计算机科学
COMPUTER SCIENCE

基于MILP的GIFT积分区分器搜索及优化

祖锦源, 刘杰, 石一鹏, 张涛, 张国群

引用本文

祖锦源, 刘杰, 石一鹏, 张涛, 张国群. 基于MILP的GIFT积分区分器搜索及优化[J]. 计算机科学, 2023, 50(11A): 220900231-8.

ZU Jinyuan, LIU Jie, SHI Yipeng, ZHANG Tao, ZHANG Guoqun. Search and Optimization of GIFT Integral Distinguisher Based on MILP [J]. Computer Science, 2023, 50(11A): 220900231-8.

计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.220900231

基于 MILP 的 GIFT 积分区分器搜索及优化

祖锦源[1]　刘　杰[1,2]　石一鹏[1]　张　涛[1]　张国群[3]
1 西北工业大学软件学院　西安 710000
2 西北工业大学长三角研究院　江苏 太仓 215400
3 上海机电工程研究所　上海 200000
(zujin@mail.nwpu.edu.cn)

摘　要　Banik 等提出的轻量级分组密码 GIFT 算法已经入选了 NIST 针对国际轻量级密码算法开展的标准化竞赛的最终轮。目前已有针对其的线性分析、差分分析等的相关研究,但针对 GIFT 的积分分析仍待进一步研究。针对 GIFT 在积分密码分析过程中可分路径表达冗余的问题,提出了基于混合整数线性规划模型的积分区分器搜索求解和优化算法。首先对 GIFT 算法创建 MILP 积分分析模型,利用可分性质分别对 GIFT 算法的线性层和非线性层进行刻画。对线性层利用传播规则进行表达;对非线性 S 盒在传播规则的基础上使用贪心算法对表达式进行精简优化,得到了 15 个不等式作为约束条件。经过 MILP 求解后,得到 64 个 9 轮积分区分器。在此基础上,针对基于贪心算法的 MILP 求解模型精确度不足问题,引入 MILP 模型对 S 盒的可分性质进行重新表达,设计基于 MILP 的约简算法对 GIFT 积分区分器搜索进行优化,并重新求解 MILP 模型,最高得到了 3 个 13 轮的积分区分器。因此,基于 MILP 的 S 盒新约简算法可以优化 S 盒可分性质的表达,有效增加对 GIFT 算法的积分区分器攻击轮数,提高积分攻击效果。

关键词:积分密码分析;混合整数线性规划算法;GIFT;可分性质;SPN 网络结构
中图法分类号　TN918.1

Search and Optimization of GIFT Integral Distinguisher Based on MILP

ZU Jinyuan[1],LIU Jie[1,2],SHI Yipeng[1],ZHANG Tao[1] and ZHANG Guoqun[3]
1 College of Software,Northwestern Polytechnical University,Xi'an 710000,China
2 Yangtze River Delta Research Institute,Nerthwestern Polytechnical University,Taicang,Jiangsu 215400,China
3 Shanghai Institute of Mechanical and Electrical Engineering,Shanghai 200000,China

Abstract　The lightweight block cipher GIFT algorithm proposed by Banik et al. has been selected for the final round of the NIST standardization competition for international lightweight cryptographic algorithms. At present,there have been linear analysis,difference analysis and other related studies,but the integral analysis of GIFT still needs to be further studied. Aiming at the problem of division trails expression redundancy in the process of integral cryptanalysis of GIFT,an integral dividers solution and search optimization algorithm based on mixed integer linear programming model(MILP) is proposed. Firstly,the linear layer and the nonlinear layer of the GIFT algorithm are respectively described according to their bit division property. The linear layer is expressed by the propagation rule,the greedy algorithm is used to simplify the expression for the nonlinear S-box based on the propagation rule,and 15 inequalities are obtained as constraint conditions. 64 9-round integral discriminators are found after the MILP solution. On this basis,in order to solve the problem of insufficient accuracy of the MILP solution model based on the greedy algorithm,the MILP model is introduced to reconstruct the bit division property of the S-box. Design a MILP-based reduction algorithm to optimize the GIFT integral dividers search,and re-solve the MILP model,then obtain two 13-round integral discriminators. Therefore,the MILP-based S-box new reduction algorithm can optimize the expression of the S-box division property,and can effectively increase the number of rounds of the integral dividers attack on the GIFT algorithm,and improve the integral attack effect.

Keywords　Integral cryptanalysis,Mixed integer linear programming(MILP),GIFT,Division property,SPN network structure

1　引言

随着万物互联概念的不断发展,以无线传感器为代表的物联网器件在日常生活中越来越常见,在工业生产中得到了越来越广泛的应用。但受限于其自身的计算能力和存储空间,以及其需要在较低能量供给的生产环境中完成自身计算、

基金项目:上海航天科技创新基金(SAST2021-054);太仓市基础研究计划面上项目(TC2021JC32);中央高校基本科研业务费专项资金(D5000210638)
This work was supported by the Shanghai Aerospace Science and Technology Innovation Fund(SAST2021-054),Taicang City Basic Research Program on Project Fund(TC2021JC32) and Fundamental Research Funds for the Central Universities(D5000210638).
通信作者:刘杰(lucky_jiel@ nwpu.edu.com)

通信、控制等工作的特点，如何在轻量级环境中保障可用性和环境适配性的同时追求更高安全性，得到了越来越多的关注，并成为了当前的焦点问题。随着研究的推进，轻量级密码算法和轻量级密码协议成为兼具性能和安全性的重要解决方案。此类算法构造简单，功耗低，一般用于资源受限的环境，如 PRESENT，LEA，LED，PUFFIN，TWINE，SIMON 和 SPECK 等。

GIFT[1]是一种基于混淆扩散网络(SPN)结构的轻量级分组密码算法，根据分组长度分为 GIFT-64 和 GIFT-128 两个版本。GIFT-64 的分组大小为 64 比特，需要迭代 28 轮，GIFT-128 则为 128 比特，迭代 40 轮，且加密和解密结构保持一致，算法的非线性层和线性层均采用对合构造，硬件实现所需的存储空间更小。GIFT 密码算法源自对著名的轻量级密码算法 PRESENT 的改进，即在 PRESENT 的基础上改进设计了 S 盒和 P 置换，使得其降低了资源消耗，提高了运行速度。迄今为止，对 GIFT 算法安全性攻击的研究方向主要有差分攻击[2]、能量分析攻击[3]、相关密钥攻击[4]，以及在 GIFT 被提出时给出的积分安全性分析[1]，其中积分攻击分析自提出便对各类密码算法特别是轻量级分组密码算法产生了重要威胁。积分分析最早源自对 Square 算法的攻击方法，即 Square 攻击[5]；在此基础上，Saturation 攻击[6]和 Multiset 攻击[7]相继被提出开展进一步的攻击。随后，Knudsen 和 Wagner 对这 3 种思想加以总结、整合、改进，正式提出了积分攻击。积分分析为拥有任意加密机的密钥恢复分析方法，也即选择明文攻击[8]，通过对特定输入的选择达到对应密文在指定位置的积分性质，精心搭建积分区分器。利用得到的积分区分器进行密钥猜解恢复，在有限区间内对正确密钥进行遍历。则通过区分器对密文解密后指定位置的字节或比特进行积分的结果也即异或和为常数。

