SIMECK密码的差分中间相遇攻击改进

张 奕,吕广秋*,金晨辉,崔 霆
(网络空间部队信息工程大学,河南郑州 450001)

摘 要: Boura等人在CRYPTO 2023上提出的差分中间相遇分析(Differential Meet-in-the-middle Cryptanalysis,DMC)是一种基于中间相遇思想实施差分攻击的新型密码分析方法。凭借概率扩展(Probabilistic Extension,PE)、限制条件(Imposed Condition,IC)与并行分割(Parallel Partition,PP)技术在降低时间、数据复杂性与扩展攻击轮数上的优势,差分中间相遇攻击已在多个采用线性密钥生成算法的分组密码上取得了显著效果。然而,目前的DMC还存在两点不足:一是概率扩展后的差分区分器概率$2^{-p'}$经常小于2^{2-n}(n是密码的分组规模),会导致限制条件技术失效而无法将攻击的数据复杂性维持在非全码本(全码本攻击通常被认为是无效攻击)。虽然已有工作使用明文结构缓解这个问题,但其并没有与并行分割技术很好结合。二是受SIMECK密码中非线性密钥生成算法的影响,近期关于此密码的DMC无法有效恢复主密钥。具体来说,这些工作只恢复了轮次分散的子密钥,导致进一步推导主密钥的代价超出上界。围绕上述两个问题,本文提出了基于尾接技术的DMC模型。此模型不再按照密码算法头尾来分割待恢复的密钥,而是将尾部的部分密钥视作头部密钥,使攻击中头部轮数减少而尾部轮数增加,从而获得三重优势:一是头部轮数减少会导致差分扩散不充分,便于使用明文结构降低攻击的数据复杂性;二是将更多的被分割密钥集中在密码算法尾部的连续轮,显著降低了推导主密钥的代价;三是利用尾部相邻子密钥间更清晰的制约关系提前排除掉不可能的密钥穷举值。基于上述模型,本文能够有效结合明文结构与并行分割技术,不仅解决了原有攻击在$n-1>p'>n-2$时无法实现非全码本复杂性的问题,还提升了DMC对于采用非线性密钥生成算法的密码的分析能力。作为应用,本文分别提出了对23轮SIMECK32、31轮SIMECK48和41轮SIMECK64的主密钥恢复攻击。据我们所知,在所有能够恢复主密钥的差分攻击中,本文对SIMECK三个版本的攻击均是轮数最长的攻击。

关键词: 差分中间相遇分析;SIMECK分组密码;非线性密钥生成算法;尾接技术;并行分割技术;明文结构
基金项目: 国家自然科学基金(No.62372463,No.62302518);河南省青年人才托举工程(No.2025HYTP036)
中图分类号: TN918.1;TP309.7 **文献标识码:** A **文章编号:** 0372-2112(2026)04-1820-13
电子学报URL:http://www.ejournal.org.cn **DOI:**10.12263/DZXB.20251191

Improved Differential Meet-in-the-Middle Attack against Cipher SIMECK

ZHANG Yi, LÜ Guangqiu*, JIN Chenhui, CUI Ting
(*Cyber Space Force Information Engineering University*, *Zhengzhou*, *Henan* 450001, *China*)

Abstract: Differential meet-in-the-middle cryptanalysis (DMC), proposed by Boura et al. at CRYPTO 2023, is a novel method to mount differential attacks based on the meet-in-the-middle idea. Benefiting from the advantages of the probabilistic extension (PE), imposed condition (IC) and parallel partition (PP) techniques in reducing time and data complexities and extending attack rounds, differential meet-in-the-middle attacks have achieved significantly improved results on many block ciphers employing linear key schedules. However, two limitations of the existing DMC remain. Firstly, the probability of the differential distinguisher under PE, denoted by $2^{-p'}$, is often below 2^{2-n} (where n is the block size), causing the IC technique to fail to maintain the non-full-codebook data complexity—a scenario usually deemed invalid for attacks. Although the plaintext structure technique has been adopted in some studies as a mitigation, its integration with the PP technique remains inadequate. Secondly, owing to the nonlinear key schedule of the SIMECK cipher, recent DMC attacks have been unable to recover the master key effectively. Specifically, these attacks only recover round keys with scattered round numbers, making the cost of deriving the master key unacceptable. Motivated by the two issues above, this paper introduces a new DMC model based on the tail-jointing technique. Rather than partitioning the key bits to be enumerated according to position, this model treats some tail key bits as head key bits, yielding fewer head rounds and more tail rounds, thereby offering three advantages. First, fewer head rounds cause insufficient differential diffusion, enabling the use of plaintext structures to reduce data complexity. Second, more key bits concentrated in consecutive tail rounds significantly lowers the cost of master key derivation. Third, more explicit constraints between adjacent tail key bits enable early elimination of impossi-

收稿日期:2026-02-03;录用日期:2026-03-25;责任编辑:宋甲英
*通信作者:吕广秋

ble enumerations. Based on the above model, this paper effectively integrates the plaintext structure technique with the PP technique to achieve non-full-codebook data complexity when $n-1>p'>n-2$, and strengthens DMC's effectiveness in analyzing ciphers that adopt a nonlinear key schedule. As an application, this paper proposes master key recovery attacks on 23-round SIMECK32, 31-round SIMECK48, and 41-round SIMECK64, respectively. As far as we know, among all differential attacks capable of recovering master keys, our attacks on the three versions of SIMECK achieve the longest rounds.

Keywords: differential meet-in-the-middle attack; SIMECK block cipher; nonlinear key schedule; tail-jointing technique; parallel partition technique; plaintext structure

Foundation Item(s): National Natural Science Foundation of China (No.62372463, No.62302518); Young Elite Scientists Sponsorship Program of Henan (No.2025HYTP036)

0　引言

中间相遇分析[1]和差分分析[2]是分组密码安全性分析的两种基础性方法。为了降低穷举密钥的代价,前者将密钥分割处理并建立两部分密钥的内在联系,后者利用密码输入、输出差分分布中的高概率的差分特征(即差分区分器)来高效区分正确、错误密钥。Boura等人[3]在CRYPTO 2023上结合差分分析与中间相遇分析的核心思想,提出了差分中间相遇分析(Differential Meet-in-the-middle Cryptanalysis,DMC),并提出了扩展攻击轮数的并行分割(Parallel Partition,PP)技术与降低数据复杂性的限定条件(Imposed Condition,IC)技术。随后Ahmadian等人[4]在EUROCRYPTO 2024上将DMC推广到截断型DMC,放宽了并行分割的使用条件,并结合差分分析中的状态猜测技术、概率扩展技术优化密钥猜测策略。在ASIACRYPT 2024上,Song等人[5]提出了先局部使用DMC,再对剩余部分使用传统差分攻击的广义DMC,以更好地平衡时间、内存、存储复杂性,并用明文结构优化了数据复杂性。在ASIACRYPT 2025上,M'Foukh等人[6]进一步推广了概率扩展与状态猜测在差分中间相遇分析上的应用,用一种形似Demirci-Selçuk中间相遇攻击[7-8]的方式构建DMC。总的来说,DMC已在众多采用线性密钥生成算法的密码上取得了突出结果。

SIMON和SPECK[9]是美国国家安全局在2013年设计的两种轻量级分组密码,因为轮函数简单而得到了大量第三方安全性分析。SIMECK是Yang等人[10]结合SIMON和SPECK两者的特点在CHES 2015上提出的类SIMON分组密码,其使用的是非线性密钥生成算法。目前为止,文献[11-15]从轮函数差分概率精确计算、最优差分特征、差分特征的聚合效应等方面对类SIMON密码的差分性质进行了充分的研究,此外还有大量工作从差分活跃情况、基于MILP的高概率差分特征的搜索[16-17]等方面分析广义Feistel结构密码的差分性质,本文关注的重点是如何利用这些差分性质更好地恢复主密钥。

最近,文献[18]补全了文献[5]中广义DMC缺失的并行分割技术。文献[19]针对类SIMON密码结构提出了一种不同于文献[20]的动态密钥猜测技术,他们称之为密钥选择猜测技术,并采用约束规划来寻找最优的攻击方案。Michel和M'Foukh[21]基于类SIMON密码多个旋转等价差分特征改进了限定条件技术的优化效果。

该工作面临的问题与挑战主要有以下两点:(1)正如文献[14,21]指出,对于非线性密钥生成算法,子密钥与主密钥之间的关系随轮次增大而变得愈发复杂,此时无法像线性密钥生成算法那般低成本地推导出主密钥。这一事实早已体现于针对SIMON与SIMECK的相关密钥分析工作[22-26]中,但直到近期应用DMC分析SIMECK[19,21]时仍未有较好的措施;(2)DMC通常需用限定条件技术[3]来维持非全码本的数据复杂性(即复杂性小于2^n),然而此技术要求$p'\leqslant n-2$($2^{-p'}$是概率扩展下的差分区分器概率,n是密码的分组规模)。虽然使用文献[5,27]中的明文结构可以降低数据复杂性,但他们并未给出与并行分割技术结合的方法,无法发挥并行分割技术对攻击的显著提升效果。

针对上述问题与挑战,本文对差分中间相遇攻击的改进如下:

(1)基于尾接技术建立了新的DMC模型。新模型较原有模型额外增加了密码$E^k=E_1^{k_{\text{in}}^{(1)}}\circ\tau^{k_c}\circ E_2^{k_{\text{out}}}\circ E_3^{k_m}\circ E_0^{k_{\text{in}}^{(0)}}$的尾接部分$E_1^{k_{\text{in}}^{(1)}}$,此部分将原本应向$E_0^{k_{\text{in}}^{(0)}}$扩展的部分续接到$\tau^{k_c}$尾部,不仅使待恢复的子密钥被均匀分割,还使其中更多比特聚集在连续轮中,从而减少推导主密钥所需的穷举量,并可基于相邻密钥的简单关系建立更多密钥制约关系,加速错误密钥的筛选。

(2)基于上述模型,结合明文结构与并行分割技术,解决了原有基于并行分割技术的DMC在$n-1\geqslant p'>n-2$时无法实现非全码本复杂性的问题。

(3)将上述技术应用于SIMECK密码,建立了更多密钥关系并降低了恢复主密钥的难度,分别得到了SIMECK32、SIMECK48和SIMECK64的23、31和41轮主密钥恢复攻击。据我们所知,在以恢复主密钥为目标的差分攻击中,本文结果的攻击轮数最长。相关结果如表1所示。

表1 SIMECK的主要结果

Table 1 The main attack results against SIMECK

版本	攻击轮数/完整轮数	攻击方法	数据复杂性	时间复杂性	存储复杂性	成功率/%	时间复杂性÷成功率	是否恢复主密钥	出处
SIMECK32	21/32	差分中间相遇	2^{32}	$2^{63.64}$	2^{20}	63.2	$2^{64.303}$	否	文献[19]
	22/32	差分	2^{32}	$2^{57.9}$	—	47.1	$2^{58.987}$	否	文献[28]
	22/32	差分	2^{31}	2^{57}	—	36.0	$2^{58.474}$	是	文献[14]
	23/32	线性	$2^{31.91}$	$2^{61.78}$	—	53.2	$2^{62.691}$	是	文献[29]
	23/32	差分中间相遇	$2^{31.02}$	$2^{61.47}$	$2^{41.02}$	63.2	$2^{62.133}$	是	本文
	23/32	线性	$2^{31.5}$	2^{58}	—	7.0	$2^{61.837}$	是	文献[14]
	24/32	差分中间相遇	2^{31}	2^{63}	—	63.2	$2^{63.663}$	否	文献[21]
SIMECK48	28/36	差分	2^{46}	$2^{68.3}$	—	46.8	$2^{69.396}$	否	文献[28]
	29/36	差分中间相遇	2^{47}	$2^{93.28}$	2^{36}	63.2	$2^{93.943}$	否	文献[19]
	30/36	线性	$2^{47.66}$	$2^{92.2}$	—	86.7	$2^{92.406}$	是	文献[29]
	30/36	差分	2^{47}	2^{85}	—	6.0	$2^{89.059}$	是	文献[14]
	31/36	差分中间相遇	$2^{47.42}$	$2^{94.94}$	$2^{50.42}$	63.2	$2^{95.602}$	是	本文
	32/36	线性	2^{47}	2^{87}	—	10.0	$2^{90.322}$	是	文献[14]
	33/36	差分中间相遇	2^{48}	$2^{95.27}$	2^{71}	63.2	$2^{95.933}$	否	文献[21]
SIMECK64	35/44	差分	2^{63}	$2^{116.3}$	—	55.5	$2^{117.150}$	否	文献[28]
	35/44	差分中间相遇	2^{63}	$2^{125.49}$	2^{39}	63.2	$2^{126.153}$	否	文献[19]
	37/44	线性	$2^{63.09}$	$2^{121.25}$	—	47.7	$2^{122.318}$	是	文献[29]
	40/44	差分	2^{63}	2^{121}	—	19.0	$2^{123.396}$	是	文献[14]
	40/44	差分	2^{64}	2^{122}	—	55.0	$2^{122.863}$	是	文献[14]
	41/44	差分中间相遇	2^{63}	$2^{126.21}$	2^{92}	63.2	$2^{126.873}$	否	文献[21]
	41/44	差分中间相遇	$2^{63.41}$	$2^{126.19}$	$2^{62.41}$	63.2	$2^{126.852}$	是	本文
	42/44	线性	$2^{63.5}$	2^{120}	—	8.0	$2^{123.644}$	是	文献[14]

1 基础知识

1.1 符号说明

本文符号说明见表2。

1.2 SIMECK密码简介

SIMECKn[10]是基于Feistel结构设计的分组密码，分组规模为n，密钥规模为$2n$，旋转常数为$(a,b,c)=(0,5,1)$。根据参数$n\in\{32,48,64\}$可将SIMECK分成三个版本，相应的轮数分别为32、36、44。

