基于混合整数线性规划的八阵图不可能差分分析

杜小妮[①③④] 梁丽芳*[①③] 贾美纯[①③] 李锴彬[②③]

[①](西北师范大学数学与统计学院 兰州 730070)

[②](西北师范大学计算机科学与工程学院 兰州 730070)

[③](西北师范大学密码技术与数据分析重点实验室 兰州 730070)

[④](甘肃省数学与统计学基础学科研究中心 兰州 730070)

摘 要：八阵图(ESF)是基于LBlock改进的轻量级分组密码，具有优良的软硬件实现效率。针对ESF算法的安全性，该文借助自动化搜索工具，利用不可能差分分析方法，对算法进行安全性评估。首先结合ESF的结构特性和S盒的差分传播特性，建立了基于混合整数线性规划(MILP)的不可能差分搜索模型；其次利用算法 S盒的差分传播特性和密钥扩展算法中轮子密钥间的相互关系，基于一条9轮不可能差分区分器，通过向前扩展2轮向后扩展4轮，实现了对ESF算法的15轮密钥恢复攻击。分析结果表明，该攻击的数据复杂度和时间复杂度分别为$2^{60.16}$和$2^{67.44}$，均得到有效降低，且足够抵抗不可能差分分析。

关键词：八阵图(ESF)；不可能差分分析；混合整数线性规划(MILP)

中图分类号：TN918; TP309.7 **文献标识码**：A **文章编号**：1009-5896(2023)12-4391-08

DOI: 10.11999/JEIT221292

Impossible Differential Cryptanalysis of Eight-Sided Fortress Based on Mixed Integer Linear Programming

DU Xiaoni[①③④] LIANG Lifang[①③] JIA Meichun[①③] LI Kaibin[②③]

[①](*College of Mathematics and Statistic*, *Northwest Normal University*, *Lanzhou* 730070, *China*)

[②](*College of Computer Science and Engineering*, *Northwest Normal University*, *Lanzhou* 730070, *China*)

[③](*Key Laboratory of Cryptography and Data Analytics*, *Northwest Normal University*, *Lanzhou* 730070, *China*)

[④](*Gansu Provincial Research Center for Basic Disciplines of Mathematics and Statistics*, *Lanzhou* 730070, *China*)

Abstract: Eight-Sided Fortress(ESF), an improved lightweight block cipher based on LBlock, has excellent software and hardware implementation efficiency. For the security of ESF, with the help of automated search tools, the algorithm is evaluated for security using the impossible differential cryptanalysis. Firstly, an impossible differential search model based on Mixed Integer Linear Programming (MILP) is built by combining the structure of ESF algorithm and the differential propagation of S-box. Secondly, based on a 9-round impossible differential distinguisher of ESF, using the differential propagation characteristics of the S-box and the relationship of the round subkeys in the key schedule, a 15-round-attack is presented to ESF by adding two rounds in the front and adding four rounds in the end. It is found that the data complexity of plaintexts and time complexity of encryptions of the attack need are $2^{60.16}$ and $2^{67.44}$, respectively. The results show that the data complexity and time complexity have been effectively reduced, and the proposed method is able to resist impossible differential cryptanalysis.

Key words: Eight-Sided Fortress(ESF); Impossible differential cryptanalysis; Mixed Integer Linear Programming (MILP)

收稿日期：2022-10-12；改回日期：2023-04-12；网络出版：2023-04-17

*通信作者： 梁丽芳 llf_1003@163.com

基金项目：国家自然科学基金(62172337)，甘肃省自然科学基金重点项目(23JRRA685)，甘肃省基础研究创新群体项目(23JRRA684)

Foundation Items: The National Natural Science Foundation of China (62172337), The Key Project of Gansu Natural Science Foundation (23JRRA685), The Funds for Innovative Fundamental Research Group Project of Gansu Province (23JRRA684)

1 引言

近年来，伴随无线传感器网络以及射频识别技术的发展和广泛应用，需要轻量级分组密码对资源受限的设备进行数据加密。这类算法具有效率高、功耗低、占用资源少等优点，且易于在软硬件上实现。目前提出了许多轻量级分组密码算法[1–5]，比较经典的算法有PRESENT, LBlock, WARP等。

