对八阵图算法的不可能差分密码分析和线性密码分析

卫宏儒 朱一凡*

(北京科技大学数理学院 北京 100083)

摘 要：该文对八阵图(ESF)算法抵抗不可能差分密码分析和线性密码分析的能力进行了研究。ESF算法是一种具有Feistel结构的轻量级分组密码算法，它的轮函数为代换置换(SP)结构。该文首先用新的不可能差分区分器分析了12轮ESF算法，随后用线性密码分析的方法分析了9轮ESF算法。计算得出12轮不可能差分分析的数据复杂度大约为$O(2^{67})$，时间复杂度约为$O(2^{110.7})$，而9轮线性密码分析的数据复杂度仅为$O(2^{35})$，时间复杂度不大于$O(2^{15.6})$。结果表明ESF算法足够抵抗不可能差分密码分析，而抵抗线性密码分析的能力相对较弱。

关键词：分组密码；轻量级；线性密码分析；不可能差分；八阵图

中图分类号：TN918.4; TP309.7 **文献标识码**：A **文章编号**：1009-5896(2023)03-0793-07

DOI: 10.11999/JEIT221092

Impossible Differential Cryptanalysis and Linear Cryptanalysis for Eight-Sided Fortress Algorithm

WEI Hongru ZHU Yifan

(*School of Mathematics and Physics*, *University of Science and Technology*, *Beijing* 100083, *China*)

Abstract: The ability of Eight-Sided Fortress (ESF) algorithm to resist impossible differential cryptanalysis and linear cryptanalysis is studied in this paper. The ESF algorithm is a lightweight block cipher algorithm with Feistel structure, and its round function is Substitution-Permutation(SP) structure. Firstly, 12 rounds of ESF algorithm is analyzed in this paper by a new impossible differential distinguisher, and then 9 rounds of ESF algorithm is analyzed by linear cryptanalysis. It is calculated that the data complexity of 12 rounds of impossible differential analysis is about $O(2^{67})$, and the time complexity is about $O(2^{110.7})$, while the data complexity of 9 rounds of linear cryptanalysis is only $O(2^{35})$, and the time complexity is no more than $O(2^{15.6})$. The results show that ESF algorithm is able to resist impossible differential cryptanalysis, while its ability to resist linear cryptanalysis is relatively weak.

Key words: Block cipher; Lightweight; Linear cryptanalysis; Impossible differential; Eight-Sided Fortress(ESF)

1 引言

分组密码算法如PUFFIN[1]等广泛应用于各种设备和软件。文献[2]指出，物联网设备性能的限制产生了对轻量级分组密码算法的需求。八阵图(Eight-Sided Fortress, ESF)算法是Liu等人[3]提出的一种轻量级分组加密算法。该算法为Feistel结构，分组长度为64 bit，密钥长度为80 bit，轮函数为代换置换(Substitution-Permutation, SP)结构，共32轮。

文献[4]提到，对于分组密码算法，最常见的两种分析方法是差分密码分析和线性密码分析。文献[5]指出，线性密码分析利用密码算法中明密文和密钥的不平衡线性逼近来恢复某些密钥比特。文献[6]提到，不可能差分密码分析的原理来源于差分密码分析，它利用中间相错的原理推导出概率为零的差分路径，从而排除错误密钥。不可能差分分析对于许多分组密码算法都具有不错的攻击效果，如SIMON[7], Rijndael, SHACAL-2等。与此同时，线性密码分析也在不断的发展，如文献[8]提到的多线性逼近、双线性密码分析等。

关于ESF算法的安全问题，陈玉磊等人[9]改进了刘宣等人[10]提出的8轮不可能差分区分器；高红杰等人[11]在此基础上提出了12轮不可能差分区分器；尹军等人[12]搜索到925条8轮零相关线性逼近，并认为全轮ESF算法能否抵抗线性分析仍然未知。

收稿日期：2022-08-19；改回日期：2022-12-05；网络出版：2022-12-07
*通信作者： 朱一凡 s20200738@xs.ustb.edu.cn
基金项目：国家自然科学基金(61873026)，广东省重点领域研发计划(2020B0909020001)

Foundation Items: The National Natural Science Foundation of China(61873026), The Key-area Research and Development Program of Guangdong Province (2020B0909020001)

本文在新的8轮不可能差分路径基础上前后各增加2轮，先对12轮ESF算法进行了不可能差分分析。然后根据搜索得到的部分9轮ESF线性逼近表达式进行线性密码分析。

本文第2节介绍了ESF算法，第3节对一条8轮不可能差分路径进行推导，并在此基础上对12轮ESF进行了不可能差分分析。第4节首先统计各个模块的线性逼近以及成立的概率，然后进一步构造单轮和多轮的线性逼近，最后利用获得的9轮线性逼近表达式进行线性密码分析。第5节总结全文。