加密算法。如图1所示，将明文$P\in\{0,1\}^n$载入SIMECK的第1轮输入状态$(X^{(1)},X^{(0)})=P$后，利用子密钥$k^{(1)},k^{(2)},\cdots,k^{(r)}\in\{0,1\}^{n/2}$，经过$r$轮轮函数后可得密文$C=(X^{(r+1)},X^{(r)})\in\{0,1\}^n$。当$i=1,2,\cdots,r$时，第$i$轮轮函数$R_i:\{0,1\}^n\to\{0,1\}^n$将$(X^{(i)},X^{(i-1)})$映射为$(X^{(i+1)},X^{(i)})$，使$X^{(i+1)}=S^a(X^{(i)})\odot S^b(X^{(i)})\oplus S^c(X^{(i)})\oplus X^{(i-1)}\oplus k^{(i)}\overset{\text{定义}}{=}F_{(a,b,c)}(X^{(i)})\oplus X^{(i-1)}\oplus k^{(i)}$。

密钥生成算法。给定主密钥$k=k^{(4)}\|k^{(3)}\|k^{(2)}\|k^{(1)}\in\{0,1\}^{2n}$，依次取$i=1,2,\cdots,r-4$即可得到子密钥$k^{(i+4)}=F_{(0,5,1)}(k^{(i+1)})\oplus k^{(i)}\oplus c^{(i)}$。这里$c^{(i)}$是第$i$轮轮常数，具体选取方式见文献[10]。由此可知：

$$k_j^{(i+4)}=k_j^{(i+1)}k^{\frac{(i+1)}{j-5}}\oplus k^{\frac{(i+1)}{j-5}}\oplus k_j^{(i)}\oplus c_j^{(i+4)},\quad j=0,1,\cdots,n/2-1 \tag{1}$$

1.3 基本概念

差分中间相遇分析中涉及明文结构、密钥穷举策略、概率扩展技术，特回顾基本的差分概念。

定义1 （差分对应，differential） 设$\Delta X,\Delta Y\in\{0,1\}^n$分别为函数$R:\{0,1\}^n\to\{0,1\}^n$的输入、输出差分(input/out-

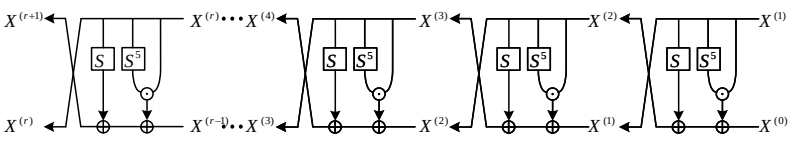


图1 SIMECK密码的加密过程

Figure 1 The encryption procedure of SIMECK

表2　符号说明

Table 2　Symbol description

符号	意义
$X^{(i)}$	第i个$n/2$比特字$X_{n/2-1}^{(i)}\|\|X_{n/2-2}^{(i)}\|\|\cdots\|\|X_0^{(i)}\in\{0,1\}^{n/2}$
$\Delta X^{(i)}$	第i个$n/2$比特字差分$\Delta X_{n/2-1}^{(i)}\|\|\Delta X_{n/2-2}^{(i)}\|\|\cdots\|\|\Delta X_0^{(i)}\in\{0,1\}^{n/2}$
$\bar{j}$	$j \bmod (n/2)$
$X^{(r\sim 0)}$	$X^{(r)}\|\|X^{(r-1)}\|\|\cdots\|\|X^{(0)}\in\{0,1\}^{(r+1)n/2}$
$X^{(r,\cdots,1,0)}$	$X^{(r)}\|\|X^{(r-1)}\|\|\cdots\|\|X^{(0)}\in\{0,1\}^{(r+1)n/2}$
$X_{(n/2-1)\sim 0}^{(i)}$	$X_{n/2-1}^{(i)}\|\|X_{n/2-2}^{(i)}\|\|\cdots\|\|X_0^{(i)}\in\{0,1\}^{n/2}$
$X_{n/2-1,\cdots,1,0}^{(i)}$	$X_{n/2-1}^{(i)}\|\|X_{n/2-2}^{(i)}\|\|\cdots\|\|X_0^{(i)}\in\{0,1\}^{n/2}$
S^j	循环左移j位函数$X^{(i)}\to X_{n/2-j-1}^{(i)}\|\|X_{n/2-j-2}^{(i)}\|\|\cdots\|\|X_{n/2-j}^{(i)}\in\{0,1\}^{n/2}$
$X^{(i)}\odot X^{(i+1)}$	$X^{(i)}$和$X^{(i+1)}$按位与
$F_{(a,b,c)}$	函数$X\to S^a(X)\odot S^b(X)\oplus S^c(X)$
$\Delta\boldsymbol{X}_j$	截断差分$\Delta\boldsymbol{X}$的第j个比特$\Delta\boldsymbol{X}_j=\{\Delta X_j:\Delta X\in\Delta\boldsymbol{X}\}\subseteq\{0,1\}$
$\Delta\boldsymbol{X}_{j_1}\oplus\Delta\boldsymbol{X}_{j_2}$	$\{x_1\oplus x_2: x_1\in\Delta\boldsymbol{X}_{j_1}, x_2\in\Delta\boldsymbol{X}_{j_2}\}\subseteq\{0,1\}$
$\boldsymbol{e}_j$	仅第j比特为1的n比特向量
$\mathbf{0}^f$	f个全0比特,即$0\|\|\cdots\|\|0\|\|0\in\{0,1\}^f$
$\#\Sigma$	集合Σ的基数
Span{•}	由集合{•}张成的线性空间
$\|k\|$	变量k的比特个数

put difference),称$\mathrm{DP}(\Delta X\xrightarrow{R}\Delta Y)=\#\{X\in\{0,1\}^n: R(X)\oplus R(X\oplus\Delta X)=\Delta Y\}/2^n$为$R$的差分对应$\Delta X\to\Delta Y$的概率。

定义2　(截断差分对应,truncated differential)　设$\Delta\boldsymbol{X},\Delta\boldsymbol{Y}\subseteq\{0,1\}^n$为$R:\{0,1\}^n\to\{0,1\}^n$的输入、输出截断差分(input/output truncated difference),称$\mathrm{DP}(\Delta\boldsymbol{X}\xrightarrow{R}\Delta\boldsymbol{Y})=\dfrac{\#\{(\Delta X,X)\in\Delta\boldsymbol{X}\times\{0,1\}^n: R(X)\oplus R(X\oplus\Delta X)\in\Delta\boldsymbol{Y}\}}{2^n\#(\Delta\boldsymbol{X})}$为$R$的截断差分对应$\Delta\boldsymbol{X}\to\Delta\boldsymbol{Y}$的概率。

由上述定义易知$\mathrm{DP}(\Delta X\xrightarrow{R}\Delta Y)=\sum_{(\Delta X,\Delta Y)\in\Delta\boldsymbol{X}\times\Delta\boldsymbol{Y}}\mathrm{DP}\left\{\Delta X\xrightarrow{R}\Delta Y\right\}/\#(\Delta\boldsymbol{X})$。

定义3(截断差分比特与状态结构)　设集合$\Delta\boldsymbol{X}\subseteq\{0,1\}^n$是截断差分,称$\Delta\boldsymbol{X}_j=\{\Delta X_j:\Delta X\in\Delta\boldsymbol{X}\}$为$\Delta\boldsymbol{X}$的第$j$个截断差分比特。特别地,若$\#(\Delta\boldsymbol{X}_j)=1$,则称$\Delta\boldsymbol{X}_j$是$\Delta\boldsymbol{X}$的确定比特,否则称$\Delta\boldsymbol{X}_j$是待定比特。再设$\alpha\in\mathrm{Span}\{\boldsymbol{e}_j: 0\leqslant j<n,\#(\Delta\boldsymbol{X}_j)=1\}$,$\alpha'=\alpha\oplus\oplus_{j:0\leqslant j<n,\Delta\boldsymbol{X}_j=\{1\}}\boldsymbol{e}_j$,称$\boldsymbol{\Omega}_\alpha(\Delta\boldsymbol{X})\times\boldsymbol{\Omega}'_\alpha(\Delta\boldsymbol{X})$是由偏移量$\alpha$与截断差分$\Delta\boldsymbol{X}$决定的状态结构,其中,$\boldsymbol{\Omega}_\alpha(\Delta\boldsymbol{X})=\alpha\oplus\mathrm{Span}\left\{\boldsymbol{e}_j: 0\leqslant j<n,\Delta\boldsymbol{X}_j=\{0,1\}\right\}$和$\boldsymbol{\Omega}'_\alpha(\Delta\boldsymbol{X})=\boldsymbol{\Omega}_{\alpha'}(\Delta\boldsymbol{X})$是$\{0,1\}^n$的两个仿射子空间。

定理1　设$\Delta\boldsymbol{X}\subseteq\{0,1\}^n$是截断差分,若$(X,X')\in\{0,1\}^{2n}$满足$X\oplus X'\in\Delta\boldsymbol{X}$,则$(X,X')\in\boldsymbol{\Omega}_X(\Delta\boldsymbol{X})\times\boldsymbol{\Omega}'_X(\Delta\boldsymbol{X})$。

证明　根据$\boldsymbol{\Omega}_\alpha(\Delta\boldsymbol{X}),\boldsymbol{\Omega}'_\alpha(\Delta\boldsymbol{X})$的定义易得证。证毕

定理2[11]　(SIMECK轮函数的差分概率)设R_i是SIMECK的轮函数,$\Delta X^{(i,i-1)}=(\Delta X^{(i)},\Delta X^{(i-1)})\in\{0,1\}^n$,$\Delta Y^{(i,i-1)}=(\Delta Y^{(i)},\Delta Y^{(i-1)})\in\{0,1\}^n$,$\alpha\in\{0,1\}^n$,仿射函数$X\to F_{(0,5,1)}(X)\oplus F_{(0,5,1)}(X\oplus\alpha)$的像集为$d$维仿射空间$U_\alpha$,则:

$$\mathrm{DP}\{\Delta X^{(i,i-1)}\xrightarrow{R_i}\Delta Y^{(i,i-1)}\}=\begin{cases}2^{-d}, & \text{如果 }\Delta X^{(i)}=\Delta Y^{(i-1)}\text{ 且 }\Delta X^{(i-1)}\oplus\Delta Y^{(i)}\in U_{\Delta X^{(i)}}\\ 0, & \text{其他情况}\end{cases}。$$

定理2　可用于计算SIMECK轮函数的截断差分概率。

定理3　(SIMECK轮函数的截断差分传播)　设$\Delta\boldsymbol{X}^{(i)}\times\Delta\boldsymbol{X}^{(i-1)}\xrightarrow{R_i}\Delta\boldsymbol{Y}^{(i)}\times\Delta\boldsymbol{Y}^{(i-1)}$是SIMECK轮函数$R_i$的截断差分对应,令:

$$J_0(i)=\left\{j: 0\leqslant j<n/2,\Delta\boldsymbol{X}_j^{(i)}=\Delta\boldsymbol{X}_{j-5}^{(i)}=\{0\}\text{且}\#(\Delta\boldsymbol{X}_j^{(i-1)})=\#(\Delta\boldsymbol{X}_{j-1}^{(i)})=1\right\}\text{且}J_1(i)=\{0,1,\cdots,n/2-1\}\backslash J_0(i)。$$

如果:

(Ⅰ)$\Delta\boldsymbol{Y}^{(i-1)}=\Delta\boldsymbol{X}^{(i)}$;

(Ⅱ)任意$j\in J_0(i)$都满足$\Delta\boldsymbol{Y}_j^{(i)}=\Delta\boldsymbol{X}_j^{(i)}\oplus\Delta\boldsymbol{X}_{j-1}^{(i)}$;

(Ⅲ)任意$j\in J_1(i)$都满足$\Delta\boldsymbol{Y}_j^{(i)}=\{0,1\}$;

那么,$\mathrm{DP}\{\Delta\boldsymbol{X}^{(i)}\times\Delta\boldsymbol{X}^{(i-1)}\xrightarrow{R_i}\Delta\boldsymbol{Y}^{(i)}\times\Delta\boldsymbol{Y}^{(i-1)}\}=1$。

证明　设$(\Delta X^{(i,i-1)},X^{(i,i-1)})\in(\Delta\boldsymbol{X}^{(i)}\times\Delta\boldsymbol{X}^{(i-1)})\times\{0,1\}^n$,记$\Delta Y^{(i,i-1)}=R_i(X^{(i,i-1)})\oplus R_i(X^{(i,i-1)}\oplus\Delta X^{(i,i-1)})$,那么$\Delta Y^{(i-1)}=\Delta X^{(i)}\in\Delta\boldsymbol{X}^{(i)}$,且:

$$\Delta Y_j^{(i)}=\begin{cases}\Delta X_{j-1}^{(i)}\oplus\Delta X_j^{(i-1)}\in\Delta\boldsymbol{X}_j^{(i)}\oplus\Delta\boldsymbol{X}_{j-1}^{(i)}, & j\in J_0(i)\\ \Delta X_j^{(i)}X_{j-5}^{(i)}\oplus X_j^{(i)}\Delta X_{j-5}^{(i)}\oplus\Delta X_j^{(i)}\Delta X_{j-5}^{(i)}\\ \qquad\oplus\Delta X_{j-1}^{(i)}\oplus\Delta X_j^{(i-1)}\in\{0,1\}, & j\in J_1(i)\end{cases}。$$

结合(Ⅰ,Ⅱ,Ⅲ)知$\Delta Y^{(i,i-1)}\in\Delta\boldsymbol{Y}^{(i)}\times\Delta\boldsymbol{Y}^{(i-1)}$。从而由截断差分概率定义知$\mathrm{DP}\{\Delta\boldsymbol{X}^{(i)}\times\Delta\boldsymbol{X}^{(i-1)}\xrightarrow{R_i}\Delta\boldsymbol{Y}^{(i)}\times\Delta\boldsymbol{Y}^{(i-1)}\}=1$。证毕

