超轻量级分组密码LiCi、LiCi-2和GRANULE的完美线性逼近

严智广,李灵琛*,韦永壮
(桂林电子科技大学广西密码学与信息安全重点实验室,广西桂林 541004)

摘 要: LiCi、LiCi-2和GRANULE密码算法均为面向资源极端受限物联网环境的超轻量级分组密码算法,其加、解密速度快且易于软硬件实现,目前备受业界广泛关注. 本文通过利用这些算法的线性结构特性,构造了多条绝对相关性为1的迭代(循环)完美线性逼近,并由此设计出全轮的完美线性逼近(线性区分器),进而完全攻破了这些密码算法,即证实了全轮的LiCi、LiCi-2和GRANULE密码算法存在严重的设计缺陷.

关键词: 轻量级分组密码;线性密码分析;完美线性逼近;Feistel结构
基金项目: 国家自然科学基金(No.62162016,No.62402132)
中图分类号: TN918;TP309.7 **文献标识码:** A **文章编号:** 0372-2112(2025)05-1453-07
电子学报URL:http://www.ejournal.org.cn **DOI:**10.12263/DZXB.20240838

Perfect Linear Approximation of Ultra-Lightweight Block Ciphers LiCi, LiCi-2 and GRANULE

YAN Zhi-guang, LI Ling-chen*, WEI Yong-zhuang
(*Guangxi Key Laboratory of Cryptography and Information Security*, *Guilin University of Electronic Technology*, *Guilin*, *Guangxi* 541004, *China*)

Abstract: LiCi, LiCi-2, and GRANULE are all ultra-lightweight block ciphers designed for resource-constrained internet of things environments. Because of their fast encryption (or decryption) speed and favorable implementation in both hardware and software platforms, which have received extensive attention. In this paper, the linear structure characteristics of these ciphers are investigated via multiple perfect linear approximations (circular iterations) with an absolute correlation of 1. Moreover, the perfect linear approximations (linear distinguishers with probability one) for the full rounds of the LiCi, LiCi-2, and GRANULE are achieved, thereby completely breaking these cryptographic algorithms. It directly means that these block ciphers have serious design flaws.

Key words: lightweight block cipher; linear cryptanalysis; perfect linear approximation; Feistel structure
Foundation Item(s): National Natural Science Foundation of China (No.62162016, No.62402132)

1 引言

随着5G技术及通信网络的飞速发展,物联网[1](Internet of Things,IoT)设备在日常生活中的需求持续上升. 这些设备之间的信息交换常常依赖于嵌入式加密算法,以确保数据传输的安全性、设备的认证以及其他敏感性服务的可靠性. 绝大多数物联网设备,尤其是传感器和微控制器,都处于存储空间小、计算性能弱、功耗低等资源受限的环境. 传统的加密算法,如高级加密标准AES[2](Advanced Encryption Standard)因其健壮的设计原则通常具有较高的实现成本并不适用于资源受限环境下的应用. 而轻量级分组密码通常具有低硬件实施成本和低能耗的特点,同时能在敏感应用中提供充足的安全保障非常适合资源环境受限的物联网设备,成为近年研究的热点. 目前已经有许多轻量级分组密码算法,如LBlock、PRESENT、SIMON、SPECK、LED、LiCi、LiCi-2、GRANULE等[3-9],它们的安全性分析对于轻量级密码的应用和新算法设计具有重要价值.

线性密码分析[10]和差分密码分析[11]是迄今为止对分组密码算法最有效的两种分析方法,并在此基础上衍生出了许多变体,如积分分析、不可能差分分析、差分中间相遇攻击、矩形攻击、多线性分析、多维零相关线性分析、

收稿日期:2024-09-12;修回日期:2025-04-16;责任编辑:李勇锋
*通讯作者:李灵琛

广义非线性不变子攻击、立方攻击等[12~19].

线性密码分析由Matsui于1993年在欧洲密码年会上提出,属于已知明文攻击,它通过研究明文和密文之间的线性关系来恢复密钥,进行线性密码分析的关键是寻找具有高线性相关性的线性逼近. 当线性逼近的线性相关性的绝对值为1时,称此时的线性逼近为完美线性逼近,但实际情况去寻找密码算法的完美线性逼近是一项具有挑战性的工作,最近,Beierle等人[20]在CRYPTO 2023上提出了特定的两轮SPN(Substitution-Permutation Network)结构密码的完美线性逼近的简易搜索算法. 但是对于高轮次及其他结构类型的密码算法的完美线性逼近的搜索仍然是待解决的一个问题.