积分攻击分析最早为攻击基于字节的密码算法而诞生，故其攻击方法同样基于字节，但当前较受关注的密码算法特别是轻量级密码大量采用基于比特设计的算法结构，不再单纯以字节为单位进行计算，导致原始的积分攻击无法对这类基于比特的密码算法进行攻击和安全性分析。Z'aba 等在 FSE2008 提出比特顺序的概念[9]，用特定比特位置的指定序列流对应原来的平衡、活跃字节等定义，利用元素出现的次数来判断是否平衡，完成了对以比特为单位的密码算法的积分分析，完善并丰富了传统积分攻击领域，极大地扩展了其适用领域。2015 年，Todo 将广义积分性质进行推广，得到了可分性质[10]的概念，并在 FSE2016 将可分性应用于基于比特涉及的密码算法[11]，给出了基于可分路径的传播规则，同时对基于可分性质的传递规则进行刻画，并对积分攻击中活跃集和平衡集的性质进行具体的数学刻画，2016 年，Xiang 等[12]首次提出了基于 MILP 的可分性质模型，并利用开源求解器 Gurobi 对 6 种轻量级密码进行自动化求解。但在 Xiang 等给出的 S 盒可分路径的表达中采用的贪心算法只限于局部最优，而非全局最优。Sun[13]和 Hu 等[14]针对更复杂线性层的可分性质给出了模型，并展开相关积分区分器搜索的研究。Shang 等将此方法应用到 PUFFIN 等多种密码算法上进行积分分析[15]。GIFT 算法的提出者给出了 GIFT 算法的积分分析结果以及 1 个具体的 9 轮积分区分器作为对 GIFT 安全性分析的结果。

2017 年，Sasaki 等[16]在差分路径寻找的基础上提出一种基于 MILP 模型的约简算法，通过简化差分路径等价表达的不等式组，获得了理论上全局最简解表达。针对原贪心算法在 S 盒表达上的冗余性问题，本文考虑将差分分析中提出的 MILP 约简思想用于积分分析攻击，优化积分分析的 MILP 模型并重新计算和求解，对 GIFT 密码算法进行积分分析，完成可分性建模和积分区分器的搜索。首先，对 GIFT 算法构造基于 MILP 的可分性模型，并且计算得到 GIFT 算法的积分区分器；然后，将 MILP 约简算法用于积分攻击的 S 盒可分路径建模，对 S 盒可分路径搜索进行优化；最后，针对新旧方法的攻击效果给出了对比说明。

2 基于比特可分性质的 MILP 模型

本节首先对可分性质的相关定义和符号进行解释说明，并针对可分性质和可分路径的含义展开阐述，随后分别详细说明了以复制、异或、与和 S 盒 4 种运算为代表的算法结构或操作对基于比特可分性质的传播规则和其对应的 MILP 不等式模型，最后对在差分攻击中提出的基于 MILP 的 S 盒约简思想展开说明。

2.1 符号说明

对于任意 $a\in F_2^n$（F_2^n 表示二元有限域 n 维向量），a 的第 i 个元素记为 $a[i]$，对 a 定义其汉明重量为 $w(a)=\sum_{i=0}^{n-1}a[i]$，则对于任意的 $a\in(F_2^{n_0}\times F_2^{n_1}\times\cdots\times F_2^{n_{m-1}})$，向量 a 的汉明重量为 $W(a)=(w(a_0),w(a_1),\cdots,w(a_{m-1}))\in Z^m$。对 k 和 k' 有 $k=(k_0,k_1,\cdots,k_{m-1})\in Z^m$，$k'=(k'_0,k_1',\cdots,k'_{m-1})\in Z^m$，则若对于任意的 i 都有 $k_i\geqslant k_i'$，则定义 $k\geqslant k'$，否则 $k\not\geqslant k'$。

比特积函数 $\pi_u(x)$ 和 $\pi_U(X)$ 的定义如下：对于任意 $u\in F_2^n$，令 $\pi_u(x)$ 为 $F_2^n\to F_2$ 上的函数，对任意 $x\in F_2^n$，有：

$$\pi_u(x)=\prod_{i=0}^{n-1}x[i]^{u[i]} \tag{1}$$

对于任意 $U\in(F_2^{n_0}\times F_2^{n_1}\times\cdots\times F_2^{n_{m-1}})$，令 $\pi_U(X)$ 为 $(F_2^{n_0}\times F_2^{n_1}\times\cdots\times F_2^{n_{m-1}})\to F_2$ 上的函数，对任意 $U=(u_0,u_1,\cdots,u_{m-1})\in(F_2^{n_0}\times F_2^{n_1}\times\cdots\times F_2^{n_{m-1}})$，$X=(x_0,x_1,\cdots,x_{m-1})\in(F_2^{n_0}\times F_2^{n_1}\times\cdots\times F_2^{n_{m-1}})$，有：

$$\pi_U(X)=\prod_{i=0}^{n-1}\pi_{u_i}(x_i) \tag{2}$$

2.2 基于比特的可分性质

定义 1（可分性质） 假设存在多重集 X：$X\in(F_2^{n_0}\times F_2^{n_1}\times\cdots\times F_2^{n_{m-1}})$，$k$ 为取值空间为 $[0,n_i]$ 的 m 维向量，若 X 具有可分性质 $D_{k^{(0)},k^{(1)},\cdots,k^{(q-1)}}^{n_0,n_1,\cdots,n_{m-1}}$，则其满足下面的约束关系：对所有 $x\in X$，且满足如下条件时，$\pi_U(X)$ 求和为偶：

$$U\in\{(u_0,\cdots,u_{m-1})\in(F_2^n)^m\mid W(U)\not\geqslant k^{(0)},\cdots,W(U)\not\geqslant k^{(q-1)}\}$$