ESF算法是2013年Liu等人[6]基于LBlock改进的轻量级分组密码算法，适用于传感器网络等资源有限的环境。该算法置换层采用了PRESENT中比特置换的设计思想，在提高软硬件实现效率的同时，使得硬件面积相比LBlock减少20个等效行。针对ESF算法的安全性分析主要是不可能差分密码分析[7,8]，该分析的思想来源于差分密码分析，利用中间相错[9]的原理推导出概率为零的差分路径，从而排除错误密钥。当所有错误密钥均被排除时，攻击者就可确定正确密钥。近些年，针对ESF算法的分析结果较多。2013年，刘宣等人[10]首次给出了ESF算法的8轮不可能差分区分器，在此区分器基础上，通过前面加2轮后面加1轮的方法，实现了对该算法的11轮攻击；2016年，陈玉磊等人采用文献[11]中的区分器，通过向前添加1轮，向后添加2轮的扩展方式实现了相同轮数的攻击，与文献[10]相比，时间复杂度和数据复杂度均有效降低；2017年，高红杰等人[12]同样采用文献[10]中的区分器，通过向前向后各添加2轮的扩展方式，实现了对ESF算法12轮攻击，与文献[11]相比，攻击轮数提高了一轮，数据复杂度仍保持不变；2018年，谢敏等人[13]首次对ESF进行了相关密钥不可能差分分析，结合算法特点构造了两条10轮相关密钥不可能差分路径，对ESF分别进行了13轮和14轮不可能差分分析；2019年，李明明等人[14]基于8轮截断不可能差分区分器，对ESF进行了13轮不可能差分分析，与文献[10–12]相比，实现了更多轮数的攻击；2021年，Li等人[15]利用自动化搜索方法，对ESF算法进行了基于比特可分性质的积分分析，给出了ESF算法9轮积分区分器的自动搜索方法；同年，Wu等人[16]同样采用自动化搜索方法搜索到9轮不可能差分区分器，并对其进行验证，且从中选取一条区分器，通过向前向后各添加3轮的扩展方式实现了15轮攻击，相比现有结果，攻击轮数明显提高。

受文献[17]的启发，本文的主要贡献包括两个方面：

(1) 利用ESF算法的结构特性，研究得到了S盒的差分传播规律，构建了基于MILP的ESF差分搜索模型，并利用中间相遇的原理，得到了 ESF算法轮数更长的不可能差分区分器。

(2) 基于9轮不可能差分区分器，通过向前添加2轮和向后添加4轮的扩展方式，给出了15轮的扩展路径，并成功实现了15轮单密钥不可能差分攻击。攻击过程的数据复杂度和时间复杂度分别为$2^{60.16}$和 $2^{67.44}$。与文献[16]相比，数据复杂度和时间复杂度均明显降低。

本文第2节简要描述ESF算法；第3节给出ESF算法基于MILP的有效差分路径的搜索算法；第4节给出ESF算法的不可能差分分析；第5节总结全文。

2 算法描述

为了便于算法描述，下面给出符号说明：

X: 64 bit明文

Y: 64 bit密文

L_i: 第i轮输出的左 32 bit

R_i: 第i轮输出的右 32 bit

K: 80 bit的主密钥

K_i: 第i轮的 32 bit子密钥

$K_{i,j}$: K_i的第j个半Byte

$K_{i,j}^h$: $K_{i,j}$的第$h$bit

S_i: 4×4的第i个S盒

P: 比特置换

$[i]_2$: 常数i的二进制表示

2.1 算法加密过程

ESF是一种轻量级分组密码算法，整体结构采用LBlock的设计准则和 PRESENT 线性层按比特置换的思想，以实现更快的扩散。ESF算法采用广义Feistel结构，算法的分组长度为64 bit，密钥长度为80 bit，迭代轮数为32轮。一轮算法加密流程如图1所示。

加密流程如下：

(1) 输入 64 bit的明文

$$X = L_0||R_0 \tag{1}$$

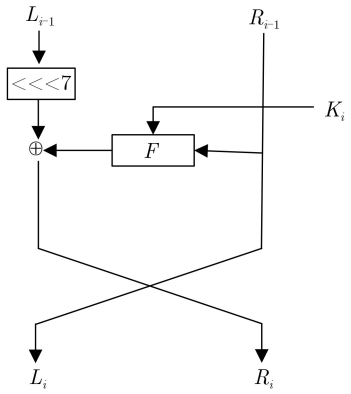

图 1 ESF 算法结构

(2) 当 $i=1,2,\cdots,31$时，

$$\left.\begin{aligned} L_i &= R_{i-1} \\ R_i &= (L_{i-1} <<< 7) \oplus F(R_{i-1}, K_i) \end{aligned}\right\} \tag{2}$$

(3) 当 $i=32$时，

$$\left.\begin{aligned} L_{32} &= (L_{31} <<< 7) \oplus F(R_{31}, K_{32}) \\ R_{32} &= R_{31} \end{aligned}\right\} \tag{3}$$

(4) 输出密文

$$Y = L_{32}||R_{32} \tag{4}$$

ESF算法的轮函数为SPN结构，如图2所示，由混淆层和置换层构成，其中混淆层是一个4×4的非线性替换，由8个并行的S盒构成，S盒如表1所示；置换P将32 bit的$b_{31}||b_{30}||\cdots||b_0$映射为$c_{31}||c_{30}||\cdots||c_0$，即

$$b_{4j}||b_{4j+1}||b_{4j+2}||b_{4j+3} \to c_j||c_{j+8}||c_{j+16}||c_{j+24},\quad j=0,1,\cdots,7 \tag{5}$$