2 ESF算法

2.1 符号说明

M：64 bit明文；C：64 bit密文；L_0：输入的左32 bit；R_0：输入的右32 bit；

K：80 bit主密钥；K_i：32 bit轮密钥；F：轮函数；P：P盒线性置换；

S：S盒替换；KS：先进行轮密钥加变换，再进行S盒替换；s_i：第i个4×4的S盒；

$\oplus$：按位进行异或；$<<<7$：循环左移7 bit；$||$：二进制字符串拼接；$\triangle$：差分；

P_{L}：明文左32 bit；P_{R}：明文右32 bit；C_{L}：密文左32 bit；C_{R}：密文右32 bit；

2.2 ESF算法简介

对于混淆层，ESF算法采用8个并行的S盒，分别记为s_0, s_1, …,s_7。具体S盒分布参考文献[12]。具体变换为：32 bit S盒输入和输出分别为式(1)和式(2)，其中$b_i=s_i(a_i),\ i=1,2,\cdots,7$

$$a=a_0||a_1||a_2||a_3||a_4||a_5||a_6||a_7 \tag{1}$$

$$b=b_0||b_1||b_2||b_3||b_4||b_5||b_6||b_7 \tag{2}$$

对于扩散层，ESF算法采用了P置换函数，将32 bit S盒输出作为输入。记输入为$b=b_{31}||b_{30}||\cdots||b_2||b_1||b_0$，$P$置换结果为$c=c_{31}||c_{30}||\cdots||c_2||c_1||c_0$。对$i=1,2,\cdots,7$，具体过程为

$$b_{4i}||b_{4i+1}||b_{4i+2}||b_{4i+3}\to c_i||c_{i+8}||c_{i+16}||c_{i+24} \tag{3}$$

对于第1轮加密算法，将64 bit明文输入分成L_0和R_0左右两部分，L_0先循环左移7 bit，然后与$F(R_0,K_1)$按位异或，得到R_1；R_0直接赋值给L_1。对于$i=1,2,\cdots,32$，每一轮加密过程可以表示为

$$R_i=(L_{i-1}<<<7)\oplus F(R_{i-1},K_i),L_i=R_{i-1} \tag{4}$$

经过32轮变换后得到64 bit密文$C=L_{32}||R_{32}$。第i轮加密流程如图1所示。

而对$i=32,31,\cdots,0$，依次计算$R_{i-1}=L_i$, $L_{i-1}=(R_i\oplus F(R_{i-1},K_i))>>>7$，可得明文$M=L_0||R_0$。

2.3 ESF算法的密钥编排

记80 bit主密钥为$K=K_{79}||K_{78}||\cdots||K_1||K_0$。对$i=1,2,\cdots,32$，循环如下操作，可得32个轮密钥：

(1)取K最左端32 bit作为K_i；

(2) $K<<<13$；

(3) $[K_{79}K_{78}K_{77}K_{76}]=s_0([K_{79}K_{78}K_{77}K_{76}])$；

(4) $[K_{75}K_{74}K_{73}K_{72}]=s_0([K_{75}K_{74}K_{73}K_{72}])$；

(5) $[K_{47}K_{46}K_{45}K_{44}K_{43}]=[K_{47}K_{46}K_{45}K_{44}K_{43}]\oplus i$。

3 ESF算法的不可能差分密码分析

3.1 ESF算法的8轮不可能差分路径

文献[13]指出，如何寻找目标加密算法的一条最优不可能差分路径是一个关键问题。本文找到如下8轮不可能差分路径，其中$b=1$, a,c,d,e,f,g,h都不为0

$$(000a|bcd0|0000|\cdots|0000)\nrightarrow(0000|\cdots|0000|0efg|h000) \tag{5}$$

轮密钥加和S盒替换两部分代表的映射记为KS。如图2所示，该路径在第4轮处发生矛盾。

根据P盒为置换的性质以及S盒为双射的性质可进行推导。从第1轮开始推导可得

$$\begin{aligned}\Delta L_4=&\Delta R_3=(\Delta L_2<<<7)\oplus P(\mathrm{KS}(\Delta R_2))\\=&(0a_{11}0b_{11}|0c_{11}0d_{11}|0a_{12}0b_{12}|0c_{12}0d_{12}|\\&\cdot 0a_{13}0b_{13}|0c_{13}\oplus abc\oplus d_{13}|da_{14}0b_{14}|0c_{14}0d_{14})\end{aligned} \tag{6}$$

$$\begin{aligned}\Delta L_3=&\Delta R_2=(\Delta L_1<<<7)\oplus P(\mathrm{KS}(\Delta R_1))\\=&(0000|000a_1|0000|000b_1|0000|000c_1|0000|000d_1)\end{aligned} \tag{7}$$

从最后一轮逆向推导可得

$$\begin{aligned}\Delta R_5=&\Delta L_6=(\Delta R_7\oplus P(\mathrm{KS}(\Delta L_7)))>>>7\\=&(0000|000e_1|0000|000f_1|0000|000g_1|0000|000h_1)\end{aligned} \tag{8}$$