根据定理3,设$R_{s\sim 1}=R_s\circ\cdots\circ R_2\circ R_1$的输入截断差分为$\Delta\boldsymbol{X}^{(1)}\times\Delta\boldsymbol{X}^{(0)}$,当$i=1,2,\cdots,s$时,依次令$R_i$的输出截断差分$\Delta\boldsymbol{X}^{(i+1)}\times\Delta\boldsymbol{X}^{(i)}$满足定理3条件。那么在子密钥独立的假设下,$R_{s\sim 1}$的截断差分路径$\boldsymbol{\Gamma}_{\mathrm{out}}=(\Delta\boldsymbol{X}^{(1)}\times\Delta\boldsymbol{X}^{(0)},\Delta\boldsymbol{X}^{(2)}\times\Delta\boldsymbol{X}^{(1)},\cdots,\Delta\boldsymbol{X}^{(s+1)}\times\Delta\boldsymbol{X}^{(s)})$概率为$\mathrm{DP}\{\boldsymbol{\Gamma}_{\mathrm{out}}\}=\prod_{i=1}^{s}\mathrm{DP}\{\Delta\boldsymbol{X}^{(i)}\times\Delta\boldsymbol{X}^{(i-1)}\xrightarrow{R_i}\Delta\boldsymbol{X}^{(i+1)}\times\Delta\boldsymbol{X}^{(i)}\}=1$。

与定理3类似，还可得到SIMECK轮函数的逆映射R_i^{-1}的截断差分传播，进而由$\Delta \boldsymbol{X}^{(s+1)} \times \Delta \boldsymbol{X}^{(s)}$生成$R_{s\sim 1}^{-1}$的截断差分路径$\boldsymbol{\Gamma}_{\text{in}}=(\Delta \boldsymbol{X}^{(s+1)} \times \Delta \boldsymbol{X}^{(s)}, \Delta \boldsymbol{X}^{(s)} \times \Delta \boldsymbol{X}^{(s-1)}, \cdots, \Delta \boldsymbol{X}^{(1)} \times \Delta \boldsymbol{X}^{(0)})$。

利用$\boldsymbol{\Gamma}_{\text{in}}, \boldsymbol{\Gamma}_{\text{out}}$，2.2节将给出DMC的攻击路径（即用于恢复子密钥的密钥穷举策略），进而说明概率扩展技术[30]。强制限定$\boldsymbol{\Gamma}_{\text{in}}, \boldsymbol{\Gamma}_{\text{out}}$中某些待定比特为{0}的作用是以降低截断差分路径概率$\text{DP}\{\boldsymbol{\Gamma}_{\text{in}}\}, \text{DP}\{\boldsymbol{\Gamma}_{\text{out}}\}$为代价来减少密钥穷举策略所需的密钥量。2.3节将用$\boldsymbol{\Gamma}_{\text{in}}$在明文处的截断差分构造明文结构，降低数据复杂性。

2 基于尾接技术与明文结构的差分中间相遇分析

本节针对性地提出了DMC的两个改进，且兼容并行分割、概率扩展技术[30]。

针对非线性密钥生成算法使待穷举密钥之间的相关性过于复杂而导致主密钥恢复代价过大的问题，本节提出了基于尾接技术的DMC模型。因为额外考虑了密码的尾接部分，可将更多待穷举密钥集中在相邻轮次，从而降低推导主密钥的代价，还可利用相邻密钥清晰的相关性建立更多筛选条件，降低错误密钥通过率。

针对DMC在$p'>n-2$时无法用限制条件技术[3]实现非全码本数据复杂性的问题，本节结合使用明文结构与并行分割技术，在$n-1>p'>n-2$时实现了非全码本复杂性。

2.1 基于尾接技术的一般化差分中间相遇模型

因为n比特密钥加$\tau^K: X \to X \oplus K \in \{0,1\}^n$可看作$f$比特密钥加$\tau^{K'}: X \to X \oplus K' \in \{0,1\}^n$和$n-f$比特密钥加$\tau^{K''}: X \to X \oplus K'' \in \{0,1\}^n$的复合$\tau^K = \tau^{K''} \circ \tau^{K'}$，其中$K'=\boldsymbol{0}^{n-f} \| K_{(f-1)\sim 0}$，$K''=K_{(n-1)\sim f} \| \boldsymbol{0}^f$。我们可将分组密码$E^k: \{0,1\}^n \to \{0,1\}^n$分解为$E^k = E_1^{k_{\text{in}}^{(1)}} \circ \tau^{k_{\text{c}}} \circ E_2^{k_{\text{out}}} \circ E_3^{k_{\text{m}}} \circ E_0^{k_{\text{in}}^{(0)}}$，其中，$k$是主密钥，$k_{\text{in}}^{(0)}, k_{\text{in}}^{(1)}, k_{\text{out}}, k_{\text{c}}, k_{\text{m}}$分别是$E_0^{k_{\text{in}}^{(0)}}, E_1^{k_{\text{in}}^{(1)}}, E_2^{k_{\text{out}}}, \tau^{k_{\text{c}}}, E_3^{k_{\text{m}}}$中涉及的子密钥，$\tau^{k_{\text{c}}}: X \to X \oplus (k_{\text{c}} \| \boldsymbol{0}^f) \in \{0,1\}^n$，$E_3^{k_{\text{m}}}$存在一个概率为$\text{DP}(\Delta_{\text{in}} \xrightarrow{E_3^{k_{\text{m}}}} \Delta_{\text{out}}) = 2^{-p}$的差分区分器$\Delta_{\text{in}} \to \Delta_{\text{out}}$。注：原有DMC模型未考虑$E_1^{k_{\text{in}}^{(1)}}$的存在，本文使用尾接技术将原本应向$E_0^{k_{\text{in}}^{(0)}}$扩展的部分续接到$\tau^{k_{\text{c}}}$尾部作为$E_1^{k_{\text{in}}^{(1)}}$，具体动机见后文。

本文约定，$k_{\text{in}} = k_{\text{in}}^{(0)} \| k_{\text{in}}^{(1)}$，$k_{\text{re}}$是除$k_{\text{in}}, k_{\text{out}}, k_{\text{c}}$外用于构造等效主密钥的密钥，$k_{\text{filter}}$是由$k_{\text{in}}, k_{\text{out}}, k_{\text{c}}, k_{\text{re}}$构造等效主密钥时未用到的密钥（对于SIMECK，任意连续4轮子密钥$k^{(i\sim i+3)}$均为等效主密钥。）$\boldsymbol{\Gamma}_{\text{in}}$是由截断差分$\{\Delta_{\text{in}}\}$按1.3节方式以概率$2^{-p_{\text{in}}}$经$(E_0^{k_{\text{in}}^{(0)}})^{-1}$传播至明文而成的截断差分路径，$\boldsymbol{\Gamma}_{\text{out}}$是由$\{\Delta_{\text{out}}\}$以概率$2^{-p_{\text{out}}}$经$E_1^{k_{\text{in}}^{(1)}} \circ \tau^{k_{\text{c}}} \circ E_2^{k_{\text{out}}}$传播至密文而成的截断差分路径，$\boldsymbol{\Gamma}_{\text{in}}, \boldsymbol{\Gamma}_{\text{out}}$中分别有$d_{\text{in}}, d_{\text{out}}$个截断比特被概率扩展技术强制取为{0}，记$p'=p+p_{\text{in}}+p_{\text{out}}$。

密钥制约关系。对于$k_{\text{in}}, k_{\text{out}}, k_{\text{c}}, k_{\text{re}}, k_{\text{filter}}$，可由密钥生成算法找到函数$f_{\text{in}}, f_{\text{out}}, h_{\text{in}}, h_{\text{out}}, u, v$和线性函数$\sigma$，使：

$$\begin{cases} f_{\text{in}}(k_{\text{in}}) = f_{\text{out}}(k_{\text{out}}) \overset{\text{定义}}{=} k_{\text{in}} \cap k_{\text{out}} \\ h_{\text{in}}(k_{\text{in}}) \oplus h_{\text{out}}(k_{\text{out}}) = \sigma(k_c) \\ u(k_{\text{in}}, k_{\text{out}}, k_{\text{c}}, k_{\text{re}}) = v(k_{\text{filter}}) \end{cases} \tag{2}$$

设式(2)分别建立了$|k_{\text{in}} \cap k_{\text{out}}|, |\sigma(k_{\text{c}})|, |v(k_{\text{filter}})|$比特等式关系。由于$(k_{\text{in}}, k_{\text{out}}, k_{\text{c}}, k_{\text{re}})$与主密钥$k$可相互导出，可知$|k_{\text{in}}|+|k_{\text{out}}|+|k_{\text{c}}|+|k_{\text{re}}|-|k_{\text{in}} \cap k_{\text{out}}|-|\sigma(k_{\text{c}})|-|v(k_{\text{filter}})| = |k|$。

注：由$(k_{\text{in}}, k_{\text{out}}, k_{\text{c}}, k_{\text{re}})$的候选值构造等效主密钥通常占主要时间复杂性，且正比于$2^{|k_{\text{re}}|}$。对于线性密钥生成算法，$k_{\text{in}} \| k_{\text{out}} \| k_{\text{c}}$的每个比特都可用于构造等效主密钥，因此$|k_{\text{re}}|$较小；然而对于非线性密钥生成算法，往往只能通过补全连续子密钥来构造等效主密钥，因此$k_{\text{in}} \| k_{\text{out}} \| k_{\text{c}}$的密钥比特轮次越分散，$|k_{\text{re}}|$就越大。

采用尾接技术的动机。本节采用尾接技术，将$E_0^{k_{\text{in}}^{(0)}}$中原本应向头部扩展的部分调整到$\tau^{k_{\text{c}}}$后向尾部扩展的$E_1^{k_{\text{in}}^{(1)}}$。当$E_1^{k_{\text{in}}^{(1)}}$为恒等变换时，上述模型退化为原有DMC模型。此技术的优势有三点：一是将更多密钥聚集在连续轮，从而得到等效主密钥的更多比特，使$|k_{\text{re}}|$减小；二是$(k_{\text{in}}^{(1)}, k_{\text{out}}, k_{\text{c}})$较$(k_{\text{in}}^{(0)}, k_{\text{out}}, k_{\text{c}})$在轮数上更接近，制约关系更清晰，有利于找出更大的$|k_{\text{in}} \cap k_{\text{out}}|, |\sigma(k_c)|$，从而提高筛选等效主密钥的能力，进而降低攻击的时间复杂性；三是$E_0^{k_{\text{in}}^{(0)}}$变短，差分$\Delta_{\text{in}}$在$E_0^{k_{\text{in}}^{(0)}}$中扩散更不充分，有利于使用明文结构降低数据复杂性。

定理4 设$E^k = E_1^{k_{\text{in}}^{(1)}} \circ \tau^{k_{\text{c}}} \circ E_2^{k_{\text{out}}} \circ E_3^{k_{\text{m}}} \circ E_0^{k_{\text{in}}^{(0)}}$的两个明密对为$(P, C), (P', C')$，令：

$$\begin{cases} A = E_2^{k_{\text{out}}} \circ E_3^{k_{\text{m}}} \circ E_0^{k_{\text{in}}^{(0)}}(P) \overset{\text{定义}}{=} A_{(n-1)\sim f} \| A_{(f-1)\sim 0} \\ A' = E_2^{k_{\text{out}}} \circ E_3^{k_{\text{m}}} \circ E_0^{k_{\text{in}}^{(0)}}(P') \\ B = (E_1^{k_{\text{in}}^{(1)}})^{-1}(C) \overset{\text{定义}}{=} B_{(n-1)\sim f} \| B_{(f-1)\sim 0} \\ B' = (E_1^{k_{\text{in}}^{(1)}})^{-1}(C') \end{cases},$$

对于任意$\Delta_{\text{in}}, \Delta_{\text{out}}$，如果：

$$\begin{cases} \Delta_{\text{in}} = E_0^{k_{\text{in}}^{(0)}}(P) \oplus E_0^{k_{\text{in}}^{(0)}}(P') \\ \Delta_{\text{out}} = (E_1^{k_{\text{in}}^{(1)}} \circ \tau^{k_{\text{c}}} \circ E_2^{k_{\text{out}}})^{-1}(C) \oplus (E_1^{k_{\text{in}}^{(1)}} \circ \tau^{k_{\text{c}}} \circ E_2^{k_{\text{out}}})^{-1}(C') \end{cases} \tag{3}$$

那么：

$$\begin{cases}\Delta_{\text{out}}=(E_2^{k_{\text{out}}})^{-1}(A)\oplus(E_2^{k_{\text{out}}})^{-1}(A')\\ \Delta_{\text{in}}=E_0^{k_{\text{in}}^{(0)}}\circ(E^k)^{-1}\circ E_1^{k_{\text{in}}^{(1)}}(B)\oplus E_0^{k_{\text{in}}^{(0)}}\circ(E^k)^{-1}\circ E_1^{k_{\text{in}}^{(1)}}(B')\\ B=A\oplus(k_{\text{c}}\|\mathbf{0}^f)\\ B'=A'\oplus(k_{\text{c}}\|\mathbf{0}^f)\end{cases}\tag{4}$$

再设$f_{\text{in}}(k_{\text{in}})=f_{\text{out}}(k_{\text{out}})\overset{\text{定义}}{=}k_{\text{in}}\cap k_{\text{out}}$且$h_{\text{in}}(k_{\text{in}})\oplus h_{\text{out}}(k_{\text{out}})=\sigma(k_{\text{c}})$,其中,$\sigma$是线性函数,则有:

$$\begin{cases}A'=E_2^{k_{\text{out}}}\left((E_2^{k_{\text{out}}})^{-1}(A)\oplus\Delta_{\text{out}}\right)\\ B'=\left(E_0^{k_{\text{in}}^{(0)}}\circ(E^k)^{-1}\circ E_1^{k_{\text{in}}^{(1)}}\right)^{-1}\left(E_0^{k_{\text{in}}^{(0)}}\circ(E^k)^{-1}\circ E_1^{k_{\text{in}}^{(1)}}(B)\oplus\Delta_{\text{in}}\right)\\ k_c=A_{(n-1)\text{~}f}\oplus B_{(n-1)\text{~}f}\\ \sigma\left(B_{(n-1)\text{~}f}\right)\oplus h_{\text{in}}(k_{\text{in}})=\sigma\left(A_{(n-1)\text{~}f}\right)\oplus h_{\text{out}}(k_{\text{out}})\\ B\oplus B'=A\oplus A'\\ B_{(f-1)\text{~}0}=A_{(f-1)\text{~}0}\\ f_{\text{in}}(k_{\text{in}})=f_{\text{out}}(k_{\text{out}})\overset{\text{定义}}{=}k_{\text{in}}\cap k_{\text{out}}\end{cases}\tag{5}$$

