软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2024,35(4):1980−1992 [doi: 10.13328/j.cnki.jos.006839]

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel: +86-10-62562563

分组密码复杂线性层可分性传播的 MILP 刻画方法*

黄 明[1], 张莎莎[1], 洪春雷[2], 曾 乐[3], 向泽军[1]

[1](湖北大学 数学与统计学学院, 湖北 武汉 433062)

[2](上海大学 通信与信息工程学院, 上海 200444)

[3](Faculty of Science, The University of Melbourne, Melbourne VIC3010, Australia)

通信作者: 张莎莎, E-mail: amushasha@163.com

摘 要: 混合整数线性规划 (MILP) 作为一种自动化搜索工具, 被广泛地应用于搜索分组密码的差分、线性、积分等密码性质. 提出一种基于动态选取策略构建 MILP 模型的新技术, 该技术在不同的条件下采用不同的约束不等式刻画密码性质的传播. 具体地, 从可分性出发根据输入可分性汉明重量的不同, 分别采用不同的方法构建线性层可分性传播的 MILP 模型. 最后, 将该技术应用于搜索 uBlock 和 Saturnin 算法的积分区分器. 实验结果表明: 对于 uBlock128 算法, 该技术可以搜索到比之前最优区分器多 32 个平衡比特的 8 轮积分区分器. 除此之外, 搜索到 uBlock128 和 uBlock256 算法比之前最优区分器更长一轮的 9 和 10 轮积分区分器. 对于 Saturnin256 算法, 同样搜索到比之前最优区分器更长一轮的 9 轮积分区分器.

关键词: 混合整数线性规划; 可分性; 线性层; 汉明重量; 积分区分器

中图法分类号: TP309

中文引用格式: 黄明, 张莎莎, 洪春雷, 曾乐, 向泽军. 分组密码复杂线性层可分性传播的MILP刻画方法. 软件学报, 2024, 35(4): 1980–1992. http://www.jos.org.cn/1000-9825/6839.htm

英文引用格式: Huang M, Zhang SS, Hong CL, Zeng L, Xiang ZJ. MILP Modeling of Division Property Propagation for Block Ciphers with Complex Linear Layers. Ruan Jian Xue Bao/Journal of Software, 2024, 35(4): 1980–1992 (in Chinese). http://www.jos.org.cn/1000-9825/6839.htm

MILP Modeling of Division Property Propagation for Block Ciphers with Complex Linear Layers

HUANG Ming[1], ZHANG Sha-Sha[1], HONG Chun-Lei[2], ZENG Le[3], XIANG Ze-Jun[1]

[1](Faculty of Mathematics and Statistics, Hubei University, Wuhan 433062, China)

[2](School of Communication and Information Engineering, Shanghai University, Shanghai 200444, China)

[3](Faculty of Science, The University of Melbourne, Melbourne VIC3010, Australia)

Abstract: As an automatic search tool, mixed integer linear programming (MILP) is widely used to search for differential, linear, integral, and other cryptographic properties of block ciphers. In this study, a new technique of constructing MILP models based on a dynamic selection strategy is proposed, which uses different constraint inequalities to describe the propagation of cryptographic properties under different conditions. Specifically, according to the different Hamming weights of the input division property, this study adopts different methods to construct MILP models of the division property propagation with linear layers. Finally, this technique is applied to search for integral distinguishers of uBlock and Saturnin algorithms. The experimental results show that the proposed technique can obtain an 8-round integral distinguisher with 32 more balance bits than the previous optimal integral distinguisher for the uBlock128 algorithm. In addition, this study gets 9- and 10-round integral distinguishers for uBlock128 and uBlock256 algorithms which are one round longer than the previous optimal integral distinguishers. For the Saturnin256 algorithm, the study finds a 9-round integral distinguisher which is one round

* 基金项目: 湖北省教育厅科学研究计划 (D2020104); 国家自然科学基金 (61802119); 武汉市科技局应用基础前沿项目 (2020010601012189)
收稿时间: 2022-08-26; 修改时间: 2022-10-15; 采用时间: 2022-11-22; jos 在线出版时间: 2023-07-28
CNKI 网络首发时间: 2023-07-31

longer than the previous optimal integral distinguisher.

Key words: mixed integer linear programming (MILP); division property; linear layer; Hamming weight; integral distinguisher

随着计算机和网络技术的飞速发展, 世界已进入信息化时代. 在信息的传播过程中, 如何确保数据的安全是密码学领域的一个重要研究方向. 分组密码具有加解密速度快、结构简单等特点, 被广泛地应用于数据加密、消息鉴别、消息认证及密钥管理. 另一方面, 分组密码的使用离不开对密码算法广泛的安全性分析. 积分攻击[1]是Knudsen 等人于 2002 年提出的一种选择明文攻击, 该攻击方法的核心步骤是构造密码算法的积分区分器, 通过上述积分区分器可以将密码算法和随机置换进行区分, 从而进行密钥恢复攻击. 可分性 (division property) [2]是 Todo 在 EUROCRYPT 2015 上提出一种广义积分性质, 利用可分性可以对密码算法积分性质进行更加精确的刻画, 其中一个显著的应用是首次在理论上对 MISTY1 算法进行了全轮攻击[3] , 随后, Sun 等人给出了具体可分性集合大小的下界[4]. 可分性最初被提出之时, Todo 仅给出了基于字的可分性刻画[2]. 为了更加精确地刻画积分性质, Todo 等人在 FSE 2016 提出基于比特的可分性 (bit-based division property)[5], 然而上述方法受限于复杂度只能用于不超过 32 比特的分组密码.

混合整数线性规划 (mixed integer linear programming, MILP) 是一种在线性约束条件下求解线性目标函数的数学问题. 2011 年 Mouha 等人[6]将 MILP 应用于搜索分组密码算法差分和线性活跃 S 盒数量的下界. 随后, Sun 等人[7]在 ASIACRYPT 2014 上进行了更加深入的研究, 并提出利用 MILP 求解基于比特密码算法的活跃 S 盒下界. Xiang 等人[8] 在 ASIACRYPT 2016 首次将 MILP 应用于可分性传播的刻画, 并借用 MILP 求解器有效地搜索分组长度大于 32 比特且线性层为比特置换结构密码算法的积分区分器. 随后, 通过 MILP 模型搜索具有复杂线性层分组密码的积分区分器成为重要的研究方向.

目前, 利用 MILP 模型搜索复杂线性层密码算法积分区分器的方法主要有如下 4 种.

Sun 等人[9]的方法 (记为 $\mathcal{SW}$ 方法): 给定一个矩阵 $M \in \mathbb{F}_2^{n\times n}$, Sun 等人提出任意的线性变换均可以用一系列复制和异或操作进行建模. 该方法可以应用于任何复杂的线性层, 但是它会引入大量无效的可分迹, 从而导致输出比特更快地失去平衡. 因此, 该方法可能无法得到最优的积分区分器.

Zhang 等人[10]的方法 (记为 $\mathcal{ZR}$ 方法): 给定一个可逆矩阵 $M \in \mathbb{F}_2^{n\times n}$, Zhang 等人通过研究发现矩阵 M 的有效可分迹与 M 可逆子矩阵之间具有一一对应的关系. 因此, 作者将刻画线性层比特可分性的传播转化为刻画可逆子矩阵. 该方法可以完全精确地刻画线性层的可分性传播, 但是它仅可以应用于二元矩阵.

ElSheikh 等人[11]的方法 (记为 $\mathcal{EY}$ 方法): 给定一个可逆矩阵 $M \in \mathbb{F}_2^{n\times n}$, ElSheikh 等人在 $\mathcal{ZR}$ 方法的基础上通过输入可分性搜索使得对应子矩阵为满秩的输出可分性, 从而获得有效的可分迹. 在上述过程中, 由于需要确定线性层的输入可分性, 因此随着加密轮数的增加, 其线性层输入可分性的数量会非常庞大, 从而导致上述过程难以实现. 因此, 作者仅将该思路应用于密码算法的第 1 轮加密, 而其他轮数则仍然使用 $\mathcal{SW}$ 方法.

Hong 等人[12]的方法 (记为 $\mathcal{HZ}$ 方法): 给定一个可逆矩阵 $M \in \mathbb{F}_2^{n\times n}$, Hong 等人利用线性层优化实现算法获得矩阵 M 的优化实现, 随后根据可分性的传播规则对矩阵 M 的优化实现进行建模, 从而更加精确地刻画矩阵 M 的可分性传播. 该方法尽管可以应用于任意复杂的线性层, 但是它只能删除 $\mathcal{SW}$ 方法引入的部分无效可分迹.

针对上述几种方法存在的局限性, 本文进一步研究复杂线性层可分性传播的刻画方法, 并提出一种新的动态选取可分性传播的技术, 该技术根据输入可分性的汉明重量选取不同的刻画方法, 进而达到模型精确程度和求解效率之间的折中. 对一个复杂线性层矩阵 $M \in \mathbb{F}_2^{n\times n}$, 如果其输入可分性的汉明重量 $wt(u) = i\ (1 \leqslant i \leqslant n-1)$, 那么使用 $\mathcal{ZR}$ 方法精确刻画矩阵 M 所有输入可分性汉明重量为 i 的可分性的传播需要的不等式数量 $\#\mathcal{L}_{\mathcal{ZR}_i} = C_n^i$. 当 i 的取值趋近于 $n/2$ 时, $\#\mathcal{L}_{\mathcal{ZR}_i}$ 的值将趋于最大值; 相反地, 当 i 的取值趋近于 1 或 $n-1$ 时, $\#\mathcal{L}_{\mathcal{ZR}_i}$ 的值将趋于最小值. 受启发于上述思想, 本文将输入可分性按汉明重量的不同进行分类, 并采用不同的方法刻画不同汉明重量下的可分性传播, 即在输入可分性汉明重量趋于 $n/2$ 时, 采用 $\mathcal{HZ}$ 方法画线性层的可分性传播; 否则, 采用 $\mathcal{ZR}$ 方法刻画线性层的可分性传播. 相比于 $\mathcal{SW}$ 方法、$\mathcal{EY}$ 方法和 $\mathcal{HZ}$ 方法, 该技术可以更加精确地刻画线性层的可分性传播; 相比于 $\mathcal{ZR}$ 方法, 该技术可以应用于任意复杂的线性层. 为了体现本文技术的有效性, 我们将该技术应用于搜索

uBlock[12]和 Saturni[13]算法的积分区分器, 且均获得了比之前最优积分区分器长一轮的区分器, 具体的代码与实验结果分别见 https://gitee.com/hm0813/MILP_BDP 与表 1, 其中 C^i, A^i, B^i, U^i 分别表示 i 个常数比特, 活跃比特, 平衡比特, 以及未知比特. 值得注意的是: 在文献 [13] 中, 作者提出一种完全精确刻画复杂线性层矩阵的可分性传播方法, 但是该方法受限于约束条件为高次约束, 因此不能直接应用于 MILP 建模, 且该方法限制矩阵的阶数最大为 64 阶, 而本文的方法可以应用于更高阶数的线性层矩阵.

