3,4,5,8$，由A_0和A'_0的值计算中间状态值$Y_1[l]$和$Y_1{}'[l]$。利用性质3(此时$i=0$)，筛选满足$\Delta Y_1[j]=P^{-1}(\Delta B_0)[j]\oplus P^{-1}(\Delta B_0)[2]$, $j=1,5$和$\Delta Y_1[j]=P^{-1}(\Delta B_0)[j]$，$j=3,4,8$的明文对，此时剩余明文对的数量为$2^{28}\times 2^{-5\times 4}=2^8$。对于剩余的明文对，图2截断差分路径成立的概率为$2^{-8}$，则只有一对明文满足图2截断差分路径。

步骤3 利用步骤2筛选出的满足截断差分路径的明文对构造相应的δ-集，猜测密钥$K_1[l]$, $l=1,3,4,5,6,7,8$和$K_2[8]$解密δ-集得到其他明文集。具体地：

(1) 选择满足截断差分路径的明文对$(A_0||B_0)$，猜测$K_1[l]$, $l=1,3,4,6,7,8$部分加密A_0得到$Y_1[l]$, $l=1,3,4,6,7,8$，再经过P置换得到

$$Z_1[8]=Y_1[1]\oplus Y_1[3]\oplus Y_1[4]\oplus Y_1[6]\oplus Y_1[7]\oplus Y_1[8] \quad (17)$$

再异或$B_0[8]$得到$A_1[8]$，猜测密钥$K_2[8]$得到$X_2[8]$值。

(2) 改变$X_2[8]$的值，不妨令$X'_2[8]=X_2[8]\oplus\alpha$, $\alpha\in[1,15]$，该活动半字节遍历2^4个所有可能值，满足定义的δ-集。计算$\Delta Y_2[8]=S(X_2[8])\oplus S(X'_2[8])$，再经过P置换得到$\Delta Z_2[1,3,4,5,8]$，异或(00000000)后得到$\Delta A_0[1,3,4,5,8]$的值，则其他明文的左半部分的值为$A'_0=A_0\oplus\Delta A_0$。

(3) 在(1)猜测密钥$K_1[l]$, $l=1,3,4,6,7,8$的基础上继续猜测$K_1[5]$，部分加密A_0和A'_0，经过S盒计算出$\Delta Y_1[1,3,4,5,8]$，经过P置换再异或$\Delta A_1=\Delta X_2=(0000000\alpha)$得到$\Delta B_0$的值，则可以得到与$A'_0$对应的明文的右半部分值$B'_0=B_0\oplus\Delta B_0$。

(4) 根据不同的α值，计算δ-集对应的所有明文集，加密得到相应的密文集。

步骤4　猜测相关密钥，解密步骤3得到密文集，计算所有的$(P^{-1}(\Delta A_9))[5]$的值，判断是否落在预计算Hash表T中。

(1) 对于步骤3得到明文对$(A_0||B_0, A'_0||B'_0)$和对应的密文对$(A_{13}||B_{13}, A'_{13}||B'_{13})$，猜测密钥$K_{13}$得出中间状态值$\Delta Y_{13}[5]$，进而得到$P^{-1}(\Delta A_{11})[5] = \Delta Y_{13}[5] \oplus P^{-1}(\Delta A_{13})[5]$。

(2) 猜测密钥$K_{12}[1,3,4,5,8]$得出$Y_{12}[1,3,4,5,8]$和$Y'_{12}[1,3,4,5,8]$的值，再根据P置换的线性关系，计算$A_{10}[5] = P(Y_{12})[5] \oplus B_{13}[5] = Y_{12}[1] \oplus Y_{12}[3] \oplus Y_{12}[4] \oplus Y_{12}[5] \oplus Y_{12}[8] \oplus B_{13}[5]$和$A'_{10}[5]$的值。继续猜测密钥$K_{11}[5]$，求出$X_{11}[5]$和$X'_{11}[5]$的值，经过S盒得到$Y_{11}[5]$和$Y'_{11}[5]$，进而得到差分值$\Delta Y_{11}[5]$。

(3) 由于$(P^{-1}(\Delta A_9))[5] = (P^{-1}(\Delta B_{10}))[5] = \Delta Y_{11}[5] \oplus P^{-1}(\Delta A_{11})[5]$，利用(1)和(2)计算出来的值可以求出$(P^{-1}(\Delta A_9))[5]$。判断计算出来的值是否与预计算哈希表$T$发生碰撞，如果碰撞成功就恢复出相关子密钥。