证明　因为$C=E_k(P),C'=E_k(P')$,将A,A',B,B'代入式(3)即可得式(4)。再将题设密钥关系式代入式(4)即可得式(5)。证毕

基于定理4的式(5),可给出图2所示攻击思路:将$k_{\text{in}}\|k_{\text{out}}$分割为$k_{\text{in}}$和$k_{\text{out}}$两部分独立地穷举,分别由$(B,k_{\text{in}})$和$(A,k_{\text{out}})$得到$(B,k_{\text{in}},B')$和$(A,k_{\text{out}},A')$;再根据$A,A',B,B'$和$k_{\text{in}},k_{\text{out}},k_{\text{c}}$的关系:

$$\begin{aligned}&f_{\text{out}}(k_{\text{out}})\|A_{(f-1)\text{~}0}\|(A\oplus A')\|\left(\sigma(A_{(n-1)\text{~}f})\oplus h_{\text{out}}(k_{\text{out}})\right)\\ =&f_{\text{in}}(k_{\text{in}})\|B_{(f-1)\text{~}0}\|(B\oplus B')\|\left(\sigma(B_{(n-1)\text{~}f})\oplus h_{\text{in}}(k_{\text{in}})\right)\end{aligned}\tag{6}$$

匹配(B,k_{in},B')和(A,k_{out},A')得$(k_{\text{in}},k_{\text{out}},k_{\text{c}}=A_{n-f}\oplus B_{n-f},k_{\text{filter}})$;然后穷举$k_{\text{re}}$,由$(k_{\text{in}},k_{\text{out}},k_{\text{c}},k_{\text{re}})$构造等效主密钥,并用$k_{\text{filter}}$进一步筛选,最后对通过筛选的等效主密钥候选值进行加密测试以确定正确的主密钥。

注:基于文献[3-4]的并行分割技术,虽然匹配(B,k_{in})和(A,k_{out})前未穷举k_{c},但$k_{\text{c}}=A_{(n-1)\text{~}f}\oplus B_{(n-1)\text{~}f}$仍可提供制约关系$\sigma(B_{(n-1)\text{~}f})\oplus h_{\text{in}}(k_{\text{in}})=\sigma(A_{(n-1)\text{~}f})\oplus h_{\text{out}}(k_{\text{out}})$,且在匹配后可求出$k_{\text{c}}=A_{(n-1)\text{~}f}\oplus B_{(n-1)\text{~}f}$。

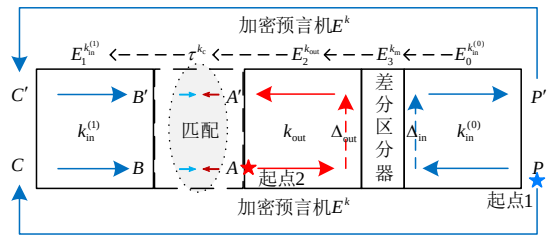


图2　基于尾接技术的差分中间相遇攻击框架

Figure 2　DMC attack framework based on the tail-jointing technique

2.2　密钥穷举策略与概率扩展技术

本节利用$\boldsymbol{\Gamma}_{\text{in}},\boldsymbol{\Gamma}_{\text{out}}$减少$k_{\text{in}},k_{\text{out}}$的穷举量,并分析使用概率扩展技术时DMC有效的条件。

在2.1节中我们简单地将$E_0^{k_{\text{in}}^{(0)}},E_2^{k_{\text{out}}}$涉及的密钥记为$k_{\text{in}}^{(0)},k_{\text{out}}$。但在具体攻击中,$k_{\text{in}}^{(0)},k_{\text{out}}$的作用仅仅是由$(P,\Delta_{\text{in}})$计算$P'=(E_0^{k_{\text{in}}^{(0)}})^{-1}\left(E_0^{k_{\text{in}}^{(0)}}(P)\oplus\Delta_{\text{in}}\right)$,由$(A,\Delta_{\text{out}})$计算$A'=E_2^{k_{\text{out}}}\left((E_2^{k_{\text{out}}})^{-1}(A)\oplus\Delta_{\text{out}}\right)$。这两个计算过程中往往不涉及$E_0^{k_{\text{in}}^{(0)}},E_2^{k_{\text{out}}}$中的全部密钥,以SIMECK密码为例说明。

2.2.1　SIMECK的密钥穷举策略

假设需要由函数$E_{r_s\text{~}r_0}$的输入$X^{(r_0,r_0-1)}$、输出差分$\Delta X^{(r_s,r_s-1)}$及尽可能少的密钥比特$\kappa\subseteq\bigcup_{i=0}^{s}k^{(r_i)}$计算$\left(X^{(r_0,r_0-1)}\right)'=E_{r_s\text{~}r_0}^{-1}\left(E_{r_s\text{~}r_0}(X^{(r_0,r_0-1)})\oplus\Delta X^{(r_s,r_s-1)}\right)$。当$\Delta X^{(r_s,r_s-1)}$表示区分器输入差分$\Delta_{\text{in}}$时,序列$\{r_i\}_{i=0}^{s}$满足$r_i+1=r_{i+1}$且$E_{r_s\text{~}r_0}=R_{r_s}\circ\cdots\circ R_{r_1}\circ R_{r_0}$;当$\Delta X^{(r_s,r_s-1)}$表示区分器输出差分$\Delta_{\text{out}}$时,序列$\{r_i\}_{i=0}^{s}$满足$r_i=r_{i+1}+1$且$E_{r_s\text{~}r_0}=R_{r_s}^{-1}\circ\cdots\circ R_{r_1}^{-1}\circ R_{r_0}^{-1}$。

根据SIMECK密码的轮函数的定义,对于$i=0,1,\cdots,s-2,j=0,1,\cdots,n/2-1$,有

$$\begin{cases}\Delta X_j^{(r_i)}=\Delta X_j^{(r_{i+1})}X^{\frac{(r_{i+1})}{j-5}}\oplus X_j^{(r_{i+1})}\Delta X^{\frac{(r_{i+1})}{j-5}}\\ \qquad\qquad\oplus\Delta X_j^{(r_{i+1})}\Delta X^{\frac{(r_{i+1})}{j-5}}\oplus\Delta X^{\frac{(r_{i+1})}{j-1}}\oplus\Delta X_j^{(r_{i+2})}\\ X_j^{(r_{i+2})}=X_j^{(r_{i+1})}X^{\frac{(r_{i+1})}{j-5}}\oplus X^{\frac{(r_{i+1})}{j-1}}\oplus X_j^{(r_i)}\oplus k_j^{(r_{i+1})}\end{cases}\tag{7}$$

由此可递归建立$(X^{(r_0,r_0-1)})'=X^{(r_0,r_0-1)}\oplus\Delta X^{(r_0,r_0-1)}$关于密钥$k_j^{(r_{i+1})}$和$X^{(r_0,r_0-1)},\Delta X^{(r_s,r_s-1)}$的计算公式,即攻击路径,从而得到相应的密钥穷举策略,确定所需穷举的子密钥比特。

注:当$\Delta X^{\frac{(r_{i+1})}{j,j-5}}=\mathbf{0}^2$时,$\Delta X_j^{(r_i)}=\Delta X^{\frac{(r_{i+1})}{j-1}}\oplus\Delta X_j^{(r_{i+2})}$,此时计算$\Delta X_j^{(r_i)}$不涉及状态$X^{\frac{(r_{i+1})}{j,j-5}}$,因而不涉及用于计算$X^{\frac{(r_{i+1})}{j,j-5}}$的密钥$k^{\frac{(r_i)}{j,j-5}}$。所以,当$\left\{\Delta X^{(r_s,r_s-1)}\right\}$在$E_{r_s\text{~}r_0}$中传播而成的截断差分路径中取值为$\{0\}$的确定比特越多,出现$\Delta X^{\frac{(r_{i+1})}{j,j-5}}=\mathbf{0}^2$的情况越多,计算$(X^{(r_0,r_0-1)})'$涉及的密钥越少。

2.2.2　概率扩展技术与DMC有效的条件

概率扩展技术的目的是用$\bigcup_{i=0}^{s}k^{(r_i)}$中尽可能少的密钥去计算$\left(X^{(r_0,r_0-1)}\right)'$,方法是由$E_{r_s\text{~}r_0}$的输入截断差分$\left\{\Delta X^{(r_s,r_s-1)}\right\}$建立截断差分路径$\boldsymbol{\Gamma}=\left(\Delta\boldsymbol{X}^{(r_s,r_s-1)},\Delta\boldsymbol{X}^{(r_{s-1},r_{s-1}-1)},\cdots,\Delta\boldsymbol{X}^{(r_0,r_0-1)}\right)$的过程中,强制令某些待定比特为$\{0\}$,使得计算$\left(X^{(r_0,r_0-1)}\right)'$时涉及的密钥数最少。

DMC有效的条件。基于2.1节假设,$\boldsymbol{\Gamma}_{\text{in}},\boldsymbol{\Gamma}_{\text{out}}$分别

是$\{\Delta_{\text{in}}\},\{\Delta_{\text{out}}\}$生成的截断差分路径，概率分别为$2^{-p_{\text{in}}},2^{-p_{\text{out}}}<1$。DMC有效的条件是定理4的式(3)成立，为使其成立，P与相应的C,P',C'应满足明文对(P,P')在E^k各处的差分符合$\boldsymbol{\Gamma}_{\text{in}},\boldsymbol{\Gamma}_{\text{out}}$中相应位置的截断差分。此条件在子密钥独立的假设下以$2^{-p-p_{\text{out}}-p_{\text{in}}}$的概率成立。理由如下：根据差分对应、截断差分对应的概率定义，在子密钥独立假设下，对于任意$X\in\{0,1\}^n$，输入$(X,X\oplus\Delta_{\text{in}})$在$(E_0^{k_{\text{in}}^{(0)}})^{-1}$各处差分符合$\boldsymbol{\Gamma}_{\text{in}}$的概率是$2^{-p_{\text{in}}}$；输入$\left(E_3^{k_{\text{in}}}(X),E_3^{k_{\text{in}}}(X\oplus\Delta_{\text{in}})\right)$在$E_1^{k_{\text{in}}^{(1)}}\circ\tau^{k_{\text{c}}}\circ E_2^{k_{\text{out}}}$各处差分符合$\boldsymbol{\Gamma}_{\text{out}}$的概率$2^{-p-p_{\text{out}}}$。令$P=(E_0^{k_{\text{in}}^{(0)}})^{-1}(X)$，那么任意$P\in\{0,1\}^n$使输入$\left(P,(E_0^{k_{\text{in}}^{(0)}})^{-1}(E_0^{k_{\text{in}}^{(0)}}(P)\oplus\Delta_{\text{in}})\right)$在$E_k$各处差分符合$\boldsymbol{\Gamma}_{\text{in}},\boldsymbol{\Gamma}_{\text{out}}$各轮截断差分的概率为$2^{-p-p_{\text{out}}-p_{\text{in}}}$。

2.3 基于明文结构、并行分割技术的差分中间相遇攻击

原始差分中间相遇攻击[3-4]需在穷举密钥时访问解密预言机以获取特定明文对，因此数据复杂性通常为2^n个已知明密文，即全码本。虽然可用限定条件技术[3]，将所需数据限制为2^{n-x}个明密对(这些明密对的特定x个明文比特取常数)，但此技术仅在$2^{p+x}\leqslant 2^{n-x}$时有效。当$p>n-2$时，$x<1$，因此无法使用限定条件技术降低数据复杂性。文献[5,28]利用明文结构与定理1，提出了仅需访问加密预言机的差分中间相遇攻击，将数据复杂性控制为2^{p+1}，但并未给出与并行分割技术结合的方法，无法发挥并行分割技术对攻击的显著提升效果。注：上述分析未考虑概率扩展技术，即$p_{\text{in}},p_{\text{out}}=0$；当考虑概率扩展技术时，需要用$p'=p+p_{\text{in}}+p_{\text{out}}$代替$p$。

本节在文献[5,16,28]的基础上，基于定理4，提出结合明文结构与并行分割技术的方法。在2.1节前提假设下，本节记$\boldsymbol{\Gamma}_{\text{in}}$在明文处的截断差分$\Delta\boldsymbol{P}$有$n_{\text{in}}$个确定比特，$\boldsymbol{\Gamma}_{\text{out}}$在$A$处的截断差分$\Delta\boldsymbol{A}$有$n_A$个确定比特，并额外假设$n_{\text{in}}>0$。因为使用尾接技术后$E_0^{k_{\text{in}}^{(0)}}$变短，$E_1^{k_{\text{in}}^{(1)}}$变长，上述假设$n_{\text{in}}>0$是常见情况。记$\Sigma$是$\text{Span}\left\{\boldsymbol{e}_j:0\leqslant j<n,\#(\Delta\boldsymbol{P}_j)=1\right\}$的$N$元子集。攻击框架如图2所示，具体细节见算法1。

复杂性分析。在算法1中，$\#\boldsymbol{P}=\#\boldsymbol{P}'=N2^{n-n_{\text{in}}}$，$H_{\text{in}}[k_{\text{in}}\cap k_{\text{out}}]$平均包含$k_{\text{in}}$的$2^{|k_{\text{in}}|-|k_{\text{in}}\cap k_{\text{out}}|}$个可能值，$H_{\text{out}}[k_{\text{in}}\cap k_{\text{out}}]$平均包含$k_{out}$的$2^{|k_{\text{out}}|-|k_{\text{in}}\cap k_{\text{out}}|}$个可能值。建表阶段中Step4.2.1利用$\boldsymbol{\Gamma}_{\text{in}}$中强制取$\{0\}$的截断差分比特可过滤掉$2^{-p_{\text{in}}}$的$(P,P',k_{\text{in}})$，Step4.2.3利用式(6)中$B\oplus B'=\Delta A\in\Delta\boldsymbol{A}$的条件和$\boldsymbol{\Gamma}_{\text{out}}$在$\Delta\boldsymbol{A}$的确定比特可过滤掉$2^{-n_A}$的$(B,B',k_{\text{in}})$。查表阶段中Step4.3.1利用$\boldsymbol{\Gamma}_{\text{out}}$中强制取$\{0\}$的截断差分比特可过滤掉$2^{-p_{\text{out}}}$的$(A,A',k_{\text{out}})$。

