改进的减轮E2算法中间相遇攻击

杜小妮*①③ 孙 瑞①② 郑亚楠① 梁丽芳①
①(西北师范大学数学与统计学院 兰州 730070)
②(西北师范大学密码技术与数据分析重点实验室 兰州 730070)
③(甘肃省数学与统计学基础学科研究中心 兰州 730070)

摘 要：E2算法是AES首轮征集的15个候选算法之一，具有优良的软硬件实现效率和较强的安全性。该文利用多重集和差分枚举技术，对E2算法进行中间相遇攻击。首先以E2-128为例，改进了已有的4轮中间相遇区分器，将5轮密钥恢复攻击预计算复杂度降低为2^{31}次5轮算法加密。其次针对E2-256，将所得区分器向后增加两轮，构造了6轮中间相遇区分器，并实现了9轮中间相遇攻击，攻击所需的数据复杂度为2^{105}个选择明文，存储复杂度为2^{200} byte，时间复杂度为2^{205}次9轮算法加密。与现有对E2算法的安全性分析结果相比，该文实现了对E2-256最长轮数的攻击。

关键词：分组密码；E2算法；中间相遇攻击；差分枚举技术
中图分类号：TN918.2; TP309.7 **文献标识码**：A **文章编号**：1009-5896(2024)00-0001-08
DOI: 10.11999/JEIT230655

Improved Meet-in-the-middle Attacks on Reduced-round E2

DU Xiaoni①③ SUN Rui①② ZHENG Yanan① LIANG Lifang①
①(*College of Mathematics and Statistic, Northwest Normal University, Lanzhou* 730070, *China*)
②(*Key Laboratory of Cryptography and Data Analytics, Northwest Normal University, Lanzhou* 730070, *China*)
③(*Gansu Provincial Research Center for Basic Disciplines of Mathematics and Statistics, Lanzhou* 730070, *China*)

Abstract: E2 is one of the 15 candidate algorithms in the first round of AES, which has the characteristics of excellent software and hardware implementation efficiency and strong security. The meet-in-the-middle attacks on E2 are carried out in this paper by using multiset tabulation technique and differential enumeration technique. First, E2-128 is taken as an example to improve the existing 4-round meet-in-the-middle distinguisher, and the pre-computation complexity of 5-round key recovery attack is reduced to 2^{31} 5-round encryptions. Second, for E2-256, a 6-round distinguisher is constructed from the new 4-round distinguisher by extending two rounds backward, and then a 9-round meet-in-the-middle attack is presented, whose data complexity is 2^{105} chosen plaintexts, memory complexity is 2^{200} byte, and time complexity is 2^{205} 9-round encryptions. Compared with the existing security analysis results of E2, the scheme achieves the longest number of attack rounds for E2-256.

Key words: Block cipher; E2; Meet-in-the-middle attack; Differential enumeration technique

1 引言

随着射频识别技术和无线传感器等资源受限设备的广泛应用，其中的信息安全问题引起了人们的重视，而轻量级分组密码算法LBlock[1]，FUTURE[2]和RAIN[3]等具有功耗低、效率高和占用资源小等特点，符合在该类环境下应用的各项要求。目前对轻量级分组密码算法的安全性分析方法主要有差分分析[4]、线性分析[4]、不可能差分分析[5]和中间相遇攻击[3]等。

1977年，Diffie等人[6]首次提出了中间相遇攻击，其思想是利用存储复杂度来降低攻击过程中所需的时间复杂度。尽管预计算阶段只需计算1次存储复杂度，但若涉及的密钥过多，则会超过穷举复

收稿日期：2023-07-03；改回日期：2023-12-20；网络出版：2024-02-04
*通信作者： 杜小妮 ymldxn@126.com
基金项目：甘肃省自然科学基金重点资助项目(23JRRA685)，国家自然科学基金(62172337)，甘肃省基础研究创新群体项目(23JRRA684)
Foundation Items: The Key Project of Gansu Natural Science Foundation (23JRRA685), The National Natural Science Foundation of China (62172337), The Funds for Innovative Fundamental Research Group Project of Gansu Province (23JRRA684)

杂度，因此学者们致力于减少需要猜测的密钥量和预计算阶段的参数个数，以保证在时间复杂度较低的情况下尽可能降低存储复杂度。Dunkelman等人[7]和Shi等人[8]运用中间相遇攻击思想，并结合多重集、差分枚举和密钥桥技术，对分组密码AES[4], MIBS[9], TWINE[10]和Joltik-BC[11]等进行安全性分析时均取得了很好的效果。

E2算法[12]是日本NTT公司设计的一种分组密码，其分组长度为128 bit，支持的密钥长度包括128, 192和256 bit，分别记为E2-128, E2-192和E2-256。由于轮函数采用SPS结构，加大了分析难度，因而对该算法的安全性分析较少，主要集中为截断差分攻击[13]和不可能差分攻击[14]。2015年，官等人[15]首次在不考虑初始和末端变换的前提下，对E2-128和E2-256分别进行了5轮和6轮的中间相遇攻击，但攻击轮数较少且预计算复杂度较高。本文受文献[9]启发，改进了E2算法的中间相遇攻击，因分析时不考虑密钥扩展方案，故该算法所有版本分析过程一致。主要贡献如下：

(1) 利用多重集和差分枚举技术，结合算法截断差分性质，改进了文献[15]的4轮中间相遇区分器，将6个字节决定的后续字节，降为由4个字节决定，并以E2-128为例实现了5轮密钥恢复攻击，使得预计算复杂度由2^{48}降低为2^{31}次5轮算法加密；