也即当集合 X 满足：

$$\bigoplus_{x\in X}\pi_U(x)=\begin{cases}\text{不确定}, & \text{若存在 } k\in K,\text{使得 } W(U)\geqslant k\\ 0 & \text{其他情况}\end{cases}$$

时，称 X 具有可分性质 $D_K^{n_0,n_1,\cdots,n_{m-1}}$，其中 K 表示符合条件的向量 k 的集合。基于比特的可分性质，即令上述式子中的 $n_0=n_1=\cdots=n_{m-1}=1$，是特殊情况下的可分性表达，即为 $D_K^{1,1,\cdots,1}$，等价 $D_K^{1^m}$。

定义 2（可分路径） 设输入多重集为 X，X 具有可分性质，且初始可分性质为 $D_k^{n_0,n_1,\cdots,n_{m-1}}$，经 i 轮传播后的可分性质

记为 $D_{K_i}^{n_0,n_1,\cdots,n_{m-1}}$,则得到如下的传播路径:

$\{k\}\triangleq K_0\to K_1\to\cdots\to K_r$

因此对于任意向量:

$(k_0,k_1,\cdots,k_r)\in(K_0,K_1,\cdots,K_r)$

一定存在向量 k_{i-1} 能够传播到 k_i,那么一定存在一条 r 轮的可分路径$(k_0,k_1,\cdots,k_r)$。

2.3 基于比特可分性质的传播规则

规则 1(复制操作) 设 F 为 F_2 上的复制函数,其输入 $x\in X$ 多重集,其输出为$(y_0,y_1)=(x,x)$,则输入多重集 X 对应于满足可分性质 $D_K^{t^2}$ 的输出多重集 Y 的可分性质为 $D_{\{k\}}^{1^2}$,其中:

$$K=\begin{cases}\{(0,0)\}, & k=0\\ \{(0,1),(1,0)\}, & k=1\end{cases}\tag{3}$$

规则 2(异或操作) 设 F 为 $F_2\times F_2$ 上的异或函数,输入为(x_0,x_1),其输出为 $y=x_0\oplus x_1$,则输入多重集 X 对应于满足可分性质 D_K^t 的输出多重集 Y 的可分性质为 $D_K^{t^2}$,其中:

$$K=\begin{cases}\{(0)\}, & k=(0,0)\\ \{(1)\}, & k=(0,1)\text{或}(1,0)\\ \varnothing, & k=(1,1)\end{cases}\tag{4}$$

规则 3(与操作) 设 F 为 $F_2\times F_2$ 上与函数,其输入为(x_0,x_1),其输出为 $y=x_0\wedge x_1$,则输入多重集 X 对应于满足可分性质 D_K^t 的输出多重集 Y 的可分性质为 $D_K^{t^2}$,其中:

$$K=\begin{cases}\{(0)\}, & k=(0,0)\\ \{(1)\}, & \text{其他}\end{cases}\tag{5}$$

规则 4(非线性 S 盒) S 盒即针对特殊的输入设定指定的输出,不同于其他线性操作,针对不同的 S 盒一般使用代数正规型对其输入输出关系进行描述。利用文献[12]中的算法,可以通过 S 盒的代数正规型对可分性质穿越 S 盒的过程进行刻画。通过遍历初始可分性质 $D_K^{1^n}$ 对非线性 S 盒输出集合的可分性质进行求解。若 S 盒为 n 比特输入,则可以通过对其所有 2^n 个输入可分性质依次判定 2^n 个输出可分性质是否成立,进而可得到其所有的可分路径。

2.4 基于比特可分性质的 MILP 模型

将可分性质转换为 MILP 模型,即将利用传播规则获得的可分路径转换为可用于构造 MILP 模型的限制条件,通过建立 MILP 模型进行求解,获得基于比特可分性质的积分区分器。

模型 1(复制模型) 令$(a)\to(b_0,b_1)$为代表复制操作的传播过程,则其传播规则的不等式描述如下:

$$\begin{cases}a-b_0-b_1=0\\ a,b_0,b_1\in F_2\end{cases}\tag{6}$$

模型 2(异或模型) 令$(a_0,a_1)\to(b)$为代表异或操作的传播过程,则其传播规则的不等式描述如下:

$$\begin{cases}a_0+a_1-b=0\\ a_0,a_1,b\in F_2\end{cases}\tag{7}$$

模型 3(与模型) 令$(a_0,a_1)\to(b)$为代表与操作的传播过程,则其传播规则的不等式描述如下:

$$\begin{cases}b-a_0\geqslant 0\\ b-a_1\geqslant 0\\ b-a_0-a_1\leqslant 0\\ a_0,a_1,b\in F_2\end{cases}\tag{8}$$

模型 4(S 盒模型) 通过利用 2.3 节中的规则 4 可计算获得 S 盒的可分路径。若 S 盒为 n 比特输入,则可分路径为 $2n$ 维向量,其中 n 维表示输入可分性质,n 维表示输出可分性质,则可获得代表可分路径的集合 P,集合 P 属于$\{0,1\}^{2n}$。将集合 P 视为 $2n$ 维点集,使用数学计算工具 SageMath 的不等式生成函数 inequality_generator()对点集 P 进行计算,可将点集转换为利用大量线性不等式进行刻画的可行域,也即获得点集凸包的 H-表示,即线性不等式组 L,L 即为 S 盒模型的不等式表达。

通常,使用 inequality_generator()获得的线性不等式组 L 中会因为不等式组规模过于庞大,导致全部添加后的 MILP 模型过载而不可求解。针对不等式组的冗余问题,Sun 等[17]提出了贪心算法来减少不等式的数量,得到简化不等式组 L^*;Sasaki 和 Todo 等[16]则提出了另一种基于 MILP 的约简算法可以达到理论上的最简不等式组 L^*。

基于上述 MILP 模型中的限制条件,可以针对复制、异或、与和非线性 S 盒的操作或算法结构部件来设置线性不等式组,从而对密码加密过程进行刻画。将轮函数对应的限制条件迭代 r 次,则可以得到用于描述 r 轮加密过程中的可分性传播的线性不等式系统,该系统的所有可行解对应于所有 r 轮可分路径。

条件 1(初始化可分性质) 令一条 r 轮的可分路径表示如下:

$(a_0^0,a_1^0,\cdots,a_{n-1}^0)\to\cdots(a_0^r,a_1^r,\cdots,a_{n-1}^r)$

设 L 是表示传播关系的线性不等式组,令可分路径从 k 开始传播,需令初始化可分性质为 $D_{\{k\}}^{1^n}$,其中 $k=\{k_0,k_1,\cdots,k_{n-1}\}$,即将不等式组 $a_i^0=k_i$ 添加进不等式组 L。