算法1 基于尾接、明文结构、并行分割技术的差分中间相遇攻击

输入：截断差分路径$\boldsymbol{\Gamma}_{\text{in}},\boldsymbol{\Gamma}_{\text{out}}$与$\text{Span}\left\{\boldsymbol{e}_j:0\leqslant j<n,\#(\Delta\boldsymbol{P}_j)=1\right\}$的$N$元子集$\Sigma$

输出：E^k的主密钥

Step1 选择明文集$\boldsymbol{P}=\bigcup_{\alpha\in\Sigma}\boldsymbol{\Omega}_\alpha(\Delta\boldsymbol{P})$与$\boldsymbol{P}'=\bigcup_{\alpha\in\Sigma}\boldsymbol{\Omega}'_\alpha(\Delta\boldsymbol{P})$，得到明文结构$\bigcup_{\alpha\in\Sigma}\left(\boldsymbol{\Omega}_\alpha(\Delta\boldsymbol{P})\times\boldsymbol{\Omega}'_\alpha(\Delta\boldsymbol{P})\right)$，其中，$\Delta\boldsymbol{P}$是$\boldsymbol{\Gamma}_{\text{in}}$在明文的截断差分；

Step2 按$f_{\text{in}}(k_{\text{in}})=k_{\text{in}}\cap k_{\text{out}}$的值对$k_{\text{in}}$的所有可能值分类并保存在以$k_{\text{in}}\cap k_{\text{out}}$为索引的表$H_{\text{in}}$中；

Step3 按$f_{\text{out}}(k_{\text{out}})=k_{\text{in}}\cap k_{\text{out}}$的值对$k_{\text{out}}$的所有可能值分类并保存在以$k_{\text{in}}\cap k_{\text{out}}$为索引的表$H_{\text{out}}$中；

Step4 对$k_{\text{in}}\cap k_{\text{out}}$的每个可能值，执行：

Step4.1 初始化表H为空集；

Step4.2(建表阶段) 对$H_{\text{in}}[k_{\text{in}}\cap k_{\text{out}}]$中$k_{\text{in}}$的每个可能值，以及$\boldsymbol{P}$中$P$的每个可能值，执行：

Step4.2.1 计算$P'=(E_0^{k_{\text{in}}^{(0)}})^{-1}(E_0^{k_{\text{in}}^{(0)}}(P)\oplus\Delta_{\text{in}})$，若计算过程中的差分值不符合$\boldsymbol{\Gamma}_{\text{in}}$相应位置的截断差分则返回**Step4.2**；

Step4.2.2 由(P,P')访问加密预言机得$C=E^k(P),C'=E^k(P')$；

Step4.2.3 计算$B=E_1^{k_{\text{in}}^{(1)}}(C),B'=E_1^{k_{\text{in}}^{(1)}}(C')$，若$\Delta B=B\oplus B'$不符合$\boldsymbol{\Gamma}_{\text{out}}$相应位置的截断差分则返回**Step4.2**；

Step4.2.4 将(B,k_{in})追加存储到表H以$G_{\text{in}}=B_{(f-1)\text{-}0}\|(B\oplus B')\|\left(\sigma(B_{(n-1)\text{-}f})\oplus h_{\text{in}}(k_{\text{in}})\right)$为地址的表中；

Step4.3(查表阶段) 对$H_{\text{out}}[k_{\text{in}}\cap k_{\text{out}}]$中$k_{\text{out}}$的每个可能值，$\{0,1\}^n$中每个$A$，执行：

Step4.3.1 计算$A'=E_2^{k_{\text{out}}}((E_2^{k_{\text{out}}})^{-1}(A)\oplus\Delta_{\text{out}})$，若计算过程中的差分值不符合$\boldsymbol{\Gamma}_{\text{out}}$相应位置的截断差分则返回**Step4.3**；

Step4.3.2 计算$G_{\text{out}}=A_{(f-1)\text{-}0}\|(A\oplus A')\|\left(\sigma(A_{(n-1)\text{-}f})\oplus h_{\text{out}}(k_{\text{out}})\right)$并访问表$H[G_{\text{out}}]$；

Step4.3.3(匹配阶段) 若$H[G_{\text{out}}]$为空集，则返回**Step4.3**；否则对$H[G_{\text{out}}]$中每个(B,k_{in})执行：

Step4.3.3.1 计算$k_{\text{c}}=A_{(n-1)\text{-}f}\oplus B_{(n-1)\text{-}f}$与$k_{\text{filter}}$；

Step4.3.3.2 对k_{re}的每个可能值，执行：

Step4.3.3.2.1 由$(k_{\text{in}},k_{\text{out}},k_{\text{c}},k_{\text{re}})$得到一个等效主密钥候选值并判断$u(k_{\text{in}},k_{\text{out}},k_{\text{c}},k_{\text{re}})=v(k_{\text{filter}})$是否成立，不成立则返回**Step4.3.3.2**；

Step4.3.3.2.2 对等效主密钥候选值进行加密测试，若测试不通过，则返回**Step4.3.3.2**；否则输出等效主密钥候选值并结束程序；

Step4.4 释放表H所占内存；

Step5 输出空值并结束程序。

匹配阶段中Step4.3.3利用式(6)可过滤掉$2^{-f-n+n_A-|\sigma(k_{\text{c}})|}=2^{-\left(2n-|k_{\text{c}}|-n_A+|\sigma(k_{\text{c}})|\right)}$的$(A,k_{\text{out}},B,k_{\text{in}})$，Step4.3.3.2.1可过滤掉$2^{-|v(k_{\text{filter}})|}$的$(k_{\text{out}},k_{\text{in}},k_{\text{c}})$。

由定理2.1知任意(P,P',k_{in})满足$\Delta\boldsymbol{P}$时，$P'\in\boldsymbol{P}'$，因此数据复杂性为$D=\#\boldsymbol{P}+\#\boldsymbol{P}'=N2^{n-n_{\text{in}}+1}$。存储表$H_{\text{in}},H_{\text{out}},H$消耗的存储复杂性为$M=N2^{(n-n_{\text{in}})+|k_{\text{in}}|-|k_{\text{in}}\cap k_{\text{out}}|-n_A-p_{\text{in}}}+2^{|k_{\text{in}}|}+2^{|k_{\text{out}}|}$。时间复杂性主要包括：

Step2，Step3对$k_{\text{in}},k_{\text{out}}$分类存储的复杂性为$T_0=$

$2^{|k_{in}|}+2^{|k_{out}|}$。

Step4.1~Step4.2 由 $V_1=N2^{(n-n_{in})+|k_{in}|}$ 个 (B,k_{in}) 计算 $\tilde{B}$ 并建表的复杂性为 $T_1=V_1=N2^{(n-n_{in})+|k_{in}|}$。

Step4.3~Step4.3.2 由 $V_2=2^{|k_{out}|+n}$ 个 (A,k_{out}) 计算 $\tilde{A}$ 并查表的复杂性为 $T_2=V_2=2^{|k_{out}|+n}$。

Step4.3.3~Step4.3.3.1 由 $V_3=2^{|k_{in}\cap k_{out}|}\times N2^{(n-n_{in})+(|k_{in}|-|k_{in}\cap k_{out}|)-p_{in}-n}\times 2^{(|k_{out}|-|k_{in}\cap k_{out}|+n)-p_{out}}\times 2^{-(2n-|k_c|-n_A+|\sigma(k_c)|)}$ 个 (A,k_{out},B,k_{in}) 计算 k_c,k_{filter} 的复杂性 $T_3=V_3=N2^{(n-n_{in})}\times 2^{|k_{in}|+|k_{out}|-(n-|k_c|+|\sigma(k_c)|)-p_{in}-p_{out}-|k_{in}\cap k_{out}|}$。

Step4.3.3.2.1 由 $V_4=2^{|k_{re}|}V_3$ 个 $(k_{in},k_{out},k_c,k_{re})$ 计算等效主密钥候选值与 $u(k_{in},k_{out},k_c,k_{re}),v(k_{filter})$，并用 $u(k_{in},k_{out},k_c,k_{re})=v(k_{filter})$ 筛选候选值的复杂性 $T_4=V_4=N2^{n-n_{in}-p-p_{in}-p_{out}+|v(k_{filter})|}\times 2^{p+|k|-n}$。

Step4.3.3.2.2 对 $V_5=2^{-|v(k_{filter})|}V_4$ 个剩余候选值进行加密测试的复杂性 $T_5=V_5=N2^{n-n_{in}-p-p_{in}-p_{out}}\times 2^{p+|k|-n}$。

注:上述各项时间复杂性的基本运算单位不同，单位换算细节由具体情况决定。

成功率。由 2.2.2 节 DMC 有效的条件知，当明文结构 $\bigcup_{\alpha\in\Sigma}(\boldsymbol{\Omega}_\alpha(\Delta\boldsymbol{P})\times\boldsymbol{\Omega}'_\alpha(\Delta\boldsymbol{P}))$ 中存在 (P,P')，其在 E^k 各处差分符合 $\boldsymbol{\Gamma}_{in},\boldsymbol{\Gamma}_{out}$ 时，算法 1 可得到正确的主密钥。因为 $\boldsymbol{P}$ 包含 $N2^{n-n_{in}}$ 个 P，而 (P,P') 在 E^k 各处差分符合 $\boldsymbol{\Gamma}_{in},\boldsymbol{\Gamma}_{out}$ 的概率是 $2^{-p-p_{in}-p_{out}}\overset{定义}{=}2^{-p'}$，通常取 $N=\lceil 2^{p'-n+n_{in}}\rceil$ 以期望得到一个满足成功条件的 P。此时攻击中至少有一个 P 满足条件的概率是 $1-(1-2^{-p'})^{N2^{n-n_{in}}}\geqslant 0.632$。使用尾接技术时通常有 $p'\geqslant n+n_{in}$，此时 $N=2^{p'-n+n_{in}}$，成功率为 0.632。

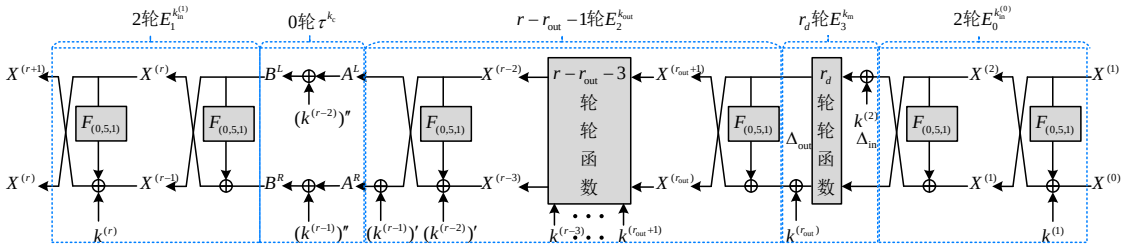
3　SIMECK的差分中间相遇分析

本节基于尾接、明文结构、并行分割、概率扩展技术分别提出了 SIMECK32、SIMECK48、SIMECK64 的 23、31、41 轮攻击。

3.1　SIMECK32的23轮差分中间相遇攻击

在 SIMECK32 的攻击中，$n=32$，我们使用文献[14]提供的概率为 $2^{-28.02}$ 的 $r_d=13$ 轮差分区分器 $(\mathbf{0}^{16},\mathbf{0}^{15}||1)\xrightarrow[2^{-p}=2^{-28.02}]{13-\text{round}}(\mathbf{0}^{15}||1,\mathbf{0}^{16})$。

如图 3 所示，令 $r_{out}=16,r=23$，可将 23=2+0+6+13+2 轮 SIMECK 划分为 $E^k=E_1^{k_{in}^{(1)}}\circ\tau^{k_c}\circ E_2^{k_{out}}\circ E_3^{k_m}\circ E_0^{k_{in}^{(0)}}$。按 1.3 节方法可得表 3 所示截断差分路径 $\boldsymbol{\Gamma}_{in},\boldsymbol{\Gamma}_{out}$，其中截断差分比特 $\Delta\boldsymbol{X}_{0,5}^{(17)}$ 强制取 $\{0\}$，因此 $d_{in}=0,d_{out}=2$，概率分别为 $2^{-p_{in}}=1,2^{-p_{out}}=0.25$，明文处截断差分 $\Delta\boldsymbol{P}$ 的确定比特数为 $n_{in}=25$。按 2.2 节密钥穷举策略可确定 $k_{in}^{(0)},k_{in}^{(1)},k_{out}$，再由式(1)确定 $(k^{(r-1,r-2)})'=k_{out}\cap k^{(r-1,r-2)}$，进而确定 $k_c=(k^{(r-1,r-2)})''=k^{(r-1,r-2)}\oplus(k^{(r-1,r-2)})'$ 与 $\sigma(k_c)=h_{in}(k_{in}^{(0)},k_{in}^{(1)})\oplus h_{out}(k_{out})$，然后由 $k_{in}^{(0)},k_{in}^{(1)},k_{out},k_c$ 确定等效主密钥 $k^{(i\sim i+3)}$ 和 k_{re} 使 $|k_{re}|$ 最小(此处取 $i=20$ 时 $|k_{re}|$ 最小)，最后确定用于筛选 $k^{(i\sim i+3)}$ 的 k_{filter}。表 4 记录了所有密钥参数。



注:$k^{(r-1)}=(k^{(r-1)})''\oplus(k^{(r-1)})',k^{(r-2)}=(k^{(r-2)})''\oplus(k^{(r-2)})'$。