(2) 构造了新的6轮中间相遇区分器，所需参数仅为24个，保证了在预计算阶段复杂度较低，是目前已知的最好结果；

(3) 将 (2) 所得区分器向前扩展1轮，向后扩展2轮，实现了9轮E2-256中间相遇攻击，攻击轮数相较于文献[15]增加4轮，是目前已知的对E2-256最长轮数的攻击，所需数据复杂度为2^{105}个选择明文，存储复杂度为2^{200} byte，时间复杂度为2^{205}次9轮算法加密。

本文结构安排如下：第2节给出必要的符号说明，并简要介绍E2算法及中间相遇攻击的相关定义及性质；第3节改进已有的4轮中间相遇区分器，并进行5轮E2-128中间相遇攻击；第4节构造6轮中间相遇区分器，并进行9轮E2-256的中间相遇攻击；第5节总结全文。

2 预备知识

本节首先对所涉及的符号进行说明，其次描述E2算法加密流程及其轮函数，最后介绍中间相遇攻击的相关知识。

2.1 符号说明

M, C 明文，密文

L_i, R_i 第i轮左支，右支64 bit输入

$R_i[a]$ R_i的第a个字节遍历，其他字节固定，$1 \le a \le 8$

$R_i^j[a]$ $R_i[a]$的第j个取值，$0 \le j \le 255$

$\Delta R_i^j[a]$ 状态差分值$R_i^j[a] \oplus R_i^0[a]$

$\mathrm{K}^{(l)}$ 第l次轮密钥加操作，$l = 1, 2$

X_i, Y_i, Z_i 第i轮经过$\mathrm{K}^{(1)}$，第1个S盒，P置换的输出

X_i', Y_i', Z_i' 第i轮经过$\mathrm{K}^{(2)}$，第2个S盒，字节置换BRL的输出

$X[a]$ 向量X的第a个字节

2.2 E2算法介绍

E2算法整体采用Feistel结构，分组长度为128 bit，迭代轮数为12轮。如图1所示，明文M在经过初始变换IT、12轮迭代变换以及末端变换FT后得到密文C，其中RK_1和RK_2是IT变换轮密钥，RK_3和RK_4是FT变换轮密钥。具体步骤如下：

(1) 128 bit的明文M经过初始变换IT，得到$\mathrm{IT}(M)$。

(2) 令$\mathrm{IT}(M) = L_1 \| R_1$，其中$L_1, ; R_1$分别为$\mathrm{IT}(M)$的左支，右支各64 bit。将$L_1 \| R_1$按照如下方式迭代12轮，得到$L_{13} \| R_{13}$。

$$\begin{cases} L_{i+1} = R_i, \\ R_{i+1} = L_i \oplus \mathrm{F}(R_i, K_i), \end{cases} \quad 1 \le i \le 12,$$

其中F表示轮函数，$K_i = K_i^{(1)} \| K_i^{(2)} (1 \le i \le 12)$表示第$i$轮的轮密钥。

(3) 对$R_{13} \| L_{13}$应用末端变换FT，得到密文$C = \mathrm{FT}(R_{13} \| L_{13})$。

轮函数F为$\mathrm{BRL} \circ \mathrm{S} \circ \mathrm{K}^{(2)}(K_i^{(2)}, \mathrm{P} \circ \mathrm{S} \circ \mathrm{K}^{(1)}(K_i^{(1)}, R_i))$，P置换表示为

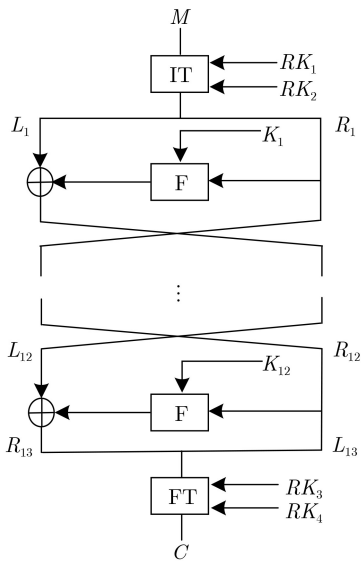

图 1 E2算法加密流程

$$(Z_i[1],Z_i[2],\cdots,Z_i[8])^{\mathrm{T}}=P\cdot(Y_i[1],Y_i[2],\cdots,Y_i[8])^{\mathrm{T}}$$

其中，

$$\boldsymbol{P}=\begin{pmatrix}0&1&1&1&1&1&1&0\\1&0&1&1&0&1&1&1\\1&1&0&1&1&0&1&1\\1&1&1&0&1&1&0&1\\1&1&0&1&1&1&0&0\\1&1&1&0&0&1&1&0\\0&1&1&1&0&0&1&1\\1&0&1&1&1&0&0&1\end{pmatrix}。$$

字节置换BRL为

$$\mathrm{BRL}:\mathbb{F}_{2^8}^8\to\mathbb{F}_{2^8}^8:(Z_i'[1],Z_i'[2],\cdots,Z_i'[8])\to(Y_i'[2],Y_i'[3],\cdots,Y_i'[1])$$

显然有

$$\mathrm{BRL}^{-1}:\mathbb{F}_{2^8}^8\to\mathbb{F}_{2^8}^8:(Y_i'[1],Y_i'[2],\cdots,Y_i'[8])\to(Z_i'[8],Z_i'[1],\cdots,Z_i'[7])$$

