密码学报 ISSN 2095-7025 CN 10-1195/TN
Journal of Cryptologic Research, 2021, 8(1): 124–131

E-mail: jcr@cacrnet.org.cn
http://www.jcr.cacrnet.org.cn
Tel/Fax: +86-10-82789618

CHAM 算法的安全性分析*

陈少真[1,2], 李 航[1], 付志新[1], 任炯炯[1]

1. 战略支援部队信息工程大学, 郑州 450001
2. 密码科学技术国家重点实验室, 北京 100878
通信作者: 付志新, E-mail: fzx_math@163.com

摘 要: 本文主要研究基于 ARX 结构的轻量级分组密码 CHAM 算法, 利用不可能差分分析、零相关线性分析对其进行安全性分析. 首先, 利用线性不等式组对算法的每个组件进行等价刻画, 描述了差分特征和线性掩码的传播规律, 建立了基于 MILP (混合整数规划问题) 的不可能差分和零相关线性自动化搜索模型. 其次, 根据 CHAM 算法四分支广义 Feistel 结构的特点, 得到 CHAM 算法特定形式 (输入或者输出差分 (掩码) 仅含有一个非零块) 下的最长不可能差分路径和零相关线性路径具有的性质, 优化了搜索策略, 缩小了搜索空间. 最后, 利用搜索算法, 遍历特定的输入输出集合, 共得到 CHAM-64 的 5 条 19 轮不可能差分区分器, CHAM-128 的 1 条 18 轮不可能差分区分器和 15 条 19 轮零相关线性区分器, 均为目前公开发表的最长同类型区分器.

关键词: 轻量级分组密码; CHAM 算法; 自动化搜索
中图分类号: TN918.1 **文献标识码:** A DOI: 10.13868/j.cnki.jcr.000425

中文引用格式: 陈少真, 李航, 付志新, 任炯炯. CHAM 算法的安全性分析[J]. 密码学报, 2021, 8(1): 124–131. [DOI: 10.13868/j.cnki.jcr.000425]

英文引用格式: CHEN S Z, LI H, FU Z X, REN J J. Security analysis of CHAM cipher[J]. Journal of Cryptologic Research, 2021, 8(1): 124–131. [DOI: 10.13868/j.cnki.jcr.000425]

Security Analysis of CHAM Cipher

CHEN Shao-Zhen[1,2], LI Hang[1], FU Zhi-Xin[1], REN Jiong-Jiong[1]

1. PLA Strategic Support Force Information Engineering University, Zhengzhou 450001, China
2. State Key Laboratory of Cryptology, Beijing 100878, China
Corresponding author: FU Zhi-Xin, E-mail: fzx_math@163.com

Abstract: This paper analyzes the security of ARX structure cipher CHAM by impossible difference analysis and zero-correlation linear analysis. Firstly, each component of the cipher is characterized equivalently by using a set of linear inequalities. The propagation characteristics of the differential features and linear masks are described, then an MILP (Mixed Integer Linear Programming) impossible differential and zero-correlation linear automated search model are established. Secondly, according to the characteristics of the four-branch generalized Feistel structure of CHAM, the properties of the

* 基金项目: 数学工程与先进计算国家重点实验室开放课题 (2018A03); 国家密码发展基金 (MMJJ20180203) ; 信息保障技术重点实验室开放课题 (KJ-17-002)

Foundation: Open Fund of State Key Laboratory of Mathematical Engineering and Advanced Computing (2018A03); National Cryptography Development Fund of China (MMJJ20180203) ; Open Fund of Science and Technology on Information Assurance Laboratory (KJ-17-002)

收稿日期: 2020-03-18 定稿日期: 2020-05-28

longest impossible differential path and zero-correlated linear path in the specific form (the input or output differential contains only one non-zero block) of CHAM are obtained, the search strategy is optimized, and the search space is reduced. Finally, by using the search algorithm, traversing a specific set of inputs and outputs, five 19-round impossible differential distinguishers of CHAM-64, one 18-round impossible differential distinguisher of CHAM-128 and fifteen 19-round zero-correlation linear distinguishers of CHAM-128 are found, they are the longest publicly available distinguishers of the same type known so far.