2.2 密钥扩展算法

ESF算法主密钥长度为80 bit，经过更新，每轮产生32 bit的轮子密钥。首先将$K=(k_{79}k_{78}\cdots k_1k_0)$存储在寄存器中，取最左端的32 bit密钥作为$K_1$，对于$i=1,2,\cdots,31$轮密钥更新如下：

(1) $K <<< 13$；

(2) $[k_{79}k_{78}k_{77}k_{76}] = S_0[k_{79}k_{78}k_{77}k_{76}]$,
$[k_{75}k_{74}k_{73}k_{72}] = S_0[k_{75}k_{74}k_{73}k_{72}]$,
$[k_{47}k_{46}k_{45}k_{44}k_{43}] = [k_{47}k_{46}k_{45}k_{44}k_{43}] \oplus [i]_2$;

(3) 取最左端的32 bit作为轮密钥K_{i+1}。

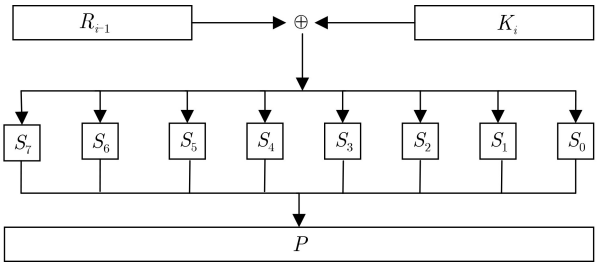

图 2 ESF 算法轮函数

3 基于MILP的有效差分路径搜索

3.1 ESF算法S盒的差分传播特性

定义1 (S盒差分分布表[17]) 设$m,n\in\mathbb{N}$，从F_2^m到F_2^n的非线性映射(称S盒)记为$S:F_2^m\to F_2^n$，给定$\alpha\in F_2^m,\beta\in F_2^n$，定义

$$\left.\begin{aligned} IN_S(\alpha,\beta) &= \{x\in F_2^m : S(x\oplus\alpha)\oplus S(x)=\beta\} \\ N_S(\alpha,\beta) &= \#IN_S(\alpha,\beta) \end{aligned}\right\} \tag{6}$$

其中$N_S(\alpha,\beta)$表示第α行第β列的取值。由式(6)可构造ESF算法S盒的差分分布表(此处以S_0为例)，如表2所示。

定理1[18] 若给定S盒的输入差分值，那么对应S盒的输出差分值至少有1 bit的概率为1，且称概率为1的bit为未受干扰比特。

分析表2可知，给定S_0盒的输入差分值，其输出差分存在一定的规律。例，当$\alpha=0010$，β的取值分别为1001, 1010, 1100, 1101, 1110, 1111，观察发现输出差分的第3 bit取值为1，其余3 bit的取值可为1或0，输出差分可记为$1**$ ($*$ 表示未知比特)。同理，根据ESF算法8个S盒的差分分布表，给定S盒的输入差分值，输出差分值存在的传播特性如表3所示。

输入差分为某些值时，其输出差分存在相应的概率，如表4所示。

3.2 基于MILP的有效差分路径搜索算法

利用逻辑状态模型和凸闭包计算，将3.1节中S盒的差分传播特性用不等式表示，由此来移除不可能差分路径，使得可行域的集合逼近ESF算法的有效差分路径。搜索ESF算法加密方向有效路径见算法1。

4 ESF算法的不可能差分分析

4.1 不可能差分分析

不可能差分分析由差分分析演变而来，近年来成为分组密码安全性分析的常用方法之一。其基本

表 1 ESF的S盒

	x															
	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
S_0	3	8	f	1	a	6	5	b	e	d	4	2	7	0	9	c
S_1	f	c	2	7	9	0	5	a	1	b	e	8	6	d	3	4
S_2	8	6	7	9	3	c	a	f	d	1	e	4	0	b	5	2
S_3	0	f	b	8	c	9	6	3	d	1	2	4	a	7	5	e
S_4	1	f	8	3	c	0	b	6	2	5	4	a	9	e	7	d
S_5	f	5	2	b	4	a	9	c	0	3	e	8	d	6	7	1
S_6	7	2	c	5	8	4	6	b	e	9	1	f	d	3	a	0
S_7	1	d	f	0	e	8	2	b	7	4	c	a	9	3	5	6