因分析过程中未用到E2算法的密钥扩展方案和IT、FT变换，故不再详述。具体可参考文献[12]。

2.3 中间相遇攻击

性质1　(S盒的性质)[16]给定S盒的非零输入差分Δ_{in}和输出差分Δ_{out}，方程$\mathrm{S}(x)\oplus\mathrm{S}(x\oplus\Delta_{\mathrm{in}})=\Delta_{\mathrm{out}}$平均有一个解。

定义1　称允许元素出现多次且不计顺序的集合为多重集。

定义2　若E2-128的某个字节遍历256个值，其他15 byte取固定值，称这样的结构为δ - 集，其中，遍历256个值的字节为活跃字节，其余为非活跃字节。

若攻击过程中涉及的多重集参数多，则预计算阶段需要较大的存储空间，为降低预计算阶段存储复杂度，引入性质2。

性质2　(多重集的存储)[16]任给一个含有256个字节的多重集，其所有可能的取值数量为$2^{506.17}$，而存储这些可能的多重集仅需要512 bit。

中间相遇攻击是一种选择明文攻击，其攻击原理为：将加密过程分解成两部分，首先根据构造的区分器选择明文，并对明文进行加密得到对应的密文；其次猜测相关密钥，加密明文对和解密密文对的若干字节或比特，判断是否构成中间数据的碰撞，若碰撞成功，则猜测密钥是正确的，否则为错误密钥，需排除。具体描述如下：

将加密过程分解成E_1和E_2两个部分，假设其对应的密钥分别为K_1'和K_2'，则加密算法可表示成$C=\mathrm{E}_2(\mathrm{E}_1(M,K_1'),K_2')$，攻击过程为：

(1) 对每一个选择明文M，计算$\mathrm{E}_1(M,K_1')$，将结果存储起来；

(2) 将明文M所对应的密文C用所猜测的密钥K_2'进行部分解密，得$\mathrm{E}_2^{-1}(C,K_2')$；

(3) 验证$\mathrm{E}_1(M,K_1')=\mathrm{E}_2^{-1}(C,K_2')$是否成立，若成立，则表明$(K_1',K_2')$为正确密钥，否则为错误密钥，需排除。

重复以上步骤，过滤所有错误密钥，最终得到正确密钥。

3　5轮E2-128的中间相遇攻击

本节利用多重集和差分枚举技术改进已有的4轮中间相遇区分器，并以E2-128为例进行5轮密钥恢复攻击，有效地降低预计算复杂度。

3.1 改进的4轮中间相遇区分器

在文献[15]中，E2-128的$\Delta R_4[7]$由6个字节完全确定，本节通过对E2-128结构分析发现，仅利用4个字节可得到文献[15]中的4轮中间相遇区分器，从而改进了区分器，具体见定理1。图2给出了相关截断差分路径，其中“$*$”表示任意非0字节，“?”表示未知字节。

定理1　若δ - 集的活跃字节为$R_2[8]$，则经过4轮加密后得到的多重集$\Delta\Re_4[7]:=\{R_4^0[7]\oplus R_4^0[7],R_4^1[7]\oplus R_4^0[7],\cdots,R_4^{255}[7]\oplus R_4^0[7]\}$完全由$X_2[8],X_2'[2],X_3[1],X_3'[8]$决定。

证明：由于$R_2[8]$遍历2^8个所有可能状态值，则$\{\Delta R_2^0,\Delta R_2^1,\cdots,\Delta R_2^{255}\}$遍历$2^8$个无序状态，经过密钥异或得到$\{\Delta X_2^0,\Delta X_2^1,\cdots,\Delta X_2^{255}\}$，因而有：

(1) 若已知$X_2[8]$，则$\Delta X_2[8]$经过S盒后得$\Delta Y_2[8]=\mathrm{S}(X_2[8])\oplus\mathrm{S}(\Delta X_2[8]\oplus X_2[8])$，经过P置换得到$\Delta Z_2[2,3,4,7,8]$，即活跃字节为第$2,3,4,7,8$ byte；若已知$X_2'[2]$，由于$\Delta X_2'[2]=\Delta Z_2[2]$，同理经过S盒和BRL置换可得$\Delta Z_2'[1]$；

(2) 若已知$X_3[1]$，由于$\Delta X_3[1]=\Delta R_3[1]=\Delta Z_2'[1]\oplus\Delta R_1[1]=\Delta Z_2'[1]$，同理可得$\Delta Z_3[2,3,4,5,6,8]$；

(3) 若已知$X_3'[8]$，因为$\Delta X_3'[8]=\Delta Z_3[8]$，同理可得$\Delta Z_3'[7]$；由图2可知$\Delta R_2=(0000000*)$，故$\Delta R_4[7]=\Delta Z_3'[7]$。

由以上分析可知多重集$\Delta\Re_4[7]$完全由$X_2[8],X_2'2],X_3[1],X_3'[8]$决定。　证毕

3.2 5轮E2-128的中间相遇攻击

基于3.1得到的4轮区分器，本节进行5轮E2-128中间相遇攻击，具体见图3，其中e表示活跃字节。

利用文献[15]的方法，计算5轮密钥恢复攻击的复杂度，主要可分为如下两个阶段。

预计算阶段：预计算复杂度为$12\times4\times(2^8)^4/(16\times5)\approx2^{31}$次5轮算法加密；存储复杂度为$2^{32+8}=2^{40}$ byte。

在线阶段：数据复杂度为12个选择明文；时间复杂度为$12\times 2^{6\times 8}\times 6/(16\times 5)\approx 2^{47.9}$次5轮算法加密。