LiCi算法是Patil等人[7]于2017年提出的一种面向物联网环境的超轻量级分组密码,该算法基于经典的Feistel结构,分组长度为64 bit,密钥长度为128 bit,迭代轮数为31轮. 鉴于LiCi算法足够的安全冗余,为了追求更优的性能,Khairnar等人[8]于2019年提出了LiCi算法的后继版本LiCi-2,其将迭代轮缩减至25轮,轮密钥数量减半,并减少了使用循环移位的数量,获得了更好的软硬件性能以适用于资源极度受限的环境,如6LoWPAN(IPv6 Low Power Wireless Personal Area Network)等. LiCi和LiCi-2的设计者根据分析结果均声称算法能有效抵抗差分分析、线性分析、零相关线性分析、Bcilique分析等分析方法. 2019年,韦永壮等人[21]基于S盒的差分特性并结合中间相遇思想构造了LiCi算法10轮的不可能差分区分器,并对其进行了16轮的不可能差分分析. 随后在2020年,信文倩等人[22]基于比特的可分性质并结合MILP(Mixed Integer Linear Programming)自动化搜索技术得到了LiCi算法12轮的积分区分器,并对其进行了13轮的积分分析. 同年,王红艳等人[23]同样基于MILP技术搜索到了LiCi算法12轮的积分区分器,并提出了LiCi算法的一种新的等价结构. 2022年,Zhang等人[24]通过观察LiCi-2算法S盒的差分特性构造了LiCi-2算法概率为1的10轮差分区分器,并使用自动化搜索技术分别在单密钥背景下搜索到了LiCi-2算法240条不可能差分区分器,在相关密钥背景下搜索到了65条18轮相关密钥不可能差分区分器,对LiCi-2算法进行了25轮的相关密钥多不可能差分密码分析,证明了LiCi-2算法在相关密钥条件下无法抵抗这种攻击.

GRANULE算法是由Bansod等人[9]于2018年提出的超轻量级分组密码,该算法基于Feistel结构,分组长度为64 bit,密钥长度为80/128 bit,迭代轮数为32轮,设计者根据分析结果声称该算法能有效抵抗差分分析、线性分析、零相关线性分析、Biclique分析等分析方法. 2019年,石淑英等人[25]利用中间相错技术找到了GRANULE算法多条5轮不可能差分区分器,并通过向前后各扩展3轮对11轮的GRANULE算法进行了不可能差分分析. 同年,方玉颖等人[26]通过研究GRANULE算法S盒的比特级分离特性,结合混合整数线性规划(MILP)思想,构建了GRANULE算法的积分特征自动化搜索模型,搜索到了GRANULE算法的10轮积分区分器. 随后在2020年,武小年等人[27]通过研究S盒的差分特性并结合中间相遇思想采用自动化搜索的方法,搜索到了GRANULE算法144条7轮不可能差分区分器. 2021年,Li等人[28]基于GRANULE算法结构的比特分离特性并使用MILP的自动化搜索技术,搜索到了10轮积分区分器,并选用8轮的积分区分器通过向后扩展4轮对12轮的GRANULE算法进行了积分分析. 2021年,赵晨曦[29]基于GRANULE算法S盒的差分特性并利用自动化搜索的方法,得到了一条7轮的不可能差分区分器,使用密钥分割技术对GRANULE算法进行了13轮的不可能差分分析. 2023年,刘先蓓等人[30]基于GRANULE算法P置换和移位异或的特性,构造了一条新的7轮不可能差分区分器,对GRANULE-80/128分别进行了13、14轮的不可能差分分析. 2024年,武小年等人[31]基于布尔可满足性问题(Boolean SATisfiability problem,SAT)构建了GRANULE算法更高效的不可能差分区分器搜索模型,搜索到了多条10轮不可能差分区分器,并通过向区分器前后各扩展3轮对16轮的GRANULE算法进行了不可能差分分析.

本文通过研究LiCi、LiCi-2、GRANULE算法结构的线性传播特性,构造了多条绝对相关性为1的迭代(循环)线性特征(完美线性逼近),使用这些绝对相关性为1的线性特征构造了绝对相关性为1的任意轮数的完美线性逼近(线性区分器),分析结果表明LiCi、LiCi-2、GRANULE算法无法抵抗线性分析,存在严重的设计缺陷.

2 基础知识

2.1 符号说明

本文的符号定义如表1所示.