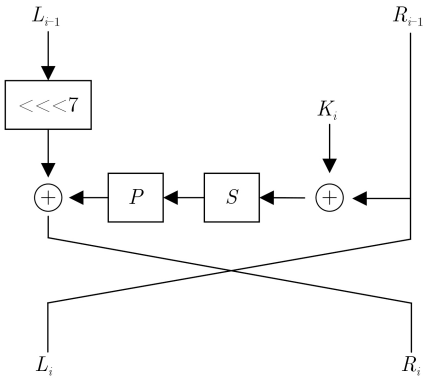

图 1 ESF加密轮函数

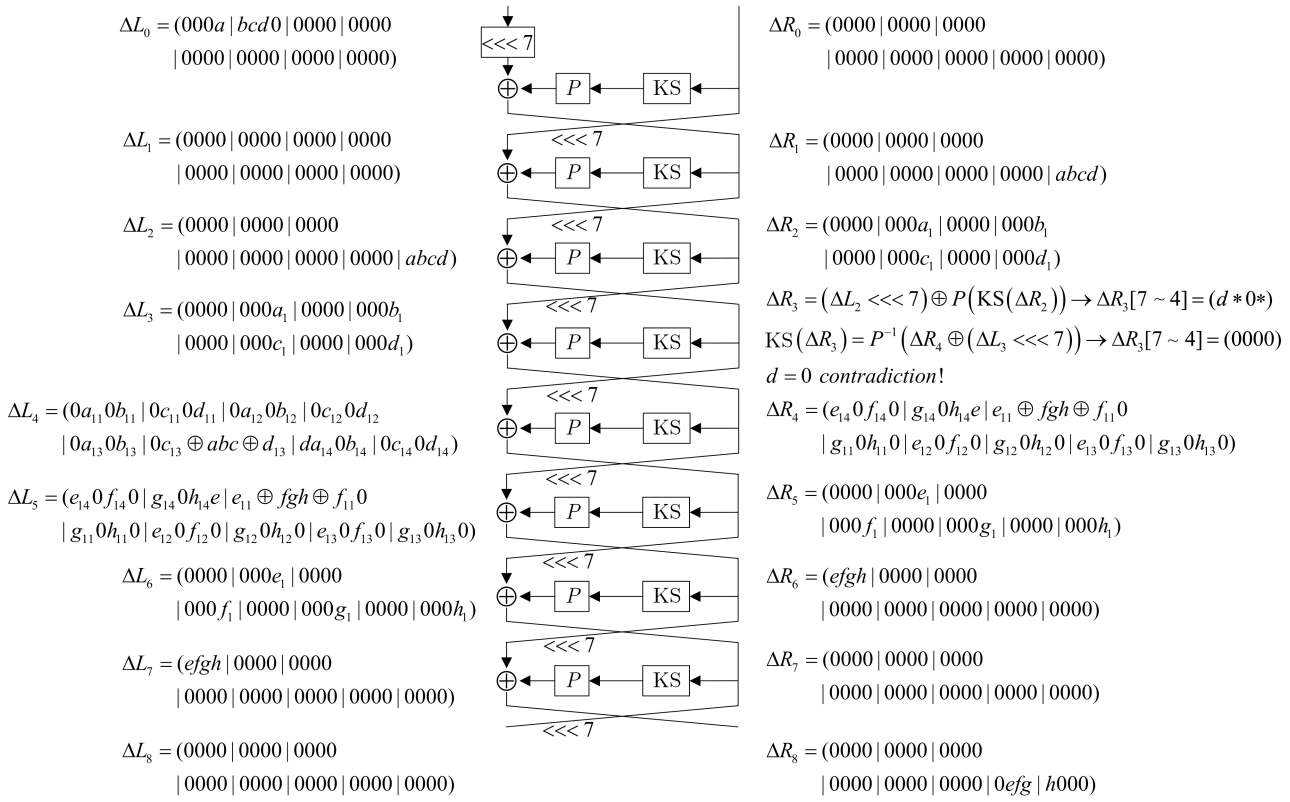

图 2 ESF的8轮不可能差分路径

$$\Delta R_4 = \Delta L_5 = (e_{14}0f_{14}0|g_{14}0h_{14}e|e_{11}\oplus fgh\oplus f_{11}0 |g_{11}0h_{11}0|e_{12}0f_{12}0|g_{12}0h_{12}0|e_{13}0f_{13}0|g_{13}0h_{13}0) \tag{9}$$

因为

$$\begin{aligned}\mathrm{KS}(\Delta R_4) =& P^{-1}(\Delta R_5 \oplus (\Delta L_4 <<< 7))\\ =&(d_{11}d_{12}c\oplus d_{13}d_{14}|00d0|a_{12}a_{13}a_{14}a_{11}\\ &|0000|b_{12}b_{13}b_{14}b_{11}|0000|c_{12}c_{13}\\ &\oplus ac_{14}c_{11}|e_1b\oplus f_1g_1h_1)\end{aligned} \tag{10}$$

观察$\mathrm{KS}(\Delta R_4)$可知第5轮中8个S盒中的s_3, s_5输出异或全为0，因此输入异或ΔR_4的相应位置也全为0。于是$\Delta R_4 = (e_{14}0f_{14}0|g_{14}0h_{14}e|e_{11}\oplus fgh\oplus f_{11}0|0000|e_{12}0f_{12}0|0000|e_{13}0f_{13}0|g_{13}0h_{13}0)$。

又因为

$$\begin{aligned}\mathrm{KS}(\Delta R_3) =& P^{-1}(\Delta R_4 \oplus (\Delta L_3 <<< 7))\\ =&(a_1\oplus e_{14}b_1\oplus e_{11}\oplus fc_1\oplus e_{12}d_1\oplus e_{13}\\ &|0g00|f_{14}h\oplus f_{11}f_{12}f_{13}|0000|g_{14}00g_{13}\\ &|0000|h_{14}00h_{13}|e000)\end{aligned} \tag{11}$$

观察$\mathrm{KS}(\Delta R_3)$可知第4轮中8个S盒中的s_4, s_6输出异或全为0，因此输入异或ΔR_3的相应位置也全为0。由此可得出$b=0$，这与$b=1$矛盾。

3.2 ESF算法的12轮不可能差分分析

如图3所示，向前后各自增加两轮路径可得到ESF算法的12轮不可能差分路径

$$\begin{aligned}&(t_{32}\cdots t_2t_1, x_8000|000x_1|x_5000|000x_2|x_6000|000x_3|x_7000|000x_4) \to\\ &(000a|bcd0|0000|\cdots|0000) \nrightarrow (0000|\cdots|0000|0efg|h000) \to\\ &(0000|00y_1y_5|0000|00y_2y_6|0000|00y_3y_7|0000|00y_4y_8,\\ &0u_10v_1|0p_10q_1|0u_20v_2|0p_20q_2|0u_3ev_3\oplus f|gp_3\oplus h0q_3|0u_40v_4|0p_40q_4)\end{aligned} \tag{12}$$