相较于文献[15]，改进的4轮中间相遇区分器中$\Delta R_4[7]$仅由4个字节完全确定，在进行5轮E2-128密钥恢复攻击时，预计算复杂度得到了有效降低，具体攻击结果对比见表1。

4 9轮E2-256的中间相遇攻击

本节主要构造6轮中间相遇区分器，并进行9轮密钥恢复攻击以及复杂度分析。由于9轮密钥恢复攻击最终的时间复杂度为2^{205}次9轮加密，超过了E2-128和E2-192穷举攻击的时间复杂度，所以本节仅讨论E2-256的9轮中间相遇攻击。

4.1 6轮中间相遇区分器

基于3.1节得到的4轮中间相遇区分器，向后增加2轮，构造6轮中间相遇区分器，具体截断差分路径见图4。类似地，有如下定理。

定理2 若δ - 集的活跃字节为$R_2[8]$，则经过

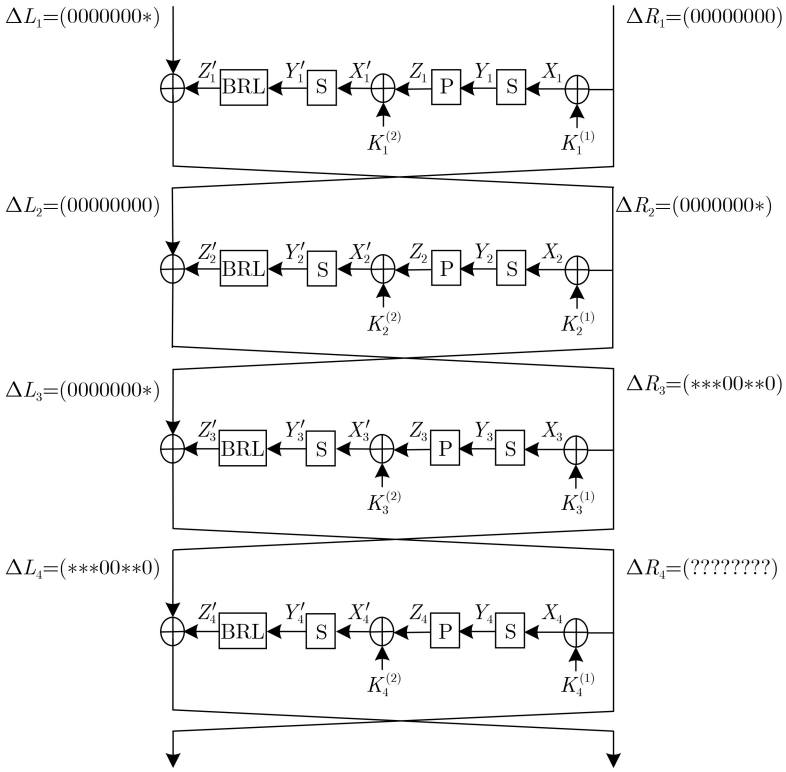

图 2 4轮E2-128中间相遇区分器

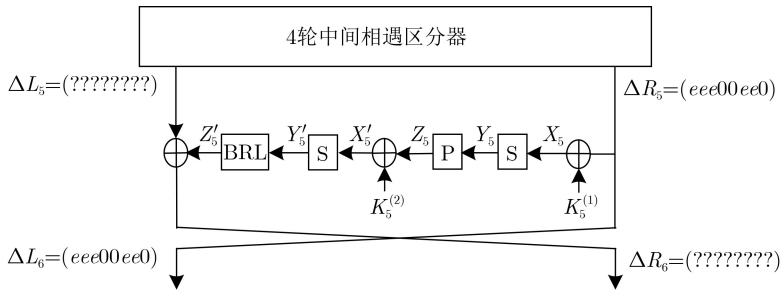

图 3 5轮E2-128中间相遇攻击

表 1 E2算法攻击结果对比

来源	攻击方法	算法版本	轮数	时间复杂度	预计算复杂度	数据复杂度
文献[13]	截断差分	E2-128/E2-128	7/8	-	-	$2^{91}/2^{94}$
文献[14]	不可能差分	E2-128/E2-256	7/8	$2^{115.5}/2^{214}$	-	$2^{120}/2^{121}$
文献[15]	中间相遇攻击	E2-128	5	2^{48}	2^{48}	14
本文	中间相遇攻击	E2-128	5	$2^{47.9}$	2^{31}	12
本文	中间相遇攻击	E2-256	9	2^{205}	$2^{200.6}$	2^{105}

6轮加密后得到的多重集$\Delta\Re_6[7] := \{R_6^0[7] \oplus R_6^0[7], R_6^1[7] \oplus R_6^0[7], \cdots, R_6^{255}[7] \oplus R_6^0[7]\}$完全由$X_2[8], X_2'[2,3,4,7,8], X_3[1,2,3,6,7], X_3', X_4, X_4'[1], X_5[8], X_5'[8]$共30个字节决定。

证明：若已知$X_2[8]$，由定理1的证明过程可得$\Delta Z_2[2,3,4,7,8]$。

(1) 若已知$X_2'[2,3,4,7,8]$，因为$\Delta X_2'[2,3,4,7,8] = \Delta Z_2[2,3,4,7,8]$，则经过S盒后可得差分值$\Delta Y_2'[2,3,4,7,8]$，经过BRL置换，可得$\Delta Z_2'[1,2,3,6,7]$；