表1 符号约定

符号	意义
$RK_i=(RK_i^1,RK_i^2)$	第i轮的轮密钥
L_i/R_i	第i轮的左/右分支32比特输入
S	S盒替换操作
$\overline{S}$	8个S盒的并行替换操作,即$\overline{S}(x_7,x_6,\cdots,x_0)=\big(S(x_7),S(x_6),\cdots,S(x_0)\big)$
$\oplus$	逐比特异或(XOR)运算
$\lll n/\ggg n$	循环左/右移n比特
$\cdot$	逻辑与(AND)运算
$\|\|$	比特串拼接操作
$A[i]$	比特串A的第i比特,其中第0比特表示最低有效位
$\sum$	连续异或运算
$\langle x,y\rangle$	两个n比特串的内积操作,即$\langle x,y\rangle=\sum_{i=0}^{n-1}\big(x[i]\cdot y[i]\big)$

2.2 完美线性逼近

回顾线性逼近的基本性质,首先使用下式定义函数$E:\mathbb{F}_2^n\to\mathbb{F}_2^n$的仿射逼近[20]:

$$\langle \alpha, x\rangle + \langle \beta, E(x)\rangle = c \tag{1}$$

其中,$\alpha \in \mathbb{F}_2^n, \beta \in \mathbb{F}_2^n, c \in \mathbb{F}_2$. 当$c=0$时称作线性逼近. 一个线性逼近的相关性定义如下:

$$\mathrm{cor}_E(\alpha,\beta) := \frac{1}{2^n}\sum_{x\in\mathbb{F}_2^n}(-1)^{\langle \alpha,x\rangle \oplus \langle \beta,E(x)\rangle} \tag{2}$$

如果式(1)的绝对相关性等于1,即存在一个常数c,使得对于所有的x均成立,此时称其为一个完美的线性逼近,可以用元组(α,β,c)或仅用(α,β)表示. 如果$(\alpha,\beta)\neq(0,0)$,称完美线性逼近为非平凡的,反之则为平凡的完美线性逼近. 在线性分析中只考虑非平凡的完美线性逼近,因此在后文中所有的完美线性逼近默认为非平凡线性逼近. 对于一个完美线性逼近若$\alpha=\beta$,称其为迭代完美线性逼近. 若存在两条完美线性逼近(α,β)和(α',β'),其中$\alpha=\beta', \beta=\alpha'$,此时称这两条完美线性逼近构成了一条循环完美线性逼近.

2.3　LiCi和LiCi-2算法简介

LiCi[7]和LiCi-2[8]算法均为平衡Feistel结构,分组长度为64 bit,密钥长度为128 bit,迭代轮数分别为31轮和25轮. 每轮均由S盒替换、循环移位、异或运算组成. 算法结构分别如图1和图2所示.

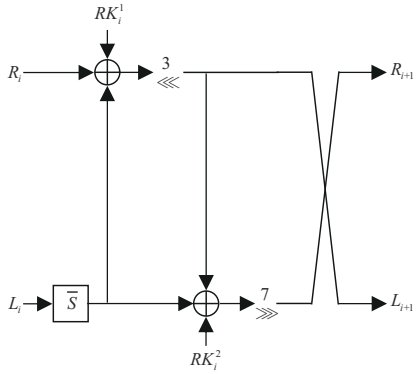

图1　LiCi算法结构

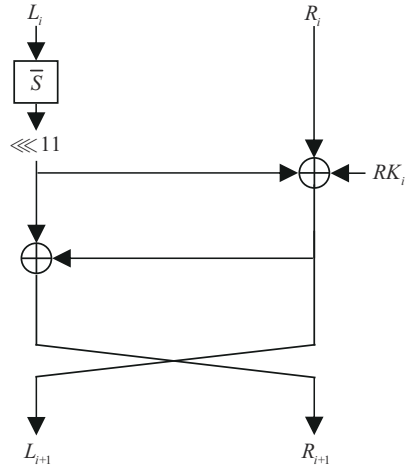

图2　LiCi-2算法结构

LiCi算法第i轮加密过程的公式表示如下:

$$\begin{cases} L_{i+1} = \left(\overline{S}(L_i) \oplus R_i \oplus RK_i^1\right) \lll 3 \\ R_{i+1} = \left(\overline{S}(L_i) \oplus L_{i+1} \oplus RK_i^2\right) \ggg 7 \end{cases} \tag{3}$$

LiCi-2算法第i轮加密过程的公式表示如下:

$$\begin{cases} L_{i+1} = \left(\overline{S}(L_i) \lll 11\right) \oplus R_i \oplus RK_i \\ R_{i+1} = \left(\overline{S}(L_i) \lll 11\right) \oplus L_{i+1} \end{cases} \tag{4}$$

S盒替换:LiCi和LiCi-2算法均并行使用8个相同的4比特S盒进行S盒替换操作,所使用的4比特S盒如表2所示.