条件 2(终止规则) 当多重集 X 不具有可分性质时即终止,其充分必要条件为其输出可分性质的集合等价于其所有单位向量的集合。若成功搜索到一个单位向量,则该单位向量对应的比特位置不平衡,通过多轮对单位向量的搜索即可发现本轮多重集 X 是否不具有可分性质。根据上述性质可构造目标函数:

$Obj:\mathrm{Min}(a_0^r,a_1^r,\cdots,a_{n-1}^r)$

完整的 MILP 模型需要限制条件和目标函数,通过不等式组 L 和函数 Obj 完成模型搭建。令初始可分性质经第 i 轮迭代后得到的可分性质为 $D_{\{K_i\}}^{1^n}$,当 K_{r+1} 首次等于所有 n 个单位向量的集合时停止搜索,通过对初始可分性质的遍历即可对密码算法的 r 轮的积分区分器 $D_{\{K_r\}}^{1^n}$ 进行搜索。

2.5 基于 MILP 的 S 盒约简方法

在对比特可分性传播路径的建立过程中,考虑到用于表示最小凸集 H-表示的不等式组规模的庞大和冗余会使 MILP 模型难以在有限时间内完成求解。实际上,排除有限的可分路径仅需要其中的部分 S 盒不等式即可约束凸集可达到 MILP 上可行域的目的。为了计算上的可行性,可以在不影响原有约束有效性的同时尽可能地减少不等式的数量,以便于进行不等式求解。

贪心算法的基本思想是令可行域中除去可分路径的凸集为 B,依次选择排除凸集 B 中最多点的不等式,直到凸集 B 中所有的点都被所选择的不等式排除。这种算法使用局部最优思想得到一个较优解,但无法保证所得到的不等式数量最优,且不等式的优先级不明确。

基于 MILP 的约简思想进行最优不等式组的选择,其

基本思想如下：首先计算凸集 B 中的每个点可以被哪些不等式排除，设定约束条件为每一个点至少被一个不等式所排除，同时设定每一个不等式最多可以选择一次，令不等式组数量为 m，凸集 B 中点的个数为 n，不等式是否被选择为 x_i，其中 $i\in(0,1,\cdots,m-1)$，则约束条件如下：

$$R_j: x_{a_0}+x_{a_1}+\cdots+x_{a_p}\geqslant 1$$

其中，$j\in\{0,1,\cdots,n-1\}$，$A=\{a_0,a_0,\cdots,a_p \mid$ 不等式 a_i 可以排除点 $j\}$。

设定目标函数为最少的不等式数量，进行 MILP 求解，即：

$$Obj: \mathrm{Min}(x_0,x_1,\cdots,x_{n-1})$$

3 基于 MILP 的 GIFT 积分区分器搜索算法

本节首先对 GIFT 密码的算法结构展开说明，并针对算法部件构建其 MILP 模型，利用 Gurobi 求解器计算获得 GIFT 算法最高 9 轮积分区分器。

3.1 GIFT 算法描述

GIFT 算法是一种基于 SPN 网络结构进行设计的轻量级分组密码，根据分组长度的不同可分为两个版本：GIFT-64-128 的分组长度为 64 比特，GIFT-128-128 的分组长度为 128 比特。此外，P 置换和迭代次数也有所不同。本文即针对 GIFT-64-128 进行基于比特可分性的积分分析，下文中提到的 GIFT 均指 GIFT-64-128。

GIFT 所用的轮加密主要由非线性 S 层、线性置换 P 层以及密钥加层 3 步运算组成。

非线性 S 层：GIFT 算法的非线性 S 层由 16 个 4×4 的非线性 S 盒构成。S 盒置换表如表 1 所列，x 经过代换变为 $S(x)$。

表 1 GIFT 算法的 S 盒规格

Table 1 Specification of GIFT S-box

x	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
$S(x)$	1	A	4	C	6	F	3	9	2	D	B	7	5	0	8	E

线性置换 P 层：GIFT 算法的线性置换层仅对分组中的位置顺序进行变换，也即 P 置换。P 置换表如表 2 所列，x 经过代换变为 $P(x)$，其中 x 和 $P(x)$ 均代表分组中的位置信息。

表 2 GIFT 算法的 P 置换

Table 2 P permutation of GIFT

x	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
$P(x)$	0	17	34	51	48	1	18	35	32	49	2	19	16	33	50	3	4	21	38	55	52	5	22	39	36	53	6	23	20	37	54	7
x	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	32	33	34	35
$P(x)$	56	9	26	43	40	57	10	27	24	41	58	11	12	29	46	63	60	13	30	47	44	61	14	31	28	45	62	15	8	25	42	59

密钥加层：密钥加层包含轮密钥加和轮常数加两个部分。轮密钥加是指使用轮密钥生成算法生成轮密钥后，使用轮密钥 RK 参与运算：

$$RK=U\parallel V=\{u_0,u_1,\cdots,u_{15},v_0,v_1,\cdots,v_{15}\}$$

分别和分组中的 b_{4i+1}，b_{4i} 比特进行异或运算，即：

$$b_{4i+1}\leftarrow b_{4i+1}\oplus u_i,\ b_{4i}\leftarrow b_{4i}\oplus v_i,\ i\in\{0,1,\cdots,15\}$$

轮常数加是指将每一轮分组的第 3,7,11,15,19,23 位都分别与轮常数 $C=c_5c_4c_3c_2c_1c_0$ 的一位异或，且每一轮的第 63 位都和“1”异或，即：

$$b_{63}\leftarrow b_{63}\oplus 1,\ b_{23}\leftarrow b_{23}\oplus c_5,\ b_{19}\leftarrow b_{19}\oplus c_4,\ b_{15}\leftarrow b_{15}\oplus c_3,\ b_{11}\leftarrow b_{11}\oplus c_2,\ b_7\leftarrow b_7\oplus c_1,\ b_3\leftarrow b_3\oplus c_0$$

设 S 盒输入为 $x=(x_3,x_2,x_1,x_0)$，输出为 $y=(y_3,y_2,y_1,y_0)$，则输入和输出满足如下表达式，也即 S 盒的代数正规型为：

$$\begin{cases} y_0=x_0*x_1+x_0+x_1+x_2+x_3+1 \\ y_1=x_0*x_1+x_0*x_2+x_0+x_2+x_3 \\ y_2=x_0*x_3+x_1*x_2*x_3+x_1*x_3+x_1+x_2 \\ y_3=x_0*x_2*x_3+x_0+x_1*x_3 \end{cases}$$

