

改进的全轮HALFLOOP-48相关调柄攻击

孙晓萌 张文英* 苑兆忠

(山东师范大学信息科学与工程学院 济南 250358)

摘要: HALFLOOP是一类基于调柄机制、结构类似AES的轻量级分组密码,用于保护第4代高频无线电系统中的自动链路消息。由于其行移位与列混合操作具有使差分快速扩散的特点,寻找具有实际可行性的长轮数、高概率的差分区分器,并实现对完整轮HALFLOOP-48的有效攻击仍是亟待解决的关键问题。为此,该文提出一个新的截断差分三明治区分器框架,并基于布尔可满足性(SAT)方法实现自动化搜索最优差分区分器。该框架将密码分为3个子密码层, E_0 和 E_1 使用字节级模型, E_m 使用比特级模型。为突破大型S盒差分特征建模的瓶颈,该文提出基于仿射子空间的降维方法,将高维向量的差分特征分解为两个低维子向量,显著降低了SAT的约束规模。其次,为提高区分器概率,将 E_0 与 E_1 的依赖关系系统地分为3层,逐一计算每层概率并相乘,得到了概率高达 $2^{-43.2}$ 的8轮HALFLOOP-48截断差分三明治区分器,且给出了满足该差分路径的明文对实例。最终,利用该实际差分路径,对完整轮数的HALFLOOP-48算法发起密钥恢复攻击。与已有结果相比,该文结果在时间复杂度上减少了 $2^{25.4}$,在内存复杂度上减少了 2^{10} 。结果说明HALFLOOP算法无法抵抗相关调柄下的三明治攻击。

关键词: 轻量级分组密码; 相关调柄攻击; 截断三明治区分器; 布尔可满足性问题; 密钥恢复攻击

中图分类号: TN918; TP309

文献标识码: A

文章编号: 1009-5896(2026)03-0001-11

DOI: 10.11999/JEIT251014

CSTR: 32379.14.JEIT251014

1 引言

HALFLOOP作为一种采用密钥调柄机制的分组密码^[1],其在防止信息欺骗、保护数据传输及保障高频无线通信链路安全方面具有重要应用价值。自其公布以来,HALFLOOP系列算法即引起了密码分析领域的广泛关注。Dansarie等人^[2]率先对HALFLOOP-24进行了分析,提出了多种场景下的差分攻击。随后,Leander等人^[3]针对完整轮数HALFLOOP-48和减轮HALFLOOP-96提出了时间-数据-内存折中(Time-Data-Memory-Trade-Off, TDM-TO)攻击及DS(Demirci-Selçuk)中间相遇攻击。特别地,其针对完整轮HALFLOOP-48的TDM-TO攻击虽在理论上降低了时间复杂度,但其要求在线阶段枚举全部 2^{64} 个可能的调柄值以获取对应密文,这在当前计算能力下显然不切实际。Lin等人^[4]则致力于搜索高概率差分特征,找到了HALFLOOP-48的最佳6轮相关调柄差分特征(概率为 $2^{-29.48}$)及若干概率低于 2^{-48} 的8轮差分特征。综上所述,针对完整轮HALFLOOP-48的攻击,寻找具有实际可行的高概率区分器,以支撑有效的密钥恢复攻击,仍是亟待解决的关键问题。

飞去来器(Boomerang)攻击^[5]通过组合两条短

轮数高概率的差分特征($\alpha \rightarrow \beta$ 与 $\gamma \rightarrow \delta$, 概率分别为 p 和 q),以构建概率为 p^2q^2 的区分器。然而该攻击的实际效果高度依赖于两条差分特征之间的兼容性:Murphy^[6]指出在某些基于S盒的密码中,独立选择的两条差分特征之间可能互不兼容,从而导致差分特征不存在;如果差分特征间存在依赖性,则实际概率可能显著高于 p^2q^2 。为更系统地研究这种依赖关系并提升攻击效率,Dunkelman等人^[7]对Biryukov等人^[8]提出的所有依赖情况进行归纳,提出了三明治(Sandwich)攻击,其核心思想是在上差分特征(E_0)与下差分特征(E_1)之间引入一个中间层(E_m),即 $E = E_1 \circ E_m \circ E_0$ 。这种结构已被证明对多种密码原语的攻击效果有显著提升^[5,9-11]。

近年来,自动化搜索方法由于具有精确度高、操作简易、效率较高等优点,已经成为密码安全分析领域应用最为广泛的工具,如基于布尔可满足性问题(Boolean SAT is fiability problem, SAT)、混合整数线性规划(Mixed Integer Linear Programming, MILP)等自动化搜索技术。然而其在高效且精确地建模大型S盒(如8 bit AES的S盒)的差分特征上仍面临挑战^[12-14]:尽管以往工作利用代数几何的性质优化建模策略以减少刻画差分特征的不等式或合取范式,但其求解时间超出内存范围,无法寻找长轮数的差分特征^[12,13];Ma等人^[14]使用了分块降维策略以描述特征,但在降维时会丢失部分路径,导致其统计的特征概率与实际概率有偏差。

基于上述研究背景及待解决的问题,本文聚焦HALFLOOP-48算法实际化攻击,主要贡献如下:

收稿日期: 2025-09-26; 改回日期: 2026-01-08; 网络出版: 2026-01-27

*通信作者: 张文英 zhangwenying@sdmu.edu.cn

基金项目: 国家自然科学基金(62272282)

Foundation Item: The National Natural Science Foundation of China (62272282)

(1)提出新的8 bit S盒差分特征的建模方法——仿射子空间降维方法。本方法将八维输出差分按最高有效位划分为互斥子集,并在固定各子集最高位后,建模剩余的七维差分向量,实现了对大型S盒差分特征的完全覆盖及概率的高效评估。

(2)构建了HALFLOOP-48算法最优截断三明治区分器。本文深入分析了上差分特征(E_0)与下差分特征(E_1)间的依赖关系,即对 E_m 层的概率精确计算。由此发现了一条概率为 $2^{-46.415}$ 的3轮差分特征。进一步利用 E_m 层多条差分特征的聚集效应,构造了概率高达 $2^{-43.2}$ 的8轮最优截断三明治区分器。

(3)实现了对全轮HALFLOOP-48的高效密钥恢复攻击。以上述8轮区分器为基础,提出了对完整轮HALFLOOP-48算法的两种密钥恢复攻击:三明治密钥恢复攻击的数据复杂度为 $2^{32.8}$,时间复杂度为 $2^{96.2}$,内存复杂度为 $2^{42.8}$;矩形密钥恢复攻击的数据复杂度为 $2^{16.2}$,时间复杂度为 $2^{99.2}$,内存复杂度为 $2^{26.2}$ 。与已有的工作相比,本文攻击方案在时间与内存复杂度上均显著降低,对比结果详见表1。

2 预备知识

2.1 HALFLOOP-48算法描述

HALFLOOP-48是HALFLOOP轻量级分组密码算法成员之一,采用48 bit分组长度、128 bit密

表1 HALFLOOP-48算法分析结果

攻击场景	攻击轮数	时间复杂度	数据复杂度	存储复杂度	文献
DS中间相遇攻击	10	2^{122}	13	2^{57} B	[3]
相关调柄攻击	8	$2^{92.71}$	$2^{33.27}$	$2^{36.385}$ B	[4]
相关调柄三明治攻击	10	$2^{96.2}$	$2^{32.8}$	$2^{42.8}$ B	第5节
相关调柄矩形攻击	10	$2^{99.2}$	$2^{16.2}$	$2^{26.2}$ B	第5节