表 1 密码算法的积分区分器

密码算法	轮数	积分区分器	数据复杂度	参考
uBlock128	7	$(C^4A^{124})\to(B^{128})$	2^{124}	[14]
	8	$(C^4A^{124})\to((BU^2B)^{32})$	2^{124}	[15]
	8	$(C^4A^{124})\to((BUB^2)^{32})$	2^{124}	第3.1节
	9	$(ACA^{124})\to((U^3B)^{32})$	2^{127}	第3.1节
uBlock256	8	$(C^4A^{252})\to(B^{256})$	2^{252}	[14]
	8	$((C^{32}A^{96})^2)\to((U^3B)^{64})$	2^{192}	[15]
	9	$(C^8A^{248})\to((BU^2B)^{64})$	2^{248}	[15]
	10	$(C^3A^{253})\to((U^3B)^{64})$	2^{253}	第3.1节
	10	$(ACA^{253})\to(B^{256})$	2^{255}	第3.1节
Saturnin256	8	—	2^{253}	[16]
	9	$(C^{20}A^{236})\to(B^{256})$	2^{236}	第3.2节

注: —表示文献[16]仅给出代数次数评估, 未提供具体的积分区分器

1 基础知识

本节将介绍一些常用符号, 比特可分性的相关性质与二元矩阵定义以及 MILP 的 Indicator 约束和建模规则.

1.1 符 号

本节将对文中常用符号进行描述. $\mathbb{F}_2$ 表示只含有 0 和 1 两个元素的有限域, $\oplus$ 和+分别表示有限域 $\mathbb{F}_2$ 和整数环 $\mathbb{Z}$ 上的加法, $\mathbb{F}_2^n$ 表示 $\mathbb{F}_2$ 上的 n 维向量空间. 对于任意向量 $\boldsymbol{a}\in\mathbb{F}_2^n$, 记 $\boldsymbol{a}$ 的第 i 个的坐标为 a_i, 则 $\boldsymbol{a}$ 的汉明重量可以表示为 $wt(\boldsymbol{a})=\sum_{i=0}^{n-1}a_i$. 给定任意两个向量 $\boldsymbol{k}=(k_0,k_1,\ldots,k_{n-1}),\boldsymbol{k}'=(k'_0,k'_1,\ldots,k'_{n-1})\in\mathbb{F}_2^n$, 若对于任意的 i 都有 $k_i\geqslant k'_i$, 则称 $\boldsymbol{k}\geqslant\boldsymbol{k}'$; 否则, $\boldsymbol{k}\not\geqslant\boldsymbol{k}'$.

- 比特乘积函数 $\pi_u(\boldsymbol{x})$: 给定任意的 $\boldsymbol{u}\in\mathbb{F}_2^n$, 记 $\pi_u(\boldsymbol{x})$ 为一个 $\mathbb{F}_2^n\to\mathbb{F}_2$ 的函数. 对任意的 $\boldsymbol{x}\in\mathbb{F}_2^n$ 定义 $\pi_u(\boldsymbol{x})$ 如下:

$$\pi_{\boldsymbol{u}}(\boldsymbol{x})=\prod_{i=1}^{n}x_i^{u_i}.$$

- 代数正规型 ANF: 若 $f(\boldsymbol{x})$ 为一个 $\mathbb{F}_2^n\to\mathbb{F}_2$ 上的布尔函数, 则 $f(\boldsymbol{x})$ 的代数正规型表示为:

$$f(\boldsymbol{x})=\bigoplus_{\boldsymbol{u}\in\mathbb{F}_2^n}a_{\boldsymbol{u}}^f\left(\prod_{i=1}^{n}x_i^{u_i}\right)=\bigoplus_{\boldsymbol{u}\in\mathbb{F}_2^n}a_{\boldsymbol{u}}^f(\pi_{\boldsymbol{u}}(\boldsymbol{x})),$$

其中, $a_{\boldsymbol{u}}^f\in\{0,1\}$ 表示单项式 $\pi_{\boldsymbol{u}}(\boldsymbol{x})$ 的系数, 它的具体取值只与 f 和 $\boldsymbol{u}$ 有关.

1.2 比特可分性的相关性质与二元矩阵定义

比特可分性包括二子集比特可分性和三子集比特可分性. 本文只考虑二子集比特可分性, 因此本文提到的比

特可分性均表示二子集比特可分性.

定义 1. 比特可分性[5]. 令 $\mathbb{X}$ 是元素在 $\mathbb{F}_2^n$ 上的多重集, $\mathbb{K}$ 是元素在 $\mathbb{F}_2^n$ 上的集合, $\boldsymbol{u}\in\mathbb{F}_2^n$. 如果 $\mathbb{X}$ 满足如下条件, 那么称 $\mathbb{X}$ 有可分性 $\mathcal{D}_{\mathbb{K}}^{1,n}$:

$$\bigoplus_{\boldsymbol{x}\in\mathbb{X}}\pi_{\boldsymbol{u}}(\boldsymbol{x})=\begin{cases}\text{未知}, & \text{如果存在}\boldsymbol{k}\in\mathbb{K},\text{使得}\boldsymbol{u}\succcurlyeq\boldsymbol{k};\\ 0, & \text{其他}.\end{cases}$$

定义 2. 可分迹[8]. 记 f_r 为一个迭代分组密码的轮函数, 假设算法的输入集合有初始可分性 $\mathcal{D}_{\mathbb{K}_0}^{n,m}$, 记可分性经过轮函数 f_r 传播 i 轮后的可分性为 $\mathcal{D}_{\mathbb{K}_i}^{n,m}$, 则有如下的可分性传播链:

$$\{\boldsymbol{k}\}\triangleq\mathbb{K}_0\xrightarrow{f_r}\mathbb{K}_1\xrightarrow{f_r}\mathbb{K}_2\xrightarrow{f_r}\cdots\xrightarrow{f_r}\mathbb{K}_r,$$

并且对任意的 $\boldsymbol{k}_i^*\in\mathbb{K}_i$ $(i\geqslant 1)$, 一定存在向量 $\boldsymbol{k}_{i-1}^*\in\mathbb{K}_{i-1}$ 使得 $\boldsymbol{k}_{i-1}^*$ 可以传播到 $\boldsymbol{k}_i^*$. 进一步地, 对于 $(\boldsymbol{k}_0,\boldsymbol{k}_1,\ldots,\boldsymbol{k}_r)\in\mathbb{K}_0\times\mathbb{K}_1\times\ldots\times\mathbb{K}_r$, 如果对于任意的 $i\in\{1,2,\ldots,r\}$, k_{i-1} 都可以传播到那么就称 $(\boldsymbol{k}_0,\boldsymbol{k}_1,\ldots,\boldsymbol{k}_r)$ 为一条 r 轮的可分迹.

定义 3. 二元矩阵[13]. 对矩阵 $M'=(m'_{i,j})_{s\times s}\in F_{2^m}^{s\times s}$, 我们将其内部元素 $m'_{i,j}$ 表示成一个扩域 $\mathbb{F}_{2^m}\simeq\mathbb{F}[x]/(g(x))$ 上的一个多项式, 其中 g 是 $\mathbb{F}_2$ 上的一个 m 次不可约多项式, 如果矩阵 M' 中的元素均为 0 或者 1, 则称 M' 为一个二元矩阵. 否则, M' 为一个非二元矩阵.