3.2 GIFT 算法的密钥扩展和轮常数扩展算法

密钥扩展：将 128 比特的密钥视为一个 4×32 的矩阵，即：

$$\begin{bmatrix} k_{31},\cdots,k_1,k_0 \\ k_{63},\cdots,k_{33},k_{32} \\ k_{95},\cdots,k_{65},k_{64} \\ k_{127},\cdots,k_{97},k_{96} \end{bmatrix}$$

每轮的密钥扩展算法将密钥矩阵的第一行以 16 比特为单位分为两组，即 $(k_0,k_1,\cdots,k_{15})$ 和 $(k_{16},k_{17},\cdots,k_{31})$，将低 16 比特向左循环移动 12 位，高 16 比特向左循环移动 2 位，即：

$$(k_0,k_1,\cdots,k_{15})\rightarrow(k_{12},k_{13},\cdots,k_{11})$$

$$(k_{16},k_{17},\cdots,k_{31})\rightarrow(k_{18},k_{19},\cdots,k_{17})$$

最后，将密钥矩阵以行为单位，整体向上循环移动 1 行，即完成本轮的密钥扩展。

轮常数扩展：每轮共有 6 位轮常数进入轮函数参与运算。轮常数扩展算法首先将首轮的轮常数置 0，即：

$$C=(c_5,c_4,c_3,c_2,c_1,c_0)=(0,0,0,0,0,0)$$

更新时轮常数循环左移 1 位，并将 c_5 进行异或计算，得到新一轮的轮常数，即：

$$C=(c_5,c_4,c_3,c_2,c_1,c_0)\rightarrow(c_4,c_3,c_2,c_1,c_0,c_5\oplus c_4\oplus 1)$$

3.3 GIFT 算法的已知积分区分器

在 GIFT 算法[1]作者对 GIFT 抵御积分分析攻击的安全性进行了分析，分别对 GIFT-64 和 GIFT-128 找到了最高 9 轮和最高 11 轮的积分区分器，并给出了 GIFT-64 的具体积分区分器，如表 3 所列。

表 3 GIFT 算法的 9 轮积分区分器

Table 3 9 rounds integral divider of GIFT algorithm

名称	状态	可分性质
9 轮积分区分器	输入	(aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa aaaaaaaaaaaaaaaaaaaaaaaaaaaaacaa)
	输出	(??bb??bb??bb??bb??bb??bb??bb??bb ??bb??bb??bb??bb??bb??bb??bb)

注：a 为活跃比特；c 为常数比特；?为不确定比特；b 为平衡比特。

3.4 GIFT 算法的 MILP 模型

在可分性质的传播规则中并没有常数异或的模型或规律，即轮密钥加和轮常数加操作的前后可分性质不会发生改变，输入可分性质和输出可分性质保持一致，因此在构建有关 GIFT 的 MILP 模型时可以忽略轮密钥加和轮常数加层，只考虑非线性 S 盒和线性置换 P 层前后可分性质的变化。应用

文献[12]提出的算法可以计算 GIFT 的 S 盒可分路径,发现共 49 条 S 盒可分路径,如表 4 所列。

表 4　GIFT 算法 S 盒的可分路径

Table 4　S box division trails of GIFT algorithm

输入可分	输出可分			
0,0,0,0	0,0,0,0			
0,0,0,1	0,0,0,1	0,0,1,0	0,1,0,0	1,0,0,0
0,0,1,0	0,0,0,1	0,0,1,0	0,1,0,0	1,0,0,0
0,0,1,1	0,0,0,1	0,0,1,0	1,1,0,0	
0,1,0,0	0,0,0,1	0,0,1,0	0,1,0,0	1,0,0,0
0,1,0,1	0,0,1,0	0,1,0,1	1,0,0,0	
0,1,1,0	0,0,1,1	0,1,0,0	1,0,0,1	1,0,1,0
0,1,1,1	0,1,0,1	1,0,1,1	1,1,1,0	
1,0,0,0	0,0,0,1	0,0,1,0	0,1,0,0	1,0,0,0
1,0,0,1	0,0,1,1	0,1,0,0	1,0,0,0	
1,0,1,0	0,0,1,1	0,1,0,0	1,0,0,0	
1,0,1,1	0,1,1,0	1,0,1,1	1,1,0,1	
1,1,0,0	0,0,1,1	0,1,0,0	1,0,0,0	
1,1,0,1	0,0,1,1	0,1,0,1	1,0,0,0	
1,1,1,0	0,1,0,0	1,0,0,1	1,0,1,0	
1,1,1,1	1,1,1,1			

利用函数 inequality_generator()对可分路径进行转换,生成线性不等式,得到 360 个表达式用于描述 S 盒的可分路径;最后利用贪心算法对线性集合进行优化化简,得到 15 个精简不等式集合。令进行 GIFT 的 S 盒操作前后的可分性质变化表示如下:

$$(x_3,x_2,x_1,x_0)\xrightarrow{S}(y_3y_2,y_1,y_0)$$

则利用贪心算法得到的用于表达 S 盒可分性质的精简不等式组 L_S 如下:

$$L_S\begin{cases}x_0+x_1+x_2+x_3-y_0-y_1-y_2-y_3\geqslant 0\\-4*x_0-5*x_1-3*x_2-3*x_3+y_0+y_1+\\3*y_2+2*y_3+8\geqslant 0\\-x_0+3*x_1-2*x_2-3*x_3+3*y_0-4*y_1-\\2*y_2-y_3+7\geqslant 0\\-x_1-x_2-x_3+y_0+y_1+3*y_2+2*y_3\geqslant 0\\3*x_0-y_0-y_1-2*y_2-y_3+2\geqslant 0\\-2*x_0-x_2-2*y_0+2*y_1+y_2-y_3+4\geqslant 0\\-x_0+x_3-y_0-2*y_1-y_2+y_3+3\geqslant 0\\-6*x_0-5*x_1-x_2-3*x_3+3*y_0+5*y_1+\\y_2+2*y_3+8\geqslant 0\\x_0+3*x_1+x_2-2*y_0-y_1-2*y_2-2*y_3+2\geqslant 0\\3*x_0+x_2-y_0-y_1-2*y_2-2*y_3+2\geqslant 0\\-x_0-x_2-x_3+y_0+2*y_1+2*y_2+3*y_3\geqslant 0\\-x_0-x_2+y_0+y_1-y_2+2\geqslant 0\\x_0+x_2+2*x_3-2*y_0-y_1-2*y_2-y_3+2\geqslant 0\\-x_0-2*x_1-2*x_2+y_0+y_1+2*y_2+y_3+2\geqslant 0\\-2*x_0-x_3+2*y_0-2*y_1+y_2-y_3+4\geqslant 0\end{cases}$$