Key words: lightweight block cipher; CHAM; automated search

1 引言

轻量级密码算法具有资源占用量较少的优点, 特别适用于 RFID (Radio Frequency Identification)、无线传感器网络 (WSN) 等资源和计算能力有限的设备和环境. 近年来, 关于轻量级分组密码的研究越来越受到人们的关注, 很多轻量级算法陆续被提出, 比如 PRESENT [1], MIBS [2], LEA [3] 等算法. 为了更好地实现安全性和效率的折中, 涌现出了一批基于 ARX 结构的轻量级分组密码. ARX 型密码算法采用模加运算、循环移位和异或运算三种运算, 其中只有模加运算为非线性运算. 为了便于软硬件的快速实现, ARX 型密码算法的非线性组件规模一般较小, 但是由于模加运算的迭代次数较高, 其仍然具有较强的安全性. 为了提高 LEA 算法对资源受限环境的适应性, 在 ICISC 2017, Koo B 等 [4] 提出了一个新的分组密码家族 CHAM 算法.

在基于统计学方法的攻击如差分类、线性类、积分类等密码攻击过程中, 需要寻找有效的区分器, 区分器的好坏, 直接关系到密码攻击的效果, 找到更长轮数的区分器, 往往意味着在密码分析中能取得更好的攻击结果. 自动化搜索算法充分考虑了密码算法特点, 结合其线性和非线性组件性质, 通过计算机, 可在有效时间内给出特定条件下的所有区分器, 在具体应用中往往能比传统方法搜索到效果更好、条数更多的区分器. 目前常用的自动化搜索算法主要包括基于 SAT(布尔可满足性问题) 的自动化搜索算法和基于 MILP(混合整数规划问题) 的自动化搜索算法.

MILP 问题是运筹学中的一类优化问题, 旨在线性约束条件下求解目标函数的最值. 最近几年, 为了获取分组密码中活跃 S 盒数量的下界, 进而评估分组密码抵抗差分和线性攻击的能力, 很多密码学者将该问题转换为 MILP 问题, 取得了非常好的结果 [5,6]. 后来模加运算差分概率的计算也转化为了 MILP 问题, 用于搜索 ARX 型分组密码算法的区分器 [7,8]. 基于 MILP 自动化搜索技术发展越来越成熟, 显示出强大的密码分析能力, 借助 MILP 的求解工具 Gurobi, 可以在一定的时间内搜索得到相应的区分器.

本文旨在利用不可能差分分析、零相关线性分析对 CHAM 算法进行安全性分析. 首先利用不等式组对算法的每个组件进行等价刻画, 描述了差分特征和线性掩码的传播规律, 其次针对 CHAM 算法四分支广义 Feistel 结构的特点, 优化了不可能差分区分器和零相关线性区分器的搜索策略, 缩小了搜索空间, 进而基于 MILP 工具设计了有效的搜索算法. 依靠搜索算法, 共得到 CHAM-64 的 5 条 19 轮不可能差分区分器, CHAM-128 的 1 条 18 轮不可能差分区分器和 15 条 19 轮零相关线性区分器, 这是 CHAM 算法目前找到的最长零相关特征和最长不可能差分特征. 与已有结果的对比如表 1 所示.

2 CHAM 算法

CHAM 是一个四分支广义 Feistel 结构的分组密码族, 每个密码由 CHAM-n/m 表示, 分组长度为 n 比特, 密钥长度为 m 比特. 表 2 显示了该家族的密码及其参数列表, 在这里, r、w 和 kw 分别表示迭代的轮数、一个分支（字）的长度以及密钥的字数.

2.1 CHAM 算法的轮函数

明文 $P = (X_0[0], X_0[1], X_0[2], X_0[3])$ 作为加密函数的输入, 利用轮函数加密 r 轮可以得到密文 $C = (X_r[0], X_r[1], X_r[2], X_r[3])$. 值得注意的是, CHAM 算法的奇数轮和偶数轮对应轮函数的参数不同,

表 **1** CHAM 算法区分器比较
Table 1 Comparison of distinguishers about CHAM family

攻击方法	算法	区分器轮数	来源
不可能差分	CHAM-64	18	[4]
		19	本文
	CHAM-128	15	[4]
		18	本文
零相关线性	CHAM-64	21	[4]
	CHAM-128	18	[4]
		19	本文

表 **2** CHAM 系列算法参数表
Table 2 Parameters table of CHAM family

	n	m	r	w	kw
CHAM-64/128	64	128	80	16	8
CHAM-128/128	128	128	80	32	4
CHAM-128/256	128	256	96	32	8

