CN 43-1258/TP
ISSN 1007-130X

计算机工程与科学
Computer Engineering & Science

第 40 卷第 7 期 2018 年 7 月
Vol. 40, No. 7, Jul. 2018

文章编号:1007-130X(2018)07-1199-07

ESF 算法的相关密钥不可能差分分析*

谢　敏,杨　盼

(西安电子科技大学综合业务网理论及关键技术国家重点实验室,陕西 西安 710071)

摘　要:ESF 算法是一种具有广义 Feistel 结构的 32 轮迭代型轻量级分组密码。为研究 ESF 算法抵抗不可能差分攻击的能力,首次对 ESF 算法进行相关密钥不可能差分分析,结合密钥扩展算法的特点和轮函数本身的结构,构造了两条 10 轮相关密钥不可能差分路径。将一条 10 轮的相关密钥不可能差分路径向前向后分别扩展 1 轮和 2 轮,分析了 13 轮 ESF 算法,数据复杂度是 2^{60} 次选择明文对,计算量是 2^{23} 次 13 轮加密,可恢复 18 bit 密钥。将另一条 10 轮的相关密钥不可能差分路径向前向后都扩展 2 轮,分析了 14 轮 ESF 算法,数据复杂度是 2^{62} 选择明文对,计算复杂度是 $2^{43.95}$ 次 14 轮加密,可恢复 37 bit 密钥。

关键词:ESF 算法;轻量级密码算法;相关密钥不可能差分分析攻击

中图分类号:TP309.7　　**文献标志码**:A

doi:10.3969/j.issn.1007-130X.2018.07.008

Related-key impossible differential cryptanalysis on ESF

XIE Min, YANG Pan

(State Key Laboratory of Integrated Service Networks, Xidian University, Xi'an 710071, China)

Abstract: ESF is a lightweight block cipher based on a modified 32-round Feistel structure. In order to study the ESF algorithm's ability to resist the impossible differential attack, we use related-key impossible differential cryptanalysis to analyze the security of ESF for the first time. And two 10-round related-key impossible differential paths are constructed based on the characteristics of the key extended algorithm and the structure of round functions. Then a related-key impossible differential attack on 13-round ESF is proposed by adding 1 round at the top and 2 rounds at the bottom to a 10-round related-key impossible differential path. The attack has a complexity of 2^{23} 13-round encryptions and about 260 chosen plaintexts with 18 recovered key-bits. A related-key impossible differential attack on a 14-round ESF is also proposed by adding 2 rounds both at the top and the bottom to another 10-round related-key impossible differential path, which has a complexity of $2^{43.95}$ 14-round encryptions and about 2^{62} chosen plaintexts with 37 recovered key-bits.

Key words: ESF algorithm; light weight cipher algorithm; related-key impossible differential attack

1　引言

随着电子信息技术的发展,低功耗设备如无线传感器网络、射频识别技术 RFID(Radio Frequency IDentification)等应用越来越广泛。由于实际的需求,应用于这些特殊环境的加密算法需要满足一些特性,例如更高的计算速度、更低的功耗等。在这种情况下,传统的分组密码如 AES(Advanced Encryption Standard)[1]、DES(Data Encryption Standard)[2]由于速度、功耗等原因无法满足需求,因此应用于这些设备上的轻量级分组密码算法自然也逐渐成为人们关注的焦点。学者们设计了越来越多的轻量级分组密码,如 PRESENT[3]、

* 收稿日期:2017-05-05;修回日期:2017-06-28
基金项目:国家自然科学基金(61373170,U0835004,U1536202);国家 111 创新引智基地资助项目(B08038)
通信地址:710071 陕西省西安市太白南路 2 号西安电子科技大学 106 信箱
Address: Post Box 106, Xidian University, 2 Taibai South Rd, Xi'an 710071, Shaanxi, P. R. China