(2) 若已知$X_3[1,2,3,6,7]$，由于$\Delta X_3[1,2,3,6,7] = \Delta R_3[1,2,3,6,7] = \Delta R_1[1,2,3,6,7] \oplus \Delta Z_2'[1,2,3,6,7]$，与(1)证明类似，可得$\Delta X_3' = \Delta Z_3$；若已知$X_3'$，同理可得$\Delta Z_3'$；

(3) 若已知X_4，由于$\Delta X_4 = \Delta R_4 = \Delta R_2 \oplus \Delta Z_3'$，同理可得$\Delta X_4' = \Delta Z_4$；若已知$X_4'[1]$，可得$\Delta Z_4'[8]$；

(4) 若已知$X_5[8]$，因$\Delta X_5[8] = \Delta R_5[8] = \Delta R_3[8] \oplus \Delta Z_4'[8]$，同理可得$\Delta X_5'[2,3,4,7,8] = \Delta Z_5[2,3,4,7,8]$；

(5) 若已知$X_5'[8]$，可得$\Delta Z_5'[7]$，更进一步地，由图4可知$\Delta R_6[7] = \Delta X_4[7] \oplus \Delta Z_5'[7]$。

由以上分析可知多重集$\Delta\Re_6[7]$完全由上述30个字节决定。　　证毕

为降低预计算阶段的复杂度，我们利用性质1将区分器参数个数减少到24个字节，具体见定理3。

定理3　若对定理2中的δ-集进行6轮加密(如图4)，则多重集$\Delta\Re_6[7]$仅由$\Delta X_2[8], \Delta Y_2[8], \Delta Y_2'[2,3,4,7,8], \Delta Y_3[1,2,3,6,7], \Delta X_4[1,2,3,6,7], \Delta Y_4[1,2,3,6,7], \Delta X_5[8], \Delta Y_5[8]$共24个字节决定。

证明：只需证明定理2的30个字节可由定理3的24个字节推出。证明分为以下5个步骤：

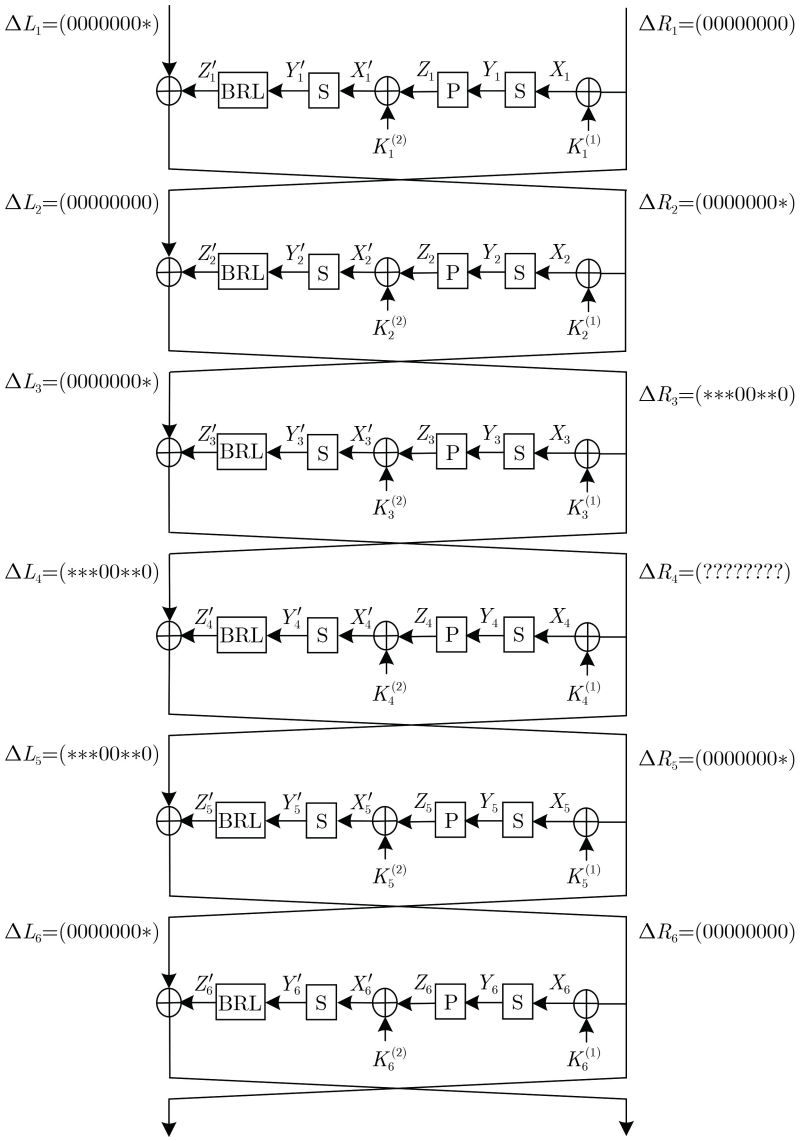

图 4 6轮E2-256中间相遇区分器

(1) 若已知$\Delta X_2[8]$和$\Delta Y_2[8]$，利用性质1，可得$X_2[8]$；

(2) 若已知$\Delta Y_2'[2,3,4,7,8]$，由于$\Delta X_2'[2,3,4,7,8]=\Delta Z_2[2,3,4,7,8]=\mathrm{P}(\Delta Y_2[8])$，利用性质1，可得$X_2'[2,3,4,7,8]$；

(3) 若已知$\Delta Y_3[1,2,3,6,7]$，由$\Delta R_1=(00000000)$可知$\Delta X_3[1,2,3,6,7]=\mathrm{BRL}(\Delta Y_2'[2,3,4,7,8])$，同理，可得$X_3[1,2,3,6,7]$并且有$\Delta X_3'=\Delta Z_3=\mathrm{P}(\Delta Y_3[1,2,3,6,7])$；