表2　LiCi和LiCi-2算法的4比特S盒

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

2.4　GRANULE算法简介

GRANULE算法[9]采用经典的平衡Feistel结构,分组长度为64 bit,密钥长度支持80和128 bit两种长度,迭代轮数为32轮. 其中轮函数F由P置换、S盒替换、循环移位、异或运算组成. 该算法结构如图3所示.

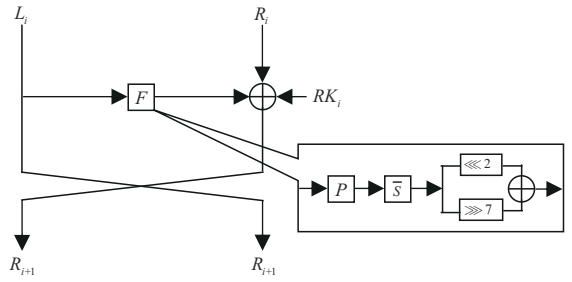

图3　GRANULE算法结构

GRANULE算法第i轮加密过程的公式表示如下:

$$\begin{cases} L_{i+1} = \left(\overline{S}(P(L_i)) \lll 2\right) \oplus \left(\overline{S}(P(L_i)) \ggg 7\right) \oplus R_i \oplus RK_i \\ R_{i+1} = L_i \end{cases} \tag{5}$$

P置换:将32 bit数据按照P置换表进行排列,将数据的第i比特移动到第$P(i)$比特,GRANULE算法中使用的P置换表如表3所示.

S盒替换:GRANLUE算法并行使用8个相同的4比

表3　GRANULE算法的P置换表

i	31	30	29	28	27	26	25	24
$P(i)$	23	22	21	20	31	30	29	28
i	23	22	21	20	19	18	17	16
$P(i)$	11	10	9	8	27	26	25	24
i	15	14	13	12	11	10	9	8
$P(i)$	7	6	5	4	15	14	13	12
i	7	6	5	4	3	2	1	0
$P(i)$	3	2	1	0	19	18	17	16

特S盒进行S盒替换操作,所使用的4比特S盒如表4所示.

表4 GRANULE算法的4比特S盒

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

3 LiCi、LiCi-2和GRANULE算法的完美线性逼近

3.1 LiCi算法的完美线性逼近

定理1 LiCi算法存在如图4所示的从第i轮到第$i+1$轮的1轮迭代完美线性逼近,计算公式如下:

$$\left(00000000\mathrm{FFFFFFFF},00000000\mathrm{FFFFFFFF},\sum_{j=0}^{31}(RK_i^1\oplus RK_i^2)[j]\right) \tag{6}$$

证明 由LiCi算法第i轮加密过程式(3)可得:

$$R_{i+1}=\left(\overline{S}(L_i)\oplus\left((\overline{S}(L_i)\oplus R_i\oplus RK_i^1)\lll 3\right)\oplus RK_i^2\right)\ggg 7$$

等式两边同时与FFFFFFFF做内积运算可得:

$$\begin{aligned}\left\langle \mathrm{FFFFFFFF},R_{i+1}\right\rangle=&\left\langle \mathrm{FFFFFFFF},R_i\right\rangle\oplus\left\langle \mathrm{FFFFFFFF},RK_i^1\right\rangle\\&\oplus\left\langle \mathrm{FFFFFFFF},RK_i^2\right\rangle.\end{aligned}$$

移项变形可得:

$$\begin{aligned}&\left\langle 00000000\mathrm{FFFFFFFF},L_i\|R_i\right\rangle\\&\oplus\left\langle 00000000\mathrm{FFFFFFFF},L_{i+1}\|R_{i+1}\right\rangle\\&=\sum_{j=0}^{31}(RK_i^1\oplus RK_i^2)[j])\end{aligned} \tag{7}$$

证毕.