第1步，选择符合式(13)和式(14)条件的明文结构

$$L_0 = (t_{32}\cdots t_2t_1) \tag{13}$$

$$\begin{aligned}R_0 =&(x_8a_1a_2a_3|a_4a_5a_6x_1|x_5a_7a_8a_9|a_{10}a_{11}a_{12}x_2\\ &|x_6a_{13}a_{14}a_{15}|a_{16}a_{17}a_{18}x_3|x_7a_{19}a_{20}a_{21}\\ &|a_{22}a_{23}a_{24}x_4)\end{aligned} \tag{14}$$

其中，$a_i\,(1\le i\le 24)$为常值，$t_j\,(1\le j\le 32)$和$x_k\,(1\le k\le 8)$遍历所有可能的值。从而一个结构为明文集合，包含2^{40}个明文，大约可以得到$\binom{2^{40}}{2}\approx 2^{79}$个明文对。

第2步，选择2^N个结构，共有2^{N+40}个明文，共可以得到2^{N+79}个明文对。筛选所有数据对中密文差分满足$(\Delta L_{12}, \Delta R_{12})$形式的数据对。满足如下形式的情况共有$2^{24}$种，因此概率为$2^{-40}$ $(=2^{24}\times 2^{-64})$

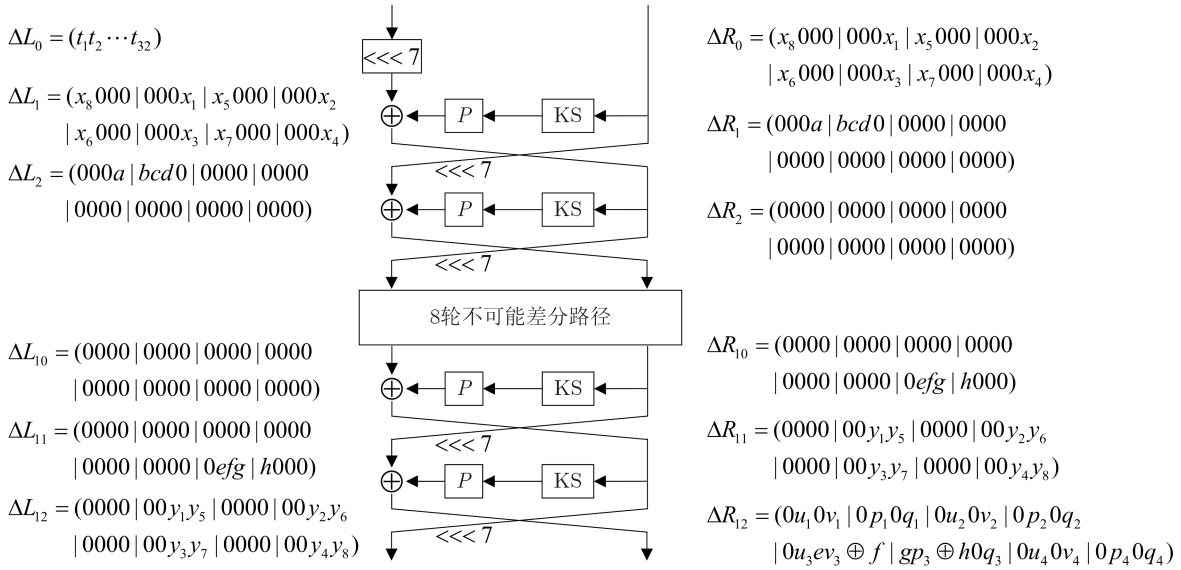

图 3 ESF的12轮不可能差分路径

$$\Delta L_{12} = (0000|00**|0000|00**|0000|00** \\ |0000|00**) \tag{15}$$

$$\Delta R_{12} = (0*0*|0*0*|0*0*|0*0*|0*0* \\ |0*0*|0*0*|0*0*) \tag{16}$$

从而经过这一步过滤，大约剩余2^{N+39}(等于$2^{N+79} \times 2^{-40}$)个数据对。

第3步：(1)猜测最后一轮子密钥K_{12}的16位$K_{12}[3 \sim 0]$, $K_{12}[11 \sim 8]$, $K_{12}[19 \sim 16]$, $K_{12}[27 \sim 24]$，对剩余所有的数据对，记对应的密文分别为(L_{12}, R_{12})和(L_{12}^*, R_{12}^*)，设

$$R_{12} \oplus R_{12}^* = (0u_1 0v_1|0p_1 0q_1|0u_2 0v_2|0p_2 0q_2|0u_3 ev_3 \\ \oplus f|gp_3 \oplus h0q_3|0u_4 0v_4|0p_4 0q_4) \tag{17}$$