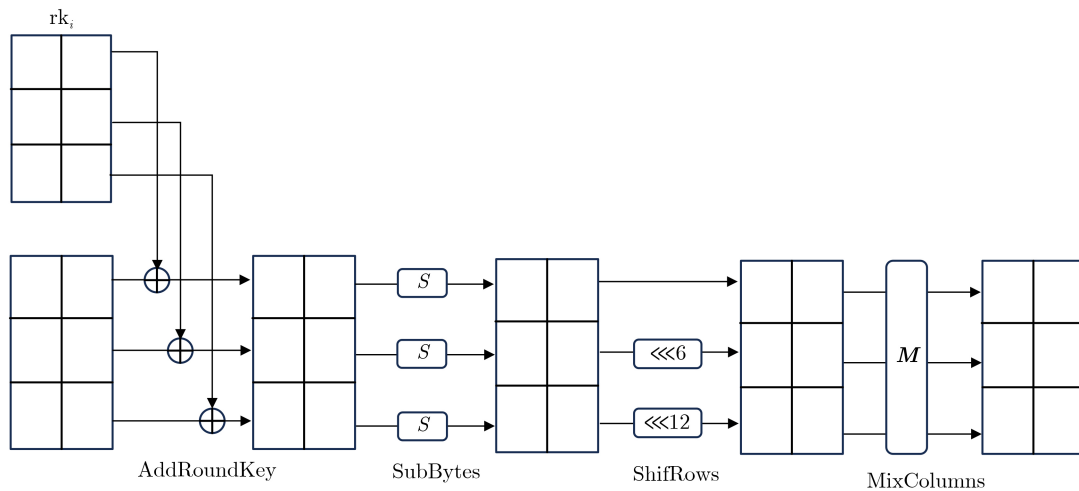


图1 HALFLOOP-48的轮函数

钥 K 及64 bit调柄 T ,迭代轮数为10轮。其轮函数包含4个操作:轮密钥加、字节替换、行移位和列混合(末轮替换为轮密钥加)。明文和中间状态均排列成一个 3×2 的矩阵,代表48 bit的分组长度。状态分组如式(1),其中, $S_{i,j} \in \mathbb{F}_2^8, 1 \leq i, j \leq 3$

$$\mathbf{SM} = \begin{bmatrix} S_{1,1} & S_{1,2} \\ S_{2,1} & S_{2,2} \\ S_{3,1} & S_{3,2} \end{bmatrix} \quad (1)$$

轮密钥加(AddRoundKey, ARK):第 i 轮中间状态与轮密钥 rk_i 进行逐位异或运算。

字节替换(SubBytes, SB):状态中的每个字节应用AES的8 bit S盒^[15]。

行移位(RotateRows, RR):状态矩阵 \mathbf{SM} 的各行分别向左移动0,6和12 bit。

列混合(MixColumns, MC):状态矩阵 \mathbf{SM} 的每列左乘有限域 \mathbb{F}_2^8 (由不可约二进制多项式 $M(x) = x^8 + x^4 + x^3 + x + 1$ 定义)上的3阶矩阵 \mathbf{M}

$$\mathbf{M} = \begin{bmatrix} 9 & 1 & 2 \\ 2 & 9 & 1 \\ 1 & 2 & 9 \end{bmatrix} \quad (2)$$

密钥编排(KeySchedule):密钥 K 分为两个64 bit子块 K' 和 K'' ,使得 $K = K' || K''$ 。对128 bit密钥 $(K' \oplus T) || K''$ 使用AES-128的密钥编排算法扩展生成11个48 bit的密钥。有关算法更多细节描述见文献[1]。图1给出了HALFLOOP-48的轮函数。

2.2 飞去来器连接表

飞去来器连接表(Boomerang Connection Table, BCT)刻画了上差分特征和下差分特征依赖关系^[10]。设 S 是 \mathbb{F}_2^n 上的一个置换,则 $BCT(\alpha, \beta)$ 表示为

$$\#\{x \in \{0, 1\}^n | S^{-1}(S(x) \oplus \beta) \oplus S^{-1}(S(x \oplus \alpha) \oplus \beta) = \alpha\} \quad (3)$$

其中, $\alpha, \beta \in \mathbb{F}_2^8$, α 为上差分特征中S盒的输入差分, β 为下差分特征中S盒的输出差分。若 E_m 仅具有单轮非线性层S盒, 则两条差分特征的依赖概率为 $BCT(\alpha, \beta)/2^n$ 。

2.3 由相关调柄衍生的轮密钥差分

为了构造高概率区分器, 需设计特定调柄差分 ΔT , 使其在密钥编排中产生的轮密钥差分 Δrk_i 与内部状态差分尽可能抵消, 从而减少活跃字节数量, 提高特征概率^[16]。Lin等人^[4]的调柄差分特征在第2轮导致状态差分扩散, 不适用于本文攻击; 而本文通过让调柄差分与明文差分抵消, 将状态差分首次出现所在的轮数延迟至第4轮。

通过遍历不同活跃字节数目的调柄差分, 本文确定了一种最优调柄差分特征: 在前2轮实现轮密钥差分 Δrk_i 的完全抵消, 并在后续轮中最小化活跃字节数量。具体而言, 令 $x \in \mathbb{F}_2^{48}$ 为明文, $T \in \mathbb{F}_2^{64}$ 为调柄, $K \in \mathbb{F}_2^{128}$ 为密钥, 调柄中的单字节差分为 $\delta \in \mathbb{F}_2^8$ 。使用 $T \oplus K$ 与 $T' \oplus K = T \oplus \Delta T \oplus K$ (其中 $\Delta T = 0^{16} \parallel \delta \parallel 0^{24}$)分别加密明文 x 和 $x' = x \oplus 0^{16} \parallel \delta \parallel 0^{24}$ 。每轮的轮密钥的差分特征如表2所示。其中 $S(\delta) \triangleq S(x) \oplus S(x \oplus \delta)$ 表示当输入差分为 δ 时的输出差分。由于密钥的线性编排, 轮密钥中的 δ 值相同。

3 相关调柄截断三明治区分器

本节构建了HALFLOOP-48算法8轮的截断三明治区分器。该区分器由 E_0 , E_m 和 E_1 构成, 分别覆盖第1~4轮、第5~7轮和第8轮。 E_0 , E_1 按照字节级截断差分特征传播, 连接层 E_m 按照比特级截断差分特征传播。此外, E_0 和 E_1 两条截断差分特征在 E_m 中的依赖关系(概率)被归纳为3层, 每层的概率相乘, 得到最优截断三明治区分器的概率。

3.1 构建 E_0 与 E_1

基于2.3节所述的最优轮密钥差分特征, 本节

表2 轮密钥差分特征

轮密钥	差分特征
Δrk_1	$0^{16} \parallel \delta \parallel 0^{24}$
Δrk_2	0
Δrk_3	0
Δrk_4	$\delta \parallel 0^{24} \parallel \delta \parallel 0^8$
Δrk_5	$0^{16} \parallel \delta \parallel 0^{24}$
Δrk_6	$\delta \parallel 0^{16} \parallel S(\delta) \parallel \delta \parallel 0^8$
Δrk_7	$0^8 \parallel S(\delta) \parallel 0^{24} \parallel S(\delta)$
Δrk_8	$\delta \parallel 0^{16} \parallel S(\delta) \parallel 0^{16}$
Δrk_9	$S(S(\delta)) \parallel S(\delta) \parallel \delta \parallel 0^8 \parallel \delta \parallel 0^8$
Δrk_{10}	$\delta \parallel 0^8 \parallel S(\delta) \parallel S(\delta) \parallel 0^{16}$
Δrk_{11}	$S(\delta) \parallel 0^{24} \parallel S((\delta)) \parallel S(\delta)$

分别分析 E_0 和 E_1 的截断差分特征传播, 见图2左侧。图2左侧 E_m 的上方为 E_0 , 下方为 E_1 。

图2中, 明文状态的截断差分字节以灰色表示, 非活跃字节以白色表示, 粉色表示轮密钥的截断差分字节。第 r 轮密钥中第 (i, j) 字节的差分记为 $\Delta rk_{i,j}^r$, 同理, ARK, SB, RR, MC操作后的内部状态中第 (i, j) 字节的差分分别表示为 $\Delta x_{i,j}^r$, $\Delta y_{i,j}^r$, $\Delta z_{i,j}^r$, $\Delta w_{i,j}^r$ 。根据表2, 对于给定的 $\Delta rk_{3,1}^1$, 设明文对为 $(p_i, p_i \oplus \Delta rk_{3,1}^1)$, 其中 $0 \leq i \leq 255$, 则第2, 3轮的轮密钥没有差分。因此第2, 3轮加密后, 中间状态也没有差分。当 w_3 和 rk_4 在第4轮进行异或时, 状态 x_4 被引入 $x_{1,1}^4$ 和 $\Delta x_{2,2}^4$ 。因截断差分经过比特级RR操作, $y_4 \rightarrow z_4$ 产生两种差分特征, 如图3展示。

图3左侧表示截断差分经过S盒与RR后在 $S_{2,1}$ 最左两比特为0的概率为 2^{-2} 。同理, 图3右侧表示截断差分经过S盒与RR后在 $S_{2,2}$ 最右6 bit为0的概率为 2^{-6} 。经过RR后, $S_{1,1}$ 和 $S_{2,1}$ 的差分状态活跃, 则经过MC后第1列的最小分支数为4, 即 $z_4 \rightarrow w_4$ 全扩散的概率近似于1。综上, 图2中 E_0 的概率为 2^{-4} 。

在下差分特征 E_1 中, 设置差分 $\nabla x_{1,1}^9$, $\nabla x_{2,1}^9$, $\nabla x_{3,1}^9$ 和 $\nabla x_{2,2}^9$ 与相应字节的 ∇rk_9 相抵消。因此, E_1 的概率为1。描述 E_0 和 E_1 的字节级截断差分SAT模型在5.2节展示。