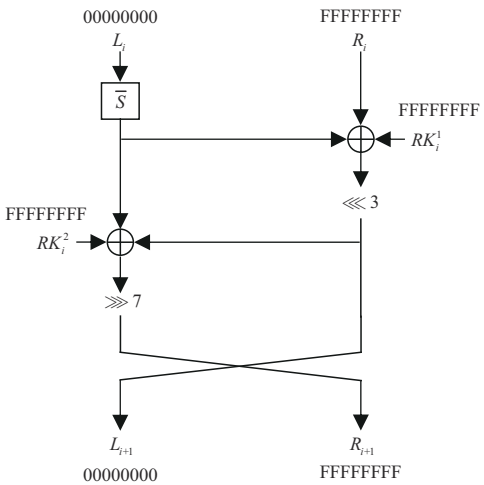

图4 LiCi算法的1轮迭代完美线性逼近

推论1 将定理1中的1轮迭代完美线性逼近迭代r轮可以得到LiCi算法从第i轮到第$i+r$轮的r轮完美线性逼近:

$$\left(00000000\mathrm{FFFFFFFF},00000000\mathrm{FFFFFFFF},\sum_{i}^{i+r-1}\sum_{j=0}^{31}(RK_i^1\oplus RK_i^2)[j]\right) \tag{8}$$

3.2 LiCi-2算法的完美线性逼近

定理2 LiCi-2算法存在如下从第i轮到第$i+1$轮的1轮迭代完美线性逼近.

$$\left(00000000\|\Gamma,00000000\|\Gamma,\left\langle\Gamma,RK_i\right\rangle\right) \tag{9}$$

其中,$\Gamma\in\mathbb{F}_2^{32}/0^{32}$.

证明 由LiCi-2算法第i轮加密过程式(4)可得

$$R_{i+1}=\left(\overline{S}(L_i)\lll 11\right)\oplus\left(\overline{S}(L_i)\lll 11\right)\oplus R_i\oplus RK_i=R_i\oplus RK_i.$$

等式两边同时与$\Gamma\in\mathbb{F}_2^{32}/0^{32}$做内积运算可得:

$$\left\langle\Gamma,R_{i+1}\right\rangle=\left\langle\Gamma,R_i\right\rangle\oplus\left\langle\Gamma,RK_i\right\rangle$$

移项变形可得:

$$\begin{aligned}&\left\langle 00000000\|\Gamma,L_i\|R_i\right\rangle\oplus\left\langle 00000000\|\Gamma,L_{i+1}\|R_{i+1}\right\rangle\\&=\left\langle\Gamma,RK_i\right\rangle\end{aligned} \tag{10}$$

证毕.

推论2 将定理2中的1轮迭代完美线性逼近迭代r轮可以得到LiCi-2算法从第i轮到第$i+r$轮的r轮完美线性逼近:

$$\left(00000000\|\Gamma,00000000\|\Gamma,\sum_{i}^{i+r-1}\left\langle\Gamma,RK_i\right\rangle\right) \tag{11}$$

3.3 GRANULE算法的完美线性逼近

定理3 GRANULE算法存在由如下第i轮到第$i+1$轮的1轮迭代完美线性逼近构成的2轮循环完美线性逼近:

$$\left(00000000\mathrm{FFFFFFFF},\mathrm{FFFFFFFF}00000000,\left\langle\mathrm{FFFFFFFF},RK_i\right\rangle\right) \tag{12}$$

$$\left(\mathrm{FFFFFFFF}00000000,00000000\mathrm{FFFFFFFF},0\right) \tag{13}$$

证明 由GRANULE算法第i轮加密过程式(5)可知:

$$\begin{cases}L_{i+1}=\left(\overline{S}(P(L_i))\lll 2\right)\oplus\left(\overline{S}(P(L_i))\ggg 7\right)\oplus R_i\oplus RK_i\\R_{i+1}=L_i\end{cases}$$

等式两边同时与FFFFFFFF做内积运算可得:

$$\begin{cases}\langle \text{FFFFFFFF}, L_{i+1}\rangle=\langle \text{FFFFFFFF}, R_i\rangle\oplus\langle \text{FFFFFFFF}, RK_i\rangle\\ \langle \text{FFFFFFFF}, R_{i+1}\rangle=\langle \text{FFFFFFFF}, L_i\rangle\end{cases}.$$

移项变形可得:

$$\begin{aligned}&\langle \text{00000000FFFFFFFF}, L_i\|R_i\rangle\\ &\quad\oplus\langle \text{FFFFFFFF00000000}, L_{i+1}\|R_{i+1}\rangle\\ &=\langle \text{FFFFFFFF}, RK_i\rangle\end{aligned}\tag{14}$$

$$\begin{aligned}&\langle \text{FFFFFFFF00000000}, L_i\|R_i\rangle\\ &\quad\oplus\langle \text{00000000FFFFFFFF}, L_{i+1}\|R_{i+1}\rangle=0\end{aligned}\tag{15}$$

证毕.