当轮数 $r(0 \leqslant i \leqslant r)$ 为偶数时, 轮函数为:

$$\begin{aligned} X_{i+1}[3] &= ((X_i[0] \oplus i) \boxplus ((X_i[1] \lll 1) \oplus \mathrm{rk}[i \bmod 2\mathrm{kw}])) \lll 8, \\ X_{i+1}[j] &= X_i[j],\ 0 \leqslant j \leqslant 2 \end{aligned}$$

当轮数 r 为奇数时, 轮函数为:

$$\begin{aligned} X_{i+1}[3] &= ((X_i[0] \oplus i) \boxplus ((X_i[1] \lll 8) \oplus \mathrm{rk}[i \bmod 2\mathrm{kw}])) \lll 1, \\ X_{i+1}[j] &= X_i[j],\ 0 \leqslant j \leqslant 2 \end{aligned}$$

以上符号 "$\boxplus$" 表示模 2^w 加, "$\oplus$" 表示按位进行异或, "$\lll$" 表示循环左移. 图1给出了 CHAM 算法 2 轮加密函数, 其中 (a_i, b_i, c_i, d_i) 表示第 i 轮的输入.

2.2 CHAM 算法的密钥生成算法

CHAM-n/k 的密钥扩展算法是利用主密钥 $K = (K[0], K[1], \cdots, K[\mathrm{kw}-1])$ 生成 $2 \cdot \mathrm{kw}$ 个 w 比特的轮子密钥 $(\mathrm{rk}[0], \mathrm{rk}[1], \cdots, \mathrm{rk}[2 \cdot \mathrm{kw}-1])$, 生成轮子密钥的过程如下所示:

$$\begin{aligned} \mathrm{rk}[i] &= K[i] \oplus (K[i] \lll 1) \oplus (K[i] \lll 8), \\ \mathrm{rk}[i+\mathrm{kw}] &= K[i] \oplus (K[i] \lll 8) \oplus (K[i] \lll 11) \end{aligned}$$

其中 $0 \leqslant i < \mathrm{kw}$. 加密过程则循环使用这些轮子密钥——加密 $2 \cdot \mathrm{kw}$ 轮循环使用一次全部轮子密钥.

3 CHAM 算法不可能差分区分器搜索

不可能差分分析由 Biham [9] 和 Knudsen [10] 分别提出, 其原理可以简单概括为: 利用概率为零的不可能差分区分器来排除错误的候选密钥, 从而恢复正确密钥.

本节我们给出一个基于 MILP 自动化搜索 CHAM 算法的不可能差分路径的模型, 并利用该模型搜

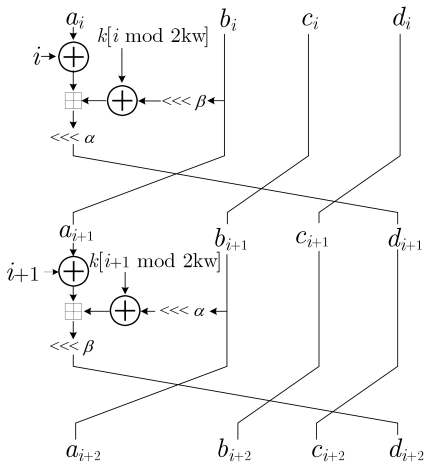

图 1 CHAM 算法轮函数
Figure 1 Round function of CHAM

索得到 19 轮 CHAM-64 和 18 轮 CHAM-128 的不可能差分路径. 对于给定的输入和输出差分, 我们首先把 CHAM 算法的每个组件用线性不等式组等价刻画并进行组合, 然后将目标函数设定为任意的常值——我们只关心不等式组是否有解而不关心目标函数的取值. 若不等式组无解, 当前的输入差分和输出差分导致一条不可能差分路径; 反之, 则对应的差分路径存在.

3.1 差分特征传播规律

轻量级分组密码 CHAM 算法的加密函数较为简单, 仅仅包含分支运算、循环移位运算、常数异或运算以及模加运算, 其中模加运算是唯一的非线性运算, 其余均为线性运算. 我们知道, 与常数进行异或不影响差分的传播, 分支运算同样不改变差分, 因此仅需用不等式组刻画循环移位操作和模加操作.