图3　SIMECK各版本差分中间相遇攻击框架

Figure 3　The framework of attacks against all versions of SIMECK

表3　SIMECK各版本的截断差分路径

Table 3　The main attack results against SIMECK

23轮SIMECK32的截断差分路径 $\boldsymbol{\Gamma}_{in},\boldsymbol{\Gamma}_{out},p_{in}=0,p_{out}=2$			
E^k	i		$\Delta X_{15}^{(i-1)}\|\|\cdots\|\|\Delta X_1^{(i-1)}\|\|\Delta X_0^{(i-1)}$
$E_0^{k_{in}^{(0)}}$	1	$\mathbf{0}^{10}\|\|*\|\|\mathbf{0}^3\|\|1\|\|*$	$\mathbf{0}^5\|\|*\|\|\mathbf{0}^3\|\|*^2\|\|\mathbf{0}^2\|\|1\|\|*^2$
	2	$\mathbf{0}^{15}\|\|1$	$\mathbf{0}^{10}\|\|*\|\|\mathbf{0}^3\|\|1\|\|*$
	3	$\mathbf{0}^{16}$	$\mathbf{0}^{15}\|\|1$
$E_3^{k_m}$	⋮	$\Delta X^{(3,2)}=\Delta_{in}\xrightarrow[2^{-p}=2^{-28.02}]{13-\text{round}}\Delta_{out}=\Delta X^{(16,15)}$	
$E_2^{k_{out}}$	16	$\mathbf{0}^{15}\|\|1$	$\mathbf{0}^{16}$

续表

23轮SIMECK32的截断差分路径 $\boldsymbol{\Gamma}_{in},\boldsymbol{\Gamma}_{out},p_{in}=0,p_{out}=2$			
	17	$\mathbf{0}^{10}\|\|\mathbf{0}\|\|\mathbf{0}^3\|\|1\|\|\mathbf{0}$	$\mathbf{0}^{15}\|\|1$
	18	$\mathbf{0}^9\|\|*\|\|\mathbf{0}^3\|\|1\|\|*\|\|1$	$\mathbf{0}^{14}\|\|1\|\|\mathbf{0}$
	19	$\mathbf{0}^4\|\|*\|\|\mathbf{0}^3\|\|*^3\|\|0\|\|1\|\|*^3$	$\mathbf{0}^9\|\|*\|\|\mathbf{0}^3\|\|1\|\|*\|\|1$
	20	$\mathbf{0}^3\|\|*^3\|\|0\|\|*^4\|\|1\|\|*^4$	$\mathbf{0}^4\|\|*\|\|\mathbf{0}^3\|\|*^3\|\|0\|\|1\|\|*^3$
	21	$*\|\|0\|\|*^{14}$	$\mathbf{0}^3\|\|*^3\|\|0\|\|*^4\|\|1\|\|*^4$
τ^{k_c}	22	$*^{16}$	$*\|\|0\|\|*^{14}$
$E_1^{k_{in}^{(1)}}$	23	$*^{16}$	$*^{16}$

续表

23轮SIMECK32的截断差分路径$\Gamma_{\text{in}},\Gamma_{\text{out}},p_{\text{in}}=0,p_{\text{out}}=2$			
	24	$*^{16}$	$*^{16}$
31轮SIMECK48的截断差分路径$\Gamma_{\text{in}},\Gamma_{\text{out}},p_{\text{in}}=0,p_{\text{out}}=1$			
E^k	i	$\Delta X_{23}^{(i)}\|\|\cdots\|\|\Delta X_1^{(i)}\|\|\Delta X_0^{(i)}$	$\Delta X_{23}^{(i-1)}\|\|\cdots\|\|\Delta X_1^{(i-1)}\|\|\Delta X_0^{(i-1)}$
$E_0^{k_{\text{in}}^{(0)}}$	1	$\mathbf{0}^{18}\|\|*\|\|\mathbf{0}^3\|\|1\|\|*$	$\mathbf{0}^{13}\|\|*\|\|\mathbf{0}^3\|\|*^2\|\|\mathbf{0}^2\|\|1\|\|*^2$
	2	$\mathbf{0}^{23}\|\|1$	$\mathbf{0}^{18}\|\|*\|\|\mathbf{0}^3\|\|1\|\|*$
	3	$\mathbf{0}^{24}$	$\mathbf{0}^{23}\|\|1$
$E_3^{k_{\text{in}}}$	⋮	$\Delta X^{(3,2)}=\Delta_{\text{in}}\xrightarrow[2^{-p}=2^{-45.42}]{22-\text{round}}\Delta_{\text{out}}=\Delta X^{(25,24)}$	
$E_2^{k_{\text{out}}}$	25	$\mathbf{0}^{23}\|\|1$	$\mathbf{0}^{24}$
	26	$\mathbf{0}^{18}\|\|\mathbf{0}\|\|\mathbf{0}^3\|\|1\|\|*$	$\mathbf{0}^{23}\|\|1$
	27	$\mathbf{0}^{17}\|\|*^2\|\|\mathbf{0}^2\|\|1\|\|*^2$	$\mathbf{0}^{22}\|\|1\|\|*$
	28	$\mathbf{0}^{12}\|\|*^2\|\|\mathbf{0}^2\|\|*^3\|\|0\|\|1\|\|*^3$	$\mathbf{0}^{17}\|\|*^2\|\|\mathbf{0}^2\|\|1\|\|*^2$
	29	$\mathbf{0}^{7}\|\|*^2\|\|\mathbf{0}^2\|\|*^3\|\|0\|\|*^4\|\|1\|\|*^4$	$\mathbf{0}^{12}\|\|*^2\|\|\mathbf{0}^2\|\|*^3\|\|0\|\|1\|\|*^3$
$\tau^{k_{\text{c}}}$	30	$\mathbf{0}^2\|\|*^2\|\|\mathbf{0}^2\|\|*^3\|\|0\|\|*^{14}$	$\mathbf{0}^{7}\|\|*^2\|\|\mathbf{0}^2\|\|*^3\|\|0\|\|*^4\|\|1\|\|*^4$
$E_1^{k_{\text{in}}^{(1)}}$	31	$0\|\|*^3\|\|0\|\|*^{19}$	$\mathbf{0}^2\|\|*^2\|\|\mathbf{0}^2\|\|*^3\|\|0\|\|*^{14}$
	32	$*^{24}$	$0\|\|*^3\|\|0\|\|*^{19}$
41轮SIMECK64的截断差分路径$\Gamma_{\text{in}},\Gamma_{\text{out}},p_{\text{in}}=0,p_{\text{out}}=2$			
E^k	i	$\Delta X_{31}^{(i)}\|\|\cdots\|\|\Delta X_1^{(i)}\|\|\Delta X_0^{(i)}$	$\Delta X_{31}^{(i-1)}\|\|\cdots\|\|\Delta X_1^{(i-1)}\|\|\Delta X_0^{(i-1)}$
$E_0^{k_{\text{in}}^{(0)}}$	1	$\mathbf{0}^{26}\|\|*\|\|\mathbf{0}^3\|\|1\|\|*$	$\mathbf{0}^{21}\|\|*\|\|\mathbf{0}^3\|\|*^2\|\|\mathbf{0}^2\|\|1\|\|*^2$
	2	$\mathbf{0}^{31}\|\|1$	$\mathbf{0}^{26}\|\|*\|\|\mathbf{0}^3\|\|1\|\|*$
	3	$\mathbf{0}^{32}$	$\mathbf{0}^{31}\|\|1$
$E_3^{k_{\text{in}}}$	⋮	$\Delta X^{(3,2)}=\Delta_{\text{in}}\xrightarrow[2^{-p}=2^{-60.41}]{30-\text{round}}\Delta_{\text{out}}=\Delta X^{(33,32)}$	
$E_2^{k_{\text{out}}}$	33	$\mathbf{0}^{31}\|\|1$	$\mathbf{0}^{32}$
	34	$\mathbf{0}^{26}\|\|\mathbf{0}\|\|\mathbf{0}^3\|\|1\|\|\mathbf{0}$	$\mathbf{0}^{31}\|\|1$
	35	$\mathbf{0}^{25}\|\|*\|\|\mathbf{0}^3\|\|1\|\|*\|\|1$	$\mathbf{0}^{30}\|\|1\|\|\mathbf{0}$
	36	$\mathbf{0}^{20}\|\|*\|\|\mathbf{0}^3\|\|*^3\|\|0\|\|1\|\|*^3$	$\mathbf{0}^{25}\|\|*\|\|\mathbf{0}^3\|\|1\|\|*\|\|1$
	37	$\mathbf{0}^{15}\|\|*\|\|\mathbf{0}^3\|\|*^3\|\|0\|\|*^4\|\|1\|\|*^4$	$\mathbf{0}^{20}\|\|*\|\|\mathbf{0}^3\|\|*^3\|\|0\|\|1\|\|*^3$
	38	$\mathbf{0}^{10}\|\|*\|\|\mathbf{0}^3\|\|*^3\|\|0\|\|*^{14}$	$\mathbf{0}^{15}\|\|*\|\|\mathbf{0}^3\|\|*^3\|\|0\|\|*^4\|\|1\|\|*^4$
	39	$\mathbf{0}^{5}\|\|*\|\|\mathbf{0}^3\|\|*^3\|\|0\|\|*^{19}$	$\mathbf{0}^{10}\|\|*\|\|\mathbf{0}^3\|\|*^3\|\|0\|\|*^{14}$
$\tau^{k_{\text{c}}}$	40	$*\|\|\mathbf{0}^3\|\|*^3\|\|0\|\|*^{24}$	$\mathbf{0}^{5}\|\|*\|\|\mathbf{0}^3\|\|*^3\|\|0\|\|*^{19}$
$E_1^{k_{\text{in}}^{(1)}}$	41	$*^2\|\|0\|\|*^{29}$	$*\|\|\mathbf{0}^3\|\|*^3\|\|0\|\|*^{24}$
	42	$*^{32}$	$*^2\|\|0\|\|*^{29}$

注：其中“$0^s,1^s,*^s$”分别表示s个截断差分比特{0},{1},{0,1}；“0”标红时表示强制此比特取{0}，用以降低密钥穷举量；$2^{-p},2^{-p_{\text{in}}},2^{-p_{\text{out}}}$分别表示区分器，$\Gamma_{\text{in}},\Gamma_{\text{out}}$的概率。

表4 SIMECK各版本攻击中涉及的密钥及其关系

Table 4 The involved key bits and theirs relation in the attacks against each version of SIMECK

攻击23轮SIMECK32时涉及的密钥及关系		
$k_{\text{in}}^{(0)}$	$k^{(1)}[5,11]$	2-bit
$k_{\text{in}}^{(1)}$	$k^{(23)}[0\sim15]$	16-bit
k_{out}	$k^{(18)}[6,12]$	2-bit
	$k^{(19)}[1,5,6,7,11,12,13]$	7-bit
	$k^{(20)}[0,1,2,4,5,6,7,8,10,11,12,13,14]$	13-bit
$k_{\text{in}}\cap k_{\text{out}}$	$k^{(23)}[5,6,7,11,12\text{-}13]\Leftarrow F_{(0,5,1)}(k^{(20)})\oplus k^{(19)}\oplus c^{(19)}$	6-bit

续表

攻击23轮SIMECK32时涉及的密钥及关系		
$k_{\text{out}}\cap k^{(21,22)}$	$k^{(22)}[6,12]\Leftarrow F_{(0,5,1)}(k^{(19)})\oplus k^{(18)}\oplus c^{(18)}$	2-bit
$(k^{(21)})'$	$\mathbf{0}^{16}$	0-bit
$(k^{(22)})'$	$k^{(22)}[6,12]$	2-bit
k_{c}	$k^{(21)}[0\sim15]\Leftarrow(k^{(21)})''=k^{(21)}\oplus(k^{(21)})'$	16-bit
	$k^{(22)}[0\sim15,\text{不含}6,12]\Leftarrow(k^{(22)})''=k^{(22)}\oplus(k^{(22)})'$	14-bit
$\sigma(k_{\text{c}})$	$\mathbf{0}^{16}$	0-bit
k_{re}	$k^{(20)}[3,9,15]$	3-bit
$v(k_{\text{filter}})=\left(k^{(1)}[5,11],k^{(19)}[1]\right)\Leftarrow k_{\text{in}}^{(1)}\|\|k_{\text{out}}\|\|k_{\text{c}}\|\|k_{\text{re}}\Rightarrow$等效主密钥$k^{(20\sim23)}$		
攻击31轮SIMECK48时涉及的密钥及关系		
$k_{\text{in}}^{(0)}$	$k^{(1)}[5,19]$	2-bit
$k_{\text{in}}^{(1)}$	$k^{(31)}[0\sim23]$	24-bit
k_{out}	$k^{(26)}[19]$	1-bit
	$k^{(27)}[5,6,14,18,19,20]$	6-bit
	$k^{(28)}[0,1,4\sim7,9\sim11,13\sim15,17\sim21]$	17-bit
$k_{\text{in}}\cap k_{\text{out}}$	$k^{(31)}[5,6,14,18,19,20]\Leftarrow F_{(0,5,1)}(k^{(28)})\oplus k^{(27)}\oplus c^{(27)}$	6-bit
$k_{\text{out}}\cap k^{(29,30)}$	$k^{(30)}[19]\Leftarrow F_{(0,5,1)}(k^{(27)})\oplus k^{(26)}\oplus c^{(26)}$	1-bit
$(k^{(29)})'$	$\mathbf{0}^{24}$	0-bit
$(k^{(30)})'$	$k^{(30)}[19]$	1-bit
k_{c}	$k^{(29)}[0\sim23]\Leftarrow(k^{(29)})''=k^{(29)}\oplus(k^{(29)})'$	24-bit
	$k^{(30)}[0\sim23,\text{不含}19]\Leftarrow(k^{(30)})''=k^{(30)}\oplus(k^{(30)})'$	23-bit
$\sigma(k_{\text{c}})$	$\mathbf{0}^{24}$	0-bit
k_{re}	$k^{(28)}[2,3,8,12,16,22,23]$	7-bit
$v(k_{\text{filter}})=k^{(1)}[5,19]\Leftarrow k_{\text{in}}^{(1)}\|\|k_{\text{out}}\|\|k_{\text{c}}\|\|k_{\text{re}}\Rightarrow$等效主密钥$k^{(28\sim31)}$		
攻击41轮SIMECK64时涉及的密钥及关系		
$k_{\text{in}}^{(0)}$	$k^{(1)}[5,27]$	2-bit
$k_{\text{in}}^{(1)}$	$k^{(41)}[0\sim31]$	32-bit
k_{out}	$k^{(35)}[6,28]$	2-bit
	$k^{(36)}[1,5\sim7,11,23,27\sim29]$	9-bit
	$k^{(37)}[0,1,2,4\sim8,10\sim12,16,18,22\sim24,26\sim30]$	21-bit
	$k^{(38)}[0\sim31,\text{不含}14,20]$	30-bit
$k_{\text{in}}\cap k_{\text{out}}$	$k^{(41)}[0,1,2,4\sim8,10\sim12,16,18,22\sim24,26\sim30]\Leftarrow F_{(0,5,1)}(k^{(38)})\oplus k^{(37)}\oplus c^{(37)}$	21-bit
$k_{\text{out}}\cap k^{(39,40)}$	$k^{(39)}[6,28]\Leftarrow F_{(0,5,1)}(k^{(36)})\oplus k^{(35)}\oplus c^{(35)}$	2-bit
	$k^{(40)}[1,5\sim7,11,23,27\sim29]\Leftarrow F_{(0,5,1)}(k^{(37)})\oplus k^{(36)}\oplus c^{(36)}$	9-bit
$(k^{(39)})'$	$k^{(39)}[6,28]$	2-bit
$(k^{(40)})'$	$k^{(40)}[1,5\sim7,11,23,27\sim29]$	9-bit
k_{c}	$k^{(39)}[0\sim31,\text{不含}6,28\Leftarrow(k^{(39)})''=k^{(39)}\oplus(k^{(39)})'$	30-bit
	$k^{(40)}[0\sim31,\text{不含}1,5\sim7,11,23,27\sim29]\Leftarrow(k^{(40)})''=k^{(40)}\oplus(k^{(40)})'$	23-bit
$\sigma(k_{\text{c}})$	$\mathbf{0}^{32}$	0-bit
k_{re}	$k^{(38)}[14,20]$	2-bit
$v(k_{\text{filter}})=k^{(1)}[5,27]\Leftarrow k_{\text{in}}^{(1)}\|\|k_{\text{out}}\|\|k_{\text{c}}\|\|k_{\text{re}}\Rightarrow$等效主密钥$k^{(38\sim41)}$		