因为 GIFT 算法的非线性 S 层共包含 16 个相同的 S 盒,每个 S 盒互不影响,且每个 S 盒需 15 个不等式,故根据 S 盒位置的不同,共需要 15 * 16=240 个不等式,其非线性层的可分路径表示如下:

$$(x_{64},x_{63},\cdots,x_1,x_0)\xrightarrow{S}(y_{64},y_{63},\cdots,y_1,y_0)$$

GIFT 算法线性层为 P 置换,只对分组中的位置进行交换,不改变其可分性质,也即 P 置换只对 MILP 模型中的限制条件表达式系数的位置产生作用,而不会改变线性不等式本身的系数,且 GIFT 算法置换层的影响与其等价结构的影响是一致的。令 GIFT 的 P 置换的可分路径为:

$$(x_{64},x_{63},\cdots,x_1,x_0)\xrightarrow{P}(y_{64},y_{63},\cdots,y_1,y_0)$$

则构成 P 置换可分路径的线性不等式组 L_P 如下:

$$L_P:y_i=P(x_i),i\in\{0,1,\cdots,63\}$$

将对非线性 S 盒和线性置换 P 层进行 MILP 建模所得的线性不等式组 L_S 和 L_P 联立,得到的集合即为对 GIFT 密码加密轮函数的约束,搜索 r 轮即将约束条件迭代 r 轮。目标函数即设为第 r 轮的输出可分性质之和的最小值。此时通过设定初始的可分性质 $D_k^{[64]}$,即可通过对 MILP 模型的求解获得积分器区分器分析结果。

3.5　GIFT 算法的积分区分器的搜索

对 GIFT 算法进行积分安全性分析,完成 GIFT 密码各算法部件对可分性的约束条件和目标函数,使用数学工具 Gurobi 编写搜索算法。令 K_r 为 r 轮后的输出可分路径集合,S 为 r 轮后的输出平衡位置集合,MILP 模型为 M,则搜索算法具体如算法 1 所示。

算法 1　MILP 搜索积分区分器算法

```
输入:GIFT 的 MILP 模型 M,分组长度 n
输出:平衡比特位置的集合 S
1. Initialize(S);/* 初始化 S 为所有比特位 */
2. FOR i in range(0,n) do
3.     IFM has feasible solution THEN;
4.       Optimize(M);/* 使用 Gurobi 优化求解 M */
5.       IFM.ObjVal==1 do;/* 求当前目标函数的值,若为 1 即发现
         了一条以单位向量结束的可分路径,否则输出 S,搜索终止 */
6.         For v in M.getVars() do;
7.           IF v.X==1 THEN;
8.             S.remove(v.VarName);/* 使用 API 函数来找出到
               该单位向量中 1 的位置,则该位置的比特不平衡,从 S
               中删去该位置 */
9. M.addConstr(
10.    VarName==0);
11.    Update(M);
12.      BREAK;/* 在模型 M 中添加限制条件,将搜索到的比特位
         置零,然后更新 M */
13.        END IF;
14.          END FOR;
15.        ELSE;
16.          RETURN S;/* 当目标函数不为 1 时输出 S,搜索终止 */
17.        END IF;
18.      ELSE;
19.          RETURNS;/* 当 M 无可行解时输出 S,搜索终止 */
20.      END IF;
21.  END FOR;
22.  RETURNS;/* 重复执行 n 次后输出 S,搜索终止 */
```

使用上述算法对 GIFT 密码进行分析,搜索获得了最高 9 轮区分器,且并没有找到更高轮的结果。首先对积分区分器中使用的符号进行说明,令 a,b,c,? 分别表示活跃比特、平衡比特、常数比特、未知比特,且对比特顺序规定序列的高位从左到右依次排列。在遍历初始可分性质活跃 63 比特的情况下对 GIFT 算法进行搜索,成功求解获得到 64 个 9 轮积分区分器,其中输出位置中存在的平衡比特证明该积分区分器可用于积分攻击。表 5 仅给出 4 个 9 轮积分区分器作为结果说明。

表 5 GIFT 算法的 9 轮积分区分器

Table 5 9 rounds integral divider of GIFT algorithm

名称	状态	可分性质
9 轮积分区分器 1	输入	(aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaac)
	输出	(??b??b??b??b??b??b??b??b ??b??b??b??b??b??b??bb???)
9 轮积分区分器 2	输入	(aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaca)
	输出	(??b??b???b???b???b???b ???b???b???b??b???b???b????)
9 轮积分区分器 3	输入	(aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa aaaaaaaaaaaaaaaaaaaaaaaaaaaaacaa)
	输出	(??bb??bb??bb??bb??bb??bb??bb??bb ??bb??bb??bb??bb??bb??bb??bb??bb)
9 轮积分区分器 4	输入	(aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa aaaaaaaaaaaaaaaaaaaaaaaaaaaacaaa)
	输出	(??bb??bb??bb??bb??bb??bb??bb???b ??bb??bb??bb??bb???b??bb??bb??bb)

注:a 为活跃比特;c 为常数比特;? 为不确定比特;b 为平衡比特。

根据表 4 和表 5 可知,当 GIFT 算法输入可分性质中第 3 位为常数比特,其他位为活跃比特时,得到的 9 轮积分区分器与 GIFT 提出者在原论文中给出的 9 轮积分区分器一致,验证了该积分区分器搜索算法的正确性。

4 基于 MILP 的 S 盒约简及积分区分器搜索优化

本节首先利用 MILP 的约简算法对 GIFT 的 S 盒可分路径进行分析,并对 GIFT 算法的 S 盒表达式进行约简,重新建立并优化 MILP 模型,对其计算求解得到 GIFT 密码最高 13 轮积分区分器。