分别计算并检验式(18)—式(21)是否都成立

$$S_0(L_{12}[3 \sim 0] \oplus K_{12}[3 \sim 0]) \oplus S_0(L_{12}^*[3 \sim 0] \\ \oplus K_{12}[3 \sim 0]) = (q_1 q_2 q_3 q_4) \tag{18}$$

$$S_2(L_{12}[11 \sim 8] \oplus K_{12}[11 \sim 8]) \oplus S_2(L_{12}^*[11 \sim 8] \\ \oplus K_{12}[11 \sim 8]) = (p_1 p_2 p_3 p_4) \tag{19}$$

$$S_4(L_{12}[19 \sim 16] \oplus K_{12}[19 \sim 16]) \oplus S_4(L_{12}^*[19 \sim 16] \\ \oplus K_{12}[19 \sim 16]) = (v_1 v_2 v_3 v_4) \tag{20}$$

$$S_6(L_{12}[27 \sim 24] \oplus K_{12}[27 \sim 24]) \oplus S_6(L_{12}^*[27 \sim 24] \\ \oplus K_{12}[27 \sim 24]) = (u_1 u_2 u_3 u_4) \tag{21}$$

式(18)—式(21)如果全部成立，则保留相应的数据对，否则丢弃。能通过这一步的概率为2^{-16}，因此大约剩余2^{N+23}($= 2^{N+39} \times 2^{-16}$)个数据对。

(2)猜测剩余每个数据对最后一轮子密钥K_{12}的剩余比特，计算相应密文，获得(L_{11}, R_{11})和(L_{12}^*, R_{12}^*)。

第4步，猜测最后第2轮的子密钥K_{11}的8 bit $K_{11}[3 \sim 0]$, $K_{11}[7 \sim 4]$。对剩余的每个数据对，设$R_{11} \oplus R_{11}^* = (0000|00y_1y_2|0000|00y_3y_4|0000|00y_5y_6|0000|00y_7y_8)$，计算检验式(22)和式(23)是否成立

$$S_0(L_{11}[3 \sim 0] \oplus K_{11}[3 \sim 0]) \oplus S_0(L_{11}^*[3 \sim 0] \\ \oplus K_{11}[3 \sim 0]) = (y_2 y_4 y_6 y_8) \tag{22}$$

$$S_1(L_{11}[7 \sim 4] \oplus K_{11}[7 \sim 4]) \oplus S_1(L_{11}^*[7 \sim 4] \\ \oplus K_{11}[7 \sim 4]) = (y_1 y_3 y_5 y_7) \tag{23}$$

如果全部满足，则保留相应的数据对，否则丢弃。能通过这一步的概率为2^{-8}，因此大约剩余2^{N+15}($= 2^{N+23} \times 2^{-8}$)个数据对。

第5步，猜测第1轮子密钥K_1的全部比特，对剩余的每一个数据对，计算R_1和R_1^*，筛选出满足条件$R_1 \oplus R_1^* = (000a|bcd0|0000|0000|0000|0000|0000|0000)$的数据对，通过这一步过滤的概率约为$2^{-32}$，因此大约剩余$2^{N-17}$($= 2^{N+15} \times 2^{-32}$)个数据对。

第6步，猜测第2轮子密钥K_2的8 bit值$K_2[27 \sim 24]$, $K_2[31 \sim 28]$。对每一个剩余的数据对，设$R_0 \oplus R_0^* = (x_1 000|000x_2|x_3 000|000x_4|x_5 000|000x_6|x_7 000|000x_8)$，计算并检验式(24)和式(25)是否成立

$$S_6(R_1[27 \sim 24] \oplus K_2[27 \sim 24]) \oplus S_6(R_1^*[27 \sim 24] \\ \oplus K_2[27 \sim 24]) = (x_3 x_5 x_7 x_1) \tag{24}$$

$$S_7(R_1[31 \sim 28] \oplus K_2[31 \sim 28]) \oplus S_7(R_1^*[31 \sim 28] \\ \oplus K_2[31 \sim 28]) = (x_2 x_4 x_6 x_8) \tag{25}$$

同时满足两个等式的概率约为2^{-8}，因此大约剩余2^{N-25}($= 2^{N-17} \times 2^{-8}$)个数据对。如果等式全部成立，则说明相应的数据对满足8轮不可能差分，所建议的密钥猜测值错误，这时删除相应的密钥猜测值$(K_1, K_2[31 \sim 24], K_{11}[7 \sim 0], K_{12})$，共80 bit。完成第6步筛选后，大约剩余$2^{80} \times \left(1 - 2^{-4}\right)^{2^{N-17}} \le 1$个密钥猜测值，计算得$N = 27$。

3.3 复杂度分析

综上所述，基于12轮ESF不可能差分路径的攻击的数据复杂度大约为$O(2^{67})(2^{27+40})$。将第2步—第6步的时间复杂度依次相加

$$\begin{aligned}&(12\times 2^{N+79}\times 2)+(2^{-1}\times 2^{16}\times 2^{N+39}\times 2+2^{-1}\\&\quad\times 2^{16}\times 2^{N+23}\times 2)+(2^{-2}\times 2^{8}\times 2^{N+23}\times 2)\\&\quad+(2^{64}\times 2^{N+15}\times 2)+(2^{-2}\times 2^{8}\times 2^{N-17}\times 2)\\&\approx 2^{110.7}\end{aligned}\tag{26}$$

可知时间复杂度约为$O(2^{110.7})$。分析结果表明，12轮的ESF算法足以抵抗不可能差分攻击。

4 ESF算法的线性密码分析

4.1 S盒的线性逼近

ESF算法采用了8个不同的S盒，每个S盒的具体分布已经由文献[12]给出。观察可知每个S盒的输入输出都是4 bit，并且每个S盒都为双射。记S盒的输入为x，输出为y，于是有$x,y\in\{0,1\}^4$。