对于循环移位操作, 由于它仅仅是将输入的比特位置进行置换, 因而我们很容易构建线性等式组对其进行刻画.

对于模加操作, 文献 [11] 进行了刻画, 长度为 n 比特的差分特征 (α,β,γ) 满足 $\alpha \boxplus \beta = \gamma$ 当且仅当

$$
\begin{aligned}
&\alpha[0]+\beta[0]+\gamma[0]-2d=0,\\
-&\alpha[i]-\beta[i]-\gamma[i]+\alpha[i+1]+\beta[i+1]+\gamma[i+1]\geqslant -2,\\
&\alpha[i]+\beta[i]+\gamma[i]-\alpha[i+1]-\beta[i+1]-\gamma[i+1]\geqslant -2,\\
&\alpha[i]+\beta[i]+\gamma[i]+\alpha[i+1]+\beta[i+1]-\gamma[i+1]\geqslant 0,\\
&\alpha[i]+\beta[i]+\gamma[i]+\alpha[i+1]-\beta[i+1]+\gamma[i+1]\geqslant 0,\\
&\alpha[i]+\beta[i]+\gamma[i]-\alpha[i+1]+\beta[i+1]+\gamma[i+1]\geqslant 0,\\
-&\alpha[i]-\beta[i]-\gamma[i]+\alpha[i+1]-\beta[i+1]-\gamma[i+1]\geqslant -4,\\
-&\alpha[i]-\beta[i]-\gamma[i]-\alpha[i+1]+\beta[i+1]-\gamma[i+1]\geqslant -4,\\
-&\alpha[i]-\beta[i]-\gamma[i]-\alpha[i+1]-\beta[i+1]+\gamma[i+1]\geqslant -4
\end{aligned}
$$

其中 d 是二元变量, $0<i<n$.

3.2 搜索策略

在上一小节中, CHAM 算法加密函数的每个运算的差分特征传播都用一组线性不等式进行了刻画. 通过组合所有的不等式, 整个不等式体系能够完美刻画差分特征在 CHAM 算法中的传播规律, 其给出的每个解就是一条可能的差分路径. 而对于给定的输入差分和输出差分, 如果不等式组无解, 那么当前的输

入输出差分将导致一条不可能差分路径. 由于时间的约束, 我们很难遍历整个输入差分和输出差分空间, 而仅仅搜索特定形式输入输出差分的集合, 通过遍历输入差分和输出差分的特定集合, 我们可以确定该集合中是否存在不可能差分路径.

因为 CHAM 算法是四分支广义 Feistel 结构, 所以我们不难得出 CHAM 算法的最长不可能差分路径具有性质 1. 这里 "最长" 仅仅指的是在输入或输出差分仅含有一个非零比特块的情况下, 并非针对所有的不可能差分区分器.

性质 1 对于 CHAM 算法的最长不可能差分路径, 若输入差分只有一个非零块, 则一定形如 $(\alpha,0,0,0)$ 或 $(0,0,0,\beta)$, 其中 $\mathrm{wt}(\alpha)>0$,$\mathrm{wt}(\beta)>0$; 若输出差分只有一个非零块, 则一定形如 $(\gamma,0,0,0)$ 或 $(0,\eta,0,0)$, 其中 $\mathrm{wt}(\gamma)>0$,$\mathrm{wt}(\eta)>0$.

证明: 以输入差分的形式的证明为例, 假设 r 轮不可能差分路径为 $(\alpha_1,\alpha_2,\alpha_3,\alpha_4) \xrightarrow{r\text{-round}} (\beta_1,\beta_2,\beta_3,\beta_4)$.

若非零块位于第二个字, 即形如 $(0,\alpha_2,0,0)$. 根据差分的传播规律, 输入差分可以自然的向上传播一轮, 得到差分 $(0,0,\alpha_2,0)$. 因此, 存在 $(r+1)$ 轮的不可能差分路径 $(0,0,\alpha_2,0)\rightarrow(0,\alpha_2,0,0) \xrightarrow{r\text{-round}} (\beta_1,\beta_2,\beta_3,\beta_4)$, 与 r 轮不可能差分路径最长矛盾.

若非零块位于第三个字, 即形如 $(0,0,\alpha_3,0)$. 根据差分的传播规律, 输入差分可以自然的向上传播一轮, 得到差分 $(0,0,0,\alpha_3)$. 因此, 存在 $(r+1)$ 轮的不可能差分路径 $(0,0,0,\alpha_3)\rightarrow(0,0,\alpha_3,0) \xrightarrow{r\text{-round}} (\beta_1,\beta_2,\beta_3,\beta_4)$, 与 r 轮不可能差分路径最长矛盾.