4.1 基于约简算法的 GIFTS 盒可分路径求解

利用 2.5 节中提到的 MILP 约简模型进行求解,得到优化后的不等式组的个数被缩减为 12 个。令 GIFT 的 S 盒可分路径表示如下:

$$(x_3,x_2,x_1,x_0)\xrightarrow{S}(y_3y_2,y_1,y_0)$$

则由优化约简算法得到的构成 S 盒可分路径的线性不等式组 L_S 如下(数量上相比于贪心算法的线性不等式组少了 3 个,且有 8 个不等式约束与原约束完全不同):

$$L_S\begin{cases}-4*x_0-5*x_1-3*x_2-3*x_3+y_0+y_1+3*y_2+2*y_3+8\geqslant 0\\ -x_0+3*x_1-2*x_2-3*x_3+3*y_0-4*y_1-2*y_2-y_3+7\geqslant 0\\ x_1+x_3-y_0-3*y_1-2*y_2+y_3+3\geqslant 0\\ x_0+x_1+x_2+x_3-y_0-y_1-y_2-y_3\geqslant 0\\ -x_0-x_2-x_3+y_0+y_1-2*y_2-y_3+4\geqslant 0\\ -2*x_0-x_2-2*y_0+2*y_1+y_2-y_3+4\geqslant 0\\ -x_1-x_2+y_0+y_1+2*y_2+y_3\geqslant 0\\ 2*x_2+2*x_3-y_0-y_1-y_3+1\geqslant 0\\ -3*x_0-2*x_1-x_2+3*y_0+3*y_1+y_2+2*y_3+2\geqslant 0\\ -2*x_0-x_1-x_2-3*x_3+3*y_0+3*y_1+5*y_2+6*y_3\geqslant 0\\ x_0+x_2-2*y_0-y_1-3*y_2+y_3+3\geqslant 0\\ 5*x_0+x_1+x_2-2*y_0-2*y_1-3*y_2-3*y_3+3\geqslant 0\end{cases}$$

将新的约束条件替换原 MILP 中的 S 盒约束条件,即在保障凸集相同的前提下将混合整数线性规划中的可行域替换为优化后的线性不等式组表达的可行域,有效解决了 S 盒约束条件的冗余问题并大大提高了积分区分器的搜索能力。

4.2 基于 S 盒约简的 GIFT 积分区分器搜索优化

基于约简后的 S 盒可分路径线性不等式组,对 GIFT 建立基于 MILP 的积分攻击安全性分析的约束条件和目标函数,然后在限制条件的基础上对目标函数进行优化计算。根据积分区分器性质可知,随着活跃比特数增加,求解得到积分区分器轮数越高的可能性就越大,故本文以活跃 63 比特的初始可分性质进行遍历,且本节结果均以此初始可分性质进行搜索所得。从 9 轮开始搜索,得到了 GIFT 最高 13 轮区分器,但没有找到 14 轮积分区分器。当使用优化后的 MILP 模型进行 9 轮求解时,得到 64 个积分区分器。当输入最低位为常数,其他比特为活跃比特时,得到的积分区分器和上述利用贪心算法得到的结果不同,其他 63 个积分区分器均相同。表 6 给出上述不同积分区分器的对比。

表 6 GIFT 算法的 9 轮积分区分器对比

Table 6 Comparison of 9 rounds integral divider of GIFT algorithm

名称	状态	可分性质
MILP 优化 9 轮积分区分器	输入	(aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaac)
	输出	(??????????????????b???????????b???b ???b???b???b??????????????????????)
贪心算法 9 轮积分区分器	输入	(aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaac)
	输出	(???b???b???b???b???b???b???b???b ???b???b???b???b???b???b??bb????)

注:a 为活跃比特;c 为常数比特;? 为不确定比特;b 为平衡比特。

基于 S 盒约简进行 GIFT 积分区分器搜索优化后进行 9 轮积分区分器搜索得到的其他 63 个积分区分器和第 3 章得到的结果一致。当 GIFT 算法输入可分性质中第 3 位为常数比特,其他位为活跃比特时,得到的 9 轮积分区分器与 GIFT 提出者在原论文中给出的 9 轮积分区分器一致,验证了该积分区分器搜索改进的正确性。

根据上述结果可知,MILP 优化后的 S 盒约简表达式与贪心算法得到的 S 盒约简表达式在 MILP 模型中表示的单轮凸集相同,但是划分的可行域有所不同,经过多轮迭代后导致可行域的划分发生了偏移,进而影响到了凸集表示,故在进行 9 轮积分区分器的两种模型求解中得到了 1 个不同的积分区分器和 63 个相同的积分区分器,且前者在 10 至 13 轮可以搜索到有效的积分区分器,而后者无法搜索到。前者第 10 轮、11 轮、12 轮、13 轮分别可以找到 9 个、5 个、3 个、3 个积分区分器,表 7 中分别列出一个积分区分器作为示例。

在进行更高轮的搜索时,利用优化后的 MILP 模型成功搜索到 GIFT 的 9 轮以上的积分区分器,最高得到 13 轮积分区分器,比原模型高 4 轮。当输入的 64 位比特位置中第 28,39 或 62 位为常数,其他比特位置为活跃比特时,分别可以搜索到 GIFT 算法 13 轮加密的 3 个积分区分器,其中输出位置中存在的平衡比特证明该积分区分器可用于积分攻击,可以使用该积分区分器输出可分性质中的平衡比特进行积分攻击和密钥恢复。表 8 列出了 GIFT 算法的 13 轮积分区分器的最终结果。

表 7　GIFT 算法的 10,11,12,13 轮积分区分器对比

Table 7　Comparison of 10,11,12,13 rounds integral divider of GIFT algorithm

轮数	算法名称	状态	可分性质
10	MILP 优化后积分区分器寻找	输入	(aaaaaaaaaaaaaaaaaaaaa aaaaaaaaaaaaaaaaaaaaa aaaaaaaaaaaaaaaaacaaa)
		输出	(???b??bb???b??bb???bb ??b???b??b????????bb??b ???bb??????b???b???b?)
	贪心算法积分区分器寻找	输入	—
		输出	—
11	MILP 优化后积分区分器寻找	输入	(aaaaaaaaaaaaaaaaaaaaa aaaaaaaaaaaaaaaaaaaaa aaaaaaaaaaaaaaacaaaaa)
		输出	(??b???bb??bbb??bb?bb? ?bb?bbb??????bb??bb??b ???b????????bb??bbbbbb)
	贪心算法积分区分器寻找	输入	—
		输出	—
12	MILP 优化后积分区分器寻找	输入	(aaaaaaaaaaaaaaaaaaaaa aaaaaaaaaaaaaaaaaaaaa aacaaaaaaaaaaaaaaaaaa)
		输出	(??bbbb??b??b??b???bb? ???b??b?b????b???b???b b???bb?b???bbb??b??bb)
	贪心算法积分区分器寻找	输入	—
		输出	—
13	MILP 优化后积分区分器寻	输入	(aaaaaaaaaaaaaaaaaaaaa aaaaaaaaaaaaaaaacaaaaaa aaaaaaaaaaaaaaaaaaaaa)
		输出	(??bb???b??bb??b???b?? ?????b????b???b???????b ?b????b???bb???b????)
	贪心算法积分区分器寻找	输入	—
		输出	—