HIGHT[4]、MIBS[5]、LBlock、TWIS[6]等。

ESF(Eight-Sided Fortress)算法[7]是刘宣等人在研究了吴文玲学者设计的LBlock算法[8]后设计的。他们发现置换层按位进行能获得更好的扩散性,而且按位置换的数据在较少的轮数中能够快速扩散,从而增加了密码抵抗攻击的能力。因此,他们借鉴PRESENT算法中P层置换的形式对LBlock算法进行了改进,最终提出了"八阵图算法"ESF。ESF算法使用Feistel结构的变体,共有32轮迭代,加解密结构相同,加解密速度快,实现方便,适合多种软硬件平台。

相关密钥攻击是由Knudsen[9]和Biham[10]各自独立提出的,其主要思想是利用密钥扩展算法的一些性质,通过分析不同密钥之间的某些关系对加解密结果造成的影响来得到密钥信息,这种攻击方法在分组密码的分析中得到了广泛应用。不可能差分分析是利用概率为0的差分排除那些导致概率为0的差分出现的候选密钥,该分析方法是差分密码分析的一个扩展。

目前对ESF算法进行安全性分析的文献不多,文献[7]利用8轮的不可能差分路径,对11轮的ESF算法进行不可能差分分析,时间复杂度是2^{64}次选择明文对,计算量是$2^{75.5}$次11轮加密,可恢复16 bit密钥。文献[11]利用相同的8轮不可能差分路径,对11轮的ESF算法进行不可能差分分析,需要2^{53}次选择明文对和2^{32}次11轮加密,可恢复16 bit密钥。

2 ESF算法

2.1 符号及术语说明

M:64 bit明文;

C:64 bit密文;

K:80 bit主密钥;

RK_r:32 bit轮密钥;

F:轮函数;

S:4×4 S盒;

$\oplus$:按位异或运算符;

P:置换层;

$\lll$:循环左移运算符;

$\|$:二进制字符联接;

$[i]_2$:常数i的二进制表示。

2.2 ESF算法

轻量级分组密码算法ESF的数据处理流程基于SPN轮函数和Feistel结构,密钥长度80 bit,分组长度是64 bit,迭代轮数为32轮。ESF算法的加密流程和轮函数如图1所示。设$M=L_1\|R_1$表示64 bit明文,对于$1\leqslant r\leqslant 32$,加密流程如下:

$$\begin{cases}R_{r+1}=(L_r\lll 7)\oplus F(R_r,RK_r)\\ L_{r+1}=R_r\end{cases}$$

最后输出密文$C_L\|C_R$,其中$C_L=L_{33}$,$C_R=R_{33}$。

非线性混淆层:ESF算法的非线性混淆层由8个并行的S盒构成,如表1所示。

Table 1 S boxes

表1 S盒

S_0	3,8,F,1,A,6,5,B,E,D,4,2,7,0,9,C	S_4	1,F,8,3,C,0,B,6,2,5,4,A,9,E,7,D
S_1	F,C,2,7,9,0,5,A,1,B,8,6,D,3,4	S_5	F,5,2,B,4,A,9,C,0,3,E,8,D,6,7,1
S_2	8,6,7,9,3,C,A,F,D,1,E,4,0,B,5,2	S_6	7,2,C,5,8,4,6,B,E,9,1,F,D,3,A,0
S_3	0,F,B,8,C,9,6,3,D,1,2,4,A,7,5,E	S_7	1,D,F,0,E,8,2,B,7,4,C,A,9,3,5,6

P置换定义如下:设$b=b_7\|b_6\|b_5\|b_4\|b_3\|b_2\|b_1\|b_0$,$c=P(b)=c_7\|c_6\|c_5\|c_4\|c_3\|c_2\|c_1\|c_0$,则$b_{4i}\|b_{4i+1}\|b_{4i+2}\|b_{4i+3}\rightarrow c_i\|c_{i+8}\|c_{i+16}\|c_{i+24}$,$1\leqslant i<8$。