表 2 ESF 的S_0盒差分分布表

	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	0	0	2	0	2	2	2	0	0	0	2	2	0	4	0
2	0	0	0	0	0	0	0	0	0	2	2	0	4	2	2	4
3	0	2	2	2	0	0	0	2	0	4	0	2	2	0	0	0
4	0	0	0	0	0	0	0	0	0	4	4	0	0	4	4	0
5	0	0	2	0	4	2	0	0	2	0	2	2	0	0	2	0
6	0	2	2	4	0	2	2	4	0	0	0	0	0	0	0	0
7	0	0	2	0	4	2	0	0	2	2	0	2	0	2	0	0
8	0	0	0	2	0	2	2	2	0	0	0	2	2	4	0	0
9	0	2	2	0	0	2	2	0	0	2	2	0	0	2	2	0
a	0	2	2	2	0	0	0	2	0	0	4	2	2	0	0	0
b	0	2	2	0	0	2	2	0	0	0	0	0	4	0	0	4
c	0	2	0	0	4	0	2	0	2	2	0	2	0	2	0	0
d	0	0	0	4	0	0	0	4	4	0	0	0	0	0	0	4
e	0	2	0	0	4	0	2	0	2	0	2	2	0	0	2	0
f	0	2	2	0	0	2	2	0	4	0	0	0	0	0	0	4

表 3 ESF的S盒差分传播特性

S_0		S_1		S_2		S_4		S_5		S_6	
α	β	α	β	α	β	α	β	α	β	α	β
0010	$1***$	0100	$*1**$	0010	$***1$	0100	$***1$	0100	$***1$	0010	$**1*$
0100	$1***$	1000	$*1**$	1000	$***1$	1011	$***1$	1011	$***1$	0100	$**1*$
0110	$0***$	1100	$*0**$	1010	$***0$	1111	$***0$	1111	$***0$	0110	$**0*$

表 4 ESF的S盒差分概率传播特性

S	S_0	S_6
α	1000	0001
β	$****$	$****$
P	$\frac{1}{8}$	$\frac{1}{8}$

思想是利用概率为0的差分路径来构建区分器，通过该区分器排除导致概率为0的差分出现的候选密钥，将筛选后剩下的密钥作为正确密钥。不可能差分的定义如下。

定义2 对于一个迭代分组密码算法，设明文对(X, X^*)的差分值为$\Delta X = \alpha$，第r轮输出对(Y, Y^*)

算法1 搜索 ESF 算法加密方向的有效差分路径

输入： 64 bit的明文输入差分ΔX,

输出：加密后的输出差分集合List.

1. set = $\{\Delta X\}$；

2. 如果set中包含部分比特已知的差分；

3. for ΔX in set

2. List.append(ΔX)；

4. $\Delta x_0 - \Delta x_1 - \Delta x_2 + \Delta x_3 - \Delta y_0 + 2 \geq 0$； #当$\alpha_0 = 0110$, $\beta_0 = 0****$时的不等式约束，对于其他S盒有类似性质

5. $\Delta r_1 + \Delta \mathrm{k}_1 + \Delta m_1 - 2d \geq 0, d \geq \Delta r_1, d \geq \Delta \mathrm{k}_1, d \geq \Delta m_1$, $\Delta r_1 + \Delta \mathrm{k}_1 + \Delta m_1 \leq 2$； #异或的约束条件

6. $\sum_{i=0}^{3} \Delta x_i - 4A \leq 0$, $\sum_{i=0}^{3} \Delta x_i - A \geq 0$, $4\sum_{i=0}^{3} \Delta y_i - \sum_{i=0}^{3} \Delta x_i \geq 0$, $4\sum_{i=0}^{3} \Delta x_i - \sum_{i=0}^{3} \Delta y_i \geq 0$； #$S$盒约束条件

7. S盒差分传播特性得到的213个不等式约束条件；

8. 利用GUROBI求解MILP模型，判断是否存在可行解；

9. 若存在可行解，则输出set.append(满足上述条件的输出差分ΔY)；

10. set = set $-(\Delta X)$，重复执行上述步骤1-步骤9，直到set全为未知的比特；

11. return List.

的差分值为 $\Delta Y=\beta$，若$P(\Delta Y=\beta|\Delta X=\alpha)=0$，则称$(\alpha \nrightarrow \beta)$为一条 r轮不可能差分。

基于一条$r-1$轮不可能差分区分器$(\alpha \nrightarrow \beta)$，$r$轮不可能差分分析流程如下：

(1) 选择明文对(X,X^*)满足输入差分α，加密得到相应的密文对(Y,Y^*)；

(2) 猜测第r轮的轮密钥K_r，解密密文对，得到相应的中间值(D,D^*)，判断$D\oplus D^*=\beta$是否成立。若成立，则对应的猜测值为错误密钥。

(3) 重复以上步骤，直到密钥唯一确定。

假设通过上述攻击可以得到$|K|$ bit密钥，且每个明密文对可以淘汰2^{-t}的密钥量，要保证正确密钥被唯一确定，所需明密文对n必须满足

$$(2^{|K|}-1)\times(1-2^{-t})^n<1 \tag{7}$$

4.2 ESF算法的不可能差分攻击

基于3.2节中的算法1，从加解密方向各找一条概率为1的差分路径，利用中间相遇的思想，将其拼接并筛选出一条概率为0的最优差分路径，搜索轮数最长的不可能差分区分器流程见算法2。将此思想应用于不可能差分分析中，可获得轮数更长的不可能差分区分器。