1.3 MILP 的 Indicator 约束与可分性的建模规则

MILP 模型是一种在线性约束条件下求解线性目标函数的数学问题, 该模型 $\mathcal{M}$ 通常包含目标函数 (记为 $\mathcal{M}.obj$), 约束条件 (记为 $\mathcal{M}.con$) 和变量的取值范围 (记为 $\mathcal{M}.var$). 例如, 公式 (1) 给出了一个简单的 MILP 模型.

$$\mathcal{M}=\begin{cases}\mathcal{M}.obj\leftarrow\min\{x_1+2x_2+x_3\}\\ \mathcal{M}.con\leftarrow x_1+x_2+x_3\geqslant 2\\ \mathcal{M}.con\leftarrow x_1+x_2\leqslant 1\\ \mathcal{M}.var\leftarrow x_1,\ x_2,\ x_3\in\{0,\ 1\}\end{cases}\tag{1}$$

当求解 $\mathcal{M}$ 的目标函数 $x_1+2x_2+x_3$ 的最小值时, 变量 $x_1,\ x_2,\ x_3\in\{0,\ 1\}$ 需要同时满足约束条件 $x_1+x_2+x_3\geqslant 2$ 和 $x_1+x_2\leqslant 1$, 即上述变量的取值范围为所有约束条件的交集. 对于上述一般的 MILP 模型, 其变量需要满足所有的约束条件. 为了提高 MILP 模型的实用性, MILP 求解器一般内置了各种广义约束的添加方法, 例如 Indicator 约束. 相比于一般的 MILP 模型, 使用 Indicator 约束的 MILP 模型可以根据不同的初始条件设置不同的约束条件, 约束条件的形式为 $\mathcal{M}'.con\leftarrow z=f\rightarrow\mathcal{L}$, 其中 $f\in\{0,1\}$. 例如, 公式 (2) 给出了使用 Indicator 约束的 MILP 模型.

$$\mathcal{M}'=\begin{cases}\mathcal{M}'.obj\leftarrow\min\{x_1+2x_2+x_3\}\\ \mathcal{M}'.con\leftarrow x_3=1\rightarrow x_1+x_2+x_3\geqslant 2\\ \mathcal{M}'.con\leftarrow x_3=0\rightarrow x_1+x_2\leqslant 1\\ \mathcal{M}'.var\leftarrow x_1,\ x_2,\ x_3\in\{0,\ 1\}\end{cases}\tag{2}$$

模型 $\mathcal{M}'$ 中的约束条件表示当 $x_3=1$ 时, 变量 $x_1,\ x_2,\ x_3$ 需要满足约束条件 $x_1+x_2+x_3\geqslant 2$, 而 $x_3=0$ 时, 变量 $x_1,\ x_2,\ x_3$ 则可以违反约束条件 $x_1+x_2+x_3\geqslant 2$, 但需要满足约束条件 $x_1+x_2\leqslant 1$. 关于 Indicator 约束的详细内容请参考文献 [17].

本文利用 Indicator 约束构建 MILP 模型的过程中, 主要涉及以下 3 个建模规则, 更多建模规则请参考文献 [9,10].

模型 1. 复制[9]. 记 $a\xrightarrow{\text{复制}}(b_0,b_1,\ldots,b_{l-1})$ 表示将比特变量 a 复制为 l 个比特变量 $b_0,b_1,\ldots,b_{l-1}$, 下面的线性约束可描述复制操作的可分性传播.

$$\begin{cases}a-b_0-b_1-\ldots-b_{l-1}=0\\ a,b_0,b_1,\ldots,b_{l-1}\in\{0,1\}\end{cases}.$$

模型 2. 异或[9]. 记 $(a_0,a_1,\ldots,a_{l-1})\xrightarrow{\text{异或}}b$ 表示将 l 个比特变量 $a_0,a_1,\ldots,a_{l-1}$ 异或为比特变量 b, 下面的线性约束可描述异或操作的可分性传播.

$$\begin{cases}a_0+a_1+\ldots+a_{l-1}-b=0\\ a_0,a_1,\ldots,a_{l-1},b\in\{0,1\}\end{cases}.$$

模型 3. i 阶可逆子矩阵[10]. 记 $(u_0,u_1,\ldots,u_{n-1})\xrightarrow{M}(v_0,v_1,\ldots,v_{n-1})$ 表示复杂线性层矩阵 M 的可分迹, 下面的线性约束可描述输入汉明重量 $wt(u)=i\,(1\leqslant i\leqslant n-1)$ 的可分性传播, 其中 $M(j,*)$ 表示由矩阵 M 的第 j 行组成的行向量.

$$\begin{cases}\left(\bigoplus_{j=t_0}^{t_{i-1}}M(j,*)\right)(u_0,u_1,\ldots,u_{n-1})^{\mathrm{T}}-\sum_{j=t_0}^{t_{i-1}}v_j-(i-1),\quad t_0,t_1,\ldots,t_{i-1}\in\{0,1,\ldots,n-1\}\\ u_0,u_1,\ldots,u_{n-1},v_0,v_1,\ldots,v_{n-1}\in\{0,1\}\end{cases}.$$

更为具体的描述请参考文献 [10].

2 基于动态选取策略刻画线性层可分性传播

本节提出一种基于动态选取策略构建 MILP 模型的新方法, 该方法针对线性层不同汉明重量的输入可分性, 采取不同的技术刻画线性层的可分性传播. 对于一个 $\mathbb{F}_2^n$ 上的线性变换, 当输入可分性的汉明重量趋近 $n/2$ 时, 利用 $\mathcal{HZ}$ 方法刻画线性层的可分性传播; 否则, 将利用 $\mathcal{ZR}$ 方法刻画线性层的可分性传播. 本节将首先介绍 $\mathcal{ZR}$ 方法和 $\mathcal{HZ}$ 方法, 并简要分析上述两种方法的优缺点; 其次, 详细介绍动态选取策略构建 MILP 模型的建模过程; 最后, 从理论上证明动态选取策略构建 MILP 模型不弱于 $\mathcal{SW}$ 方法、$\mathcal{EY}$ 方法、$\mathcal{HZ}$ 方法.

2.1 两种刻画线性层可分性传播的方法

本文主要通过动态选择 $\mathcal{ZR}$ 方法和 $\mathcal{HZ}$ 方法构建可分性传播的 MILP 模型, 因此本节先详细介绍上述两种方法.

2.1.1 $\mathcal{ZR}$ 方法简介

Zhang 等人[10]通过研究线性层可分性传播和线性层可逆子矩阵之间的关系, 提出精确刻画线性层可分性传播的方法.

定理 1[10]. 对矩阵 $M\in\mathbb{F}_2^{n\times n}$, 记 $\boldsymbol{u},\boldsymbol{v}\in\mathbb{F}_2^n$ 分别为矩阵 M 的输入可分性和输出可分性, 即 $(u_0,u_1,\ldots,u_{n-1})\xrightarrow{M}(v_0,v_1,\ldots,v_{n-1})$. $\boldsymbol{u}\xrightarrow{M}\boldsymbol{v}$ 是一条有效可分迹的充要条件是 $M_{v,u}$ 是可逆的, 其中 $M_{v,u}$ 表示以 $I_v=\{i,v_i=1\}$ 的索引作为行, $I_u=\{i,u_i=1\}$ 的索引作为列构成的 M 的子矩阵.

根据上述定理, 线性层的有效可分迹对应的子矩阵一定是可逆矩阵. 因此, Zhang 等人通过一组不等式 (记为 $\mathcal{L}_{\mathcal{ZR}}$) 刻画了线性层的所有可逆子矩阵, 从而构建线性层的可分性传播模型. 然而, 上述不等式刻画仅适用于二元矩阵. 对二元矩阵 $M'=(m'_{i,j})_{s\times s}\in F_{2^m}^{s\times s}$, 令 $n=s\times m$, 可以将 M' 表示成其本原矩阵 $M=(m_{i,j})_{n\times n}\in\mathbb{F}_2^{n\times n}$, 并将本原矩阵的行划分为 m 个陪集: $S_0=\{0,m,\ldots,(s-1)\times m\},S_1=\{1,m+1,\ldots,(s-1)\times m+1\},\ldots,S_{m-1}=\{m-1,2m-1,\ldots,sm-1\}$, 则在不同陪集中对应元素的列没有相同的非 0 元素, 因此在刻画二元矩阵可分性传播的过程中可以分别考虑每一列的异或, 即只需刻画每个陪集对应的行所组成的可逆子矩阵, 所需不等式的数量为 $\#\mathcal{L}_{\mathcal{ZR}}=m\left(\sum_{i=1}^{s-1}C_s^i+1\right)=m\times(2^s-1)$. 对于非二元矩阵的本原矩阵 $M=(m_{i,j})_{n\times n}\in\mathbb{F}_2^{n\times n}$ 则无法与二元矩阵一样进行矩阵行的陪集划分. 通常需要将矩阵的所有行作为一个集合, 从而刻画所有阶的可逆子矩阵. 当 $i\in\{1,2,\ldots,n-1\}$ 时, 刻画 i 阶可逆子矩阵所需不等式的数量为 $\#\mathcal{L}_{\mathcal{ZR}_i}=C_n^i$; 当 $i\in\{0,n\}$ 时, 需要约束条件 $w(\boldsymbol{u})=w(\boldsymbol{v})$ 刻画可分性的传播. 因此, 利用 $\mathcal{ZR}$ 方法需要 $\#\mathcal{L}_{\mathcal{ZR}}=\sum_{i=1}^{n-1}\#\mathcal{L}_{\mathcal{ZR}_i}+1=\sum_{i=1}^{n-1}C_n^i+1=2^n-1$ 个约束不等式刻画非二元矩阵 $M\in\mathbb{F}_2^{n\times n}$ 的所有有效可分迹. 目前, 大多数密码算法线性层矩阵对应本原矩阵的阶数 n 均大于等于 16, 即利用 $\mathcal{ZR}$ 方法刻画非二元矩阵的可分性传播时, 需要的不等式数量至少为 $\#\mathcal{L}_{\mathcal{ZR}}=2^{16}-1=65535$. 受限于约束不等式的数量, 自动化求解器无法在有限的时间求解该方法构建的自动化模型.

2.1.2 $\mathcal{HZ}$ 方法简介

记密码算法线性层操作为 $\boldsymbol{y}=M\boldsymbol{x}\,(\boldsymbol{x},\boldsymbol{y}\in\mathbb{F}_2^n,M\in\mathbb{F}_2^{n\times n})$, 线性层优化实现算法按照可分性传播的角度可分为如下两类: (1) 线性层优化实现算法中异或操作的两个变量中不存在相同的元素, 例如 Paar 算法[18]; (2) 线性层优化实现算法中异或操作的两个变量中可能存在相同的元素, 例如 BP 算法[19]和 XZ 算法[20]. 研究表明: 当异或操作的

两个变量中不存在相同的元素时, 该优化实现刻画的可分性传播会删除 $\mathcal{SW}$ 方法中部分无效的可分迹; 当异或操作的两个变量中可能存在相同的元素时, 该优化实现刻画的可分性传播不仅会删除 $\mathcal{SW}$ 方法中部分无效可分迹, 同时也会引入 $\mathcal{SW}$ 方法中不包含的无效可分迹.