3.2 构建 E_m

本文中, E_m 层的起始点位于第5轮的状态 x_5 , 并在第7轮的状态 w_7' 处结束, 如图2(b)所示。在 E_m 中, 如果上差分特征和下差分特征在相同位置的S盒都处于活跃状态, 称这两处的S盒为相互依赖的S盒, 简称为依赖S盒, 如图2(b)中差分 ρ_1 和 γ_1 所在S盒为依赖S盒。否则, 上差分或下差分特征处在同一位置上, 且只有1个S盒为活跃状态的, 称其为独立S盒。在图2(b)中, 红色字节表示该依赖S盒由上差分特征传播而来, 加密方向的差分特征传播被标记为红线。蓝色字节表示该依赖S盒是由下差分特征传播而来的, 解密方向的传播被标记为蓝线。上(下)差分特征中, 经异或操作后未确定活跃性的字节用橙色(绿色)表示。在第5轮中, $\Delta x_{3,1}^5$ 的活跃性是未确定的, 因为 $\Delta w_{3,1}^4$ 可能会与 $\Delta rk_{3,1}^5$ 抵消。在RR之后, $\Delta z_{2,1}^5$, $\Delta z_{3,1}^5$, $\Delta z_{2,2}^5$ 和 $\Delta z_{3,2}^5$ 的活跃性也无法确定, 从而MC后的差分活跃性也未知。因此, E_m 中的每个操作需要使用基于比特级SAT模型加以描述, 该模型在5.1节详述。

加密方向的差分在 w_7 已完全扩散, 但解密方向的差分在 w_7' 后的差分是非活跃的, 即两条差分特征在第7轮后互相独立。因此, E_m 层的结束位置在第7轮的MC。为了确保该飞去来器能够返回(即

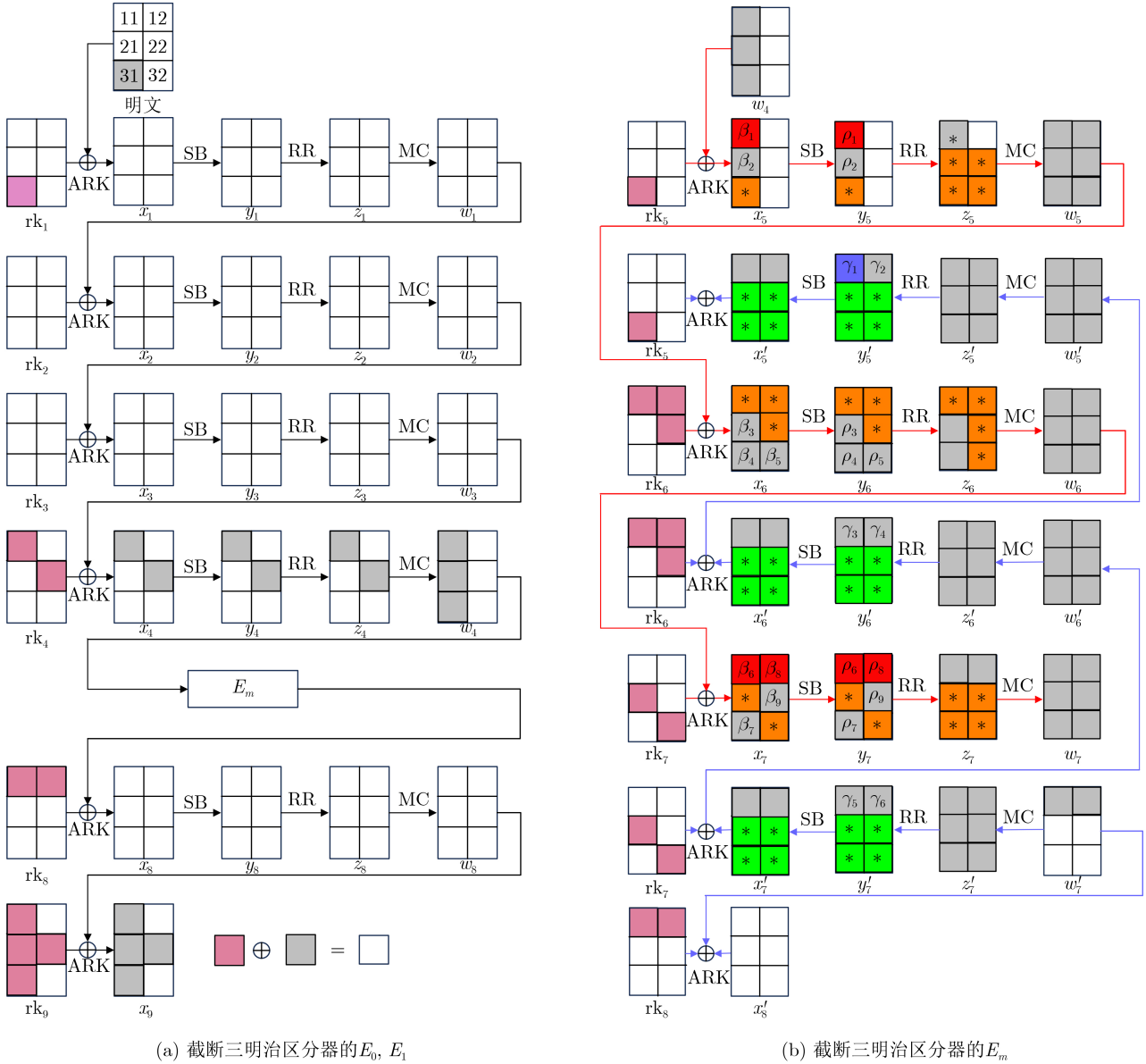


图2 截断三明治区分器

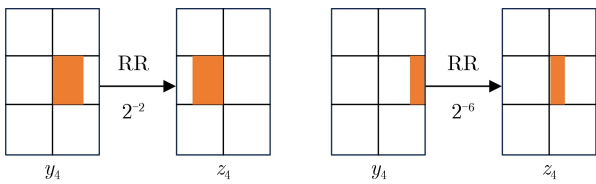


图3 活跃字节 $S_{2,2}$ 在RR下产生的两条差分特征

两条特征兼容), 3.3节将深入分析两条截断差分特征在 E_m 中的依赖关系。

3.3 E_0 与 E_1 兼容的概率计算

当固定 E_m 的输入差分和 E_m 的输出差分时, 差分特征 E_0 与 E_1 的依赖关系即 E_m 的概率概括为3层: (1) 两条差分特征在依赖S盒处的概率; (2) 下差分特征在靠近 E_m 结束位置的依赖S盒的差分值传播到 E_m 开始位置的依赖S盒差分值的概率; (3) 两条差

分特征中独立S盒影响依赖S盒的概率。综上, E_m 的总概率 $r = r' \cdot r''$, 其中 r' 由第1, 2层计算(式(1)), r'' 由第3层计算(式(2))。

设 E_m 中有 n 个依赖S盒, 第 R 轮为 E_m 的起始位置, 第 R' 轮为 E_m 的结束位置。在上差分特征中, 第 R 轮的第 i 个依赖S盒的输入差分记为 α_R^i , 下差分特征中该依赖S盒的输出差分记为 β_R^i 。特别地, β_R^i 是下差分特征中最接近 E_m 起始位置的差分。由于 E_m 的输入差分是截断的, 本文考虑了BCT所有可能的输入差分 α_R^i 和相应的输出差分 β_R^i 。则第 R 轮中 E_0 与 E_1 兼容性概率如式(4)所示

$$r'_R = \sum_{\beta_R^i} \sum_{\alpha_R^i} \frac{\text{BCT}(\alpha_R^i, \beta_R^i)}{2^n} \cdot \text{pr}(\beta_R^i \leftarrow \beta_{R'}^i) \quad (4)$$

其中, 式(4)的首个因子计算第1层, 即上差分特征

和下差分特征在第*i*个依赖S盒处的概率；第2个因子计算第2层，即下差分特征中的 $\beta_{R'}^i$ 传播到 β_R^i 的概率，其中 $\beta_{R'}^i$ 表示下差分特征中最接近 E_m 结束位置的差分。进一步， r' 由每轮的依赖S盒概率累乘所得，即 $\prod_{j=R}^{R'} r'_j$

$$r'_j = \sum_{\delta_j^i} \text{DDT}(\delta_j^i, \lambda_{j+1}^i) \quad (5)$$

式(5)计算第3层，即第*j*轮中的第*i*个独立S盒影响第*j+1*轮中第*i+1*个依赖S盒的差分值概率。进一步，

$$r' = \frac{\sum_{\beta_1} \text{BCT}(\beta_1, \gamma_1) \cdot \Pr\left(\gamma_1 \xrightarrow{3\text{-round}} \gamma_5\right) \cdot \sum_{\beta_6} \text{BCT}(\beta_6, \gamma_5) \cdot \sum_{\beta_8} \text{BCT}(\beta_8, \gamma_6)}{2^8 \cdot 2^{16} \cdot 2^8} \quad (6)$$