ESF算法的分组长度为64 bit，遍历所有可能差分的复杂度过高，故只对汉明重量为1的输入/输出差分进行搜索。基于算法2，搜索并选取其中一条9区分器(0100 0000 0000 0000) $\nrightarrow$ (1000 0000 0000 0000)，在此区分器基础上通过向前扩展2轮向后扩展4轮实现了对ESF算法进行15轮不可能差分攻击。具体路径如图3 所示，其中“$*$”取任意值。

定理2　利用9轮不可能差分区分器对ESF算法进行15轮不可能差分分析，攻击过程明文量为$2^{60.16}$，时间复杂度为$2^{67.44}$。

依据 4.1 节中的攻击原理，不可能差分攻击过程如下。

(1) 选择明文结构：输入差分选择满足如式(8)形式的明文对

$$\left.\begin{aligned}\Delta L_0&=(0*0*\ 0*0*\ 0*0*\ 0*1*\ 0*0*\ 0*0*\ 0*0*\ 0*0*)\\ \Delta R_0&=(*\,000\,0000\ *\ 000\,0000\ *\ 000\,0000\ *000\,0000)\end{aligned}\right\} \tag{8}$$

该结构由2^{20}个明文生成，共有 $2^{20}\times 2^{20}\times 1/2=2^{30}$个明文对。若选择$2^n$个明文结构，则构成$2^{n+39}$个明密文对。

(2) 密文筛选：输出差分选择满足如式 (9) 的密文对

$$\left.\begin{aligned}\Delta L_{15}&=(0*0*\ 0*0*\ 0*0*\ 0*0*\ 0*0*\ 0*0*\ 0*0*\ 0*0*)\\ \Delta R_{15}&=(****\ \ ****\ ****\ ****\ ****\ ****\ ****\ ****)\end{aligned}\right\} \tag{9}$$

经此步骤过滤大约剩余$2^{n+39}\times 2^{-16}=2^{n+23}$个数据对。

(3) 猜测密钥：

(a) 猜测K_{15}，共32 bit。在K中对应的位置为$K_{57-54},K_{53-50},K_{49-46},K_{45-42}$，$K_{41-38},K_{37-34},K_{33-30},K_{29-26}$。对剩余密文对进行解密运算，由$L_{14}<<<7=P\cdot S(R_{14}\oplus K_{15})\oplus R_{15}$可知，排除不满足$\Delta L_{14}=(0000\ 000*\ 0000\ 000*\ 0000\ 000*\ 0000\ 000*)$的数据对，则剩余数据对个数为$2^{n+23}\times 2^{-28}=2^{n-5}$。此步骤的时间复杂度为

$$2\times 1/8\times\sum_{i=1}^{8}2^{n+(27-4i)}\times 2^{4i}=2^{n+28}。$$

(b) 猜测$K_{14,6},K_{14,4},K_{14,2},K_{14,0}$。它们在$K$中对应的位置为$K_{66-63},K_{58-55},K_{48-45},K_{40-37}$，由于$K_{57-55},K_{48-45},K_{40-37}$在(a)中已被猜测，故只需猜测剩余5 bit。对剩余数据对进行一轮解密运算，依次验证式(10)

$$\left.\begin{aligned}&S_6(L_{14,6}\oplus K_{14,6})\\ &\quad\oplus S_6(L_{14,6}\oplus\Delta L_{14,6}\oplus K_{14,6}\oplus\Delta K_{14,6})\\ &\quad=\Delta R^2_{14,7}||\Delta R^2_{14,5}||\Delta R^2_{14,3}||\Delta R^2_{14,1}\\ &S_4(L_{14,4}\oplus K_{14,4})\oplus S_4\ (L_{14,4}\oplus\Delta L_{14,4}\oplus K_{14,4}\\ &\quad\oplus\Delta K_{14,4})=\Delta R^0_{14,7}||\Delta R^0_{14,5}||\Delta R^0_{14,3}||\Delta R^0_{14,1}\end{aligned}\right\} \tag{10}$$

是否成立，经排除不满足式(10)的数据对后，剩余数据对个数为$2^{n-5}\times 2^{-16}=2^{n-21}$。此步骤的时间复杂度为

算法2 寻找最长不可能差分区分器轮数

输入：加密后的差分路径集合E.List, 解密后的差分路径集合D.List

输出：输出最长不可能差分区分器轮数

```
r = 0;
for i in range len(E.List)
    for j in range len(D.List)
        if E.List[i] ≠ D.List[j];
            if r > i + j
                r = r;
            else
                r = i + j;
return r.
```