2.3 ESF的密钥扩展算法

密钥扩展算法是把80 bit的主密钥经过一系列的运算产生32个32 bit的轮密钥。设80 bit主

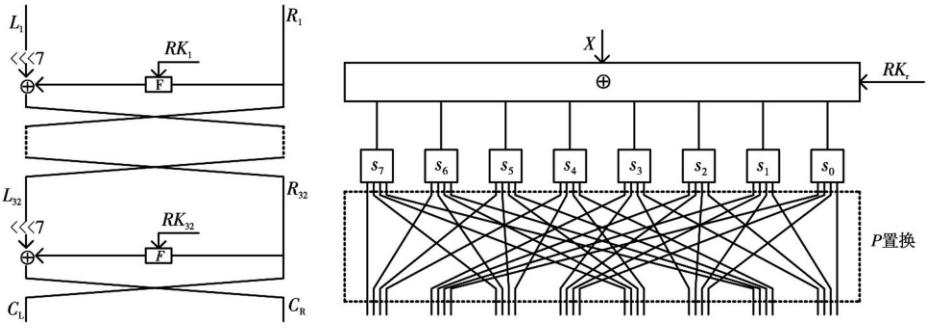

Figure 1 Encryption process and round function of ESF

图1 ESF算法的加密流程及轮函数F

密钥为 $K=k_{79}k_{78}k_{77}k_{76}\cdots k_3k_2k_1k_0$,并存入密钥寄存器,最左端为 k_{79},最右端为 k_0。将最左端 32 bit 取出作为第一轮的子密钥 RK_1,第 2～32 轮的子密钥由下面方法得到:

对 $i=1,2,\cdots,31$:

$K<<<13$;

$[k_{79}k_{78}k_{77}k_{76}]=S_0[k_{79}k_{78}k_{77}k_{76}]$;

$[k_{75}k_{74}k_{73}k_{72}]=S_0[k_{75}k_{74}k_{73}k_{72}]$;

$[k_{47}k_{46}k_{45}k_{44}k_{43}]=[k_{47}k_{46}k_{45}k_{44}k_{43}]\oplus[i]_2$;

把 K 的左边 32 bit 作为第 $i+1$ 轮的子密钥输出。

3　ESF 算法的相关密钥不可能差分分析

ESF 算法的密钥扩展算法中第 1 轮的子密钥是直接从主密钥 K 中截取的,并没有经过 S 盒。设主密钥 $K=k_{79}k_{78}k_{77}k_{76}\cdots k_3k_2k_1k_0$,定义 K^i 为 K 的第 $i\ (i=19,18,\cdots,1,0)$ 个半字节,则第 1 轮子密钥 $RK_1=k_{79}k_{77}k_{76}k_{75}\cdots k_{49}k_{48}$。定义 $RK_i^j(i=1,2,\cdots,32;j=7,6,\cdots,1,0)$ 为第 i 轮子密钥的第 j 个半字节,左侧 RK_i^7 为最高位。我们通过选择特定的密钥差分和明文差分,使这两者的差分异或值为 0,以减少活动 S 盒的个数来得到较长的差分路径。

3.1　针对 13 轮 ESF 算法的相关密钥不可能差分分析

当 $\Delta K^{17}=8$ 即 $\Delta RK_1^5=8$ 时,非零密钥差分在第 20 轮以后才可能经过 S 盒,所以选择 2～11 轮的相关密钥不可能差分路径如下:

$$(00000000,00000000)\xrightarrow{\Delta K^{17}=8}(00000000,00000000)$$

表 2 为 ESF 算法的 10 轮相关密钥不可能差分路径。从表 2 中可以看出,由加密方向和解密方向得到的第 7 轮中间状态矛盾。

根据该不可能差分路径,我们可以对 13 轮算法进行相关密钥不可能差分攻击。其基本思想是在该路径前面添加一轮,在该路径后面添加两轮,通过不可能差分把错误密钥淘汰并筛选出正确密钥。13 轮相关密钥不可能差分攻击的示意图见图 2,具体过程如下:

步骤 1　选择 2^4 个明文生成一个结构,其中 L_1 的第 1、9、17、25 bit 可以随意取值,剩余的 60 bit 的取值必须保证差分为 0,即要保证输入的明文差分满足 $\Delta L_{1,1}^7\|\Delta L_{1,1}^5\|\Delta L_{1,1}^3\|\Delta L_{1,1}^1=a_4\|a_1\|a_2\|a_3$,其中 a_1,a_2,a_3,a_4 取所有可能的值,所以一个结构包含 $2^4\times2^4\times(1/2)=2^7$ 个明文对。选取 2^n 个这样的结构,可以形成 2^{n+7} 个明文对。