(4) 若已知$\Delta X_4[1,2,3,6,7]$和$\Delta Y_4[1,2,3,6,7]$，则有：

(a) 由$\Delta R_6=(00000000)$可知，$\Delta X_4=\Delta Z_5'=(***00**0)$，利用性质1可得$X_4$；

(b) 同理，由于$\Delta Y_3'=\mathrm{BRL}^{-1}(\Delta R_2\oplus\Delta R_4)=\mathrm{BRL}^{-1}(\Delta X_2\oplus\Delta X_4)$，可得$X_3'$；

(c) $\Delta X_4'[1,2,3,6,7]=\Delta Z_4[1,2,3,6,7]=\mathrm{P}(\Delta Y_4[7])$，$\Delta Y_5'[2,3,4,7,8]=\mathrm{BRL}^{-1}(\Delta Z_5'[1,2,3,6,7])=\mathrm{BRL}^{-1}(\Delta X_4[1,2,3,6,7])$；

(5) 若已知$\Delta X_5[8]$和$\Delta Y_5[8]$，由$\Delta R_3=(***00**0)$可知$\Delta Y_4'[1]=\mathrm{BRL}^{-1}(\Delta Z_4'[8])=\mathrm{BRL}^{-1}(\Delta X_5[8])$，此外，利用性质1及(c)得到的$\Delta X_4'[1]$，可得$X_4'[1]$和$X_5[8]$；又因为$\Delta X_5'[2,3,4,7,8]=\Delta Z_5[2,3,4,7,8]=\mathrm{P}(\Delta Y_5[8])$，同理，由(c)得到的$\Delta Y_5'[2,3,4,7,8]$可得$X_5'[8]$。

综上，多重集$\Delta\Re_6[7]$仅由24个字节决定，相较于定理2，参数个数减少了6个字节。 证毕

4.2 9轮E2-256的中间相遇攻击

利用4.1节构造的6轮中间相遇区分器，向前扩展1轮，向后扩展2轮，实现了9轮E2-256中间相遇攻击，具体攻击过程见图5，其中α,β,e和γ均为活跃字节，攻击所需数据复杂度为2^{105}个选择明文，存储复杂度为2^{200} byte，时间复杂度为2^{205}次9轮算法加密。

中间相遇攻击由两个阶段组成：预计算阶段和在线阶段。

预计算阶段：穷举定理3的24个字节，共有2^{192}个参数值，即得到2^{192}个多重集，并将其存储在Hash表T中。

在线阶段：首先找到满足图5截断差分路径的明文对；其次构造包含明文对的δ-集；最后猜测涉及的轮密钥并得到$\Delta R_7[7]$所对应的多重集，检验其是否存在于Hash表T中，若存在，则猜测密钥是正确密钥，否则为错误密钥。具体步骤如下：

(1) 选择满足图5差分形式的明文对，即$\Delta L_1=(\beta\beta 00\beta\beta 0)$，$\Delta R_1=(0000000\alpha)$，故一个明文结构有$2^{2\times 8}=2^{16}$种可能取值，即有$2^{16}\times(2^{16}-1)/2\approx 2^{31}$对明文差分，由于满足截断差分特征的概率为$2^{-(5+5+2+3)\times 8}=2^{-120}$，因此需选取$2^{120-31}=2^{89}$个明文结构，共有$2^{89+16}=2^{105}$个选择明文。

(2) 因为$\Delta X_9=\Delta R_9=(eee00ee0)$，故只需猜测密钥$K_9^{(1)}[1,2,3,6,7]$，可得$\Delta X_9[1,2,3,6,7]$，进而可得$\Delta Y_9[1,2,3,6,7]$；同理猜测密钥$K_9^{(2)}$，得到$\Delta Z_9$；筛选满足$\Delta Z_9[1,2,3,6,7]=\mathrm{P}(\Delta Y_9[6])$的明文对$(L_1\parallel R_1)$。

(3) 利用步骤(2)筛选出的明文对构造相应的δ-集。首先猜测密钥$K_1^{(1)}[8]$，得到$X_1[8]$；令$X_1^*[8]=X_1[8]\oplus\alpha,\alpha\in[0,255]$，该活跃字节遍历$2^8$个所有可能值，满足区分器中定义的$\delta$-集。

(4) 由于$\Delta Z_1[2,3,4,7,8]=\mathrm{P}(\Delta Y_1[8])=\mathrm{P}(\mathrm{S}(X_1[8])\oplus\mathrm{S}(X_1^*[8]))$，猜测密钥$K_1^{(2)}[2,3,4,7,8]$，可得$\Delta Z_1'[1,\ 2,3,6,7]$；又根据算法结构，可得$\Delta L_1[1,2,3,6,7]$，进而有$L_1^*=L_1\oplus\Delta L_1$，$R_1^*=R_1\oplus\Delta R_1$，因此可利用步骤(3)得到的$\delta$-集求出所有的明文集，加密得到对应的密文集。

(5) 选择步骤(4)得到的任一明文对$(L_1\parallel R_1,L_1^*\parallel R_1^*)$和对应的密文对$(L_{10}\parallel R_{10},L_{10}^*\parallel R_{10}^*)$，猜测密钥$K_8^{(1)}[1,3,4,5,8]$，可得$\Delta Y_8[1,3,4,5,8]$，又由P置换可得$\Delta Z_8[8]=\Delta Y_8[1]\oplus\Delta Y_8[3]\oplus\Delta Y_8[4]\oplus\Delta Y_8[5]\oplus\Delta Y_8[8]$，则猜测密钥$K_8^{(2)}[8]$，经过BRL置换可得$\Delta Z_8'[7]$。