因此, 对于 CHAM 算法的最长不可能差分路径, 若输入差分只有一个非零字, 则一定形如 $(\alpha,0,0,0)$ 或 $(0,0,0,\beta)$.

同理可证, 对于 CHAM 算法的最长不可能差分路径, 若输出差分只有一个非零字, 则一定形如 $(\gamma,0,0,0)$ 或 $(0,\eta,0,0)$.

综上所述, 命题得证. □

在搜索输入 (输出) 差分仅有 1 个非零块的最长不可能差分路径时, 我们首先对路径的轮数预估一个上界, 然后递减轮数进行搜索, 直至找到不可能差分路径为止. 根据性质 1, 我们可以排除掉最长不可能差分路径的输入 (输出) 差分所不具有的形式, 而不需要遍历全部的输入 (输出) 差分.

3.3 CHAM 算法的不可能差分区分器

CHAM 算法的分组长度是 64 比特或 128 比特, 遍历所有可能的输入输出差分对复杂度太高, 所以我们只考虑三种特殊的情况: 输入、输出差分的重量均为 1 比特 (称为一进一出); 输入、输出差分的重量分别为 1 比特、2 比特 (称为一进二出); 输入、输出差分的重量均为 2 比特、1 比特 (称为二进一出). 在搜索时, 我们利用性质 1 来降低时间复杂度.

对于 CHAM-64 算法, 搜索得到 5 条一进二出的 19 轮不可能差分区分器, 结果如表 3 所示.

表 **3** CHAM-64 不可能差分路径
Table 3 Impossible differential path of CHAM-64

$(0,0,0,e_{14}) \nrightarrow (0,e_{2,7},0,0)$	$(0,0,0,e_{14}) \nrightarrow (0,e_{2,6},0,0)$
$(0,0,0,e_{14}) \nrightarrow (0,e_{2,5},0,0)$	$(0,0,0,e_{14}) \nrightarrow (0,e_{2,4},0,0)$
$(0,0,0,e_{14}) \nrightarrow (0,e_{2,3},0,0)$	

对于 CHAM-128 算法, 搜索得到 1 条一进二出的 18 轮不可能差分区分器 $(0,0,0,e_{30}) \nrightarrow (e_{23},0,0,e_0)$.

4 CHAM 算法零相关线性区分器搜索

零相关分析方法由 Bogdanov 和 Rijmen [12] 于 2012 年提出, 该方法首先要构造一条零相关路径, 通常让线性掩码在非零偏差下从两头向中间传播并相遇, 若任何一个位置产生矛盾, 则找到一条零相关路径 [13]. 构造完零相关路径后, 就可以利用区分器对密钥进行恢复.

本节我们给出一个基于 MILP 自动化搜索 CHAM 算法的零相关线性路径的模型, 并利用该模型搜索得到 19 轮 CHAM-128 的零相关线性路径. 搜索模型与基于 MILP 搜索不可能差分路径的模型相似, 同样利用不等式组对算法的每个组件进行等价刻画并组合, 我们不关心目标函数是什么, 而只关心不等式体系是否有解. 若无解, 则当前的输入掩码和输出掩码导致一条零相关线性路径.

4.1 线性掩码传播规律

为了搜索 CHAM 算法的零相关线性路径, 需要首先考虑分支操作、循环移位操作和模加操作这些基本操作的线性掩码传播. 对于循环移位操作, 由于它仅仅将输入的比特位置进行置换, 因而我们很容易构建线性等式组对其进行描述. 对于分支操作和模加操作, 文献 [14] 进行了精准刻画.

假设分支操作的输入掩码是 α, 输出掩码是 β 和 γ, 掩码的长度都为 n 比特, 则可用如下等式来刻画每个比特上的掩码传播:

$$\alpha[i]+\beta[i]+\gamma[i]-2d=0$$

其中 d 是二元变量, $0\leqslant i<n$.