尽管上差分特征 $\beta_2 \rightarrow \rho_2$, $\beta_3 \rightarrow \rho_3$, $\beta_4 \rightarrow \rho_4$ 和 $\beta_5 \rightarrow \rho_5$ 与下差分特征相互独立，但会影响上差分特征中依赖S盒的差分值 β_6 与 β_8 ，则 r'' 计算为

$$r'' = \frac{\sum_{\beta_2} \text{DDT}(\beta_2, \rho_2) \cdot \sum_{\beta_3} \text{DDT}(\beta_3, \rho_3) \cdot \sum_{\beta_4} \text{DDT}(\beta_4, \rho_4) \cdot \sum_{\beta_5} \text{DDT}(\beta_5, \rho_5)}{2^8 \cdot 2^8 \cdot 2^8} \quad (7)$$

下差分特征的 $\beta_7 \rightarrow \rho_7$, $\beta_9 \rightarrow \rho_9$ 与上差分特征相互独立，因此其概率无需计算。综上所述，本节为HALFLOOP-48算法构建了一个8轮的截断三明治区分器，为精准计算区分器中 E_m 概率，第4节将重点阐述如何用SAT高效建模基于8比特S盒的差分分布表(Differential Distribution Table, DDT)和飞去来器连接表(BCT)。

4 基于仿射子空间的降维方法

自动化差分特征搜索技术(如MILP/SAT)在应用于AES等密码的大型S盒时，生成海量不等式或合取范式(Conjunctive Normal Form, CNF)而导致搜索失败。为高效建模此类大型S盒的DDT或BCT，本节提出一种基于仿射子空间的降维方法以减少所需约束的数量达到有效搜索差分特征的目的。

4.1 八维输入差分降为七维输入差分

本节通过使用*f*函数将八维输入差分向量降至七维

$$\left. \begin{aligned} f(2i-1) &= f(2i) = i, 1 \leq i \leq 127 \\ f(0) &= f(255) = 0 \end{aligned} \right\} \quad (8)$$

已知任意两个向量 $\mathbf{x}, \mathbf{y} \in \mathbb{F}_2^8$ 形成一个一维仿射子空间(即 $\{\mathbf{x}, \mathbf{y}\} = \mathbf{x} \oplus \{0, \mathbf{x} \oplus \mathbf{y}\}$)。因此，相邻输入差分 $2i-1$ 和 $2i$ 自然形成一个仿射子空间，可通过 $\{2i-1, 2i\}$ 映射到*i*实现八维输入差分到七维向量的有效降维。

4.2 八维输出差分降为七维输出差分

对于每个降维后的七维输入差分*i*，其对应的输出差分与传播概率通过以下3步构建：

r'' 由每轮独立S盒的概率累乘所得，即 $\prod_{j=R}^{R'} r''_j$ 。

3.4 E_m 概率的计算实例

本节将使用3.3节所述方法计算三明治区分器中 E_m 的概率。为方便读者理解，设图2(b)中上差分特征的橙色字节和下差分特征的绿色字节差分为0，即异或操作导致差分抵消。在第5轮中， $S_{1,1}$ 为依赖S盒；在第7轮中， $S_{1,1}, S_{1,2}$ 为依赖S盒，因此 $\beta_1 \rightarrow \gamma_1$, $\beta_6 \rightarrow \gamma_5$ 与 $\beta_8 \rightarrow \gamma_6$ 的传播概率可由BCT计算。此外，还需要确保差分传播 $\gamma_5 \rightarrow \gamma_1$ 存在，则 r' 的计算公式为

(1)对两个输出差分集合取交集 N^i ，并优化概率赋值。令 ΔO^i 表示DDT(或BCT)中输入差分为*i*的所有可能输出差分集合。交集 $N^i = \Delta O^{2i-1} \cap \Delta O^{2i}$, $1 \leq i \leq 127$ ，作为七维输入差分*i*的输出差分集合。设 $\beta \in N^i$ ，则降维后的差分特征*i* \rightarrow β 的概率

$\Pr(i \rightarrow \beta) = \max(\Pr(2i-1 \rightarrow \beta), \Pr(2i \rightarrow \beta))$ ，其中 $\max()$ 取两者中的最大值。该步保证在降维后的差分特征*i* \rightarrow β 中仍能体现降维前两条差分特征 $2i-1 \rightarrow \beta$ 与 $2i \rightarrow \beta$ 的存在。降维后差分特征概率取的是实际差分特征的概率，所以其概率也保证准确。

以HALFLOOP算法的BCT为例，输入差分0x01有127个非0输出差分，其中有124个概率为 2^{-7} 的输出差分，2个概率为 $2^{-5.415}$ 的输出差分，1个概率为 2^{-6} 的输出差分。输入差分0x02的输出差分同上，将其分为3种情况：(a)输入差分0x01和0x02有61个概率相同的输出差分；(b)有3个概率不同的非0输出差分；(c)其余64个输出差分在一个输入差分下为0，另一个输入差分下非0。因此，只采用前两种情况作为输出差分 β ，即 β 满足： $\#\{S(x \oplus 0x01) \oplus S(x) = \beta\} \neq 0$ ； $\#\{S(x \oplus 0x02) \oplus S(x) = \beta\} \neq 0$ 。

本步筛选了对于输入的七维差分*i*的不可能输出差分，并为保留的输出差分赋予最大的传播概率。

(2)将 N^i 中的元素按最高有效位划分。将 N_0^i 中的每个八维输出差分向量 (y_0, y_1, \dots, y_7) 根据其最高

有效位划分为两个互斥子集: $N_0^i = \{(y_1, y_2, \dots, y_7) \in N^i | y_0 = 0\}$, $N_1^i = \{(y_1, y_2, \dots, y_7) \in N^i | y_0 = 1\}$ 。

(3)附加二维概率向量。为 N_0^i 和 N_1^i 中的元素附加二维差分传播概率变量 (p_0, p_1) , 则差分特征 $i \rightarrow \beta$ 的概率为

$$\left. \begin{aligned} (p_0, p_1) = (0, 0), \text{ 概率为 } 1 \\ (p_0, p_1) = (0, 1), \text{ 概率为 } 2^{-7} \\ (p_0, p_1) = (1, 0), \text{ 概率为 } 2^{-6} \\ (p_0, p_1) = (1, 1), \text{ 概率为 } 2^{-5.415} \end{aligned} \right\} \quad (9)$$

基于上述3步, 8 bit S盒的BCT(或DDT)的1八维差分特征(八维输入差分、八维输出差分、二维概率)降为16维差分特征(七维输入差分、七维输出差分、二维概率)。最后利用自动化工具LogicFriday, 为HALFLOOP算法的BCT生成了8355个CNF子句, 其中建模 N_0^i 的子句为4 147个, 建模 N_1^i 的子句为4 208个。同样也为DDT生成了8 202个CNF子句。

4.3 PRESENT的4比特BCT降维实例

为阐述降维细节, 本节以PRESENT算法的4 bit S盒为例, 将高维差分特征向量降为两组低维子向量。如输入差分0x0011和0x0100分别对应9和10个可能的非零输出差分, 则差分特征 $0x010 \rightarrow \Delta O$ 的概率表示为

$$\left. \begin{aligned} (p_0, p_1) = (0, 0), \text{ 概率为 } 1 \\ (p_0, p_1) = (0, 1), \text{ 概率为 } 2^{-3} \\ (p_0, p_1) = (1, 0), \text{ 概率为 } 2^{-2} \\ (p_0, p_1) = (1, 1), \text{ 概率为 } 2^{-1} \end{aligned} \right\} \quad (10)$$

(1)生成输入差分0x0011和0x0100的所有可能且非重复的输出差分交集 N^3 , $N^3 = \{0010, 0110, 0111, 1000, 1001, 1010, 1011, 1100, 1101, 1110, 1111\}$ 。

(2)遍历 N^3 中所有元素。若元素的最高比特为0, 将其添加到 N_0^3 中, 则 $N_0^3 = \{010, 110, 111\}$ 。若最高比特为1, 将其添加到 N_1^3 中, 则 $N_1^3 = \{000, 001, 010, 011, 100, 101, 110, 111\}$ 。