在文献 [12] 中, Hong 等人通过理论证明了利用 Paar 算法的优化实现刻画线性层可分性传播的精确程度不弱于 $\mathcal{SW}$ 方法. 同时, 利用 BP 和 XZ 算法的优化实现刻画线性层可分性传播可以进一步减少 $\mathcal{SW}$ 方法中的无效可分迹, 但其也引入了一些 $\mathcal{SW}$ 方法中不存在的无效可分迹. 因此, 作者通过同时考虑上述几种优化实现构建线性层可分性传播的 MILP 模型. 考虑到线性层优化实现算法中只是使用辅助变量减少了可分性传播过程中异或的次数, $\mathcal{HZ}$ 方法刻画的可分迹组成的子矩阵不一定都是可逆的, 该方法通常不能删除 $\mathcal{SW}$ 方法中的所有无效可分迹.

综上所述, $\mathcal{ZR}$ 方法和 $\mathcal{HZ}$ 方法均存在各自的优缺点. $\mathcal{ZR}$ 方法可以完全精确地刻画线性层的可分性传播, 但是它不能应用于非二元矩阵; 对于 $\mathcal{HZ}$ 方法, 它可以应用于任意复杂的线性层. 但是该方法仅能优于 $\mathcal{SW}$ 方法, 无法保证达到完全精确刻画线性层的可分性传播. 为了权衡精确性和实用性, 本节将介绍一种新技术刻画复杂线性层矩阵的可分性传播.

2.2 基于动态选取策略构建线性层可分性传播的 MILP 模型

在刻画复杂线性层矩阵 $M\in\mathbb{F}_2^{n\times n}$ 可分迹 $\boldsymbol{u}\xrightarrow{M}\boldsymbol{v}$ 的过程中, $\mathcal{ZR}$ 方法精确刻画输入汉明重量为 i $(1\leqslant i\leqslant n-1)$ 的可分迹所需不等式的数量为 $\#\mathcal{L}_{\mathcal{ZR}_i}=C_n^i$, 显然随着输入可分性汉明重量的逐渐增加使用 $\mathcal{ZR}$ 方法刻画可分性传播所需的不等式数量先增加后减少, 并在输入可分性汉明重量趋近 $n/2$ 时达到最大. 事实上, 当输入可分性汉明重量对应的可分迹刻画不等式数量较多时, 我们可以用 $\mathcal{HZ}$ 方法代替 $\mathcal{ZR}$ 方法, 且此时 MILP 模型可以在有限的时间内求解, 我们将这种根据输入可分性汉明重量的不同而采取不同方法刻画可分迹构建 MILP 模型的方法称为动态选取策略, 并且结合 Indicator 约束建模, 我们可以很自然的实现上述 MILP 建模.

对矩阵 $M\in\mathbb{F}_2^{n\times n}$, 其输入可分性汉明重量 $wt(\boldsymbol{u})\in\{0,1,\ldots,n\}$ 共 $n+1$ 情况, 我们将这 $n+1$ 种情况根据 $\mathcal{ZR}$ 方法所需不等式数量进行分类: 即将集合 $\{0,1,\ldots,n\}$ 划分为 $\{0,n\},\Theta_{\mathcal{ZR}},\Theta_{\mathcal{HZ}}$ 这 3 个部分, 其中 $\Theta_{\mathcal{ZR}}$ 表示 $\mathcal{ZR}$ 方法中精确刻画可分迹所需不等式数量较少的那些输入汉明重量的集合, $\Theta_{\mathcal{HZ}}=\{1,2,\ldots,n-1\}\backslash\Theta_{\mathcal{ZR}}$. 由于 Indicator 约束 $z=f\to\mathcal{L}$ 中 $f\in\{0,1\}$, 而输入汉明重量的取值并不只有 0 和 1 两种情况, 在使用 Indicator 约束对输入汉明重量进行分类时需要借助临时变量表示不同的汉明重量. 具体地, 对 $wt(\boldsymbol{u})\in\{0,1,\ldots,n\}$, 用 $\lfloor\log_2 n\rfloor+1$ 维向量 $\boldsymbol{a}=(a_0,a_1,\ldots,a_{\lfloor\log_2 n\rfloor})\in\{(0,0,\ldots,0),(0,0,\ldots,1),\ldots,(1,0,\ldots,0)\}$ 表示输入可分性汉明重量的全部情况, 其中 $2^{\lfloor\log_2 n\rfloor}a_0+2^{\lfloor\log_2 n\rfloor-1}a_1+\ldots+2^0a_{\lfloor\log_2 n\rfloor}=wt(\boldsymbol{u})$. 然后将向量 $\boldsymbol{a}$ 的维数扩充 3 维:

$$\begin{cases}(\underbrace{0,0,\ldots,0,0}_{\lfloor\log_2 n\rfloor+1\text{个}0})\\(0,0,\ldots,0,1)\\(0,0,\ldots,1,0)\\(0,0,\ldots,1,1)\\\quad\vdots\\(0,1,\ldots,1,0)\\(0,1,\ldots,1,1)\\(1,0,\ldots,0,0)\end{cases}\to\begin{cases}(\underbrace{0,0,\ldots,0,0}_{\lfloor\log_2 n\rfloor+1\text{个}0},a_{\lfloor\log_2 n\rfloor+1},a_{\lfloor\log_2 n\rfloor+2},a_{\lfloor\log_2 n\rfloor+3})\\(0,0,\ldots,0,1,a_{\lfloor\log_2 n\rfloor+1},a_{\lfloor\log_2 n\rfloor+2},a_{\lfloor\log_2 n\rfloor+3})\\(0,0,\ldots,1,0,a_{\lfloor\log_2 n\rfloor+1},a_{\lfloor\log_2 n\rfloor+2},a_{\lfloor\log_2 n\rfloor+3})\\(0,0,\ldots,1,1,a_{\lfloor\log_2 n\rfloor+1},a_{\lfloor\log_2 n\rfloor+2},a_{\lfloor\log_2 n\rfloor+3})\\\quad\vdots\\(0,1,\ldots,1,0,a_{\lfloor\log_2 n\rfloor+1},a_{\lfloor\log_2 n\rfloor+2},a_{\lfloor\log_2 n\rfloor+3})\\(0,1,\ldots,1,1,a_{\lfloor\log_2 n\rfloor+1},a_{\lfloor\log_2 n\rfloor+2},a_{\lfloor\log_2 n\rfloor+3})\\(1,0,\ldots,0,0,a_{\lfloor\log_2 n\rfloor+1},a_{\lfloor\log_2 n\rfloor+2},a_{\lfloor\log_2 n\rfloor+3})\end{cases},$$

其中, $a_{\lfloor\log_2 n\rfloor+1},a_{\lfloor\log_2 n\rfloor+2},a_{\lfloor\log_2 n\rfloor+3}$ 的取值根据前 $\lfloor\log_2 n\rfloor+1$ 个变量表示的汉明重量以及汉明重量的分类情况 $\{0, n\}$, $\Theta_{\mathcal{ZR}},\Theta_{\mathcal{HZ}}$ 分别取 $(1,0,0),(0,1,0),(0,0,1)$. 具体地, 当 $wt(\boldsymbol{u})\in\{0,n\}$ 时, $a_{\lfloor\log_2 n\rfloor+1}=1$; 当 $wt(\boldsymbol{u})\in\Theta_{\mathcal{ZR}}$ 时, $a_{\lfloor\log_2 n\rfloor+2}=1$; 当 $wt(\boldsymbol{u})\in\Theta_{\mathcal{HZ}}$ 时, $a_{\lfloor\log_2 n\rfloor+3}=1$. 然后对这 $n+1$ 个扩充维数后的点集进行不等式刻画 (不等式记为 $\mathcal{L}_{wt}$), 并将 $\mathcal{L}_{wt}$ 添加到 MILP 模型中. 显然 $a_{\lfloor\log_2 n\rfloor+1},a_{\lfloor\log_2 n\rfloor+2},a_{\lfloor\log_2 n\rfloor+3}$ 与 Indicator 约束 $z=f\to\mathcal{L}$ 中的 f 对应, 而相应的 $\mathcal{L}$ 分别选

取 $w(\boldsymbol{u})=w(\boldsymbol{v}),\mathcal{L}_{\mathcal{ZR}},\mathcal{L}_{\mathcal{HZ}}$, 至此, 动态选取策略构建 MILP 模型的过程结束. 值得注意的是, 在上述动态选取过程中我们将输入可分性汉明重量分为 3 类: $\{0,n\},\Theta_{\mathcal{ZR}},\Theta_{\mathcal{HZ}}$, 事实上, 在集合 $\Theta_{\mathcal{ZR}}$ 中, 每个汉明重量对应的不等式数量较少, 但集合中所有元素的不等式求和的数量依旧比较大, 因此我们可以对集合 $\Theta_{\mathcal{ZR}}$ 进行再次分类, 只需将向量 $\boldsymbol{a}$ 的维数与 $n+1$ 个点进行相应的更改即可. 例如: 将输入可分性汉明重量分类情况由 3 种情况更改为 r 种情况, 即向量 $\boldsymbol{a}$ 的扩充维数由 3 维改为 r 维, 此时 $\Theta_{\mathcal{ZR}}$ 分为 $r-2$ 部分: $\Theta_{\mathcal{ZR}0},\Theta_{\mathcal{ZR}1},\ldots,\Theta_{\mathcal{ZR}r-3}$, 同时 $(a_{\lfloor\log_2 n\rfloor+1},a_{\lfloor\log_2 n\rfloor+2},a_{\lfloor\log_2 n\rfloor+3})$ 更改为 $a'_{\lfloor\log_2 n\rfloor+1},a'_{\lfloor\log_2 n\rfloor+2},\ldots,a'_{\lfloor\log_2 n\rfloor+r}$, 其中 $a'_{\lfloor\log_2 n\rfloor+1}=a_{\lfloor\log_2 n\rfloor+1}$, $a'_{\lfloor\log_2 n\rfloor+r}=a_{\lfloor\log_2 n\rfloor+2}$, 而 $a'_{\lfloor\log_2 n\rfloor+2},a'_{\lfloor\log_2 n\rfloor+3},\ldots,a'_{\lfloor\log_2 n\rfloor+r-1}$ 的取值则根据新的 $\Theta_{\mathcal{ZR}}$ 的分类情况分别取 $(1,0,\ldots,0)$, $(0,1,\ldots,0)$, $(0,0,\ldots,1)$. 下面将通过一个例子介绍基于动态选取策略构建线性层可分性传播 MILP 模型的具体过程.