假设模加操作的输入掩码是 α 和 β, 输出掩码是 γ, 掩码的长度都为 n 比特, 则可用如下等式来刻画每个比特上的掩码传播:

$$\begin{aligned}
s[i+1]-\gamma[i]-\alpha[i]+\beta[i]+s[i]&\geqslant 0,\\
s[i+1]+\gamma[i]+\alpha[i]-\beta[i]-s[i]&\geqslant 0,\\
s[i+1]+\gamma[i]-\alpha[i]-\beta[i]+s[i]&\geqslant 0,\\
s[i+1]-\gamma[i]+\alpha[i]-\beta[i]+s[i]&\geqslant 0,\\
s[i+1]+\gamma[i]-\alpha[i]+\beta[i]-s[i]&\geqslant 0,\\
s[i+1]-\gamma[i]+\alpha[i]+\beta[i]-s[i]&\geqslant 0,\\
-s[i+1]+\gamma[i]+\alpha[i]+\beta[i]+s[i]&\geqslant 0,\\
s[i+1]+\gamma[i]+\alpha[i]+\beta[i]+s[i]&\leqslant 4
\end{aligned}$$

其中 $0\leqslant i<n$, $s[i]$ 是二元状态变量. 值得注意的是, 还有一个额外的约束条件 $s[n]=0$, 因此, 我们可以用 $8n+1$ 个约束条件来刻画模加操作的线性逼近.

4.2 搜索策略

在上一小节中, CHAM 算法加密函数的每个运算的线性掩码的传播都用一组线性不等式进行了刻画. 通过组合所有的不等式, 整个不等式体系能够完美刻画线性掩码在 CHAM 算法中的传播规律. 与不可能差分路径搜索相似的, 在模型中加入输入掩码和输出掩码的约束条件后即可搜索零相关线性路径.

为了降低搜索零相关线性路径的时间复杂度, 我们给出 CHAM 算法的最长零相关线性路径具有性质 2. 这里的 “最长” 仅仅指的是在输入或输出掩码仅含有一个非零比特块的情况下, 并不是针对所有的零相关线性路径.

性质 2 对于 CHAM 算法的最长零相关线性路径, 若输入掩码只有一个非零块, 则一定形如 $(\alpha,0,0,0)$ 或 $(0,0,0,\beta)$, 其中 $\mathrm{wt}(\alpha)>0$, $\mathrm{wt}(\beta)>0$; 若输出掩码只有一个非零块, 则一定形如 $(\gamma,0,0,0)$ 或 $(0,\eta,0,0)$, 其中 $\mathrm{wt}(\gamma)>0$, $\mathrm{wt}(\eta)>0$.

证明: 以输入掩码的形式的证明为例, 假设 r 轮零相关线性路径为 $(\alpha_1,\alpha_2,\alpha_3,\alpha_4)\xrightarrow{r\text{-round}}(\beta_1,\beta_2,\beta_3,\beta_4)$.

若非零块位于第二个字, 即形如 $(0,\alpha_2,0,0)$. 根据掩码的传播规律, 输入掩码可以自然的向上传播一轮, 得到掩码 $(0,0,\alpha_2,0)$. 因此, 存在 $(r+1)$ 轮的零相关线性路径 $(0,0,\alpha_2,0)\rightarrow(0,\alpha_2,0,0)\xrightarrow{r\text{-round}}(\beta_1,\beta_2,\beta_3,\beta_4)$, 与 r 轮零相关线性路径最长矛盾.

若非零块位于第三个字, 即形如 $(0,0,\alpha_3,0)$. 根据掩码的传播规律, 输入掩码可以自然的向上传播一轮, 得到掩码 $(0,0,0,\alpha_3)$. 因此, 存在 $(r+1)$ 轮的不可能差分路径 $(0,0,0,\alpha_3) \to (0,0,\alpha_3,0) \xrightarrow{r\text{-round}} (\beta_1,\beta_2,\beta_3,\beta_4)$, 与 r 轮零相关线性路径最长矛盾.

因此, 对于 CHAM 算法的最长零相关线性路径, 若输入掩码只有一个非零字, 则一定形如 $(\alpha,0,0,0)$ 或 $(0,0,0,\beta)$.

同理可证, 对于 CHAM 算法的最长零相关线性路径, 若输出掩码只有一个非零字, 则一定形如 $(\gamma,0,0,0)$ 或 $(0,\eta,0,0)$.