推论3　交替使用定理3中的1轮完美线性逼近进行循环迭代,我们容易得到如下GRANULE算法从第i轮到第$i+r$轮的r轮完美线性逼近:

$$\begin{cases}\left(\text{00000000FFFFFFFF}, \text{FFFFFFFF00000000}, \sum_{j=0}^{\frac{r-1}{2}}\langle \text{FFFFFFFF}, RK_{i+2j}\rangle\right), & \text{当}r\text{为奇数时}\\ \left(\text{00000000FFFFFFFF}, \text{00000000FFFFFFFF}, \sum_{j=0}^{\frac{r}{2}-1}\langle \text{FFFFFFFF}, RK_{i+2j}\rangle\right), & \text{当}r\text{为偶数时}\end{cases}\tag{16}$$

$$\begin{cases}\left(\text{FFFFFFFF00000000}, \text{00000000FFFFFFFF}, \sum_{j=1}^{\frac{r-1}{2}}\langle \text{FFFFFFFF}, RK_{i+2j-1}\rangle\right), & \text{当}r>1\text{为奇数时}\\ \left(\text{FFFFFFFF00000000}, \text{FFFFFFFF00000000}, \sum_{j=0}^{\frac{r}{2}-1}\langle \text{FFFFFFFF}, RK_{i+2j+1}\rangle\right), & \text{当}r\text{为偶数时}\end{cases}\tag{17}$$

$$\left(\text{FFFFFFFFFFFFFFFF}, \text{FFFFFFFFFFFFFFFF}, \sum_{j=1}^{r}\langle \text{FFFFFFFF}, RK_{i+j-1}\rangle\right)\tag{18}$$

3.4　结果对比

使用本文构造的LiCi、LiCi-2和GRANULE算法任意轮数的完美线性逼近(线性区分器)可以对全轮的LiCi、LiCi-2和GRANULE发起线性密码分析(由于区分器绝对线性相关性为最大值1且为任意轮数),本文与目前已有分析结果对比如表5所示.

表5　LiCi、LiCi-2和GRANULE算法的分析结果比较

密码算法	分析方法	区分器轮数	攻击/总轮数	算法
LiCi	线性分析	4	—	文献[7]
	差分分析	4	—	文献[7]
	积分分析	12	13/31	文献[22]
	积分分析	12	—	文献[23]
	不可能差分分析	10	16/31	文献[21]
	线性分析	1~31	31/31	本文
LiCi-2	线性分析	5	—	文献[8]
	差分分析	5	—	文献[8]
	相关密钥多不可能差分分析	18	25/25	文献[24]
	线性分析	1~25	25/25	本文
GRANULE	差分分析	7	—	文献[9]
	线性分析	7	—	文献[9]
	零相关线性分析	6	6/32	文献[9]
	不可能差分分析	5	11/32	文献[25]
	积分分析	10	—	文献[26]
	不可能差分分析	7	—	文献[27]
	积分分析	10	12/32	文献[28]
	不可能差分分析	7	13/32	文献[29]
	不可能差分分析	7	14/32	文献[30]
	不可能差分分析	10	16/32	文献[31]
	线性分析	1~32	32/32	本文

3.5 实验与讨论

为了进一步验证本文所提出的线性区分器的理论正确性,对线性区分器进行了实验验证,实验结果与理论完全一致. 从分析结果上看,由于LiCi和LiCi-2算法均采用了类似的设计理念,为了追求软硬件性能,将S盒替换操作放在Feistel结构的单侧分支上,引起了线性掩码的抵消,从而导致存在概率为1的迭代完美线性逼近. 而GRANULE算法同样为了追求实现性能,在S盒替换操作后进行了两分支异或操作,引起了线性掩码的抵消,再次导致存在概率为1的迭代(循环)完美线性逼近. 因此在未来轻量级分组密码算法的设计中应避免类似的设计理念.

4 结论

本文根据LiCi、LiCi-2和GRANULE算法的结构特性,构造了多条概率为1的迭代(循环)完美线性逼近,通过这些迭代(循环)完美线性逼近构造了这些算法多条任意轮数(包括全轮)的完美线性逼近(线性区分器),通过这些完美线性逼近可以对全轮的LiCi、LiCi-2和GRANULE算法进行线性分析. 分析结果表明,LiCi、LiCi-2和GRANULE算法存在严重的设计缺陷.