例 1: 假设矩阵 $\boldsymbol{M}\in\mathbb{F}_2^{8\times 8}$, 记其输入可分性 $\boldsymbol{u}=(u_0,u_1,\ldots,u_7)\in\mathbb{F}_2^8$, 输出可分性 $\boldsymbol{v}=(v_0,v_1,\ldots,v_7)\in\mathbb{F}_2^8$. 通过如下 3 个步骤可构建该矩阵可分性传播的 MILP 模型.

● 汉明重量的点集刻画: 矩阵 $\boldsymbol{M}$ 输入可分性的汉明重量 $wt(\boldsymbol{u})\in\{0,1,\ldots,8\}$. 对 $wt(\boldsymbol{u})$ 的上述所有情况, 我们用 4 维向量 $\boldsymbol{a}=(a_0,a_1,a_2,a_3)\in\{(0,0,0,0),(0,0,0,1),\ldots,(1,0,0,0)\}$ 刻画矩阵 $\boldsymbol{M}$ 输入可分性汉明重量的所有情况, 其中 $wt(\boldsymbol{u})=8a_0+4a_1+2a_2+a_3$.

● 动态选取汉明重量: 将向量 $\boldsymbol{a}$ 的维数扩充 6 维: $(a_0,a_1,\ldots,a_9)$, 其中 $a_4,a_5,\ldots,a_9$ 的取值表示输入可分性汉明重量的分类情况, 例如下面的集合 D 的分类情况为: $\{0,n\}=\{0,8\}$, $\Theta_{\mathcal{ZR}}=\{1,2,6,7\},\Theta_{\mathcal{HZ}}=\{3,4,5\}$, 并将 $\Theta_{\mathcal{ZR}}$ 继续分为 4 个部分 $\Theta_{\mathcal{ZR}_0}=\{1\},\Theta_{\mathcal{ZR}_1}=\{2\},\Theta_{\mathcal{ZR}_2}=\{6\},\Theta_{\mathcal{ZR}_3}=\{7\}$, 此时集合 D 的动态选取规则为: 当 $a_4=1$ 时, $wt(\boldsymbol{u})$ 为 0 或 8; 当 $a_5=1$ 时, $wt(\boldsymbol{u})$ 为 1; 当 $a_6=1$ 时, $wt(\boldsymbol{u})$ 为 2; 当 $a_7=1$ 时, $wt(\boldsymbol{u})$ 为 6; 当 $a_8=1$ 时, $wt(\boldsymbol{u})$ 为 7; 当 $a_9=1$ 时, $wt(\boldsymbol{u})$ 为 4 或 5 或 6. 最后用 $(a_0,a_1,\ldots,a_9)$ 的约束不等式集 $\mathcal{L}_{wt}$ 刻画集合 D.

$$D=\begin{cases}(0,0,0,0,1,0,0,0,0,0)\\(0,0,0,1,0,1,0,0,0,0)\\(0,0,1,0,0,0,1,0,0,0)\\(0,0,1,1,0,0,0,0,0,1)\\(0,1,0,0,0,0,0,0,0,1)\\(0,1,0,1,0,0,0,0,0,1)\\(0,1,1,0,0,0,0,1,0,0)\\(0,1,1,1,0,0,0,0,1,0)\\(1,0,0,0,1,0,0,0,0,0)\end{cases},\quad \mathcal{L}_{wt}=\begin{cases}-a_4-a_5-a_6-a_8-a_9\geqslant -1\\-a_0+a_4\geqslant 0\\-a_3+a_5+a_8+a_9\geqslant 0\\-a_2+a_3-a_4-2a_5-a_8-a_9\geqslant -1\\a_2-a_7\geqslant 0\\a_2+a_4+a_5+a_9\geqslant 1\\-a_1+a_7+a_8+a_9\geqslant 0\\a_1+a_4+a_5+a_6+a_9\geqslant 1\\-a_3-a_7\geqslant -1\\a_1+a_2-a_9\geqslant 0\\-a_6-a_7\geqslant -1\\-a_1-a_2-a_9\geqslant -2\end{cases}.$$

● Indicator 约束建模: 根据上一步可知, $a_i=1$ $(4\leqslant i\leqslant 9)$ 对应矩阵 $\boldsymbol{M}$ 输入可分性汉明重量的某种分类情况. 考虑到 Indicator 约束的一般形式 $z=f\to\mathcal{L}$, 其中 $f\in\{0,1\}$. 因此可以添加如下约束刻画矩阵 $\boldsymbol{M}$ 的可分性传播.

$$\mathcal{L}_{\text{Indicator}}=\begin{cases}a_4=1\to w(\boldsymbol{u})=w(\boldsymbol{v})\\a_5=1\to\mathcal{L}_{\mathcal{ZR}_1}\\a_6=1\to\mathcal{L}_{\mathcal{ZR}_2}\\a_7=1\to\mathcal{L}_{\mathcal{ZR}_6}\\a_8=1\to\mathcal{L}_{\mathcal{ZR}_7}\\a_9=1\to\mathcal{L}_{\mathcal{HZ}}\end{cases}.$$

其中, $\mathcal{L}_{\mathcal{ZR}_i}$ 表示利用 $\mathcal{ZR}$ 方法刻画输入汉明重量为 i $(i\in\{1,2,6,7\})$ 的可分性传播使用的不等式, 具体可参照模型 3 与文献 [10], $\mathcal{L}_{\mathcal{HZ}}$ 表示利用 $\mathcal{HZ}$ 方法构建可分性传播的不等式, 具体可参照模型 1、模型 2 与文献 [9].

根据上述 3 个步骤, 通过不等式集合 $\mathcal{L}=\{8a_0+4a_1+2a_2+a_3=wt(\boldsymbol{u}),\mathcal{L}_{wt},\mathcal{L}_{\text{Indicator}}\}$ 作为约束条件, 可以构建更加精确的线性层可分性传播的 MILP 模型. 该技术的建模过程如算法 1 所示.

算法 1. 构建基于动态选取策略刻画线性层可分性传播的 MILP 模型.

输入: 一个复杂线性层矩阵 $M\in\mathbb{F}_2^{n\times n}$, 其输入可分性 $\boldsymbol{u}=(u_0,u_1,\ldots,u_{n-1})\in\mathbb{F}_2^n$, 输出可分性 $\boldsymbol{v}=(v_0,v_1,\ldots,v_{n-1})\in\mathbb{F}_2^n$, $n+1$ 个点的集合 $D=\{(a_{0,0},a_{0,1},\ldots,a_{0,\lfloor\log_2 n\rfloor+r}),\ldots,(a_{1,0},a_{1,1},\ldots,a_{1,\lfloor\log_2 n\rfloor+r}),(a_{n,0},a_{n,1},\ldots,a_{n,\lfloor\log_2 n\rfloor+r})\}$, 集合元素 $(a_0,a_1,\ldots,a_{\lfloor\log_2 n\rfloor+r})\in D$ 中 $a_i\in\{0,1\}(0\leqslant i\leqslant\lfloor\log_2 n\rfloor+r)$, 且 $2^{\lfloor\log_2 n\rfloor}a_0+2^{\lfloor\log_2 n\rfloor-1}a_1+\ldots+2^0a_{\lfloor\log_2 n\rfloor}\in\{0,1,\ldots,n\}$; 另外, r 表示将输入可分性汉明重量分为 r 种情况: $\{0,n\},\Theta_{\mathcal{ZR}_0},\Theta_{\mathcal{ZR}1},\ldots,\Theta_{\mathcal{ZR}_{r-3}},\Theta_{\mathcal{HZ}}$, 相应每种分类中对应元素 $(a_{\lfloor\log_2 n\rfloor+1},a_{\lfloor\log_2 n\rfloor+2},\ldots,a_{\lfloor\log_2 n\rfloor+r})$ 分别取 $(1,0,\ldots,0),(0,1,\ldots,0),(0,0,\ldots,1)$;

输出: 矩阵 M 可分性传播的约束条件 $\mathcal{L}$.