对一个给定的S盒，考虑有如式(27)形式的线性表达式

$$\sum_{m=0}^{3}x_{[m]}\alpha_{[m]}=\sum_{n=0}^{3}y_{[n]}\beta_{[n]}\tag{27}$$

其中，$1\le\alpha,\beta\le 15$，$x_{[m]}$表示x的二进制从右往左第m个比特，$\sum$表示逐比特异或的结果。对于每个可能的(α,β)和每个S盒，计算其对应的线性逼近式成立的概率p，以及逼近优势$|p-0.5|$。经过遍历计算，可以得到一个逼近优势表，共有约$2^{11}(=8\times 2^8)$种情况。对任意一个概率$p<0.5$的线性逼近，在等式一侧额外异或1，则可以得到一个新的线性逼近，其概率为$1-p>0.5$，逼近优势不变。对每个概率$p<0.5$的线性逼近进行上述操作。删去逼近优势为0或α, β都为0的数据，得到新的逼近优势表。观察可知，在新的逼近优势表中α,β都不为0，共剩余1104个线性逼近。表1统计了每个S盒剩余的逼近优势。

4.2 轮函数的线性逼近

ESF中其他模块都是线性的。因此将4.1节中式(27)改写为$\sum\beta\otimes y=\sum\alpha\otimes x$，其中$\alpha$, β, x, y长度都为32 bit，x, y为S盒模块输入输出，α, β在相应位置用0扩充至32 bit。考虑等式右边，由于$x=K_i\oplus R_{i-1}$，因此右边$\sum\alpha\otimes x=\sum(\alpha\otimes K_i)\oplus(\alpha\otimes R_{i-1})$。再考虑等式左边，由于$y=S(x)=P^{-1}(R_i\oplus(L_{i-1}<<<7))$，因此左边可以写成

$$\sum\beta\otimes y=\sum P(\beta)\otimes R_i\oplus\sum(P(\beta)>>>7\oplus L_{i-1})\tag{28}$$

于是每一个S盒线性逼近式能写成

$$\begin{aligned}&\sum(\alpha\otimes K_i)\oplus(\alpha\otimes R_{i-1})\\&\quad=\sum P(\beta)\otimes R_i\oplus\sum(P(\beta)>>>7\oplus L_{i-1})\end{aligned}\tag{29}$$

式(29)即为单轮ESF的线性逼近表达式。由于α, β都不为0，因此上述式子中的系数也都不为0。将所有S盒线性逼近式扩展为单轮线性逼近式。将各轮的线性逼近按顺序连接起来，筛选出仅涉及明密文和子密钥的表达式。通过这种方法，本文共获得9轮线性逼近表达式752个。其中约用到50个单轮线性逼近。

4.3 ESF算法的9轮线性密码分析

选择如式(30)的9轮线性逼近

$$\begin{aligned}&P_{\mathrm{L}}[10]\oplus P_{\mathrm{R}}[29,7,6,5,4]\oplus C_{\mathrm{L}}[19,18,15]\oplus C_{\mathrm{R}}[4]\\&\quad=K_1[7,6,5,4]\oplus K_2[18,17]\oplus K_3[4]\oplus K_5[1]\\&\qquad\oplus K_6[0]\oplus K_8[29]\oplus K_9[19,18]\end{aligned}\tag{30}$$

其逼近优势大于2^{-13}。基于上述9轮线性逼近表达式和吴文玲[14]给出的攻击算法，给出如下攻击方法：

对式(1)中涉及的12 bit密钥的每一个候选值：$K_i(i=1,2,\cdots,2^{12})$，令N_t表示使得式(30)成立的明密文对数。如果N_t是所有$N_i(i=1,2,\cdots,2^{12})$中最大的，则采用K_t。

此攻击所需要的数据复杂度不大于2^{29}(相应的成功率为0.967)，计算复杂度不大于2^{12}。类似上面，本文还可以构造如式(31)—式(48)18个9轮线性逼近

$$\begin{aligned}&P_{\mathrm{L}}[19,11]\oplus P_{\mathrm{R}}[31,11,10,9]\oplus C_{\mathrm{L}}[23,22,15]\oplus C_{\mathrm{R}}[5]\\&\quad=K_1[11,10,9]\oplus K_2[26]\oplus K_3[6]\oplus K_5[1]\\&\qquad\oplus K_6[0]\oplus K_8[30]\oplus K_9[23,22]\end{aligned}\tag{31}$$

$$\begin{aligned}&P_{\mathrm{L}}[9]\oplus P_{\mathrm{R}}[29,0]\oplus C_{\mathrm{L}}[23,22,21,20,15]\oplus C_{\mathrm{R}}[5]\\&\quad=K_1[0]\oplus K_2[18,16]\oplus K_3[4]\oplus K_5[1]\\&\qquad\oplus K_6[0]\oplus K_8[30]\oplus K_9[23,22,21,20]\end{aligned}\tag{32}$$

$$\begin{aligned}&P_{\mathrm{L}}[12]\oplus P_{\mathrm{R}}[29,15,14,12]\oplus C_{\mathrm{L}}[18,16,15]\oplus C_{\mathrm{R}}[4]\\&\quad=K_1[15,14,12]\oplus K_2[19,18]\oplus K_3[4]\oplus K_5[1]\\&\qquad\oplus K_6[0]\oplus K_8[29]\oplus K_9[18,16]\end{aligned}\tag{33}$$