注:a 为活跃比特;c 为常数比特;? 为不确定比特;b 为平衡比特;— 为未找到积分区分器。

表 8　GIFT 算法的 13 轮积分区分器

Table 8　13 rounds integral divider of GIFT algorithm

名称	状态	可分性质
13 轮积分区分器 1	输入	(aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa aaaacaaaaaaaaaaaaaaaaaaaaaaaaaaaa)
	输出	(??bb???b??bb??b???b???????b????b ???b???????b?b????b???bb???b????)
13 轮积分区分器 2	输入	(aaaaaaaaaaaaaaaaaaaaaaaaaaacaaaaaa aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa)
	输出	(??b???b?????b??????????b???bb????? ?bb??bbbb?b?b?????b???b???bb???)
13 轮积分区分器 3	输入	(aacaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa)
	输出	(???b??b????b??b???bb???b???b???b b??b???b??b???bb??bb???b??bb??bb)

注:a 为活跃比特;c 为常数比特;? 为不确定比特;b 为平衡比特。

因此,利用基于混合整数线性规划的比特可分性模型对 GIFT 算法进行建模,同时利用得到的模型对其积分区分器进行遍历搜索,将差分攻击中的 S 盒约简算法应用于上述模型,在验证其正确性的同时成功搜索出比原模型高 4 轮的积分区分器,推进了对于 GIFT 密码的积分分析轮数,可得到更好的攻击效果。此外,此方法通用性强,能够应用于其他轻量级密码中,尽管不同的轻量级密码有不同的 S 盒,但均能够使用本文使用的 S 盒约简算法对其 S 盒可分性质进行重新表达,进而完成对积分区分器的搜索优化。

结束语　本文使用 MILP 模型针对 GIFT 算法进行了可分性建模和 Gurobi 求解,搜索获得了 64 个 9 轮积分区分器;同时首次将差分攻击中用于优化 S 盒差分路径表达的 MILP 约简算法引入积分攻击分析,并对 GIFT 算法 S 盒可分路径的不等式组进行约简优化,从 15 个约束条件优化为 12 个,并重新添加新的约束条件对 MILP 模型进行优化,重新求解。结果表明,本文采用的新约简算法成功优化原模型并求解得到了 GIFT 的最高 13 轮积分区分器,比基于原有贪心算法约简的 S 盒表达式搜索得到的 9 轮区分器多 4 轮,可达到更好的积分攻击和安全性分析效果。

在构建基于比特设计的密码算法针对积分安全性分析的 MILP 模型的过程中,对非线性 S 层和线性层的约束条件的优化会对整个 MILP 模型的求解产生重要影响。未来的研究工作主要包括:基于本文所得到的 S 盒优化,寻找更加精简且高效的线性层约束条件优化方法,以提高积分安全性分析轮数,增加对积分性质对积分攻击影响的认知。

参 考 文 献

[1] BANIK S,PANDEY S K,PEYRIN T,et al. GIFT:a small present[C]// International Conference on Cryptographic Hardware and Embedded Systems. Cham:Springer,2017:321-345.

[2] ZHU B,DONG X,YU H. MILP-based differential attack on round-reduced GIFT[C]// Cryptographers' Track at the RSA Conference. Cham:Springer,2019:372-390.

[3] ZHANG J,LI L,LI Q,et al. Power analysis attack on a lightweight block cipher GIFT[C]// Proceedings of the 9th International Conference on Computer Engineering and Networks. Singapore:Springer,2021:565-574.

[4] CHEN L,WANG G,ZHANG G Y. MILP-based related-key rectangle attack and its application to GIFT,Khudra,MIBS[J]. The Computer Journal,2019,62(12):1805-1821.

[5] SUN S,HU L,WANG M,et al. Towards finding the best characteristics of some bit-oriented block ciphers and automatic enumeration of(related-key) differential and linear characteristics with predefined properties[J]. Cryptology ePrint Archive,2014.

[6] DAEMEN J,KNUDSEN L,RIJMEN V. The block cipher Square[C]// International Workshop on Fast Software Encryption. Berlin:Springer,1997:149-165.

[7] LUCKS S. The saturation attack—a bait for Twofish[C]// International Workshop on Fast Software Encryption. Berlin:Springer,2001:1-15.

[8] BIRYUKOV A,SHAMIR A. Structural cryptanalysis of SASAS[C]// International Conference on the Theory and Applications of Cryptographic Techniques. Berlin:Springer,2001:395-405.

[9] KNUDSEN L,WAGNER D. Integral cryptanalysis[C]// International Workshop on Fast Software Encryption. Berlin:Springer,2002:112-127.

[10] Z'ABA M R,RADDUM H,HENRICKSEN M,et al. Bit-pattern based integral attack[C]// International Workshop on Fast Software Encryption. Berlin:Springer,2008:363-381.

[11] TODO Y. Structural evaluation by generalized integral property[C]// Annual International Conference on the Theory and Applications of Cryptographic Techniques. Berlin:Springer,2015:287-314.

[12] TODO Y,MORII M. Bit-based division property and application to Simon family[C]// International Conference on Fast Software

Encryption. Berlin: Springer, 2016: 357-377.
[13] XIANG Z, ZHANG W, BAO Z, et al. Applying MILP method to searching integral distinguishers based on division property for 6 lightweight block ciphers[C]// International Conference on the Theory and Application of Cryptology and Information Security. Berlin: Springer, 2016: 648-678.
[14] SUN L, WANG W, WANG M Q. MILP-aided bit-based division property for primitives with non-bit-permutation linear layers [J]. IET Information Security, 2020, 14(1): 12-20.
[15] HU K, WANG Q, WANG M. Finding bit-based division property for ciphers with complex linear layers[J]. IACR Transactions on Symmetric Cryptology, 2020: 396-424.
[16] SHANG F Z, SHEN X, LIU G Q, et al. Integral cryptanalysis on PUFFIN based on MILP[J]. Journal of Cryptologic Research, 2019, 6(5): 627-638.
[17] SASAKI Y, TODO Y. New algorithm for modeling S-box in MILP based differential and division trail search[C]// International Conference for Information Technology and Communications. Cham: Springer, 2017: 150-165.
[18] 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]// International Conference on the Theory and Application of Cryptology and Information Security. Berlin: Springer, 2014: 158-178.

ZU Jinyuan, born in 2001. His main research interests include information security and cryptography.

LIU Jie, born in 1985, Ph. D, associate professor, is a member of China Computer Federation. His main research interests include cryptography and network security.