参考文献

[1] 武传坤. 物联网安全技术专栏序言(中英文)[J]. 密码学报, 2020, 7(1): 83-86.
WU C K. Preface of security techniques in internet of things column[J]. Journal of Cryptologic Research, 2020, 7(1): 83-86. (in Chinese)

[2] DAEMEN J, RIJMEN V. The Design of Rijndael: Aes-the Advanced Encryption Standard[M]. Berlin: Springer, 2020.

[3] WU W L, Zhang L. LBlock: A lightweight block cipher[C]// Applied Cryptography and Network Security: 9th International Conference (ACNS 2011). Berlin: Springer, 2011: 327-344.

[4] BOGDANOV A, KNUDSEN L R, LEANDER G, et al. PRESENT: An ultra-lightweight block cipher[C]//Cryptographic Hardware and Embedded Systems: 9th International Workshop (CHES 2007). Berlin: Springer, 2007: 450-466.

[5] 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: 1-6.

[6] GUO J, PEYRIN T, POSCHMANN A, et al. The LED block cipher[C]//Cryptographic Hardware and Embedded Systems: 13th International Workshop (CHES 2011). Berlin: Springer, 2011: 326-341.

[7] PATIL J, BANSOD G, KANT K S. LiCi: A new ultra-lightweight block cipher[C]//Proceedings of the 2017 International Conference on Emerging Trends & Innovation in ICT (ICEI 2017). Piscataway: IEEE, 2017: 40-45.

[8] KHAIRNAR S, BANSOD G, DAHIPHALE V. A light weight cryptographic solution for 6LoWPAN protocol stack[C]// Proceedings of the 2018 Computing Conference: Intelligent Computing (SAI 2018), Volume 2. Cham: Springer, 2019: 977-994.

[9] BANSOD G, PATIL A, PISHAROTY N. GRANULE: An ultra lightweight cipher design for embedded security[J/OL]. (2018-06-18)[2024-07-15]. https://eprint.iacr.org/20 18/600.

[10] MATSUI M. Linear cryptanalysis method for DES cipher[C]//Advances in Cryptology: Workshop on the Theory and Application of Cryptographic Techniques (EUROCRYPT 1993). Berlin: Springer, 1993: 386-397.

[11] BIHAM E, SHAMIR A. Differential cryptanalysis of DES-like cryptosystems[J]. Journal of Cryptology, 1991, 4: 3-72.

[12] HU Y, ZHANG Y, XIAO G. Integral cryptanalysis of SAFER[J]. Electronic Letters, 1999, 35(17): 1458-1459.

[13] BIHAM E, BIRYUKOV A, SHAMIR A. Cryptanalysis of Skipjack reduced to 31 rounds using impossible differentials[C]//Advances in Cryptology: International Conference on the Theory and Application of Cryptographic Techniques (EUROCRYPT 1999). Berlin: Springer, 1999: 12-23.

[14] BOURA C, David N, Derbez P, et al. Differential meet-in-the-middle cryptanalysis[C]//Advances in Cryptology: 43rd Annual International Cryptology Conference (CRYPTO 2023). Cham: Springer, 2023: 240-272.

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

[16] 马猛, 赵亚群. 简化版Trivium算法的线性逼近研究[J]. 通信学报, 2016, 37(6): 185-191.
MA M, ZHAO Y Q. Research on linear approximations of simplified trivium[J]. Journal on Communications, 2016, 37(6): 185-191. (in Chinese)

[17] 李灵琛, 吴文玲, 汪艳凤. 多维零相关线性分析模型的改进及在23轮LBlock-s算法中的应用[J]. 计算机学报, 2017, 40(5): 1192-1202.
LI L C, WU W L, WANG Y F. Improved multidimensional zero-correlation linear cryptanalysis and applications to 23-round LBlocks[J]. Chinese Journal of Computers, 2017, 40(5): 1192-1202. (in Chinese)

[18] WEI T, YE T, WU W, et al. Generalized nonlinear invariant attack and a new design criterion for round constants[J]. IACR Transactions on Symmetric Cryptology, 2018: 62-79.

[19] YE T, WEI Y Z, MEIER W. A new cube attack on MORUS by using division property[J]. IEEE Transactions on Computers, 2019, 68(12): 1731-1740.

[20] BEIERLE C, FELKE P, LEANDER G, et al. On perfect

linear approximations and differentials over two-round SPNs[C]//Advances in Cryptology: 43rd Annual International Cryptology Conference (CRYPTO 2023). Cham: Springer, 2023: 209-239.