(6) 由算法结构可知$\Delta R_7[7]=\Delta X_9[7]\oplus\Delta Z_8'[7]$，因$\Delta X_9[7]$和$\Delta Z_8'[7]$分别可由步骤(2)和步骤(5)给出，故而可得多重集$\Delta\Re_7[7]:=\{R_7^0[7]\oplus R_7^0[7],R_7^1[7]\oplus R_7^0[7],\cdots,R_7^{255}[7]\oplus R_7^0[7]\}$。判断多重集是否与预计算阶段Hash表T发生碰撞，若碰撞成功则恢复出正确密钥。

综上，在攻击过程中需要猜测的密钥为$K_1^{(1)}[8]$，$K_1^{(2)}[2,3,4,7,8]$，$K_8^{(1)}[1,3,4,5,8]$，$K_8^{(2)}[8]$，$K_9^{(1)}[1,2,3,6,7]$和$K_9^{(2)}$，即通过猜测$25\times 8=200$ bit密钥，可得2^{200}个多重集。由性质2可知，多重集共有$2^{506.17}$种取法，则错误密钥形成碰撞的概率为$2^{200}\times 2^{-506.17}\approx 0$。因此碰撞成功的密钥为正确密钥。

4.3 攻击复杂度分析

攻击复杂度的分析过程如下：

预计算阶段：构造Hash表T需要的预计算复杂度为$2^{192}\times 2^8\times 6/9\approx 2^{200.6}$次9轮加密；存储复杂度为$2^{192+8}=2^{200}$ byte。

在线阶段：由于4.2中步骤(1)需要加密2^{105}个选择明文，则数据复杂度为2^{105}个选择明文。

对于时间复杂度，加密2^{105}个选择明文需要2^{105}次9轮加密；同时密钥恢复阶段需猜测200 bit

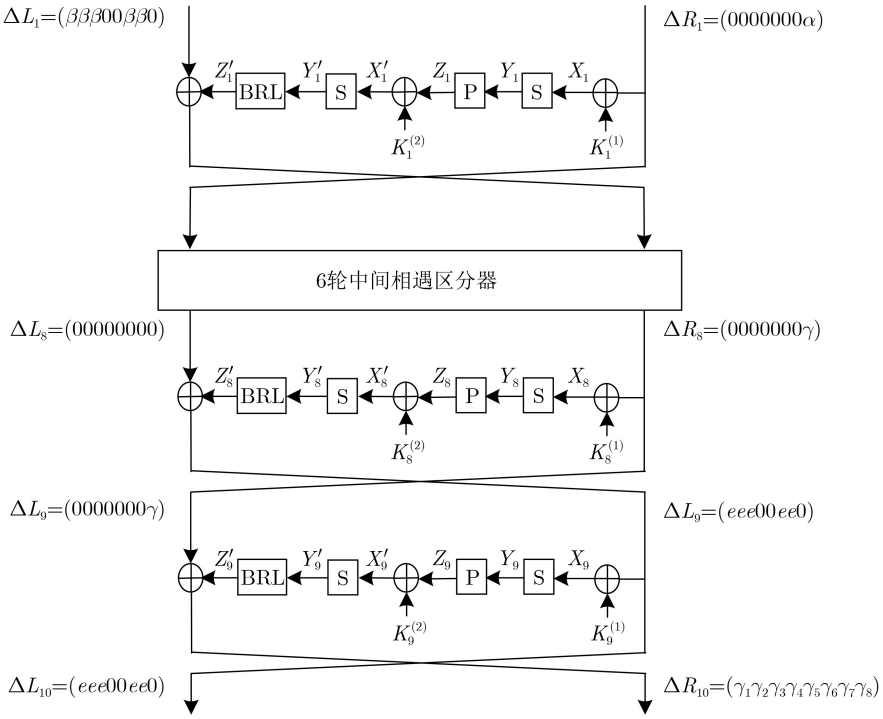

图 5 9轮E2-256中间相遇攻击

密钥，所需时间复杂度约为$2^{200}\times 2^{8}\times 2^{-3}=2^{205}$次9轮加密，故总的时间复杂度约为$2^{105}+2^{205}\approx 2^{205}$次9轮加密。

综上所述，该攻击的预计算复杂度为$2^{200.6}$次9轮加密，数据复杂度为2^{105}个选择明文，存储复杂度为2^{200} byte，时间复杂度为2^{205}次9轮加密。与已有的攻击结果对比见表1。

5　结束语

本文对减轮E2算法进行了中间相遇攻击。首先改进了已有的4轮中间相遇区分器，进行了5轮E2-128密钥恢复攻击；其次将4轮区分器向后增加两轮，构造了6轮中间相遇区分器，结合算法S盒性质、多重集以及差分枚举技术，减少了6轮区分器所需的参数个数，首次实现了9轮E2-256的中间相遇攻击。研究结果表明，本文实现了目前已知对E2-256最长轮数的攻击。

后续研究方向/计划：(1) 进一步寻找降低中间相遇攻击预计算阶段存储复杂度的方法；(2) 将中间相遇攻击与其他传统分析方法相结合，增加区分器/攻击轮数或降低时间/存储复杂度。

参 考 文 献

[1] WU Wenling and ZHANG Lei. LBlock: A lightweight block cipher[C]. Proceedings of the 9th International Conference on Applied Cryptography and Network Security, Nerja, Spain, 2011: 327–344. doi: 10.1007/978-3-642-21554-4_19.