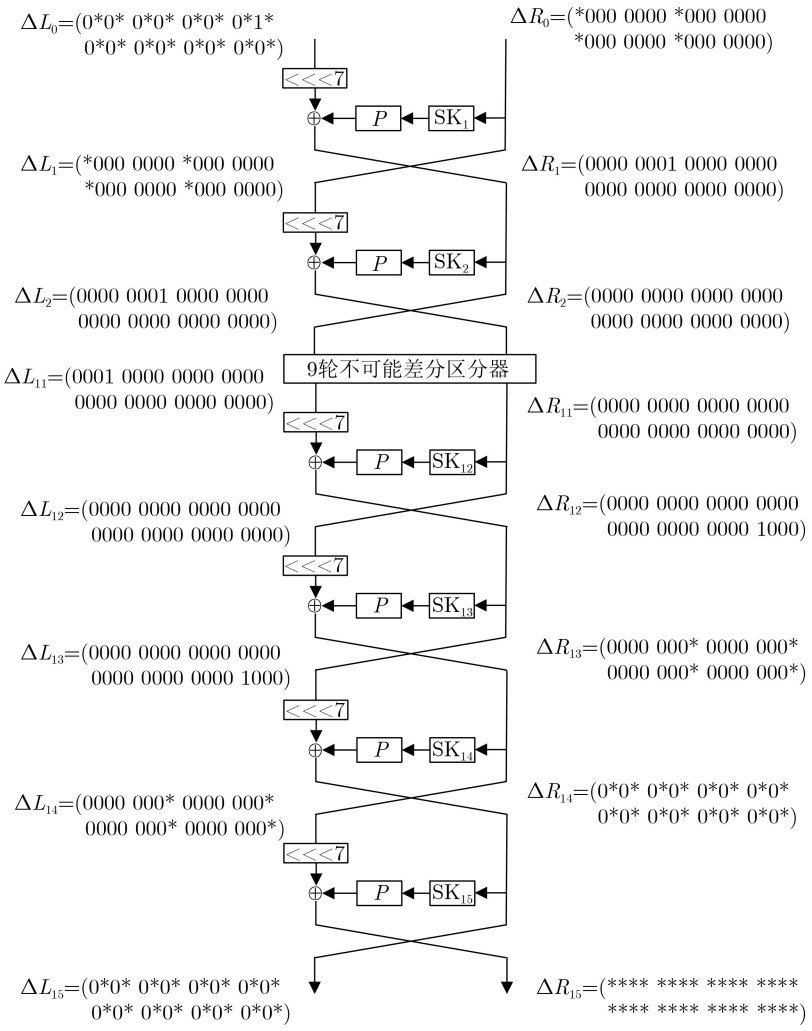

图 3 ESF的15轮不可能差分攻击

$2 \times 2^{32} \times 2^5 \times 2^{n-5} \times 2/8 = 2^{n+31}$。

(c) 猜测$K_{13,0}$。$K_{13,0}$由(a)可得，只需验证式(11)即可

$$S_0(R_{12,0} \oplus K_{13,0}) \oplus S_0(R_{12,0} \oplus \Delta R_{12,0} \oplus K_{13,0} \oplus \Delta K_{13,0}) = \Delta L^1_{12,6} || \Delta R^1_{12,4} || \Delta R^1_{12,2} || \Delta R^1_{12,0} \quad (11)$$

经排除不满足式(11)的数据对后，剩余数据对个数为$2^{n-21} \times 2^{-3} = 2^{n-24}$。此步骤的时间复杂度为

$$2 \times 2^{32} \times 2^5 \times 2^{n-21} \times 1/8 = 2^{n+14}。$$

(d) 猜测$K_{1,7}, K_{1,5}, K_{1,3}, K_{1,1}$。它们在$K$中对应的位置为$K_{79-76}, K_{71-78}, K_{63-60}, K_{55-52}$，由于$K_{55-52}$在(a)中已被猜测，只需猜测剩余12 bit。计算$L_0 <<< 7 = P \cdot S(R_0 \oplus K_1) \oplus R_1$，保留满足$\Delta L_0 = (0* \ 0* \ 0*0* \ 0*0*0*1* \ 0*0* \ 0*0* \ 0*0* \ 0*0*)$的数据对。过滤后剩余数据对个数为 $2^{n-24} \times 2^{-4} = 2^{n-28}$。此步骤的时间复杂度为

$$2 \times 2^{32} \times 2^5 \times 2^{12} \times 2^{n-24} \times 4/8 = 2^{n+25}。$$

(e) 猜测 $K_{2,6}$。排除不满足$S_6(R_{1,6} \oplus K_{2,6}) \oplus S_6(R_{1,6} \oplus \Delta R_{1,6} \oplus K_{2,6} \oplus \Delta K_{2,6}) = \Delta R^2_{2,7} || \Delta R^2_{2,5} || \Delta R^2_{2,3} || \Delta R^2_{2,1}$的数据对，经这一步排除，剩余数据对的个数为$2^{n-28} \times 2^{-3} = 2^{n-31}$。此步骤的时间复杂度为

$$2 \times 2^{32} \times 2^5 \times 2^{12} \times 2^4 \times 2^{n-28} \times 1/8 = 2^{n+23}。$$