表 1　ESF算法S盒剩余逼近优势分布统计

逼近优势	s_0	s_1	s_2	s_3	s_4	s_5	s_6	s_7
0.250	36	36	36	32	32	32	36	32
0.125	96	96	96	112	112	112	96	112

$$P_{\rm L}[19,11]\oplus P_{\rm R}[31,11,10,9,8]\oplus C_{\rm L}[18,16,15]\oplus C_{\rm R}[4]=K_1[11,10,9,8]\oplus K_2[26]\oplus K_3[6]\oplus K_5[1]\oplus K_6[27]\oplus K_8[29]\oplus K_9[18,16] \tag{34}$$

$$P_{\rm L}[8]\oplus P_{\rm R}[31,28,12]\oplus C_{\rm L}[29,19,17,16]\oplus C_{\rm R}[28]=K_1[31,28]\oplus K_2[15,13]\oplus K_3[19]\oplus K_5[15]\oplus K_6[27]\oplus K_8[21]\oplus K_9[19,17,16] \tag{35}$$

$$P_{\rm L}[9]\oplus P_{\rm R}[29,1,0]\oplus C_{\rm L}[18,16,15]\oplus C_{\rm R}[4]=K_1[1,0]\oplus K_2[18,16]\oplus K_3[4]\oplus K_5[1]\oplus K_6[0]\oplus K_8[29]\oplus K_9[18,16] \tag{36}$$

$$P_{\rm L}[8]\oplus P_{\rm R}[31,29,12]\oplus C_{\rm L}[29,27]\oplus C_{\rm R}[30]=K_1[31,29]\oplus K_2[15,13]\oplus K_3[19]\oplus K_5[15]\oplus K_6[27]\oplus K_8[23]\oplus K_9[27] \tag{37}$$

$$P_{\rm L}[12]\oplus P_{\rm R}[29,15,14,13,12]\oplus C_{\rm L}[18,16,15]\oplus C_{\rm R}[4]=K_1[15,14,13,12]\oplus K_2[19,18]\oplus K_3[4]\oplus K_5[1]\oplus K_6[0]\oplus K_8[29]\oplus K_9[18,16] \tag{38}$$

$$P_{\rm L}[9]\oplus P_{\rm R}[29,2,0]\oplus C_{\rm L}[18,16,15]\oplus C_{\rm R}[4]=K_1[2,0]\oplus K_2[18,16]\oplus K_3[4]\oplus K_5[1]\oplus K_6[0]\oplus K_8[29]\oplus K_9[18,16] \tag{39}$$

$$P_{\rm L}[8]\oplus P_{\rm R}[31,30,12]\oplus C_{\rm L}[29,27,25]\oplus C_{\rm R}[30]=K_1[31,30]\oplus K_2[15,13]\oplus K_3[19]\oplus K_5[15]\oplus K_6[27]\oplus K_8[23]\oplus K_9[27,25] \tag{40}$$

$$P_{\rm L}[7]\oplus P_{\rm R}[27,26,25,12]\oplus C_{\rm L}[29,27,26]\oplus C_{\rm R}[30]=K_1[27,26,25]\oplus K_2[14,13]\oplus K_3[19]\oplus K_5[15]\oplus K_6[27]\oplus K_8[23]\oplus K_9[27,26] \tag{41}$$

$$P_{\rm L}[7]\oplus P_{\rm R}[27,26,25,24,12]\oplus C_{\rm L}[29,27,26,24]\oplus C_{\rm R}[30]=K_1[27,26,25,24]\oplus K_2[14,13]\oplus K_3[19]\oplus K_5[15]\oplus K_6[27]\oplus K_8[23]\oplus K_9[27,26,24] \tag{42}$$

$$P_{\rm L}[9]\oplus P_{\rm R}[29,3]\oplus C_{\rm L}[18,16,15]\oplus C_{\rm R}[4]=K_1[3]\oplus K_2[18,16]\oplus K_3[4]\oplus K_5[1]\oplus K_6[0]\oplus K_8[29]\oplus K_9[18,16] \tag{43}$$

$$P_{\rm L}[5]\oplus P_{\rm R}[28,19,18,16]\oplus C_{\rm L}[12,3,2,1,0]\oplus C_{\rm R}[24,0]=K_1[19,18,16]\oplus K_2[12]\oplus K_4[11]\oplus K_5[10]\oplus K_7[5]\oplus K_8[17]\oplus K_9[3,2,1,0] \tag{44}$$

$$P_{\rm L}[6]\oplus P_{\rm R}[28,23,21,20]\oplus C_{\rm L}[12,3,2,1,0]\oplus C_{\rm R}[24,0]=K_1[23,21,20]\oplus K_2[13]\oplus K_4[11]\oplus K_5[10]\oplus K_7[5]\oplus K_8[17]\oplus K_9[3,2,1,0] \tag{45}$$

$$P_{\rm L}[6]\oplus P_{\rm R}[28,23,22]\oplus C_{\rm L}[12,3,2,1,0]\oplus C_{\rm R}[24,0]=K_1[23,22]\oplus K_2[13]\oplus K_4[11]\oplus K_5[10]\oplus K_7[5]\oplus K_8[17]\oplus K_9[3,2,1,0] \tag{46}$$

$$P_{\rm L}[5]\oplus P_{\rm R}[28,19,18,17]\oplus C_{\rm L}[12,3,2,1,0]\oplus C_{\rm R}[24,0]=K_1[19,18,17]\oplus K_2[12]\oplus K_4[11]\oplus K_5[10]\oplus K_7[5]\oplus K_8[17]\oplus K_9[3,2,1,0] \tag{47}$$

$$P_{\rm L}[5]\oplus P_{\rm R}[28,19,16]\oplus C_{\rm L}[12,3,2,1,0]\oplus C_{\rm R}[24,0]=K_1[19,16]\oplus K_2[12]\oplus K_4[11]\oplus K_5[10]\oplus K_7[5]\oplus K_8[17]\oplus K_9[3,2,1,0] \tag{48}$$