1) **begin**
2) $\mathcal{L}\leftarrow$ 刻画集合 D 中元素 $(a_0,a_1,\ldots,a_{\lfloor\log_2 n\rfloor+r})$ 的约束集 $\mathcal{L}_{wt}$
3) $\mathcal{L}\leftarrow 2^{\lfloor\log_2 n\rfloor}a_0+2^{\lfloor\log_2 n\rfloor-1}a_1+\ldots+2^0a_{\lfloor\log_2 n\rfloor}=wt(u)$ // $(a_0,a_1,\ldots,a_{\lfloor\log_2 n\rfloor})$ 与输入可分性汉明重量 $wt(\boldsymbol{u})$ 对应
4) **for** $i=0$ to n **do**
5) **if** $i\in\{0,n\}$
6) $\mathcal{L}\leftarrow(a_{\lfloor\log_2 n\rfloor+1}=1\rightarrow w(\boldsymbol{u})=w(\boldsymbol{v}))$
7) **else if** $i\in\Theta_{\mathcal{ZR}_0}\cup\Theta_{\mathcal{ZR}_1}\cup\ldots\cup\Theta_{\mathcal{ZR}_{r-3}}$
8) **for** $j=0$ to $r-3$ **do**
9) $\mathcal{L}\leftarrow(a_{\lfloor\log_2 n\rfloor+j+2}=1\rightarrow\mathcal{L}_{\mathcal{ZR}_i})$ // $\mathcal{L}_{\mathcal{ZR}_i}$ 表示用 $\mathcal{ZR}$ 方法刻画 $wt(\boldsymbol{u})=i$ 可分性传播所需不等式
10) **end for**
11) **else if** $i\in\Theta_{\mathcal{HZ}}$
12) $\mathcal{L}\leftarrow(a_{\lfloor\log_2 n\rfloor+r}=1\rightarrow\mathcal{L}_{\mathcal{HZ}})$ // $\mathcal{L}_{\mathcal{HZ}}$ 表示用 $\mathcal{HZ}$ 方法刻画可分性传播所需不等式
3) **end if**
14) **end for**
15) **return** $\mathcal{L}$
16) **end**

值得注意的是: 当 $\Theta_{\mathcal{HZ}}=\varnothing$ 时, 此时动态选取策略退化为 $\mathcal{ZR}$ 方法, 且不适用于复杂线性层矩阵 $M\in\mathbb{F}_2^{n\times n}$, 因此对上述分类情况中 $\{0,n\}$, $\Theta_{\mathcal{ZR}},\Theta_{\mathcal{HZ}}$ 的取值范围需要进行进一步的限制, 我们建议当 n=16 时, 分类为 $\{0,16\}$, $\Theta_{\mathcal{ZR}}\subseteq\{1,2,3,4,12,13,14,15\},\Theta_{\mathcal{HZ}}=\{1,2,\ldots,15\}\backslash\Theta_{\mathcal{ZR}}$; 当 n=32 时, 分类为 $\{0,32\}$, $\Theta_{\mathcal{ZR}}\subseteq\{1,2,3,29,30,31\}$, $\Theta_{\mathcal{HZ}}=\{1,2,\ldots,31\}\backslash\Theta_{\mathcal{ZR}}$; 当 $n>32$ 时, 分类为 $\{0,n\}$, $\Theta_{\mathcal{ZR}}\subseteq\{1,2,n-2,n-1\}$, $\Theta_{\mathcal{HZ}}=\{1,2,\ldots,n-1\}\backslash\Theta_{\mathcal{ZR}}$.

2.3 动态选取策略刻画线性层可分性传播的分析

动态选取策略刻画线性层可分性传播的方法并不局限于用 $\mathcal{HZ}$ 方法代替 $\mathcal{ZR}$ 方法刻画输入汉明重量对应可分迹不等式较多的情况, $\mathcal{SW}$ 方法同样适用. 本文采用 $\mathcal{HZ}$ 方法的主要原因是 $\mathcal{HZ}$ 方法刻画线性层可分性传播的精确程度不弱于 $\mathcal{SW}$ 方法[12]. 本质上动态选取策略是通过 $\mathcal{ZR}$ 方法结合 $\mathcal{SW}$ 方法或 $\mathcal{HZ}$ 方法刻画线性层的可分性传播. 假设 X 方法为 $\mathcal{SW}$ 方法和 $\mathcal{HZ}$ 方法中的任意一种, 并将 $\mathcal{ZR}$ 方法结合 X 方法记为 $\mathcal{Z}$+X. 接下来, 本节将讨论 $\mathcal{ZR}$+X 方法不弱于 X 方法的理论依据.

给定一个可逆矩阵 $P\in\mathbb{F}_2^{n\times n}$, 记其输入可分性为 $\boldsymbol{u}=(u_0,u_1,\ldots,u_{n-1})\in\mathbb{F}_2^n$. 假设将线性层的输入可分性按照汉明重量的不同划分为 m $(2\leqslant m\leqslant n)$ 类情况, 随后将上述 m 类情况分别通过 $\mathcal{ZR}$ 方法或 X 方法刻画线性层的可分性传播. 根据定理 1, 当使用 $\mathcal{ZR}$ 方法刻画线性层的可分性传播时, 其可分迹对应的 $wt(\boldsymbol{u})$ 阶子矩阵一定为可逆矩阵. 然而根据文献 [12], 当使用 X 方法刻画线性层的可分性传播时, 其可分迹对应的 $wt(\boldsymbol{u})$ 阶子矩阵一定包含置换矩阵. 因此, $\mathcal{ZR}$+X 方法刻画线性层可分性传播的可分迹由如下两部分组成: (1) 当某些输入可分性采用 $\mathcal{ZR}$ 方法刻画线性层可分性传播时, 其可分迹对应的子矩阵一定为可逆矩阵. (2) 当某些输入可分性采用 X 方法刻画线性层

可分性传播时, 其可分迹对应的子矩阵一定包含置换矩阵. 然而, 一个可逆矩阵一定包含一个置换矩阵, 但包含置换矩阵的矩阵不一定为可逆矩阵. 例如: 一个矩阵的所有元素均为 1 时, 该矩阵包含单位矩阵作为置换矩阵, 但是该矩阵并不是一个可逆矩阵. 因此, 给定相同的输入可分性, X 方法得到的可分迹一定包含 $\mathcal{ZR}$ 方法的可分迹, 这也表明 X 方法的可分迹中可能包含无效的迹. 同样地, X 方法得到的可分迹一定包含 $\mathcal{ZR}$ + X 方法的可分迹. 基于上述分析, 我们可以推导出如下命题.

命题 1. 给定一个矩阵 $M \in \mathbb{F}_2^{n\times n}$ 以及相同的输入可分性, 通过 $\mathcal{ZR}$ + X 方法得到的可分迹一定是 X 方法的可分迹的子集.

上述命题可以说明 $\mathcal{ZR}$ + X 方法不弱于 X 方法, 即 $\mathcal{ZR}$ + X 方法可以删除 X 方法中的一些无效可分迹. 因此, $\mathcal{ZR}$ + $\mathcal{HZ}$ 方法刻画线性层可分性传播的精确程度不弱于 $\mathcal{HZ}$ 方法和 $\mathcal{SW}$ 方法. 而 $\mathcal{EY}$ 方法只是将 $\mathcal{ZR}$ 方法中不等式数量太多的情况结合首轮固定输入可分性一起考虑: 若初始可分性固定, 则首轮线性层的输入可分性只有少数几种情况, 由定理 1 可知此时线性层矩阵所有有效可分迹对应的子矩阵的列只有少数几种情况, 因此刻画所有可逆子矩阵时只需考虑少数几种列确定情况下的所有行, 对每种列确定的情况下组成的新的子矩阵, 根据高斯消元法将子矩阵转化为行阶梯型矩阵, 进而将子矩阵的可逆判断等价为矩阵行向量的线性无关判断从而进行可分性传播的刻画, 而中间轮的线性层仍然采用 $\mathcal{SW}$ 方法刻画可分性的传播. 考虑到大部分情况下初始可分性传播到首轮线性层时, 线性层输入可分性汉明重量一般属于集合 $\Theta_{\mathcal{ZR}}$, 因此 $\mathcal{EY}$ 方法刻画线性层可分性传播的精确程度不强于 $\mathcal{ZR}$ + $\mathcal{SW}$ 方法. 综上所述, 动态选取策略刻画线性层可分性传播的精确程度不弱于 $\mathcal{SW}$ 方法、$\mathcal{EY}$ 方法、$\mathcal{HZ}$ 方法, 且克服 $\mathcal{ZR}$ 方法难以在有效时间内求解复杂线性层矩阵的可分性传播模型的缺点.

3 基于动态选取策略搜索密码算法的积分区分器

本节通过动态选取策略的新技术构建 MILP 模型, 并搜索 uBlock 和 Saturnin 算法的积分区分器. 在比特可分性的传播过程中, 与常数异或不会改变比特可分性质. 因此, 在构建 MILP 模型的过程中仅需要考虑 S 盒和线性层. 对于 S 盒可分性传播的 MILP 建模可以参考文献 [8,21]; 对于复杂矩阵线性层矩阵的可分性传播则采取动态选取策略进行 MILP 建模. 为了方便起见, C^i, A^i, B^i, U^i 分别表示 i 个常数比特, 活跃比特, 平衡比特, 以及未知比特.

3.1 uBlock 算法积分区分器的搜索

uBlock 算法是一族 SPN 结构的分组密码, 其分组长度 n /密钥长度 k 分别为 128/128、128/256 和 256/256 比特, 分别记 uBlock128/128, uBlock128/256 和 uBlock256/256, 迭代轮数分别为 16, 24, 24 轮. 轮结构如图 1 所示.

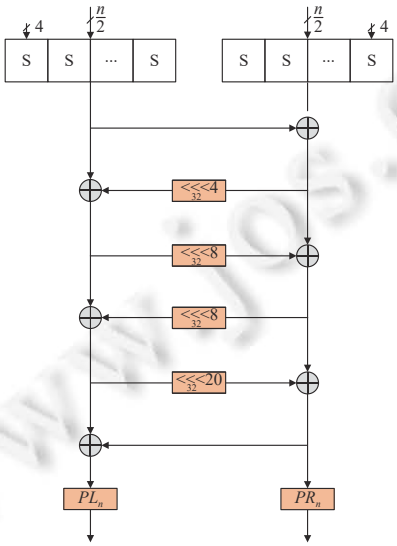


图 1 uBlock 算法轮结构

图 1 中 S 盒是一个 4 比特到 4 比特的双射, $\lll_{32} b$ 表示将输入字分成 32 比特的子块, 并在每一个子块上循环左移 b 比特, PL_n 、 PR_n 是基于字节的位置置换, 具体置换见表 2, 有关算法的详细描述请参考文献 [14].