综上所述, 命题得证. □

在搜索输入 (输出) 掩码仅有 1 个非零块的最长零相关线性路径时, 我们可以采取与不可能差分路径的搜索类似的策略. 根据性质 2, 我们可以排除掉最长零相关线性路径的输入 (输出) 掩码所不具有的形式, 而不需要遍历全部的输入 (输出) 掩码.

4.3 CHAM 算法的零相关线性区分器

搜索 CHAM 算法的零相关线性路径时, 我们只考虑三种特殊的情况: 输入、输出掩码的重量均为 1 比特 (称为一进一出); 输入、输出掩码的重量分别为 1 比特、2 比特 (称为一进二出); 输入、输出掩码的重量分别为 2 比特、1 比特 (称为二进一出). 在搜索时, 我们利用性质 2 来降低时间复杂度.

对于 CHAM-128 算法, 搜索得到 15 条二进一出的 19 轮零相关线性路径, 结果如表 4 所示, 其中 $(0,0,e_0,e_{31}) \nrightarrow (e_1,0,0,0)$ 表示当输入掩码的第三分支的第 0 比特和第四分支的第 31 比特非零、输出掩码的第一分支的第 1 比特非零时组成一条零相关线性路径.

表 **4** CHAM-128 零相关线性路径

Table 4 Zero-correlation linear path of CHAM-128

$(0,0,e_0,e_{31}) \nrightarrow (e_1,0,0,0)$	$(0,0,e_0,e_{31}) \nrightarrow (e_2,0,0,0)$
$(0,0,e_0,e_{31}) \nrightarrow (e_3,0,0,0)$	$(0,0,e_0,e_{31}) \nrightarrow (e_4,0,0,0)$
$(0,0,e_0,e_{31}) \nrightarrow (e_5,0,0,0)$	$(0,0,e_0,e_{31}) \nrightarrow (e_6,0,0,0)$
$(0,0,e_0,e_{31}) \nrightarrow (e_7,0,0,0)$	$(0,0,e_0,e_{31}) \nrightarrow (e_8,0,0,0)$
$(0,0,e_0,e_{31}) \nrightarrow (e_9,0,0,0)$	$(0,0,e_0,e_{31}) \nrightarrow (e_{10},0,0,0)$
$(0,0,e_0,e_{31}) \nrightarrow (e_{12},0,0,0)$	$(0,0,e_0,e_{31}) \nrightarrow (e_{13},0,0,0)$
$(0,0,e_0,e_{31}) \nrightarrow (e_{14},0,0,0)$	$(0,0,e_0,e_{31}) \nrightarrow (e_{15},0,0,0)$
$(0,0,e_0,e_{31}) \nrightarrow (e_{16},0,0,0)$	

选取零相关线性路径 $(0,0,e_0,e_{31}) \nrightarrow (e_1,0,0,0)$ 作为区分器, 对 CHAM 算法进行密钥恢复攻击. 将区分器前加 3 轮后加 1 轮, 可对 CHAM-128/128 攻击到 23 轮, 攻击的时间复杂度为 $2^{120.6}$ 次 23 轮 CHAM-128 加密; 将区分器前加 4 轮后加 4 轮, 可对 CHAM-128/256 攻击到 27 轮, 攻击的时间复杂度为 $2^{238.75}$ 次 27 轮 CHAM-128 加密.

5 总结

本文主要评估了 CHAM 密码算法关于不可能差分和零相关线性分析方法的安全性. 在前人工作的基础上, 基于 MILP 工具, 给出了不可能差分区分器和零相关线性区分器的搜索算法. 根据 CHAM 算法四分支广义 Feistel 结构的特点, 优化了搜索策略, 缩小了搜索空间. 利用搜索算法, 找到了 CHAM-64 的 5 条 19 轮不可能差分区分器、CHAM-128 的 1 条 18 轮不可能差分区分器和 15 条 19 轮零相关线性区分器, 均为目前公开发表的最长同类型区分器. 此外, 目前对 ARX 结构分组密码的非线性组件模加运算的一些基本密码性质尚不明确, 对其的数学刻画也较为复杂, 对模加运算的密码学性质进行深入研究, 简化其数学描述, 对提升搜索算法的效率具有重要意义, 有助于进一步改进现有的密码分析结果.