由于定义的多重集序列$\{A_9^0 \oplus A_9^0, A_9^1 \oplus A_9^0, \cdots, A_9^{15} \oplus A_9^0\}$一共有$2^{16\times 4} = 2^{64}$种取值。则一个错误密钥匹配成功的概率为$2^{60} \times 2^{-64} = 2^{-4}$。而在恢复密钥时，需要猜测$K_1[1,3,4,5,6,7,8]$, $K_2[8]$, $K_{11}[5]$, $K_{12}[1,3,4,5,8]$, K_{13}这22个半字节的密钥。利用性质4，猜测$K_1[1,3,4,5,6,7,8]$需要猜测主密钥$K[18 \sim 0]$, $K[70 \sim 67]$和$K[79 \sim 75]$；猜测$K_2[8]$需要猜测主密钥$K[37 \sim 34]$；猜测$K_{11}[5]$需要猜测主密钥$K[36 \sim 33]$；猜测$K_{12}[1,3,4,5,8]$需要猜测主密钥$K[39 \sim 36]$, $K[55 \sim 44]$和$K[67 \sim 64]$；猜测K_{13}需要猜测主密钥$K[6 \sim 0]$和$K[79 \sim 55]$。综上，在攻击过程中需要猜测主密钥$K[18 \sim 0]$, $K[39 \sim 33]$, $K[79 \sim 44]$的值，对应地，只需要猜测密钥K_{13}的全部32 bit，$K_{12}[1,3,4]$的12 bit和$K_{12}[5]$的3 bit，$K_{11}[5]$的3 bit以及$K_1[6,7,8]$的12 bit，一共62 bit的密钥。在经过一组明密文淘汰后，剩余错误密钥的数目为$(2^{62}-1) \times 2^{-4} \approx 2^{58}$，则需要16组明文可以唯一确定正确密钥。

4.3 复杂度分析

预计算阶段，构造Hash表T需要的预计算复杂度为$2^{60} \times 2^4 \times \frac{8}{13} \approx 2^{63.3}$次13轮加密运算，表$T$包含$2^{60}$个序列，每个序列占有64 bit的空间，所以需要$2^{60}$个64 bit分组长度的存储。

在线阶段，步骤1需要加密$2^{21+28} = 2^{49}$个选择明文，为了唯一确定正确密钥，还需要增加选择明文量，所以一共需要$2^{49} \times 16 = 2^{53}$个选择明文。对于时间复杂度，首先需要加密$2^{53}$个选择明文，需要$2^{53}$次13轮MIBS-80加密；然后在恢复密钥时，时间复杂度集中在构造δ集得到明密文对和猜测密钥解密密文计算$(P^{-1}(\Delta A_9))[5]$的过程，一共需要62 bit的密钥，则恢复密钥的时间复杂度约为$2^{62} \times 2^4 \times 2^{-3} \times 2^{-1} = 2^{62}$次13轮加密运算。因此，总的时间复杂度约为$2^{62} + 2^{53} \approx 2^{62}$次13轮MIBS-80加密运算。

综上所述，13轮MIBS-80中间相遇攻击的数据复杂度为2^{53}个选择明文，预计算复杂度为$2^{63.3}$次13轮加密运算，时间复杂度为2^{62}次13轮MIBS-80加密运算，存储复杂度为2^{60}个分组长度的存储。

5　12轮MIBS-80密码算法的中间相遇攻击

本节在第3节定理2的8轮中间相遇区分器基础上，前面加1轮，后面加3轮，进行12轮MIBS-80算法的中间相遇攻击，攻击路径去掉图3中13轮路径的第1轮。与第4节13轮的攻击过程相比，其明文的差分特征不再满足性质3，密文的差分特征依然满足性质2。

根据12轮MIBS-80算法的攻击路径，重新定义选择明文空间$M' = (A'_1||B'_1)$。具体地，$A'_1 = (x||x||x||x||x||x||x||a)$，$B'_1 = (b||y_1||b+y_2||b+y_3||b+y_4||y_5||y_6||b+y_7)$，其中$x$, $y_i (1 \le i \le 7)$为常值，a , b取遍所有的值，满足明文活动字节的状态。攻击过程中预计算阶段与13轮类似，在线阶段筛选满足截断差分路径的明文对时，不再考虑筛选满足性质3的明文对。