(3)附加二维概率向量。对于降维后的输入差分 $0x010$, $N_0^3 = \{01000110, 01011001, 01011101\}$ 。 $N_1^3 = \{01000010, 01000110, 01001010, 01001110, 01010001, 01010101, 01011001, 01011101\}$ 。

由此, 十维的差分特征向量降维至八维(三维输入差分、三维输出差分和二维概率)。

5 基于SAT的三明治区分器搜索模型

本节构建了HALFLOOP-48算法的SAT搜索模型, 用于自动化搜索高概率的8轮截断三明治区分器。模型包含3部分: 字节级截断差分传播的 E_0 , E_1 , 及比特级截断差分传播的 E_m 。

5.1 E_m 比特级建模

为精细计算 E_0 和 E_1 在 E_m 的依赖关系, E_m 采用比特级建模, 其关键点如下:

调柄差分与中间状态差分抵消。中间状态差分会通过异或轮密钥差分来抵消。轮密钥差分(或内部状态差分)记为 Δ_1 (或 Δ_2), 异或后的差分记为 Δ_3 。对于第 i 个有效比特($0 \leq i \leq 7$)其抵消关系用CNF子句表达为

$$\left. \begin{aligned} \overline{\Delta_3[i]} = 1 \\ \Delta_1[i] = 1 \\ \Delta_2[i] = 1 \end{aligned} \right\} \quad (11)$$

解密方向约束条件。为匹配依赖S盒的BCT, 解密方向的输出差分需受到约束。 E_0 加密方向(或 E_1 解密方向)的第 i 个依赖S盒的差分值记为 Δ_{up}^i (或 ∇_{lo}^i), 其中 $0 \leq i \leq 7$

$$\left. \begin{aligned} \overline{\Delta_{up}^i} \vee \nabla_{lo}^i = 1 \\ \Delta_{up}^i \vee \overline{\nabla_{lo}^i} = 1 \end{aligned} \right\} \quad (12)$$

5.2 E_0, E_1 字节级建模

定义向量 $(v_1, v_2, \dots, v_{12}) \in \mathbb{F}_2^{12}$ 为每个操作中的差分特征。其中 v_i ($1 \leq i \leq 6$)表示输入差分中第 i 个S盒的活跃性, v_{i+6} ($1 \leq i \leq 6$)表示输出差分中第 $i+6$ 个S盒的活跃性。若该S盒活跃则变量 v 置为1, 否则置为0。

差分活跃的字节经SB后仍活跃, 但比特级RR操作会导致相邻列的字节活跃性受影响, 因此需要评估RR操作后字节活跃的概率。增加3个辅助变量 v_{13}, v_{14}, v_{15} 以表示受影响S盒活跃性的概率。若RR前 $S_{2,1}$ 活跃, 则001表示经过RR后 $S_{2,2}$ 活跃的概率为 2^{-2} , 100表示 $S_{2,1}$ 活跃的概率为 2^{-6} 。此外, 010表示第3行中活跃S盒任意传播的概率均为 2^{-4} 。对于MC操作, 当输入差分中的一列处于活跃时, 存在19个可能的差分传播情形, 其传播概率为1或 2^{-8} , 分别用01和10表示。

5.3 E_0, E_1 与 E_m 连接处建模

在字节级模型中, 用0和1表示字节活跃性, 但活跃字节具体的差分值无法知晓。因此当截断差分特征由 E_0 传播到 E_m 层(或 E_1 传播到 E_m 层)时, 需对字节级模型中的活跃S盒进行差分遍历以连接 E_m 中比特级截断差分。设 ΔXU^i 表示 E_0 结束轮(即 E_m 起始轮)的第 i 个S盒的活跃性, ∇XL^i 表示在 E_1 的起始轮(即 E_m 的结束轮)的第 i 个S盒的活跃性。设 ΔXM^j 表示 ΔXL^i 中第 j 个比特的活跃性。若 ΔXU^i 为活跃S盒, 则 E_0 与 E_m 连接的CNF子句为

$$\Delta XU^i \vee \Delta XM^j = 1, 0 \leq j \leq 7 \quad (13)$$

同理， E_m 和 E_1 连接的CNF子句为

$$\Delta XL^i \vee \Delta XM^j = 1, 0 \leq j \leq 7 \quad (14)$$

5.4 搜索8轮最优差分特征的目标函数

为最大化8轮截断三明治区分器的概率，目标函数设为

$$\min \left(6 \sum_{R=0}^{|E_m|-1} \sum_{n=0}^5 \sum_{m=0}^5 p_0 + 7 \sum_{R=0}^{|E_m|-1} \sum_{n=0}^5 \sum_{m=0}^5 p_1 + 5.415 \sum_{R=0}^{|E_m|-1} \sum_{n=0}^5 \sum_{m=0}^5 (p_0 + p_1) \right) \quad (15)$$

5.5 8轮HALFLOOP-48最优截断三明治区分器

使用上述目标函数，本文获得了 E_m 中161条概

率为 $2^{-46.83}$ 的3轮差分特征。图4展示了3轮截断差分特征的活跃字节情况。

表3给出了其中一条差分特征， E_0 覆盖 R_1 到 R_4 ， E_1 覆盖 R_8 和 R_9 中ARK之后的内部状态，剩余轮数被 E_m 包含。 \dagger 表示 E_m 中依赖S盒产生的概率。因为上差分特征和下差分特征存在依赖关系，所以同一轮中被 \dagger 标记的概率 r 在总概率中只统计1次。 E_m 中最优差分特征概率由 2^{-24} ， $2^{-10.83}$ ， 2^{-12} 3部分相乘得到。在加密方向，4条差分特征 $0x64 \rightarrow 0x33$ ， $0x38 \rightarrow 0x64$ ， $0xa4 \rightarrow 0x2a$ 和 $0x06 \rightarrow 0x0c$ 影响了 Δx_7 ，进而影响了 x_7 和 x_7' 之间的依赖关系，因此其概率基于DDT计算得到概率为 2^{-24} 。此外，两个依赖S盒的差分传播概率需要由BCT计算，即 $0x89 \rightarrow 0x25$ 和 $0xa0 \rightarrow 0x56$ ，