表 2 位置置换 PL_n、PR_n 选择

PL_n/PR_n	置换选择
PL_{128}	{4, 0, 5, 1, 2, 7, 3, 6}
PR_{128}	{3, 4, 0, 7, 6, 2, 5, 1}
PL_{256}	{15, 8, 0, 4, 9, 14, 5, 1, 2, 6, 11, 13, 7, 3, 12, 10}
PR_{256}	{9, 2, 6, 13, 5, 15, 0, 8, 14, 4, 11, 1, 3, 10, 12, 7}

在 uBlock 算法轮结构中, S 盒的输出到 PL_n 、 PR_n 的输入的操作 $\lll_{32} b$ 中 b 的取值为 4 的倍数, 所以一系列 $\lll_{32} b$ 和 $\oplus$ 操作等价于 $n/16$ 个相同的矩阵 $M \in \mathbb{F}_2^{16\times 16}$.

$$M = \begin{pmatrix} A & B \\ B & C \end{pmatrix},$$

其中, A, B, C 均为 $\mathbb{F}_2^{8\times 8}$ 的循环矩阵.

$$A = \begin{pmatrix} 0&0&1&1&1&0&1&1 \\ 1&0&0&1&1&1&0&1 \\ 1&1&0&0&1&1&1&0 \\ 0&1&1&0&0&1&1&1 \\ 1&0&1&1&0&0&1&1 \\ 1&1&0&1&1&0&0&1 \\ 1&1&1&0&1&1&0&0 \\ 0&1&1&1&0&1&1&0 \end{pmatrix}, B = \begin{pmatrix} 1&1&0&1&0&1&1&1 \\ 1&1&1&0&1&0&1&1 \\ 1&1&1&1&0&1&0&1 \\ 1&1&1&1&1&0&1&0 \\ 0&1&1&1&1&1&0&1 \\ 1&0&1&1&1&1&1&0 \\ 0&1&0&1&1&1&1&1 \\ 1&0&1&0&1&1&1&1 \end{pmatrix}, C = \begin{pmatrix} 1&0&1&1&0&0&1&1 \\ 1&1&0&1&1&0&0&1 \\ 1&1&1&0&1&1&0&0 \\ 0&1&1&1&0&1&1&0 \\ 0&0&1&1&1&0&1&1 \\ 1&0&0&1&1&1&0&1 \\ 1&1&0&0&1&1&1&0 \\ 0&1&1&0&0&1&1&1 \end{pmatrix}.$$

对于 S 盒可分性传播的 MILP 建模采用文献 [8] 的方法; 对于复杂线性层矩阵 $M \in \mathbb{F}_2^{16\times 16}$ 可分性传播的刻画, 采用动态选取策略, 即通过算法 1 的框架构建 MILP 模型, 具体来说, 线性层输入可分性汉明重量分类情况为: $\{0,16\}$, $\Theta_{\mathcal{ZR}} = \{1,2,14,15\}$, $\Theta_{\mathcal{HZ}} = \{3,4,\ldots,13\}$, 并将 $\Theta_{\mathcal{ZR}}$ 继续分为 $\Theta_{\mathcal{ZR}_0} = \{1\}$, $\Theta_{\mathcal{ZR}_1} = \{2\}$, $\Theta_{\mathcal{ZR}_2} = \{14\}$, $\Theta_{\mathcal{ZR}_3} = \{15\}$ 这 4 种情况.

根据上述思想, 本文构建了搜索 uBlock128 算法积分区分器的 MILP 模型, 选择与文献 [15] 相同的初始可分性进行搜索得到多 32 个平衡比特的 8 轮积分区分器如下:

$$\left(C^4A^{124}\right) \overset{8轮}{\rightarrow} \left((BUB^2)^{32}\right).$$

事实上, 我们尝试过只使用 $\mathcal{ZR}$ 方法对 uBlock128 算法 8 轮积分区分器进行搜索以求得是否存在更多的平衡比特, 但其线性层需要的不等式数量为 $65535\times 8\times 8 = 4194304$ 个, 即使 MILP 模型在内存为 256 GB 的工作站中运行也会发生内存溢出, 进而无法求解. 而使用我们的模型在个人笔记本 16 GB 内存就能在有限时间内求解. 另外, 本文搜索到比之前最优区分器多一轮的 9 轮积分区分器.

$$\left(ACA^{126}\right) \overset{9轮}{\rightarrow} \left((U^3B)^{32}\right).$$

文献 [15] 中作者搜索到 uBlock256 算法的 9 轮积分区分器, 然而利用本文的模型, 则可以搜索到 uBlock256 算法的 10 轮积分区分器.

$$\left(C^3A^{253}\right) \overset{10轮}{\rightarrow} \left((U^3B)^{64}\right),$$

$$\left(ACA^{254}\right) \overset{10轮}{\rightarrow} \left(B^{256}\right).$$

3.2 Saturnin 算法积分区分器的搜索

Saturnin 算法是一种类 AES 结构算法, 分组长度和密钥长度均为 256 比特, 记为 Saturnin256/256, 默认迭代轮

数 r 为 20 轮, 使用者可以根据需求在 $r\in\{20,22,24,\ldots,62\}$ 中自由选择, 算法也可以将 2 轮看成一个合并轮, 其中算法轮结构包含 S 盒, 位置置换 Pslices 和 Psheets, 列混淆, 逆位置置换 Pslices^{-1} 和 Psheets^{-1}, 轮密钥加, 下面简述算法轮结构的具体操作.

● S 盒: 将 256 比特划分为 64 个 4 比特的半字节立方体, 如图 2 所示; 并对每个半字节做 S 盒变换, 采用 2 种不同的 S 盒, 当立方体索引为偶数时使用 S_0, 索引为奇数时使用 S_1, 其中 S_0 和 S_1 均为 4 比特到 4 比特的双射.

● 位置置换: 根据轮数 r 分别采用不同的位置置换 Pslices 和 Psheets, 其中 Pslices 和 Psheets 的操作层分别为 x,y 层和 y,z 层 (如图 3 所示).

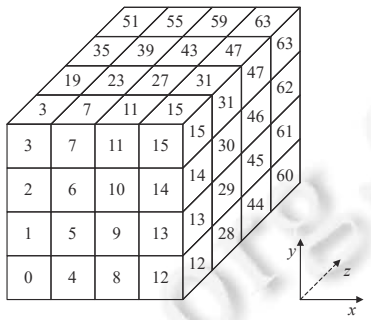


图 2 Saturnin 算法排列状态

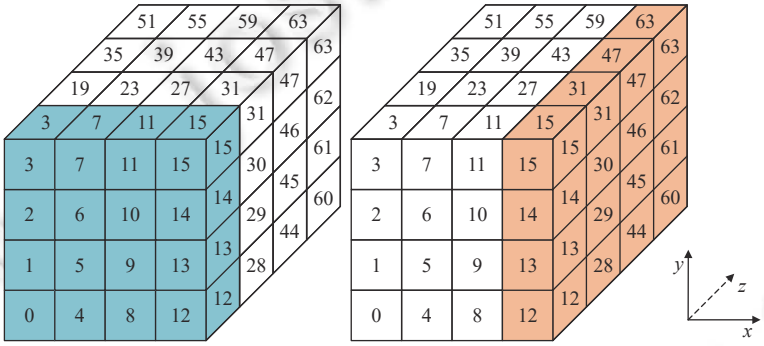


图 3 Saturnin 算法的 Pslices 和 Psheets 层

对 4 层进行相同的位置置换操作, 以一层为例, 结合轮数具体的操作为:

$$\begin{cases} r \bmod 4 = 0: \text{无操作} \\ r \bmod 4 = 1: \text{Pslices} \\ r \bmod 4 = 2: \text{无操作} \\ r \bmod 4 = 3: \text{Psheets} \end{cases} \begin{bmatrix} 3 & 7 & 11 & 15 \\ 2 & 6 & 10 & 14 \\ 1 & 5 & 9 & 13 \\ 0 & 4 & 8 & 12 \end{bmatrix} \xrightarrow{\text{Pslices}} \begin{bmatrix} 7 & 11 & 15 & 3 \\ 10 & 14 & 2 & 6 \\ 13 & 1 & 5 & 9 \\ 0 & 4 & 8 & 12 \end{bmatrix} \begin{bmatrix} 15 & 31 & 47 & 63 \\ 14 & 30 & 46 & 62 \\ 13 & 29 & 45 & 61 \\ 12 & 28 & 44 & 60 \end{bmatrix} \xrightarrow{\text{Psheets}} \begin{bmatrix} 31 & 47 & 63 & 15 \\ 46 & 62 & 14 & 30 \\ 61 & 13 & 29 & 45 \\ 12 & 28 & 44 & 60 \end{bmatrix}.$$

● 列混淆: 对立方体的全部 16 列作列变换, 使用的列混淆 MDS 矩阵 M 为:

$$M = \begin{pmatrix} \alpha^2 & \alpha^2+\alpha & 1 & 1 \\ 1 & \alpha+1 & \alpha^2+1 & \alpha^2+\alpha+1 \\ 1 & 1 & \alpha^2 & \alpha^2+\alpha \\ \alpha^2+1 & \alpha^2+\alpha+1 & 1 & \alpha+1 \end{pmatrix}, \quad \alpha = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \end{pmatrix}.$$

● 逆位置置换: 对经过列混淆操作后的位置置换根据轮数 r 做对应的逆位置置换, 有关轮密钥加和算法的详细描述请参考文献 [16].