[21] 韦永壮, 史佳利, 李灵琛. LiCi分组密码算法的不可能差分分析[J]. 电子与信息学报, 2019, 41(7): 1610-1617.
WEI Y Z, SHI J L, LI L C. Impossible differential cryptanalysis of LiCi Block cipher[J]. Journal of Electronics & Information Technology, 2019, 41(7): 1610-1617. (in Chinese)

[22] 信文倩, 孙兵, 李超. LiCi算法的基于比特积分攻击[J]. 计算机工程, 2020, 46(7): 136-142.
XIN W Q, SUN B, LI C. Bit-based integral attack on LiCi algorithm[J]. Computer Engineering, 2020, 46(7): 136-142. (in Chinese)

[23] 王红艳, 韦永壮, 刘文芬. ANU, ANU-Ⅱ和LiCi算法的积分区分器搜索[J]. 小型微型计算机系统, 2020, 41(7): 1470-1475.
WANG H Y, WEI Y Z, LIU W F. Integral distinguisher search of ANU,ANU-II and LiCi block ciphers[J]. Journal of Chinese Computer Systems, 2020, 41(7): 1470-1475. (in Chinese)

[24] ZHANG K, LAI X J, WANG L, et al. Related-key multiple impossible differential cryptanalysis on full-round LiCi-2 designed for IoT[J]. Security and Communication Networks, 2022, 2022: 3611840.

[25] 石淑英, 何骏. GRANULE算法的不可能差分分析[J]. 计算机工程, 2019, 45(10): 134-138.
SHI S Y, HE J. Impossible differential cryptanalysis of GRANULE algorithm[J]. Computer Engineering, 2019, 45(10): 134-138. (in Chinese)

[26] 方玉颖, 徐洪. 轻量分组密码GRANULE的积分特征自动化搜索[J]. 信息工程大学学报, 2019, 20(3): 346-349.
FANG Y Y, XU H. Automatic search of integral characteristics of lightweight block cipher GRANULE[J]. Journal of Information Engineering University, 2019, 20(3): 346-349. (in Chinese)

[27] 武小年, 李迎新, 韦永壮, 等. GRANULE和MANTRA算法的不可能差分区分器分析[J]. 通信学报, 2020, 41(1): 94-101.
WU X N, LI Y X, WEI Y Z, et al. Impossible differential distinguisher analysis of GRANULE and MANTRA algorithm[J]. Journal on Communications, 2020, 41(1): 94-101. (in Chinese)

[28] LI J, WANG H Y, QIU X Y, et al. Integral analysis of GRANULE and ESF block ciphers based on MILP[C]//12th International Conference on Information and Communication Systems (ICICS 2021). IEEE, 2021: 10-16.

[29] 赵晨曦. 轻量级分组密码的不可能差分分析[D]. 西安: 西安电子科技大学, 2021.
ZHAO C X. Impossible Difference Analysis of Lightweight Block Cipher[D]. Xi'an: Xidian University, 2021. (in Chinese)

[30] 刘先蓓, 刘亚. GRANULE算法的截断不可能差分分析[J]. 山西师范大学学报(自然科学版), 2023, 37(1): 41-51.
LIU X B, LIU Y. Truncated impossible differential cryptanalysis of GRANULE[J]. Journal of Shanxi Normal University (Natural Science Edition), 2023, 37(1): 41-51. (in Chinese)

[31] 武小年, 匡晶, 张润莲, 等. 基于SAT的GRANULE算法不可能差分分析[J]. 计算机应用, 2024, 44(3): 797-804.
WU X N, KUANG J, ZHANG R L, et al. SAT-based impossible differential cryptanalysis of GRANULE cipher[J]. Journal of Computer Applications, 2024, 44(3): 797-804. (in Chinese)

作者简介

严智广　男, 1999年11月出生于江西省上饶市. 现为桂林电子科技大学计算机与信息安全学院博士研究生. 主要研究方向为对称密码算法设计与分析、网络空间安全.
E-mail: zhiguang_yan@163.com

李灵琛　女, 1988年2月出生于广西壮族自治区桂林市. 现为桂林电子科技大学计算机与信息安全学院讲师. 主要研究方向为分组密码算法设计与分析.
E-mail: lilingchen601@126.com

韦永壮　男, 1976年12月出生于广西壮族自治区百色市. 现为广西密码学与信息安全重点实验室主任, 桂林电子科技大学计算机与信息安全学院教授, 博士生导师, 中国密码学会理事. 主要研究方向为密码函数、对称密码算法设计与分析.
E-mail: walker_wyz@guet.edu.cn