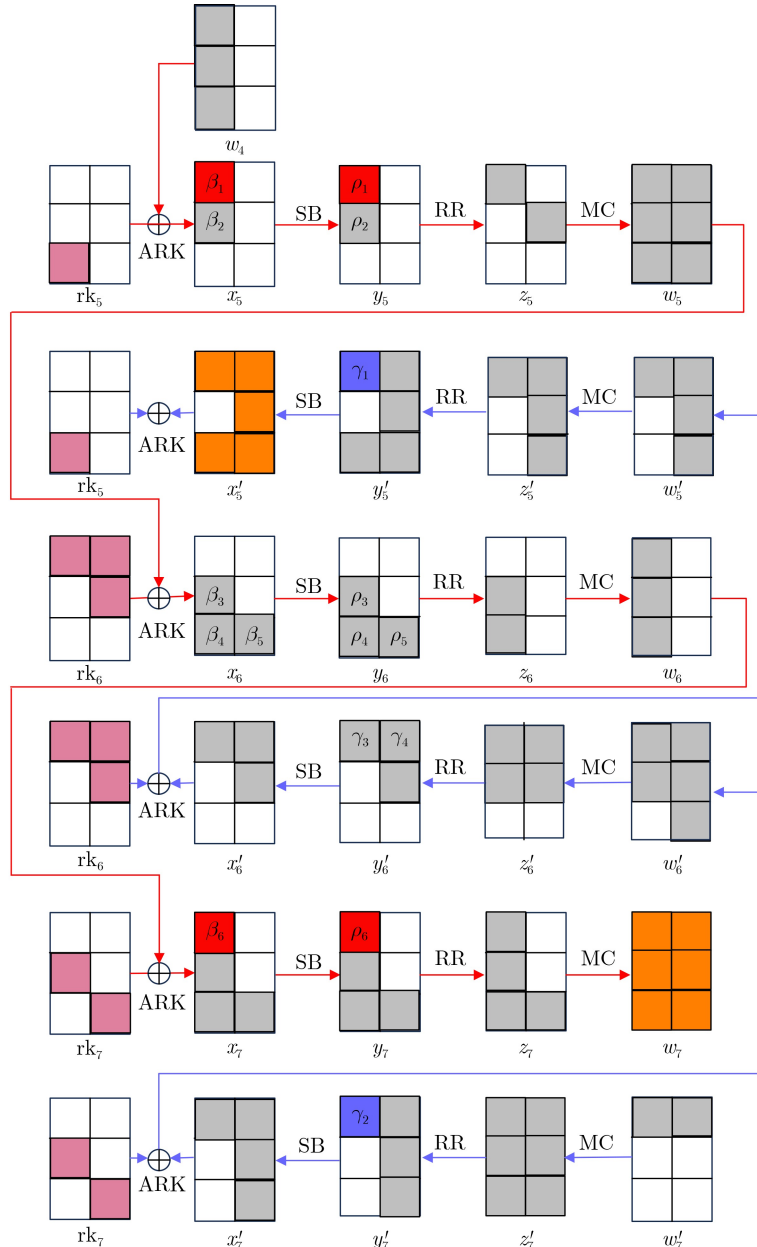


图4 E_m 的3轮最优截断差分

表3 HALFLOOP的8轮区分器

轮数	Δrk	Δx	Δy	Δw	r	轮数	∇rk	∇x	∇y	∇w	r	
上差分特征						下差分特征						
R_1	00 00	00 00	00 00	00 00	1	R_5	00 00	98 91	25 5b	fc ee	$2^{-11.415\uparrow}$	
	00 00	00 00	00 00	00 00			00 ca	00 17	00 3d			
	b0 00	b0 00	00 00	b0 00			b0 00	6c 60	33 ab	00 00		
R_2	00 00	00 00	00 00	00 00	1	R_6	b0 01	4c 76	4a 5b	d9 57	$2^{-18\uparrow}$	
	00 00	00 00	00 00	00 00			00 b0	00 8d	00 3e	db 27		
	00 00	00 00	00 00	00 00			00 00	00 00	00 00	00 00		
R_3	00 00	00 00	00 00	00 00	1	R_7	00 00	d9 57	56 38	b0 a0	$2^{-5.415\uparrow}$	
	00 00	00 00	00 00	00 00			db 00	00 27	00 af	00 00		
	00 00	00 00	00 00	00 00			00 db	00 db	00 da	00 00		
R_4	b0 00	b0 00	84 00	89 00	$(2^{-2})^2$	R_8	b0 a0	00 00	00 00	00 00	1	
	00 b0	00 b0	00 84	6c 00			00 00	00 00	00 00	00 00		
	00 00	00 00	00 00	b0 00			00 00	00 00	00 00	00 00		
R_5	00 00	89 00	c4 00	b0 01	$2^{-11.415\uparrow}$	R_9	c9 00	c9 00			$2^{-5.415\uparrow}$	
	00 00	6c 00	33 00	38 b0			a0 b0	a0 b0				
	b0 00	00 00	00 00	a4 06			b0 00	b0 00				
R_6	b0 01	00 00	00 00	a0 00	$2^{-18\uparrow}$							
	00 b0	38 00	64 00	aa 00								
	00 00	a4 06	2a 0c	30 00								
R_7	00 00	a0 00	83 00	4e 53	$2^{-5.415\uparrow}$							
	31 00	9b 00	77 00	98 a4								
	00 31	30 31	67 a4	1f f3								

两者概率相乘为 $2^{-10.83}$ 。在解密方向，下差分特征中的 $0x56 \rightarrow 0x25$ 以概率 2^{-12} 存在，确保了两条差分特征相互兼容。

计算 E_m 中截断差分特征的聚合效应。为找到其他概率的差分特征，固定图4中的活跃字节，遍历活跃字节中的差分，得到了2720条概率为 $2^{-47.83}$ 的差分特征。将概率为 $2^{-46.83}$ 和 $2^{-47.83}$ 的差分特征聚合，生成了概率为 $2^{-39.2}$ 的3轮最佳截断区分器。添加 E_0 与 E_1 的概率得到最优8轮截断区分器的概率为 $2^{-43.2}$ 。

实验验证。为确保差分路径的真实性，本文开展实验找到了一个符合该差分路径的明文4元组。按照表3中给定的上差分特征的输入差分构造明文对 (P_1, P_2) ，剩余字节固定为常量。随机生成 2^{36} 个密钥，对 2^7 个明文对加密8轮，得到 (X_8^1, X_8^2) 。然后解密 $(X_8^3, X_8^4) = (X_8^1 \oplus \nabla, X_8^2 \oplus \nabla)$ ，得到 (P_3, P_4) 。最终获得了一个符合该区分器的明文4元组 $(P_1, P_2, P_3, P_4) = (0x000000800000, 0x000000300000, 0xbabaabbcacaaa, 0xbaba7baaaa)$ 和密钥4元组 $(K_1, K_2, K_3, K_4) = (0x000000b00f0f, 0x00000000f0f, 0x000000000000, 0xc9a0b000b000)$ 。实验结果表明本文所构建的区分器真实有效。

6 全轮HALFLOOP-48密钥恢复攻击

使用上述概率为 $2^{-43.2}$ 的8轮截断三明治区分器，对HALFLOOP-48算法实施两种密钥恢复攻

击：相关调柄三明治攻击和相关调柄矩形攻击。为攻击全轮算法，本文在区分器的底部增加两轮^[17]。图5展示了对HALFLOOP-48算法完整轮数的攻击过程。

6.1 相关调柄三明治攻击

本攻击基于选择明/密文的方法^[9]。在攻击中，生成 s 个结构用于构建明文对，期望产生 y 个正确对。对于每个结构，分4个步骤进行攻击：

(1) 构造明文对。输入明文对 (P_1, P_2) ，令 $P_1[2] \oplus P_2[2] = \delta$ ，其余字节固定为常量。遍历 $\delta \in \mathbb{F}_2^8$ ，对于每个 δ ，产生 2^7 个明文对和 2^7 个调柄对 (T_1, T_2) 且令 $T_1[2] \oplus T_2[2] = \delta$ ，使得 (T_1, T_2) 与 (P_1, P_2) 的差分抵消。具体地，对于每个 δ ， P_1 都有唯一对应的 P_2 ，同时 T_1 有唯一对应的 T_2 。因此遍历 δ 共产生 $s \cdot 2^{15}$ 个 (P_1, P_2) 。

(2) 构建密文4元组 (C_1, C_2, C_3, C_4) 。加密明文对 (P_1, P_2) 以获得密文对 (C_1, C_2) 。对于每个 (C_1, C_2) ，遍历可能的 $\nabla C[0-2]$ ，构建密文对 $(C_3, C_4) = (C_1 \oplus \nabla C, C_2 \oplus \nabla C)$ ，产生 $y \cdot 2^{15+24}$ 个密文对。数据复杂度为 $\mathbb{D} = y \cdot 2^{39}$ 。

(3) 初始化计数器表CT和辅助表 $T_{\nabla C}$ 。表CT存储候选密钥 K 及其计数。对于每个表 $T_{\nabla C}$ ，其行标为中间状态 (X_{10}, X'_{10}) ，列标为 (X_9, X'_9) ，共同索引对应的猜测密钥。

(a) 猜测48 bit轮密钥 $rk_{11}[0-5]$ ，并根据密钥

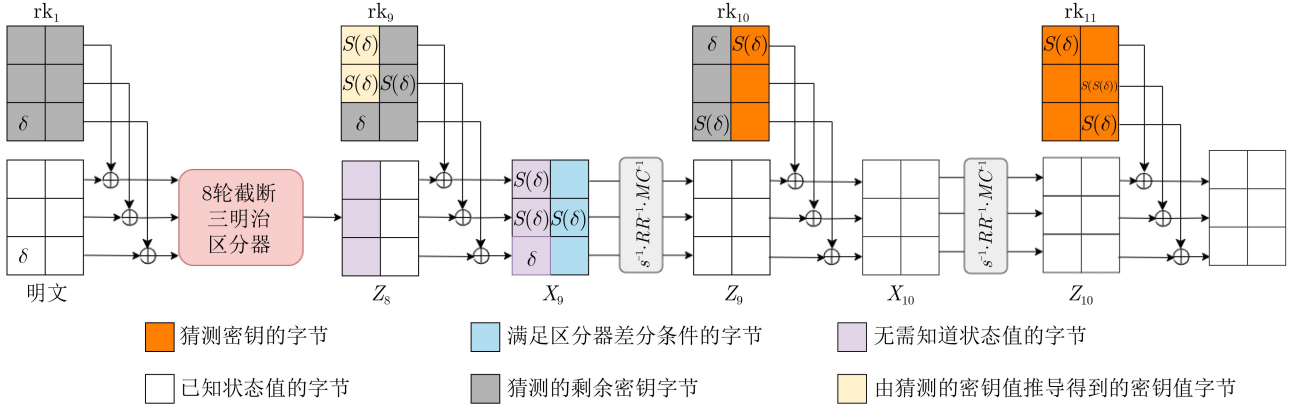


图5 对完整轮数HALFLOOP-48算法的密钥恢复攻击

编排算法推导出16比特轮密钥 $rk_9[0,1]$ 。由已知的 (C_1, C_3) 和猜测的 $rk_{11}[0-5]$ 解密计算 (X_{10}, X'_{10}) 。将猜测的密钥 $rk_{11}[0-5]$ (共 $\mathbb{D} \cdot 2^{48}$ 个)按照索引 (X_{10}, X'_{10}) 添加到表 $T_{\nabla C}$ 中。