参考文献

[1] BOGDANOV A, et al. PRESENT: An ultra-lightweight block cipher[C]. In: Cryptographic Hardware and Embedded Systems—CHES 2007. Springer Berlin Heidelberg, 2007: 450–466. [DOI: 10.1007/978-3-540-74735-2_31]

[2] IZADI M, SADEGHIYAN B, SADEGHIAHIAN S-S, et al. MIBS: A new lightweight block cipher[C]. In: Cryptology and Network Security—CANS 2009. Springer Berlin Heidelberg, 2009: 334–348. [DOI: 10.1007/978-3-642-10433-6_22]

[3] HONG D, LEE J-K, KIM D-C, et al. LEA: A 128-bit block cipher for fast encryption on common processors[C]. In: Information Security Applications—WISA 2013. Springer Cham, 2014: 3–27. [DOI: 10.1007/978-3-319-05149-9_1]

[4] KOO B, ROH D, KIM H, et al. CHAM: A family of lightweight block ciphers for resource-constrained devices[C]. In: Information Security and Cryptology—ICISC 2017. Springer Cham, 2017: 3–25. [DOI: 10.1007/978-3-319-78556-1_1]

[5] MOUHA N, WANG Q, GU D, et al. Differential and linear cryptanalysis using mixed-integer linear programming[C]. In: Information Security and Cryptology—INSCRYPT 2011. Springer Berlin Heidelberg, 2011: 57–76. [DOI: 10.1007/978-3-642-34704-7_5]

[6] SUN S, HU L, WANG P, et al. Automatic security evaluation and (related-key) differential characteristic search: Application to SIMON, PRESENT, LBlock, DES (L) and other bit oriented block ciphers[C]. In: Advances in Cryptology—ASIACRYPT 2014, Part I. Springer Berlin Heidelberg, 2014: 158–178. [DOI: 10.1007/978-3-662-45611-8_9]

[7] BIRYUKOV A, VELICHKOV V, CORRE Y L. Automatic search for the best trails in ARX: Application to block cipher speck[C]. In: Fast Software Encryption—FSE 2016. Springer Berlin Heidelberg, 2016: 289–310. [DOI: 10.1007/978-3-662-52993-5_15]

[8] SONG L, HUANG Z J, YANG Q Q. Automatic differential analysis of ARX block ciphers with application to SPECK and LEA[C]. In: Information Security and Privacy—ACISP 2016, Part II. Springer Cham, 2016: 379–394. [DOI: 10.1007/978-3-319-40367-0_24]

[9] BIHAM E, BIRYUKOV A, SHAMIR A. Cryptanalysis of Skipjack reduced to 31 rounds using impossible differentials[C]. Advances in Cryptology—EUROCRYPT '99. Springer Berlin Heidelberg, 1999: 12–23. [DOI: 10.1007/3-540-48910-X_2]

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

[11] FU K, WANG M, GUO Y, et al. MILP-based automatic search algorithms for differential and linear trails for Speck[C] In: Fast Software Encryption—FSE 2016. Springer Berlin Heidelberg, 2016: 268–288. [DOI: 10.1007/978-3-662-52993-5_14]

[12] BOGDANOV A, RIJMEN V. Linear hulls with correlation zero and linear cryptanalysis of block ciphers[J]. Designs, Codes and Cryptography, 2014, 70(3): 369–383. [DOI: 10.1007/s10623-012-9697-z]

[13] WANG M Q, WEN L. Research on zero-correlation linear cryptanalysis[J]. Journal of Cryptologic Research, 2014, 1(3): 296–310. [DOI: 10.13868/j.cnki.jcr.000028]
王美琴, 温隆. 零相关线性分析研究 [J]. 密码学报, 2014, 1(3): 296–310. [DOI: 10.13868/j.cnki.jcr.000028]

[14] CUI T T, JIA K T, FU K, et al. New automatic search tool for impossible differentials and zero-correlation linear approximations[J]. IACR Cryptology ePrint Archive, 2016: 2016/689. https://eprint.iacr.org/2016/689.pdf

作者信息

陈少真 (1967–), 河南郑州人, 博士, 教授. 主要研究领域为密码学与信息安全.
chenshaozhen@vip.sina.com

李航 (1995–), 山东菏泽人, 硕士. 主要研究领域为密码学与信息安全.
lih_student@163.com

付志新 (1996–), 江西丰城人, 硕士. 主要研究领域为密码学与信息安全.
fzx_math@163.com

任炯炯 (1995–), 甘肃天水人, 博士. 主要研究领域为密码学与信息安全.
jiongjiong_fun@163.com