计算12轮MIBS-80算法中间相遇攻击的复杂度时，由于预计算阶段具体步骤不变，则需要的预计算复杂度为$2^{60} \times 2^4 \times \frac{8}{12} \approx 2^{63.4}$次12轮加密运算，存储复杂度为$2^{60}$个分组长度的存储。在选择明文时，定义的明文空间$M'$有$2^8$种可能的取值，需要选择$2^{41}$个明文结构，可以保证有1对明文满足截断差分路径，还需要16组明文保证能唯一确定正确密钥。所以一共需要选择$2^{41+8+4} = 2^{53}$的明文量。对于时间复杂度，与13轮的攻击相比，需要猜测密钥减少了$K_1[1,3,4,5,6,7,8]$。根据性质4，一共需要猜测50 bit的密钥。所以恢复密钥的时间复杂度约为$2^{50} \times 2^4 \times 2^{-3} \times 2^{-1} = 2^{50}$，总的时间复杂度约为$2^{50} + 2^{53} \approx 2^{53.2}$次12轮MIBS-80加密运算。

6　结束语

本文评估了适用于物联网的密码MIBS算法抵抗中间相遇攻击的安全性。与其他针对Feistel结构的密码分析工作相比，本文充分利用MIBS算法的结构特点，构造8轮多重集。进一步，利用MIBS算法S盒的性质和有效的差分枚举技术，减少了8轮中间相遇区分器的参数，从而首次实现了对12轮和

13轮MIBS-80密码的中间相遇攻击。攻击过程利用差分传递的性质筛选明文对，利用轮密钥与主密钥的关系，减少了密钥猜测量，降低了时间复杂度。该攻击方法明显优于文献[8]中间相遇攻击的结果。与其他攻击方法相比，在时间复杂度和选择明文量上也有整体优势。本文的攻击思想同样适用于其他Feistel-SP结构的典型密码算法的分析，如 Camellia, E2算法等。如何结合自动化搜索算法构造较长轮数的区分器，并加大密钥筛选的力度将是下一步值得研究的工作。

参 考 文 献

[1] IZADI M, SADEGHIYAN B, SADEGHIAN S S, *et al*. MIBS: A new lightweight block cipher[C]. The 8th International Conference on Cryptology and Network Security, Kanazawa, Japan, 2009: 334–348.

[2] 杨林, 王美琴. 约减轮的MIBS算法的差分分析[J]. 山东大学学报:理学版, 2010, 45(4): 12–15,20.
YANG Lin and WANG Meiqin. Differential cryptanalysis of reduced-round MIBS[J]. *Journal of Shandong University:Natural Science*, 2010, 45(4): 12–15,20.

[3] BAY A, NAKAHARA JR J, and VAUDENAY S. Cryptanalysis of reduced-round MIBS block cipher[C]. The 9th International Conference on Cryptology and Network Security, Kuala Lumpur, Malaysia, 2010: 1–19.

[4] 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): 55–58,69.
DU Chenghang and CHEN Jiazhe. Impossible differential cryptanalysis of reduced-round MIBS[J]. *Journal of Shandong University:Natural Science*, 2012, 47(7): 55–58,69.

[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. doi: 10.3969/j.issn.1000-1220.2012.04.020.
WANG Gaoli and WANG Shaohui. Integral cryptanalysis of reduced-round MIBS block ciphe[J]. *Journal of Chinese Computer Systems*, 2012, 33(4): 773–777. doi: 10.3969/j.issn.1000-1220.2012.04.020.

[6] 于晓丽, 吴文玲, 李艳俊. 低轮MIBS分组密码的积分分析[J]. 计算机研究与发展, 2013, 50(10): 2117–2125. doi: 10.7544/issn1000-1239.2013.20111495.
YU Xiaoli, WU Wenling, and LI Yanjun. Integral attack of reduced-round MIBS block cipher[J]. *Journal of Computer Research and Development*, 2013, 50(10): 2117–2125. doi: 10.7544/issn1000-1239.2013.20111495.

[7] 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): 157–163,171. doi: 10.3969/j.issn.1000-436x.2014.07.019.
PAN Zhishu, GUO Jiansheng, CAO Jinke, *et al*. Integral attack on MIBS block cipher[J]. *Journal on Communications*, 2014, 35(7): 157–163,171. doi: 10.3969/j.issn.1000-436x.2014.07.019.