(b)猜测24 bit $rk_{10}[3-5]$ 。用 $rk_{10}[3-5]$ 对 $(X_{10}[3-5], X'_{10}[3-5])$ 作 $S^{-1} \circ RR^{-1} \circ MC^{-1}$ 得到 $(X_9[3-5], X'_9[3-5])$ 。因此,将 2^{24} 个 $rk_{10}[3-5]$,按行索引 (X_{10}, X'_{10}) ,列索引 $(X_9[3-5], X'_9[3-5])$ 添加到 $T_{\nabla C}$ 中。进而保留 $T_{\nabla C}$ 中满足区分器构建的条件,即 $\Delta X_9^{1,2}, \Delta X_9^{2,2}, \Delta X_9^{3,2}$ 为0,因此表 $T_{\nabla C}$ 存储了 $y \cdot 2^{87+24} \cdot 2^{-24}$ 个值。

(c)猜测24 bit $rk_9[3-5]$ 。 $(X_9[3-5], X'_9[3-5])$ 和 $rk_9[3-5]$ 异或后,若 $\nabla Z_8[3-5] \neq 0$ 则删除相应的密钥。 $T_{\nabla C}$ 剩余表项约有 $y \cdot 2^{87+24} \cdot 2^{-24}$ 。

(d)对 $T_{\nabla C}$ 中剩余候选密钥在表CT中计数。

(4)选择表CT中计数最高的候选密钥作为最终候选密钥,其计数记为CNC。如果 $CNC \geq \tau$,则必须穷举剩余32比特密钥才能恢复正确的密钥。

复杂度分析。本文依据文献[11]开展密钥恢复攻击的复杂度分析。采集数据的时间复杂度为 $T_0 = \mathbb{D} = s \cdot 2^{39}$ 。猜测96比特密钥的时间复杂度为 $T_1 = \mathbb{D} \cdot s \cdot 2^{96}$ 。步骤(3)中(a)~(d)的时间复杂度为 $T_2 = \mathbb{D} \cdot s \cdot 2^{96} \cdot 2^{n-48-n-1}$,其中 2^{-48} 为猜测密钥时利用的48比特条件。在步骤(4)中,穷举搜索的时间复杂度为 $T_2 = 2^{128-96}$ 。对于一个正确的候选密钥来说,表 T_s 中符合区分器条件的剩余密钥服从二项式分布 $\mathbb{B}(N, p = 2^{-41.2})$,一个错误候选密钥则服从 $\mathbb{B}(N, p = 2^{-48})$ [18,19]。设候选密钥中没有正确密钥的概率记为 α ,错误密钥在候选密钥中的概率记为 β 。因此,该攻击成功的概率 P_s 等于 $1 - \alpha$ 。当明文数据量 N 足够多时, α 和 β 的计算为[11]

$$\alpha \approx \frac{p \cdot \sqrt{1 - (\tau - 1)/N}}{(p - (\tau - 1)/N) \cdot \sqrt{2 \cdot \pi \cdot (\tau - 1)}} \cdot \exp \left[-N \cdot D \left(\frac{\tau - 1}{N} \parallel p \right) \right] \quad (16)$$

$$\beta \approx \frac{(1 - p) \cdot \sqrt{\tau/N}}{\tau/(N - p) \cdot \sqrt{2 \cdot \pi \cdot N \cdot (1 - \tau/N)}} \cdot \exp \left[-N \cdot D \left(\frac{\tau}{N} \parallel p \right) \right] \quad (17)$$

将正确对数的阈值设为 $\tau = 1$,则成功概率PS为63%。设 $y=1$,则 $s = y \cdot 2^{1-n} \cdot 1/p = 2^{-5.8}$,因此总数据复杂度为 $2^{32.8}$,总存储复杂度为 $2^{32.8} \cdot 2^8 \cdot 4 = 2^{42.8}$,总时间复杂度为 $T_0 + T_1 + T_2 + T_3 = 2^{92.2}$ 。

6.2 相关调柄矩形攻击

相关调柄三明治攻击可以转换为相关调柄矩形攻击。对明文4元组 (P_1, P_2, P_3, P_4) 进行加密,满足 $P_1[2] \oplus P_2[2] = P_3[2] \oplus P_4[2]$ 以获取密文4元组 (C_1, C_2, C_3, C_4) 。为满足区分器的差分特征条件,删除产生 $C_1 = C_3$ 且 $C_2 = C_4$ 的明文4元组。因此,对于每个 δ ,加密 2^{14} 个明文4元组,获得相应的 2^{14} 个密文4元组。对于 2^8 个 δ ,攻击的数据复杂度为 $y \cdot 2^{22}$,时间复杂度为 $T_0 = y \cdot 2^{22}$, $T_1 = s \cdot \mathbb{D} \cdot 2^{96}$, $T_2 = s \cdot \mathbb{D}^2 \cdot 2^{96} \cdot 2^{-98}$ 。当 $y=1, s = 2^{-5.8}$ 时,数据复杂度减小到 $2^{16.2}$,存储复杂度减小到 $2^{26.2}$ 。

7 结论

由于HALFLOOP的行移位和列混合操作加速了差分的扩散,难以实现对HALFLOOP算法的全轮差分攻击。为克服此难题,本文融合了字节级和比特级方法构建截断差分三明治区分器。本区分器确保了两条截断差分特征是兼容的,并且以高概率覆盖更多轮数。此外,本文对大型S盒的SAT建模提出了一种基于仿射子空间降维的新方法,本方法

也可为建模其他大型S盒提供新思路。进一步,所提截断差分三明治区分器的构建方法也可以应用到类似AES结构的其他轻量级密码算法。本文结果说明HALFLOOP-48无法抵抗相关调柄场景下的差分攻击。