[2] GUPTA K C, PANDEY S K, and SAMANTA S. FUTURE: A lightweight block cipher using an optimal diffusion matrix[C]. Proceedings of the 13th International Conference on Cryptology in Africa, Fes, Morocco, 2022: 28–52. doi: 10.1007/978-3-031-17433-9_2.

[3] 杜小妮, 郑亚楠, 梁丽芳, 等. RAIN-128算法的中间相遇攻击[J]. 电子与信息学报, 2024, 46(1): 327–334. doi: 10.11999/JEIT221593.
DU Xiaoni, ZHENG Ya'nan, LIANG Lifang, *et al*. Meet-in-the-middle attack on RAIN-128[J]. *Journal of Electronics & Information Technology*, 2024, 46(1): 327–334. doi: 10.11999/JEIT221593.

[4] 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. **(查阅网上资料, 未找到本条文献页码信息, 请确认)**.
LI Chao, SUN Bing, and LI Ruilin. Attack Method of Block Cipher and Case Analysis[M]. Beijing: Science Press, 2010. **(查阅网上资料, 未找到对应的英文翻译, 请确认)**.

[5] 蒋梓龙, 金晨辉. Saturnin算法的不可能差分分析[J]. 通信学报, 2022, 43(3): 53–62. doi: 10.11959/j.issn.1000-436x.2022045.
JIANG Zilong and JIN Chenhui. Impossible differential cryptanalysis of Saturnin algorithm[J]. *Journal on Communications*, 2022, 43(3): 53–62. doi: 10.11959/j.issn.1000-436x.2022045.

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

[7] DUNKELMAN O, KELLER N, and SHAMIR A. Improved single-key attacks on 8-round AES-192 and AES-256[C]. Proceedings of the 16th International Conference on the Theory and Application of Cryptology and Information Security, Singapore, 2010: 158–176. doi: 10.1007/978-3-642-17373-8_10.

[8] SHI Danping, SUN Siwei, DERBEZ P, *et al*. Programming the Demirci-Selçuk meet-in-the-middle attack with constraints[C]. Proceedings of the 24th International Conference on the Theory and Application of Cryptology and Information Security, Brisbane, Australia, 2018: 3–34. doi: 10.1007/978-3-030-03329-3_1.

[9] 任炯炯, 侯泽洲, 李曼曼, 等. 改进的减轮MIBS-80密码的中间相遇攻击[J]. 电子与信息学报, 2022, 44(8): 2914–2923. doi: 10.11999/JEIT210441.

REN Jiongjiong, HOU Zezhou, LI Manman, *et al*. Improved meet-in-the-middle attacks on reduced-round MIBS-80 cipher[J]. *Journal of Electronics & Information Technology*, 2022, 44(8): 2914–2923. doi: 10.11999/JEIT210441.

[10] BIRYUKOV A, DERBEZ P, and PERRIN L. Differential analysis and meet-in-the-middle attack against round-reduced TWINE[C]. Proceedings of the 22nd International Workshop on Fast Software Encryption, Istanbul, Turkey, 2015: 3–27. doi: 10.1007/978-3-662-48116-5_1.

[11] LI Manman and CHEN Shaozhen. Improved meet-in-the-middle attacks on reduced-round Joltik-BC[J]. *IET Information Security*, 2021, 15(3): 247–255. doi: 10.1049/ise2.12019.

[12] KANDA M, MORIAI S, AOKI K, *et al*. E2-a new 128-bit block cipher[J]. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, 2000, E83-A(1): 48–59.

[13] MORIAI S, SUGITA M, AOKI K, *et al*. Security of E2 against truncated differential cryptanalysis[C]. Proceedings of the 6th International Conference on Selected Areas in Cryptography, Ontario, Canada, 2000: 106–117. doi: 10.1007/3-540-46513-8_8.**(查阅网上资料,未能确认年份信息,请确认)**.

[14] WEI Yuechuan, YANG Xiaoyuan, LI Chao, *et al*. Impossible differential cryptanalysis on tweaked E2[C]. Proceedings of the 6th International Conference on Network and System Security, Wuyishan, China, 2012: 392–404. doi: 10.1007/978-3-642-34601-9_30.

[15] 官翔, 魏悦川, 杨晓元. E2算法的中间相遇攻击[J]. 计算机工程与科学, 2015, 37(3): 524–528. doi: 10.3969/j.issn.1007-130X.2015.03.019.

GUAN Xiang, WEI Yuechuan, and YANG Xiaoyuan. Meet-in-the-middle attacks on E2[J]. *Computer Engineering & Science*, 2015, 37(3): 524–528. doi: 10.3969/j.issn.1007-130X.2015.03.019.

[16] 任炯炯, 陈少真. 11轮3D密码算法的中间相遇攻击[J]. 通信学报, 2015, 36(8): 182–191. doi: 10.11959/j.issn.1000-436x.2015131.

REN Jiongjiong and CHEN Shaozhen. Meet-in-the-middle attack on 11-round 3D cipher[J]. *Journal on Communications*, 2015, 36(8): 182–191. doi: 10.11959/j.issn.1000-436x.2015131.

杜小妮：女，博士后，教授，研究方向为应用密码学.
孙 瑞：女，硕士生，研究方向为应用密码学.
郑亚楠：女，硕士生，研究方向为应用密码学.
梁丽芳：女，博士生，研究方向为应用密码学.

责任编辑：马秀强