[8] 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 Edition*, 2013, 44(3): 308–315.

[9] 付立仕, 金晨辉. MIBS-80的13轮不可能差分分析[J]. 电子与信息学报, 2016, 38(4): 848–855.
FU Lishi and JIN Chenhui. Impossible differential cryptanalysis on 13-round MIBS-80[J]. *Journal of Electronics & Information Technology*, 2016, 38(4): 848–855.

[10] 李玮, 曹珊, 谷大武, 等. 物联网中MIBS轻量级密码的唯密文故障分析[J]. 计算机研究与发展, 2019, 56(10): 2216–2228. doi: 10.7544/issn1000-1239.2019.20190406.
LI Wei, CAO Shan, GU Dawu, *et al*. Ciphertext-only fault analysis of the MIBS lightweight cryptosystem in the internet of things[J]. *Journal of Computer Research and Development*, 2019, 56(10): 2216–2228. doi: 10.7544/issn1000-1239.2019.20190406.

[11] 王永娟, 王涛, 袁庆军, 等. 密码算法旁路立方攻击改进与应用[J]. 电子与信息学报, 2020, 42(5): 1087–1093. doi: 10.11999/JEIT181075.
WANG Yongjuan, WANG Tao, YUAN Qingjun, *et al*. Side channel cube attack improvement and application to cryptographic algorithm[J]. *Journal of Electronics & Information Technology*, 2020, 42(5): 1087–1093. doi: 10.11999/JEIT181075.

[12] DIFFIE W and HELLMAN M E. Exhaustive cryptanalysis of the NBS data encryption standard[J]. *Computer*, 1977, 10(6): 74–84. doi: 10.1109/C-M.1977.217750.

[13] DERBEZ P and PERRIN L. Meet-in-the-middle attacks and structural analysis of round-reduced PRINCE[J]. *Journal of Cryptology*, 2020, 33(3): 1184–1215. doi: 10.1007/s00145-020-09345-0.

[14] LIU Ya, SHI Bing, GU Dawu, *et al*. Improved meet-in-the-middle attacks on reduced-round Deoxys-BC-256[J]. *The Computer Journal*, 2020, 63(12): 1859–1870. doi: 10.1093/comjnl/bxaa028.

[15] 肖钰汾, 田甜. 减轮SKINNY-128-384算法的中间相遇攻击[J]. 密码学报, 2021, 8(2): 338–351.

XIAO Yufen and TIAN Tian. Meet-in-the-middle attack on round-reduced skinny-128-384[J]. *Journal of Cryptologic Research*, 2021, 8(2): 338–351.

[16] DUNKELMAN O, KELLER N, and SHAMIR A. Improved single-key attacks on 8-round AES-192 and AES-256[C]. The 16th International Conference on the Theory and Application of Cryptology and Information Security, Singapore, 2010: 158–176.

[17] DERBEZ P, FOUQUE P A, and JEAN J. Improved key recovery attacks on reduced-round AES in the single-key setting[C]. The 32nd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Athens, Greece, 2013: 371–387.

[18] LI Rongjia and JIN Chenhui. Meet-in-the-middle attacks on 10-round AES-256[J]. *Designs, Codes and Cryptography*, 2016, 80(3): 459–471. doi: 10.1007/s10623-015-0113-3.

[19] SHI Danping, SUN Siwei, DERBEZ P, *et al*. Programming the Demirci-Selçuk meet-in-the-middle attack with constraints[C]. The 24th International Conference on the Theory and Application of Cryptology and Information Security, Brisbane, Australia, 2018: 3–44.

[20] CHEN Qiu, SHI Danping, SUN Siwei, *et al*. Automatic Demirci-Selçuk meet-in-the-middle attack on SKINNY with key-bridging[C]. The 21th International Conference on Information and Communications Security, Beijing, China, 2019: 233–247.

任炯炯：男，1995年生，讲师，博士，研究方向为对称密码设计与分析.

侯泽洲：男，1998年生，硕士生，研究方向为分组密码的安全性分析.

李曼曼：女，1986年生，讲师，硕士，研究方向为对称密码设计与分析.

林东东：男，1998年生，硕士生，研究方向为分组密码的安全性分析.

陈少真：女，1967年生，教授，博士生导师，研究方向为密码算法的设计与分析.

责任编辑：余　蓉