上述的15轮不可能差分攻击过程中，共猜测得到53 bit子密钥，经过分析2^{n-31}个数据对后，错误密钥还剩 $2^{53} \times (1-2^{-4})^{2^{n-31}}$ 个，而当 $n \approx 40.16$ 时，有 $(2^{53}-1) \times (1-2^{-4})^{2^{n-31}} < 1$ 成立，此时我们认为已将错误密钥全部淘汰。

攻击过程的数据复杂度为

$$2^{n+20} \approx 2^{40.16+20} = 2^{60.16}。$$

攻击过程的时间复杂度为

$$(2^{n+28}+2^{n+31}+2^{n+14}+2^{n+25}+2^{n+23})/15 \approx (2^{68.16}+2^{71.16}+2^{54.16}+2^{65.16}+2^{63.16})/15 \approx 2^{67.44}。$$

4.3 结果对比

对ESF算法分析的常用方法是不可能差分分析。本文根据ESF算法的结构特性和S盒的差分传

播特性，实现了对ESF的15轮不可能差分攻击。与文献[16]相比，在攻击轮数相同的条件下，时间复杂度和数据复杂度均得到有效降低。对比结果如表5所示。

表 5　ESF 分析方法结果对比

攻击轮数	分析方法	时间复杂度	数据复杂度	文献
11	不可能差分分析	$2^{75.5}$	2^{59}	文献[10]
11	不可能差分分析	2^{32}	2^{53}	文献[11]
12	不可能差分分析	$2^{60.45}$	2^{53}	文献[12]
13	截断不可能差分分析	$2^{61.99}$	$2^{77.39}$	文献[14]
14	相关密钥不可能差分分析	$2^{43.95}$	2^{62}	文献[13]
15	不可能差分分析	$2^{70.02}$	$2^{64.3}$	文献[16]
15	不可能差分分析	$2^{67.44}$	$2^{60.16}$	本文

5　结束语

本文利用ESF算法的S盒差分传播特性，基于中间相遇思想，构建基于MILP的自动化搜索模型，搜索ESF的不可能差分区分器。选取了其中一条区分器，利用S盒的输入输出差分特征，分别向前添加2轮向后添加4轮，对ESF算法进行15轮不可能差分攻击，且攻击的时间复杂度低于穷举攻击的复杂度，与现有结果相比，攻击效果也有较大的提升。在后续工作中，将考虑将多种分析方法结合，并优化搜索算法，找到更好的不可能差分区分器，进一步提高不可能差分攻击的轮数。

参 考 文 献

[1] BOGDANOV A, KNUDSEN L R, LEANDER G, *et al*. PRESENT: An ultra-lightweight block cipher[C]. Proceedings of the 9th International Workshop on Cryptographic Hardware and Embedded Systems-CHES 2007, Vienna, Austria, 2007: 450–466. doi: 10.1007/978-3-540-74735-2_31.

[2] WU Wenling and ZHANG Lei. LBlock: A lightweight block cipher[C]. Proceedings of the 9th International Conference on Applied Cryptography and Network Security, Nerja, Spain, 2011: 327–344. doi: 10.1007/978-3-642-21554-4_19.

[3] BANIK S, BAO Zhenzhen, ISOBE T, *et al*. WARP: Revisiting GFN for lightweight 128-bit block cipher[C]. Proceedings of the 27th International Conference on Selected Areas in Cryptography, Halifax, Canada, 2021: 535–564. doi: 10.1007/978-3-030-81652-0_21.

[4] 曹梅春, 张文英, 陈彦琴, 等. RAIN: 一种面向软硬件和门限实现的轻量分组密码算法[J]. 计算机研究与发展, 2021, 58(5): 1045–1055. doi: 10.7544/issn1000-1239.2021.20200933.
CAO Meichun, ZHANG Wenying, CHEN Yanqin, *et al*. RAIN: A lightweight block cipher towards software, hardware and threshold implementations[J]. *Journal of Computer Research and Development*, 2021, 58(5): 1045–1055. doi: 10.7544/issn1000-1239.2021.20200933.

[5] DAS A K, KAR N, DEB S, *et al*. bFLEX-γ: A lightweight block cipher utilizing key cross approach via probability density function[J]. *Arabian Journal for Science and Engineering*, 2022, 47(8): 10563–10578. doi: 10.1007/s13369-022-06651-6.

[6] LIU Xuan, ZHANG Wenying, LIU Xiangzhong, *et al*. Eight-sided fortress: A lightweight block cipher[J]. *The Journal of China Universities of Posts and Telecommunications*, 2014, 21(1): 104–108,128. doi: 10.1016/S1005-8885(14)60275-2.

[7] 吴文玲, 张蕾. 不可能差分密码分析研究进展[J]. 系统科学与数学, 2008, 28(8): 971–983. doi: 10.12341/jssms10197.
WU Wenling and ZHANG Lei. The state-of-the-art of research on impossible differential cryptanalysis[J]. *Journal of Systems Science and Mathematical Sciences*, 2008, 28(8): 971–983. doi: 10.12341/jssms10197.