参考文献

- [1] Department of Defense. MILSTD-188-141D Interoperability and performance standards for medium and high frequency radio systems[S]. Washington: Department of Defense, 2017.
- [2] DANSARIE M, DERBEZ P, LEANDER G, *et al.* Breaking HALFLOOP-24[J]. *IACR Transactions on Symmetric Cryptology*, 2022, 2022(3): 217–238. doi: [10.46586/tosc.v2022.i3.217-238](https://doi.org/10.46586/tosc.v2022.i3.217-238).
- [3] LEANDER G, RASOOLZADEH S, and STENNES L. Cryptanalysis of HALFLOOP block ciphers: Destroying HALFLOOP-24[J]. *IACR Transactions on Symmetric Cryptology*, 2023, 2023(4): 58–82. doi: [10.46586/tosc.v2023.i4.58-82](https://doi.org/10.46586/tosc.v2023.i4.58-82).
- [4] LIN Yunxue and SUN Ling. Related-tweak and related-key differential attacks on HALFLOOP-48[C]. The 22nd International Conference on Applied Cryptography and Network Security, Abu Dhabi, United Arab Emirates, 2024: 355–377. doi: [10.1007/978-3-031-54776-8_14](https://doi.org/10.1007/978-3-031-54776-8_14).
- [5] WAGNER D A. The boomerang attack[C]. The 6th International Workshop on Fast Software Encryption, Rome, Italy, 1999: 156–170. doi: [10.1007/3-540-48519-8_12](https://doi.org/10.1007/3-540-48519-8_12).
- [6] MURPHY S. The return of the cryptographic boomerang[J]. *IEEE Transactions on Information Theory*, 2011, 57(4): 2517–2521. doi: [10.1109/TIT.2011.2111091](https://doi.org/10.1109/TIT.2011.2111091).
- [7] DUNKELMAN O, KELLER N, and SHAMIR A. A practical-time related-key attack on the KASUMI cryptosystem used in GSM and 3G telephony[C]. The 30th Annual Cryptology Conference on Advances in Cryptology, Santa Barbara, USA, 2010: 393–410. doi: [10.1007/978-3-642-14623-7_21](https://doi.org/10.1007/978-3-642-14623-7_21).
- [8] BIRYUKOV A and KHOVRATOVICH D. Related-key cryptanalysis of the full AES-192 and AES-256[C]. The 15th International Conference on the Theory and Application of Cryptology and Information Security, Tokyo, Japan, 2009: 1–18. doi: [10.1007/978-3-642-10366-7_1](https://doi.org/10.1007/978-3-642-10366-7_1).
- [9] 谭林, 曾新皓, 刘加美. AES-192的相关密钥飞去来器攻击和矩形攻击[J]. *密码学报(中英文)*, 2024, 11(5): 1018–1028. doi: [10.13868/j.cnki.jcr.000723](https://doi.org/10.13868/j.cnki.jcr.000723).
TAN Lin, ZENG Xinhao, and LIU Jiamei. Related-key boomerang and rectangle attacks on AES-192[J]. *Journal of Cryptologic Research*, 2024, 11(5): 1018–1028. doi: [10.13868/j.cnki.jcr.000723](https://doi.org/10.13868/j.cnki.jcr.000723).
- [10] CID C, HUANG T, PEYRIN T, *et al.* Boomerang connectivity table: A new cryptanalysis tool[C]. The 37th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Tel Aviv, Israel, 2018: 683–714. doi: [10.1007/978-3-319-78375-8_22](https://doi.org/10.1007/978-3-319-78375-8_22).
- [11] SONG Ling, ZHANG Nana, YANG Qianqian, *et al.* Optimizing rectangle attacks: A unified and generic framework for key recovery[C]. The 28th International Conference on the Theory and Application of Cryptology and Information Security, Taipei, China, 2022: 410–440. doi: [10.1007/978-3-031-22963-3_14](https://doi.org/10.1007/978-3-031-22963-3_14).
- [12] BOURA C and COGGIA D. Efficient MILP modelings for Sboxes and linear layers of SPN ciphers[J]. *IACR Transactions on Symmetric Cryptology*, 2020, 2020(3): 327–361. doi: [10.13154/tosc.v2020.i3.327-361](https://doi.org/10.13154/tosc.v2020.i3.327-361).
- [13] ANKELE R and KÖLBL S. Mind the gap - a closer look at the security of block ciphers against differential cryptanalysis[C]. The 25th International Conference on Selected Areas in Cryptography, Calgary, Canada, 2018: 163–190. doi: [10.1007/978-3-030-10970-7_8](https://doi.org/10.1007/978-3-030-10970-7_8).
- [14] MA Sudong, JIN Chenhui, SHI Zhen, *et al.* Correlation attacks on snow-v-like stream ciphers based on a heuristic MILP model[J]. *IEEE Transactions on Information Theory*, 2024, 70(6): 4478–4491. doi: [10.1109/TIT.2023.3326348](https://doi.org/10.1109/TIT.2023.3326348).
- [15] DAEMEN J and RIJMEN V. The Design of Rijndael: AES - The Advanced Encryption Standard[M]. Berlin, Heidelberg: Springer, 2002. doi: [10.1007/978-3-662-04722-4](https://doi.org/10.1007/978-3-662-04722-4).
- [16] 蒋梓龙, 金晨辉. 对TweAES的相关调柄多重不可能差分攻击[J]. *电子与信息学报*, 2023, 45(1): 344–352. doi: [10.11999/JEIT211147](https://doi.org/10.11999/JEIT211147).
JIANG Zilong and JIN Chenhui. Related-tweak multiple impossible differential attack for TweAES[J]. *Journal of Electronics & Information Technology*, 2023, 45(1): 344–352. doi: [10.11999/JEIT211147](https://doi.org/10.11999/JEIT211147).
- [17] 张丽, 吴文玲, 张蕾, 等. 基于交换等价的缩减轮AES-128的密钥恢复攻击[J]. *计算机研究与发展*, 2021, 58(10): 2213–2221. doi: [10.7544/issn1000-1239.2021.20210549](https://doi.org/10.7544/issn1000-1239.2021.20210549).
ZHANG Li, WU Wenling, ZHANG Lei, *et al.* Key-recovery attack on reduced-round AES-128 using the exchange-equivalence[J]. *Journal of Computer Research and Development*, 2021, 58(10): 2213–2221. doi: [10.7544/issn1000-1239.2021.20210549](https://doi.org/10.7544/issn1000-1239.2021.20210549).
- [18] BLONDEAU C, GÉRARD B, and TILLICH J P. Accurate estimates of the data complexity and success probability for various cryptanalyses[J]. *Design Codes Cryptography*, 2011, 59(1/3): 3–34. doi: [10.1007/S10623-010-9452-2](https://doi.org/10.1007/S10623-010-9452-2).
- [19] 严智广, 韦永壮, 叶涛. 全轮超轻量级分组密码PFP的相关密钥差分分析[J]. *电子与信息学报*, 2025, 47(3): 729–738. doi: [10.11999/JEIT240782](https://doi.org/10.11999/JEIT240782).
- [20] YAN Zhiguang, WEI Yongzhuang, and YE Tao. Related-key differential cryptanalysis of full-round PFP ultra-

lightweight block cipher[J]. *Journal of Electronics & Information Technology*, 2025, 47(3): 729–738. doi: 10.11999/JEIT240782.

张文英：女，教授，博士生导师，研究方向为哈希函数、分组密码算法设计与分析、口令安全。

苑兆忠：男，副教授，研究方向为信息安全。

孙晓萌：女，博士生，研究方向为分组密码算法的安全性分析。

责任编辑：余蓉

Improved Related-tweak Attack on Full-round HALFLOOP-48

SUN Xiaomeng ZHANG Wenyong YUAN Zhaozhong

(School of Information Science and Engineering, Shandong Normal University, Jinan 250358, China)

Abstract:

Objective HALFLOOP is a family of tweakable AES-like lightweight block ciphers used to encrypt automatic link establishment messages in fourth-generation high-frequency radio systems. Because the RotateRows and MixColumns operations diffuse differences rapidly, long differentials with high probability are difficult to construct, which limits attacks on the full cipher. This study examines full HALFLOOP-48 and evaluates its resistance to sandwich attacks in the related-tweak setting, a critical method in lightweight-cipher cryptanalysis.

Methods A new truncated sandwich distinguisher framework is proposed to attack full HALFLOOP-48. The cipher is decomposed into three sub-ciphers, E_0 , E_1 . A model is built by applying an automatic search method based on the Boolean Satisfiability Problem (SAT) to each part: byte-wise models for E_0 , E_1 and a bit-wise model for E_m . For E_m , a method is proposed to model large S-boxes using SAT, the Affine subspace Dimensional Reduction method (ADR). ADR converts the modeling of a high-dimensional set into two sub-problems for a low-dimensional set. ADR ensures that the SAT-searched differentials exist and that their probabilities are accurate, while reducing the size of Conjunctive Normal Form (CNF) clauses. It also enables the SAT method to search longer differentials efficiently when large S-boxes appear. To improve probability accuracy in E_m , dependencies between E_0 and E_1 are evaluated across three layers, and their probabilities are multiplied. Two key-recovery attacks, a sandwich attack and a rectangle-like sandwich attack, are mounted on the distinguisher in the related-tweak scenario.

Results and Discussions The SAT-based model reveals a critical weakness in HALFLOOP-48. A practical sandwich distinguisher for the first 8 rounds with probability $2^{-43.415}$ is identified. An optimal truncated sandwich distinguisher for 8-round HALFLOOP-48 with probability $2^{-43.2}$ is then established by exploiting the clustering effect of the identified differentials. Compared with earlier results, this distinguisher is practical and extends the reach by two rounds. Using the 8-round distinguisher, both a sandwich attack and a rectangle-like sandwich attack are mounted on full-round HALFLOOP-48 under related tweaks. The sandwich attack requires data complexity of $2^{32.8}$, time complexity $2^{92.2}$ and memory complexity $2^{42.8}$. For the rectangle-like sandwich attack, the data complexity is $2^{16.2}$, with time complexity $2^{99.2}$ and memory complexity $2^{26.2}$. Compared with the previous results, these attacks reduce time complexity by $2^{25.4}$ and memory complexity by 2^{10} .

Conclusions To handle the rapid diffusion of differences in HALFLOOP, a new perspective on sandwich attacks based on truncated differentials is developed by combining byte-wise and bit-wise models. The models for E_0 and E_1 are byte-wise and extend these two parts forward and backward into E_m , which is based on bit-wise. To efficiently model the 8-bit S-box in the layer E_m , which is bit-wise. To model the 8-bit S-box in E_m efficiently, an affine subspace dimensional reduction approach is proposed. This model ensures compatibility between the two truncated differential trails and covers as many rounds as possible with high probability. It supports a new 8-round truncated boomerang distinguisher that outperforms previous distinguishers for HALFLOOP-48. Based on this 8-round truncated boomerang distinguisher, a key-recovery attack is achieved with success probability 63%. The results show that (1) the ADR method offers an efficient way to apply large S-boxes in lightweight ciphers, (2) the truncated boomerang distinguisher construction can be applied to other AES-like lightweight block ciphers, and (3) HALFLOOP-48 does not provide an adequate security margin for use in the U.S. military standard.

Key words: Lightweight block cipher; Related-tweak attack; Truncated sandwich distinguisher; Boolean SATisfiability problem (SAT); Key recovery attack