式(30)—式(48)的逼近优势全都大于2^{-16}，每次攻击的数据复杂度不大于2^{35}，计算复杂度不大于2^{13}。上述攻击最多可以解读48 bit的主密钥，整个攻击所需的数据复杂度不大于$O(2^{35})$(相应的成功率为0.967)，计算复杂度不大于$O(2^{15.6})(2\times 2^9+2^2\times 2^{10}+7\times 2^{11}+5\times 2^{12}\times 2^{13})$。

5 结论

本文用两种方法分析了ESF算法。首先在通过推导证明的 ESF算法的一条8轮不可能差分路径的基础上，通过前后各增加两轮的方法，对12轮ESF加密算法进行了不可能差分分析。然后在遍历搜索获得的752个9轮线性逼近表达式的基础上，对ESF算法进行了线性密码分析。计算结果表明，ESF算法抵抗不可能差分分析的能力较好，而抵抗线性密码分析的能力较弱。

参 考 文 献

[1] 袁庆军, 张勋成, 高杨, 等. 轻量级分组密码PUFFIN的差分故障攻击[J]. 电子与信息学报, 2020, 42(6): 1519–1525. doi: 10.11999/JEIT190506.
YUAN Qingjun, ZHANG Xuncheng, GAO Yang, *et al*. Differential fault attack on the lightweight block cipher PUFFIN[J]. *Journal of Electronics & Information Technology*, 2020, 42(6): 1519–1525. doi: 10.11999/JEIT190506.

[2] SEHRAWAT D and GILL N S. Lightweight block ciphers for iot based applications: A review[J]. *International Journal of Applied Engineering Research*, 2018, 13(5): 2258–2270.

[3] 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.

[4] 杜小妮, 段娥娥, 王天心. 基于混沌的双模块Feistel结构高安全性高速分组密码算法安全性分析[J]. 电子与信息学报, 2021, 43(5): 1365–1371. doi: 10.11999/JEIT200057.
DU Xiaoni, DUAN E E, and WANG Tianxin. Security analysis of block cipher CFE[J]. *Journal of Electronics & Information Technology*, 2021, 43(5): 1365–1371. doi: 10.11999/JEIT200057.

[5] 王念平. 一类分组密码变换簇抵抗线性密码分析的安全性评估[J]. 电子学报, 2020, 48(1): 137–142. doi: 10.3969/j.issn.0372-2112.2020.01.017.
WANG Nianping. Security evaluation against linear cryptanalysis for a class of block cipher transform cluster[J]. *Acta Electronica Sinica*, 2020, 48(1): 137–142. doi: 10.3969/j.issn.0372-2112.2020.01.017.

[6] 吴文玲, 冯登国, 张文涛. 分组密码的设计与分析[M]. 2版. 北

京: 清华大学出版社, 2009: 120–125.

WU Wenling, FENG Dengguo, ZHANG Wentao. Design and Analysis of Block Cipher[M]. 2nd ed. Beijing: Tsinghua University Press, 2009: 120–125.

[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.

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.

[8] 贾艳艳, 胡予濮, 杨文峰, 等. 2轮Trivium的多线性密码分析[J]. 电子与信息学报, 2011, 33(1): 223–227. doi: 10.3724/SP.J.1146.2010.00334.

JIA Yanyan, HU Yupu, YANG Wenfeng, *et al*. Linear cryptanalysis of 2-round trivium with multiple approximations[J]. *Journal of Electronics & Information Technology*, 2011, 33(1): 223–227. doi: 10.3724/SP.J.1146.2010.00334.

[9] 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.2016.8.018.

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.2016.8.018.

[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): 89–95. 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): 89–95. doi: 10.3969/j.issn.1007-130X.2013.09.014.

[11] 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.2017.010.028.

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.2017.010.028.

[12] 尹军, 马楚焱, 宋健, 等. 轻量级分组密码算法ESF的安全性分析[J]. 计算机研究与发展, 2017, 54(10): 2224–2231. doi: 10.7544/issn1000-1239.2017.20170455.

YIN Jun, MA Chuyan, SONG Jian, *et al*. Security analysis of lightweight block cipher ESF[J]. *Journal of Computer Research and Development*, 2017, 54(10): 2224–2231. doi: 10.7544/issn1000-1239.2017.20170455.

[13] CUI Tingting, CHEN Shiyao, FU Kai, *et al*. New automatic tool for finding impossible differentials and zero-correlation linear approximations[J]. *Science China Information Sciences*, 2021, 64(2): 129103. doi: 10.1007/s11432-018-1506-4.

[14] 吴文玲. Q的线性密码分析[J]. 计算机学报, 2003, 26(1): 55–59. doi: 10.3321/j.issn:0254-4164.2003.01.009.

WU Wenling. Linear cryptanalysis of Q block cipher[J]. *Chinese Journal of Computers*, 2003, 26(1): 55–59. doi: 10.3321/j.issn:0254-4164.2003.01.009.

卫宏儒：男，教授，硕士生导师，研究方向为数学、信息安全与密码学和物联网技术.

朱一凡：男，硕士生，研究方向为密码算法的安全性分析.

责任编辑：余　蓉