与 uBlock 算法类似, 我们对 Saturnin 算法进行积分区分器搜索时, 采用文献 [8] 的方法对 S 盒可分性传播的 MILP 建模, 对每个列混淆 MDS 矩阵 $M\in\mathbb{F}_2^{16\times 16}$ 的可分性传播, 则采用动态选取策略, 即算法 1 的框架构建 MILP

模型: 根据线性层矩阵输入可分性汉明重量的不同进行分类 $\{0,16\}$, $\Theta_{\mathcal{ZR}}=\{1,2,14,15\}$, $\Theta_{\mathcal{HZ}}=\{3,4,\ldots,13\}$, 并将 $\Theta_{\mathcal{ZR}}$ 继续分为 $\Theta_{\mathcal{ZR}_0}=\{1\}$, $\Theta_{\mathcal{ZR}_1}=\{2\}$, $\Theta_{\mathcal{ZR}_2}=\{14\}$, $\Theta_{\mathcal{ZR}_3}=\{15\}$ 这 4 种情况, 对集合 $\{0,16\}$, 使用约束条件 $w(u)=w(v)$ 表示可分性的传播, 对集合 $\{3,4,\ldots,13\}$, 则使用约束不等式集 $\mathcal{L}_{\mathcal{HZ}}$ 表示可分性的传播, 对集合 $\{1\},\{2\},\{14\},\{15\}$ 则分别使用约束不等式集 $\mathcal{L}_{\mathcal{ZR}_1}$, $\mathcal{L}_{\mathcal{ZR}_2}$, $\mathcal{L}_{\mathcal{ZR}_{14}}$, $\mathcal{L}_{\mathcal{ZR}_{15}}$ 表示可分性的传播, 其中 $\mathcal{L}_{\mathcal{HZ}}$ 表示使用 $\mathcal{HZ}$ 方法构建可分性传播的不等式, $\mathcal{L}_{\mathcal{ZR}_1}$, $\mathcal{L}_{\mathcal{ZR}_2}$, $\mathcal{L}_{\mathcal{ZR}_{14}}$, $\mathcal{L}_{\mathcal{ZR}_{15}}$ 分别表示使用 $\mathcal{ZR}$ 方法构建输入可分性汉明重量为 1, 2, 14, 15 时可分性传播的不等式.

在文献 [16] 中, 作者利用代数次数估计的方法评估 Saturnin 算法抗积分分析的能力, 当初始可分性为 253 比特活跃时, Saturnin 算法存在 8 轮的积分区分器. 而如果只使用 $\mathcal{ZR}$ 方法对 Saturnin 算法线性层可分性传播进行建模, 8 轮线性层需要的不等式数量为 $65535\times16\times8=8388480$ 个, 这比 uBlock128 算法需要的数量更多, 在内存为 256 GB 的工作站中也会发生内存溢出无法求解的情况. 然而, 利用本文技术构建 MILP 建模可以在个人笔记本 16 GB 内存上得到活跃比特更少且轮数更长的 9 轮积分区分器:

$$\left(C^{20}A^{236}\right)\overset{9轮}{\rightarrow}\left(B^{256}\right).$$

4 总 结

本文提出了一种基于动态选取策略构建 MILP 模型的新技术, 并结合比特可分性理论构建了更加精确且实用的可分性传播模型. 该技术的优势是可以对点集进行分类描述, 打破传统 MILP 模型的约束条件需要满足全部点集的局限. 例如对特定百万量级甚至更高量级的点用较少的不等式精确刻画比较困难, 因此可以根据特定需求对点进行分类, 对每类较少的点进行不等式刻画. 基于上述思想, 本文将线性层的输入可分性按照汉明重量的不同进行划分, 并当输入可分性汉明重量趋近于 $n/2$ 时, 采用 $\mathcal{ZR}$ 方法刻画线性层的可分性传播; 否则, 采用 $\mathcal{HZ}$ 方法刻画线性层的可分性传播. 为了验证该技术的有效性, 本文将该技术应用于 uBlock 和 Saturnin 算法. 实验结果表明: 该技术可以搜索到 uBlock 和 Saturnin 算法当前最优的积分区分器, 且均比之前最优积分区分器多一轮. 同时, 该技术的思想可以应用于分析分组密码的其他密码性质, 如何利用该思想改进分组密码的其他分析技术可能是未来的一个研究方向.

References:

[1] Knudsen L, Wagner D. Integral cryptanalysis. In: Proc. of the 9th Int'l Workshop on Fast Software Encryption. Leuven: Springer, 2002. 112–127. [doi: 10.1007/3-540-45661-9_9]

[2] Todo Y. Structural evaluation by generalized integral property. In: Proc. of the 34th Annual Int'l Conf. on the Theory and Applications of Cryptographic Techniques. Sofia: Springer, 2015. 287–314. [doi: 10.1007/978-3-662-46800-5_12]

[3] Todo Y. Integral cryptanalysis on full MISTY1. In: Proc. of the 35th Annual Cryptology Conf. Santa Barbara: Springer, 2015. 413–432. [doi: 10.1007/978-3-662-47989-6_20]

[4] Sun B, Hai X, Zhang WY, Cheng L, Yang ZC. New observation on division property. Science China Information Sciences, 2017, 60(9): 098102. [doi: 10.1007/s11432-015-0376-x]

[5] Todo Y, Morii M. Bit-based division property and application to SIMON family. In: Proc. of the 23rd Int'l Conf. on Fast Software Encryption. Bochum: Springer, 2016. 357–377. [doi: 10.1007/978-3-662-52993-5_18]

[6] Mouha N, Wang QJ, Gu DW, Preneel B. Differential and linear cryptanalysis using mixed-integer linear programming. In: Proc. of the 7th Int'l Conf. on Information Security and Cryptology. Beijing: Springer, 2012. 57–76. [doi: 10.1007/978-3-642-34704-7_5]

[7] Sun SW, Hu L, Wang P, Qiao KX, Ma XS, Song L. Automatic security evaluation and (related-key) differential characteristic search: Application to SIMON, PRESENT, LBlock, DES(L) and other bit-oriented block ciphers. In: Proc. of the 20th Int'l Conf. on the Theory and Application of Cryptology and Information Security. Springer, 2014. 158–178. [doi: 10.1007/978-3-662-45611-8_9]

[8] Xiang ZJ, Zhang WT, Bao ZZ, Lin DD. Applying MILP method to searching integral distinguishers based on division property for 6 lightweight block ciphers. In: Proc. of the 22nd Int'l Conf. on the Theory and Application of Cryptology and Information Security. Hanoi: Springer, 2016. 648–678. [doi: 10.1007/978-3-662-53887-6_24]

[9] Sun L, Wang W, Wang MQ. MILP-aided bit-based division property for primitives with non-bit-permutation linear layers. IET Information Security, 2020, 14(1): 12–20. [doi: 10.1049/iet-ifs.2018.5283]

[10] Zhang WY, Rijmen V. Division cryptanalysis of block ciphers with a binary diffusion layer. IET Information Security, 2019, 13(2): 87–95. [doi: 10.1049/iet-ifs.2018.5151]

[11] ElSheikh M, Youssef AM. On MILP-based automatic search for bit-based division property for ciphers with (large) linear layers. In: Proc. of the 26th Australasian Conf. on Information Security and Privacy. Cham: Springer, 2021. 111–131. [doi: 10.1007/978-3-030-90567-5_6]

[12] Hong CL, Zhang SS, Chen SW, Lin D, Xiang ZJ. More accurate division property propagations based on optimized implementations of linear layers. In: Proc. of the 17th Int'l Conf. on Information Security and Cryptology. Cham: Springer, 2021. 212–232. [doi: 10.1007/978-3-030-88323-2_11]

[13] Hu K, Wang QJ, Wang MQ. Finding bit-based division property for ciphers with complex linear layers. IACR Trans. on Symmetric Cryptology, 2020, 2020(1): 396–424. [doi: 10.13154/tosc.v2020.i1.396-424]

[14] Wu WL, Zhang L, Zheng YF, Li LC. The block cipher uBlock. Journal of Cryptologic Research, 2019, 6(6): 690–703 (in Chinese with English abstract). [doi: 10.13868/j.cnki.jcr.000334]

[15] Tian WQ, Hu B. Integral cryptanalysis on two block ciphers Pyjamask and uBlock. IET Information Security, 2020, 14(5): 572–579. [doi: 10.1049/iet-ifs.2019.0624]

[16] Canteaut A, Duval S, Leurent G, Naya-Plasencia M, Perrin L, Pornin T, Schrottenloher A. Saturnin: A suite of lightweight symmetric algorithms for post-quantum security. IACR Trans. on Symmetric Cryptology, 2020, 2020(S1): 160–207. [doi: 10.13154/tosc.v2020.iS1.160-207]

[17] Gurobi Optimization, LLC. Gurobi optimizer reference manual. 2022. https://www.gurobi.com

[18] Paar C. Optimized arithmetic for Reed-Solomon encoders. In: Proc. of the 1997 IEEE Int'l Symp. on Information Theory. Ulm: IEEE, 1997. 250. [doi: 10.1109/ISIT.1997.613165]

[19] Boyar J, Matthews P, Peralta R. Logic minimization techniques with applications to cryptology. Journal of Cryptology, 2013, 26(2): 280–312. [doi: 10.1007/s00145-012-9124-7]

[20] Xiang ZJ, Zeng XY, Lin D, Bao ZZ, Zhang SS. Optimizing implementations of linear layers. IACR Trans. on Symmetric Cryptology, 2020, 2020(2): 120–145. [doi: 10.13154/tosc.v2020.i2.120-145]

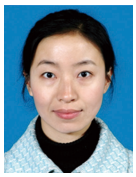
[21] Abdelkhalek A, Sasaki Y, Todo Y, Tolba M, Youssef AM. MILP modeling for (large) S-boxes to optimize probability of differential characteristics. IACR Trans. on Symmetric Cryptology, 2017, 2017(4): 99–129. [doi: 10.13154/tosc.v2017.i4.99-129]

附中文参考文献:

[14] 吴文玲, 张蕾, 郑雅菲, 李灵琛. 分组密码uBlock. 密码学报. 2019, 6(6): 690–703. [doi: 10.13868/j.cnki.jcr.000334]

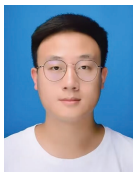
黄明(1996－), 男, 硕士, 主要研究领域为对称密码算法的安全性分析.

曾乐(2000－), 女, 本科生, 主要研究领域为对称密码算法的安全性分析.



张莎莎(1982－), 女, 博士, 副教授, 主要研究领域为对称密码算法的安全性分析.

向泽军(1990－), 男, 博士, 副教授, 主要研究领域为对称密码算法的安全性分析与设计.



洪春雷(1997－), 男, 博士生, 主要研究领域为分组密码的安全性分析.