[8] 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. doi: 10.11999/JEIT180729.
WEI Yongzhuang, SHI Jiali, and LI Lingchen. Impossible differential cryptanalysis of LiCi block cipher[J]. *Journal of Electronics & Information Technology*, 2019, 41(7): 1610–1617. doi: 10.11999/JEIT180729.

[9] 任炯炯, 侯泽洲, 李曼曼, 等. 改进的减轮MIBS-80密码的中间相遇攻击[J]. 电子与信息学报, 2022, 44(8): 2914–2923. doi: 10.11999/JEIT210441.
REN Jiongjiong, HOU Zezhou, LI Manman, *et al*. Improved meet-in-the-middle attacks on reduced-round MIBS-80 Cipher[J]. *Journal of Electronics & Information Technology*, 2022, 44(8): 2914–2923. doi: 10.11999/JEIT210441.

[10] 刘宣, 刘枫, 孟帅. 轻量级分组密码算法ESF的不可能差分分析[J]. 计算机工程与科学, 2013, 35(9): 89–93. doi: 10.3969/j.issn.1007-130X.2013.09.014.
LIU Xuan, LIU Feng, and MENG Shuai. Impossible differential cryptanalysis of lightweight block cipher ESF[J].

Computer Engineering & Science, 2013, 35(9): 89–93. doi: 10.3969/j.issn.1007-130X.2013.09.014.

[11] 陈玉磊, 卫宏儒. ESF算法的不可能差分密码分析[J]. 计算机科学, 2016, 43(8): 89–91,99. doi: 10.11896/j.issn.1002-137X.2016.08.018.
CHEN Yulei and WEI Hongru. Impossible differential cryptanalysis of ESF[J]. *Computer Science*, 2016, 43(8): 89–91,99. doi: 10.11896/j.issn.1002-137X.2016.08.018.

[12] 高红杰, 卫宏儒. 用不可能差分法分析12轮ESF算法[J]. 计算机科学, 2017, 44(10): 147–149,181. doi: 10.11896/j.issn.1002-137X.2017.10.028.
GAO Hongjie and WEI Hongru. Impossible differential attack on 12-round block cipher ESF[J]. *Computer Science*, 2017, 44(10): 147–149,181. doi: 10.11896/j.issn.1002-137X.2017.10.028.

[13] 谢敏, 杨盼. ESF算法的相关密钥不可能差分分析[J]. 计算机工程与科学, 2018, 40(7): 1199–1205. doi: 10.3969/j.issn.1007-130X.2018.07.008.
XIE Min and YANG Pan. Related-key impossible differential cryptanalysis on ESF[J]. *Computer Engineering & Science*, 2018, 40(7): 1199–1205. doi: 10.3969/j.issn.1007-130X.2018.07.008.

[14] 李明明, 郭建胜, 崔竞一, 等. ESF算法的截断不可能差分分析[J]. 密码学报, 2019, 6(5): 585–593. doi: 10.13868/j.cnki.jcr.000324.
LI Mingming, GUO Jiansheng, CUI Jingyi, *et al*. Truncated impossible difference cryptanalysis of ESF[J]. *Journal of Cryptologic Research*, 2019, 6(5): 585–593. doi: 10.13868/j.cnki.jcr.000324.

[15] LI Jun, WANG Hongyan, QIU Xueying, *et al*. Integral analysis of GRANULE and ESF block ciphers based on MILP[C]. Proceedings of 2021 12th International Conference on Information and Communication Systems (ICICS), Valencia, Spain, 2021: 10–16. doi: 10.1109/ICICS52457.2021.9464620.

[16] WU Xiaonian, YAN Jiaxu, LI Lingchen, *et al*. Impossible differential cryptanalysis on ESF algorithm with simplified MILP model[J]. *KSII Transactions on Internet and Information Systems*, 2021, 15(10): 3815–3833. doi: 10.3837/tiis.2021.10.018.

[17] 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. doi: 10.11959/j.issn.1000-436x.2020025.
WU Xiaonian, LI Yingxin, WEI Yongzhuang, *et al*. Impossible differential distinguisher analysis of GRANULE and MANTRA algorithm[J]. *Journal on Communications*, 2020, 41(1): 94–101. doi: 10.11959/j.issn.1000-436x.2020025.

[18] TEZCAN C. Improbable differential attacks on PRESENT using undisturbed bits[J]. *Journal of Computational and Applied Mathematics*, 2014, 259: 503–511. doi: 10.1016/j.cam.2013.06.023.

杜小妮：女，博士，教授，研究方向为应用密码学.
梁丽芳：女，硕士生，研究方向为应用密码学.
贾美纯：女，硕士生，研究方向为应用密码学.
李锴彬：男，硕士生，研究方向为分组密码.

责任编辑：陈 倩