注：$k[j]$表示k的第j比特。

表3和表4反映了尾接技术的优势：将$E_0^{k_{\text{in}}^{(0)}}$的部分扩展划归$E_1^{k_{\text{in}}^{(1)}}$中，可增加明文处截断差分的确定比

特数 n_{in},有助于明文结构的使用;减少了 k_{re} 的比特数,降低了计算等效主密钥的代价;建立了 $k_{\text{in}}^{(\text{l})},k_{\text{out}}$ 的多比特制约关系以降低错误密钥通过率。

结合上述参数,令算法1中 $N=\left\lceil 2^{p+p_{\text{in}}+p_{\text{out}}-n+n_{\text{in}}}\right\rceil=2^{23.02}$, $J_2=\left\{j\colon 0\leqslant j<n,\Delta\boldsymbol{P}_j=\{0,1\}\right\}=\left\{\frac{n}{2}+5,\frac{n}{2},10,6,5,1,0\right\}$,$\Sigma$是 $\text{Span}\left\{\boldsymbol{e}_j\colon 0\leqslant j<n,j\notin J_2\right\}\subseteq\{0,1^n\}$ 的任意 N 元子集,$\boldsymbol{\Omega}_\alpha(\Delta\boldsymbol{P})=\alpha\oplus\text{Span}\left\{\boldsymbol{e}_j\colon j\in J_2\right\}$, $\boldsymbol{\Omega}'_\alpha(\Delta\boldsymbol{P})=\boldsymbol{\Omega}_{\alpha\oplus\boldsymbol{e}_2\oplus\boldsymbol{e}_{n/2+1}}(\Delta\boldsymbol{P})$, $G_{\text{in}}=B_{6,12}^R\big\|(B'\oplus B)$, $G_{\text{out}}=A_{6,12}^R\big\|(A'\oplus A)$。至此可按算法1实施攻击并恢复主密钥。

在攻击中,因为 $2^{-p_{\text{in}}}=1$, Step4.2.1 中任意 (P,P',k_{in}) 的差分均满足 $\boldsymbol{\Gamma}_{\text{in}}$;因为 $\boldsymbol{\Gamma}_{\text{out}}$ 在 A 处截断差分 $\Delta\boldsymbol{A}$ 仅有1比特确定比特 $\Delta\boldsymbol{A}_{14}$, Step4.2.3 可过滤掉 $n_A=1$ 比特 (B,B',k_{in});因为 $\boldsymbol{\Gamma}_{\text{out}}$ 强制令 $\Delta\boldsymbol{X}_0^{(17)}=\Delta\boldsymbol{X}_5^{(17)}=\{0\}$, Step4.3.1 可过滤掉 $p_{\text{out}}=2$ 比特 (A,A',k_{out}); Step4.3.3 根据 $G_{\text{in}}=G_{\text{out}}$ 可过滤掉 $\left(2n-|k_{\text{c}}|-n_A+\left|\sigma(k_{\text{c}})\right|\right)=33$ 比特 $(A,k_{\text{out}},B,k_{\text{in}})$;Step4.3.3.2.1 根据 $u(k_{\text{in}},k_{\text{out}},k_{\text{c}},k_{\text{re}})=v(k_{\text{filter}})$ 可过滤 $\left|v(k_{\text{filter}})\right|=3$ 比特 $(k_{\text{in}},k_{\text{out}},k_{\text{c}})$。

攻击需检测 $\#\left(\boldsymbol{\Omega}_\alpha\left((\Delta\boldsymbol{P})\times\boldsymbol{\Omega}'_\alpha(\Delta\boldsymbol{P})\right)\right)=2N2^{n-n_{\text{in}}}=2^{31.02}$ 个明密文对,因此数据复杂性为 $D=2^{31.02}$,成功率为 $1-(1-2^{-p-p_{\text{in}}-p_{\text{out}}})^{N2^{n-n_{\text{in}}}}\approx 0.632$。存储复杂性为 $N2^{(n-n_{\text{in}})+|k_{\text{in}}|-|k_{\text{in}}\cap k_{\text{out}}|-n_A}+2^{|k_{\text{in}}|}+2^{|k_{\text{out}}|}\approx 2^{41.02}$。时间复杂性包括:

Step2, Step3 对 $k_{\text{in}},k_{\text{out}}$ 分类存储的复杂性为 $T_0=2^{|k_{\text{in}}|}+2^{|k_{\text{out}}|}=2^{18}+2^{22}$,非主要复杂性。

Step4.1~Step4.2 由 $V_1=N2^{(n-n_{\text{in}})+|k_{\text{in}}|}=2^{30.02+18}$ 个 (B,k_{in}) 计算 $\tilde{B}$ 并建表的复杂性为 $T_1=V_1=2^{48.02}$,非主要复杂性。

Step4.3~Step4.3.2 由 $V_2=2^{|k_{\text{out}}|+n}=2^{32+22}$ 个 (A,k_{out}) 计算 $\tilde{A}$ 并查表的复杂性为 $T_2=V_2=2^{54}$,非主要复杂性。

Step4.3.3~Step4.3.3.1由 $V_3=2^{|k_{\text{in}}\cap k_{\text{out}}|}\times N2^{(n-n_{\text{in}})+\left(|k_{\text{in}}|-|k_{\text{in}}\cap k_{\text{out}}|\right)-p_{\text{in}}-n_A}\times 2^{\left(|k_{\text{out}}|-|k_{\text{in}}\cap k_{\text{out}}|+n\right)-p_{\text{out}}}\times 2^{-\left(2n-|k_{\text{c}}|-n_A+\left|\sigma(k_{\text{c}})\right|\right)}=2^{6+(48.02-6-1)+(54-6-2)-33}$ 个 $(A,k_{\text{out}},B,k_{\text{in}})$ 计算 $k_{\text{c}},k_{\text{filter}}$ 的复杂性为 $T_3=V_3=2^{60.02}$ 次线性运算,折算为23轮SIMECK加密运算(即对主密钥进行23-4次轮函数得子密钥并对明文进行23次轮函数得密文)后非主要复杂性。

Step4.3.3.2.1 由 $V_4=2^{|k_{\text{re}}|}V_3=2^{63.02}$ 个 $(k_{\text{in}},k_{\text{out}},k_{\text{c}},k_{\text{re}})$ 经1次轮函数计算 $k_1^{(19)}$ 并过滤掉 2^{-1} 的候选值,再经18次轮函数得 $k_{5,11}^{(\text{l})}$ 并过滤掉 2^{-2} 的候选值,复杂性为 $T_4=V_4\times\frac{1}{23\times 2-4}+V_4\times 2^{-1}\times\frac{18}{23\times 2-4}\approx 2^{60.798}$ 次23轮加密运算。

S4.3.3.2.2 对 $V_5=2^{-\left|v(k_{\text{filter}})\right|}V_4$ 个剩余候选值进行加密测试的复杂性为 $T_5=V_5=2^{60.02}$ 次23轮加密运算。

因此,总时间复杂性为 $T_4+T_5\approx 2^{61.47}$ 次23轮加密运算。

3.2 SIMECK48的31轮差分中间相遇攻击

在SIMECK48的攻击中,$n=48$,我们使用文献[14]提供的概率为 $2^{-45.42}$ 的 $r_d=22$ 轮差分区分器 $(\mathbf{0}^{24},\mathbf{0}^{23}\|1)\xrightarrow[2^{-p}=2^{-45.42}]{22-\text{round}}(\mathbf{0}^{23}\|1,\mathbf{0}^{24})$。

与3.1节类似,如图3所示,令 $r_{\text{out}}=25,r=31$,可将31轮SIMECK划分为 $E^k=E_1^{k_{\text{in}}^{(\text{l})}}\circ\tau^{k_{\text{c}}}\circ E_2^{k_{\text{out}}}\circ E_3^{k_{\text{m}}}\circ E_0^{k_{\text{in}}^{(0)}}$。$\boldsymbol{\Gamma}_{\text{in}},\boldsymbol{\Gamma}_{\text{out}}$ 如表3所示,其中强制 $\Delta\boldsymbol{X}_5^{(26)}$ 取 $\{0\}$,因此 $d_{\text{in}}=0$, $d_{\text{out}}=1$, $2^{-p_{\text{in}}}=1,2^{-p_{\text{out}}}=0.5$, $\Delta\boldsymbol{P}$ 的确定比特数为 $n_{\text{in}}=41$;按2.2节方法可确定 $k_{\text{in}}^{(0)},k_{\text{in}}^{(\text{l})},k_{\text{out}}$,由式(1)可建立 $k_{\text{in}}^{(0)},k_{\text{in}}^{(\text{l})},k_{\text{out}},k_{\text{c}},k_{\text{re}},k_{\text{filter}}$ 等密钥之间的关系,所有密钥参数见表4。

在算法1中,令 $N=\left\lceil 2^{p+p_{\text{in}}+p_{\text{out}}-n+n_{\text{in}}}\right\rceil=2^{39.42}$, $J_2=\left\{j\colon 0\leqslant j<n,\Delta\boldsymbol{P}_j=\{0,1\}\right\}=\left\{\frac{n}{2}+5,\frac{n}{2},10,6,5,1,0\right\}$, Σ 是 $\text{Span}\left\{\boldsymbol{e}_j\colon 0\leqslant j<n,j\notin J_2\right\}\subseteq\{0,1^n\}$ 的 N 元子集, $\boldsymbol{\Omega}_\alpha(\Delta\boldsymbol{P})=\alpha\oplus\text{Span}\left\{\boldsymbol{e}_j\colon j\in J_2\right\}$, $\boldsymbol{\Omega}'_\alpha(\Delta\boldsymbol{P})=\boldsymbol{\Omega}_{\alpha\oplus\boldsymbol{e}_2\oplus\boldsymbol{e}_{n/2+1}}(\Delta\boldsymbol{P})$, $G_{\text{in}}=B_{19}^R\big\|(B'\oplus B)$, $G_{\text{out}}=A_{19}^R\big\|(A'\oplus A)$, $\Delta\boldsymbol{A}=\Delta\boldsymbol{X}^{(30,29)}$ 有 $n_A=16$ 个确定比特。至此,可实施攻击并恢复主密钥。

复杂性分析与3.1节类似,这里数据复杂性为 $2^{47.42}$,成功率为0.632,存储复杂性为 $2^{50.42}$,时间复杂性包括:

$T_0=2^{26}+2^{24}$, $T_1=2^{46.42+26}$, $T_2=2^{48+24}$, $T_3=V_3=2^{46.42+26+48+24-48-6-1-1}=2^{88.42}$,非主要复杂性。

Step4.3.3.2.1 由 $V_4=2^{|k_{\text{re}}|}V_3=2^{88.42+7}$ 个 $(k_{\text{in}},k_{\text{out}},k_{\text{c}},k_{\text{re}})$ 经27次轮函数得 $k_{5,19}^{(\text{l})}$ 并过滤掉 2^{-2} 的候选值,因此复杂性为 $T_4=V_4\times\frac{27}{31\times 2-4}\approx 2^{94.317}$ 次31轮加密运算。

Step4.3.3.2.2 对 $V_5=2^{-\left|v(k_{\text{filter}})\right|}V_4$ 个剩余候选值进行加密测试的复杂性为 $T_5=V_5=2^{93.42}$ 次31轮加密运算。

因此,总时间复杂性为 $T_4+T_5\approx 2^{94.94}$ 次31轮加密运算。

3.3 SIMECK64的41轮差分中间相遇攻击

在SIMECK64的攻击中,$n=64$,我们使用文献[14]提供的概率为 $2^{-60.41}$ 的 $r_d=30$ 轮差分区分器 $(\mathbf{0}^{32},\mathbf{0}^{31}\|1)\xrightarrow[2^{-p}=2^{-60.41}]{30-\text{round}}(\mathbf{0}^{31}\|1,\mathbf{0}^{32})$。

与3.1节类似,如图3所示,令 $r_{\text{out}}=33,r=41$,可将41轮SIMECK划分为 $E^k=E_1^{k_{\text{in}}^{(\text{l})}}\circ\tau^{k_{\text{c}}}\circ E_2^{k_{\text{out}}}\circ E_3^{k_{\text{m}}}\circ E_0^{k_{\text{in}}^{(0)}}$。$\boldsymbol{\Gamma}_{\text{in}},\boldsymbol{\Gamma}_{\text{out}}$ 如表2所示,其中 $\Delta\boldsymbol{X}_{0,5}^{(34)}$ 强制取 $\{0\}$,因此 $d_{\text{in}}=0$, $d_{\text{out}}=2$, $2^{-p_{\text{in}}}=1,2^{-p_{\text{out}}}=0.25$, $\Delta\boldsymbol{P}$ 的确定比特数为 $n_{\text{in}}=57$;按2.2节方法可得 $k_{\text{in}}^{(0)},k_{\text{in}}^{(\text{l})},k_{\text{out}}$,由式(1)可建立 $k_{\text{in}}^{(0)},k_{\text{in}}^{(\text{l})},k_{\text{out}},k_{\text{c}},k_{\text{re}},k_{\text{filter}}$ 等密钥之间的关系,所有密钥参

数见表3。

在算法1中，令$N=\left\lceil 2^{p+p_{\text{in}}+p_{\text{out}}-n+n_{\text{in}}}\right\rceil=2^{55.41}$，$J_2=\left\{j:0\leqslant j<n,\Delta \boldsymbol{P}_j=\{0,1\}\right\}=\left\{\frac{n}{2}+5,\frac{n}{2},10,6,5,1,0\right\}$，攻击中$\Sigma$是$\text{Span}\left\{\boldsymbol{e}_j:0\leqslant j<n,j\notin J_2\right\}\subseteq\{0,1^n\}$的$N$元子集，$\boldsymbol{\Omega}_{\alpha}(\Delta \boldsymbol{P})=\alpha\oplus\text{Span}\left\{\boldsymbol{e}_j:j\in J_2\right\}$，$\boldsymbol{\Omega}'_{\alpha}(\Delta \boldsymbol{P})=\boldsymbol{\Omega}_{\alpha\oplus\boldsymbol{e}_2\oplus\boldsymbol{e}_{n/2+1}}(\Delta \boldsymbol{P})$，$G_{\text{in}}=B^L_{6,28}\left\|B^R_{1,5\sim7,11,23,27\sim29}\right\|(B'\oplus B),G_{\text{out}}=A^L_{6,28}\left\|A^R_{1,5\sim7,11,23,27\sim29}\right\|(A'\oplus A),\Delta \boldsymbol{A}=\Delta \boldsymbol{X}^{(40,39)}$有$n_A=13$个确定比特。至此，可实施攻击并恢复主密钥。

复杂性分析与3.1节类似，这里数据复杂性为$2^{63.41}$，成功率为0.632，存储复杂性为$2^{62.41}$，时间复杂性包括：

$T_0=2^{34}+2^{62}$，$T_1=2^{62.41+34}$，$T_3=V_3=2^{62.41+34+62-(64-53+0)-0-2-21}=2^{124.41}$，非主要复杂性。

Step4.3~4.3.2由$V_2=2^{n+|k_{\text{out}}|}=2^{64+62}$个$(A,k_{\text{out}})$经$7\times2$次轮函数得并查表的复杂性为$T_2=V_2\times\frac{7\times2}{41\times2-4}\approx2^{123.522}$次41轮加密运算。

Step4.3.3.2.1由$V_4=2^{|k_{\text{re}}|}V_3=2^{124.41+2}$个$(k_{\text{in}},k_{\text{out}},k_{\text{c}},k_{\text{re}})$经37次轮函数得$k^{(\text{f})}_{5,19}$并过滤掉$2^{-2}$的候选值，因此复杂性为$T_4=V_4\times\frac{37}{41\times2-4}\approx2^{125.335}$次41轮加密运算。

Step4.3.3.2.2对$V_5=2^{-|v(k_{\text{filter}})|}V_4$个剩余候选值进行加密测试的复杂性为$T_5=V_5=2^{124.41}$次41轮加密运算。因此，总时间复杂性为$T_2+T_4+T_5\approx2^{126.19}$次41轮加密运算。

4 结束语

本文基于尾接技术提出了新的差分中间相遇分析模型，在保证待恢复的子密钥被均匀分割的情况下取得了三点优势：一是将待恢复的子密钥的更多比特聚集在区分器一侧的连续轮，使推导主密钥所需的穷举量减少；二是基于相邻密钥的简单关系建立更多密钥制约关系，加速错误密钥的筛选；三是使差分区分器前的差分扩展不充分，便于构造明文结构以降低数据复杂性。

本文基于上述模型，结合明文结构与并行分割技术解决了原有基于并行分割技术的差分中间相遇分析在$n-1\geqslant p'>n-2$时无法实现非全码本复杂性的问题。

作为应用，本文分别提出了23轮SIMECK32，31轮SIMECK48和41轮SIMECK64的差分中间相遇攻击。据我们所知，在以恢复主密钥为目标的差分攻击中，本文结果的攻击轮数最长。

参考文献

[1] Diffie W, Hellman M E. Special feature exhaustive cryptanalysis of the NBS data encryption standard[J]. Computer, 1977, 10(6): 74-84.

[2] Biham E, Shamir A. Differential cryptanalysis of DES-like cryptosystems[J]. Journal of Cryptology, 1991, 4(1): 3-72.

[3] Boura C, David N, Derbez P, et al. Differential meet-in-the-middle cryptanalysis[C]//Proceedings of 43rd Annual International Cryptology Conference on Advances in Cryptology - CRYPTO 2023. Cham: Springer, 2023: 240-272.

[4] Ahmadian Z, Khalesi A, M´Foukh D, et al. Improved differential meet-in-the-middle cryptanalysis[C]//Proceedings of 43rd Annual International Conference on the Theory and Applications of Cryptographic Techniques on Advances in Cryptology - EUROCRYPT 2024. Cham: Springer, 2024: 280-309.

[5] Song Ling, Liu Huimin, Yang Qianqian, et al. Generic differential key recovery attacks and beyond[C]//Proceedings of 30th International Conference on the Theory and Application of Cryptology and Information Security on Advances in Cryptology - ASIACRYPT 2024. Singapore: Springer, 2024: 361-391.

[6] M'Foukh D, Naya-Plasencia M, Neumann P. The state-test technique on differential attacks: A 26-round attack on CRAFT and other applications[C]//Proceedings of 31st International Conference on the Theory and Application of Cryptology and Information Security on Advances in Cryptology - ASIACRYPT 2025. Singapore: Springer, 2025: 253-284.

[7] Demirci H, Selçuk A A. A meet-in-the-middle attack on 8-round AES[C]//Proceedings of 15th International Workshop, FSE 2008 on Fast Software Encryption. Berlin: Springer, 2008: 116-126.

[8] Li Rongjia, Jin Chenhui. Meet-in-the-middle attacks on 10-round AES-256[J]. Designs, Codes and Cryptography, 2016, 80(3): 459-471.

[9] Beaulieu R, Shors D, Smith J, et al. The SIMON and SPECK lightweight block ciphers[C]//Proceedings of the 52nd Annual Design Automation Conference. New York: ACM, 2015: 2747946.

[10] Yang Gangqiang, Zhu Bo, Suder V, et al. The Simeck family of lightweight block ciphers[C]//Proceedings of 17th International Workshop on Cryptographic Hardware and Embedded Systems -- CHES 2015. Berlin: Springer, 2015: 307-329.

[11] Kölbl S, Leander G, Tiessen T. Observations on the SIMON block cipher family[C]//Proceedings of 35th Annual Cryptology Conference on Advances in Cryptology -- CRYPTO 2015. Berlin: Springer, 2015: 161-185.

[12] Matsui M. Linear cryptanalysis method for DES cipher[C]// Proceedings of Workshop on the Theory and Application of Cryptographic Techniques on Advances in Cryptology - EUROCRYPT ´93. Berlin: Springer, 1993: 386-397.

[13] Liu Zhengbin, Li Yongqiang, Wang Mingsheng. Optimal differential trails in SIMON-like ciphers[J]. IACR Transactions on Symmetric Cryptology, 2017, 2017(1): 358-379.

[14] Leurent G, Pernot C, Schrottenloher A. Clustering effect in Simon and Simeck[C]//Proceedings of 27th International Conference on the Theory and Application of Cryptology and Information Security on Advances in Cryptology - ASIACRYPT 2021. Cham: Springer, 2021: 272-302.

[15] Niu Chao, Li Muzhou, Zhang Jifu, et al. Improved differential and linear cryptanalysis on round-reduced SIMON[EB/OL]. (2025-02-06) [2026-02-03]. https://eprint. iacr. org/2025/178.

[16] 成磊, 沈璇, 任传伦. 广义类CLEFIA动态密码结构抵抗差分和线性密码分析的安全性评估[J]. 电子学报, 2024, 52(8): 2571-2580.
Cheng Lei, Shen Xuan, Ren Chuanlun. Security evaluation of generalized CLEFIA-like dynamic cipher structures against differential and linear cryptanalysis[J]. Acta Electronica Sinica, 2024, 52(8): 2571-2580. (in Chinese)

[17] 刘帅, 任小广, 王世雄, 等. 基于MILP的轻量级密码算法ACE与SPIX的线性分析[J]. 电子学报, 2024, 52(9): 3065-3074.
Liu Shuai, Ren Xiaoguang, Wang Shixiong, et al. Linear analysis of lightweight cipher ACE and SPIX based on mixed-integer linear programming[J]. Acta Electronica Sinica, 2024, 52(9): 3065-3074. (in Chinese)

[18] Deng Weiqing, Zhang Jianing, Wang Haoyang. Improved differential meet-in-the-middle cryptanalysis on SIMON and Piccolo[C]//Proceedings of 30th Australasian Conference, ACISP 2025 on Information Security and Privacy. Singapore: Springer, 2025: 78-97.

[19] Chakraborty D, Sahoo S, Nguyen P H, et al. An automated model to search for differential meet-in-the-middle attack: Applications to AndRX ciphers[EB/OL]. (2025-07-07)[2026-02-03]. https://eprint.iacr.org/2025/1249.

[20] Wang Ning, Wang Xiaoyun, Jia Keting, et al. Differential attacks on reduced SIMON versions with dynamic key-guessing techniques[J]. Science China Information Sciences, 2018, 61(9): 098103.

[21] Michel B, M´Foukh D, Naya-Plasencia M. Differential meet-in-the-middle attacks on Feistel ciphers[EB/OL]. (2025-10-13)[2026-02-03]. https://eprint.iacr.org/2025/1911.

[22] Hao Yonglin, Meier W. Truncated differential based known-key attacks on round-reduced SIMON[J]. Designs, Codes and Cryptography, 2017, 83(2): 467-492.

[23] Lee J K, Koo B, Kim W H. A general framework for the related-key linear attack against block ciphers with linear key schedules[C]//Proceedings of 26th International Conference on Selected Areas in Cryptography - SAC 2019. Cham: Springer, 2019: 194-224.

[24] Zhang Yi, Zhang Kai, Cui Ting. Related-key zero-correlation linear attacks on block ciphers with linear key schedules[J]. Chinese Journal of Electronics, 2024, 33(3): 672-682.

[25] Kondo K, Sasaki Y, Todo Y, et al. Analyzing key schedule of SIMON: Iterative key differences and application to related-key impossible differentials[C]//Proceedings of 12th International Workshop on Security on Advances in Information and Computer Security. Cham: Springer, 2017: 141-158.

[26] Su Ruitao, Ren Jiongjiong, Chen Shaozhen. Improved framework of related-key differential neural distinguisher and applications to the standard ciphers[EB/OL]. (2025-03-23)[2026-02-03]. https://eprint.iacr.org/2025/537.

[27] Song Ling, Yang Qianqian, Liu Huimin. Revisiting the differential meet-in-the-middle cryptanalysis[EB/OL]. (2023-09-01)[2026-02-03]. https://eprint.iacr.org/2023/1302.

[28] Qiao Kexin, Hu Lei, Sun Siwei. Differential analysis on Simeck and Simon with dynamic key-guessing techniques[C]//Proceedings of Second International Conference on Information Systems Security and Privacy. Cham: Springer, 2016: 64-85.

[29] Qin Lingyue, Chen Huaifeng, Wang Xiaoyun. Linear hull attack on round-reduced Simeck with dynamic key-guessing techniques[C]//Proceedings of 21st Australasian Conference on Information Security and Privacy. Cham: Springer, 2016: 409-424.

[30] Song Ling, Yang Qianqian, Chen Yincen, et al. Probabilistic extensions: A one-step framework for finding rectangle attacks and beyond[C]//Proceedings of 43rd Annual International Conference on the Theory and Applications of Cryptographic Techniques on Advances in Cryptology - EUROCRYPT 2024. Cham: Springer, 2024: 339-367.

作者简介

张 奕 男,1997年11月出生于江西省吉安市。现为网络空间部队信息工程大学网络空间安全专业博士研究生。主要研究方向为对称密码分析。

E-mail: yizhang0796@foxmail.com

吕广秋 男,1994年6月出生于河北省衡水市。现为网络空间部队信息工程大学讲师。主要研究方向为对称密码的设计与分析、集成电路技术。

E-mail: lgq_running@163.com

金晨辉 男,1965年3月出生于河南省周口市。现为网络空间部队信息工程大学教授。主要研究方向为密码学与信息安全。

E-mail: jinchenhui@126.com

崔 霆 男,1985年12月出生于安徽省铜陵市。现为网络空间部队信息工程大学教授。主要研究方向为密码理论与密码算法分析。

E-mail: cuiting_1209@126.com