步骤 2　对选择的明文对在 $\Delta K=0080\ \ 0000\ \ 0000\ \ 0000\ \ 0000$ 的情况下进行 13 轮加密得到密文对,过滤密文对保留那些使得输出满足如下差分的数据对:$\Delta R_{14,2}^6\|\Delta R_{14,2}^4\|\Delta R_{14,2}^2\|\Delta R_{14,2}^0=b_1\|b_2\|b_3\|b_4$,$\Delta R_{14,3}^7\|\Delta R_{14,3}^5\|\Delta R_{14,3}^3\|\Delta R_{14,3}^1=d_1\|d_2\|d_3\|d_4$,$\Delta R_{14,1}^6\|\Delta R_{14,1}^4\|\Delta R_{14,1}^2\|\Delta R_{14,1}^0=e_1\|e_2\|e_3\|e_4$,$\Delta R_{14,3}^6\|\Delta R_{14,3}^4\|\Delta R_{14,3}^2\|\Delta R_{14,3}^0=f_1\|f_2\|f_3\|f_4$,其中 $b_i,c_i,d_i,e_i,f_i\ (1\leqslant i\leqslant4)$ 取所有可能的值。此时还有 $2^{n+7}\times2^{-44}=2^{n-37}$ 个数据对剩余。

步骤 3　首先猜测密钥 RK_1^5,其在主密钥中的相应位置为 $k_{71\sim68}$。部分加密第 1 轮,保留满足 $S_5(R_1^5\oplus RK_1^5)\oplus S_5(R_1^5\oplus\Delta R_1^5\oplus RK_1^5\oplus\Delta RK_1^5)=\Delta L_{1,1}^5\|\Delta L_{1,1}^3\|\Delta L_{1,1}^1\|\Delta L_{1,1}^7$ 的数据对,此时还有 $2^{n-37}\times2^{-4}=2^{n-41}$ 个数据对剩余。此步的计算复杂度为 $2^{n-37}\times2^4\times2^{-3}\times(1/13)\approx2^{n-39.71}$。

步骤 4　猜测密钥 RK_{13}^4,其对应主密钥的位置为 $k_{69\sim66}$。由于在步骤 3 中已经猜测过 $k_{69\sim68}$,所以只需要猜测剩余的密钥比特。部分解密第 13 轮,保留满足式 $S_4(L_{14}^4\oplus RK_{13}^4)\oplus S_4(L_{14}^4\oplus\Delta L_{14}^4\oplus RK_{13}^4\oplus\Delta RK_{13}^4)=\Delta R_{14,3}^7\|\Delta R_{14,3}^5\|\Delta R_{14,3}^3\|\Delta R_{14,3}^1$ 的数据对。然后对剩余的数据对继续猜测密钥 RK_{13}^0,其在主密钥中的对应位置是 $k_{53\sim50}$,对剩余的数据对部分解密,保留满足 $S_0(L_{14}^0\oplus RK_{13}^0)$

Table 2　Related-key differential paths when $\Delta K^{17}=8$

表 2　$\Delta K^{17}=8$ 时的相关密钥不可能差分路径

Round	ΔL_i	ΔR_i	ΔRK_i	*Round*	ΔL_i	ΔR_i	ΔRK_i
2	0000 0000	0000 0000	0000 0000	12	0000 0000	0000 0000	——
3	0000 0000	0000 0000	0000 0000	11	0000 0000	0000 0000	0000 0000
4	0000 0000	0000 0000	0000 0000	10	0000 0000	0000 0000	0000 0000
5	0000 0000	0000 0000	0000 0000	9	0000 0000	0000 0000	0000 0000
6	0000 0000	0000 0000	0000 0000	8	0000 0000	0000 0000	0000 0000
7	0000 0000	0?0?0?0?	——	7	0?0?0?0?	0000 0000	0020 0000

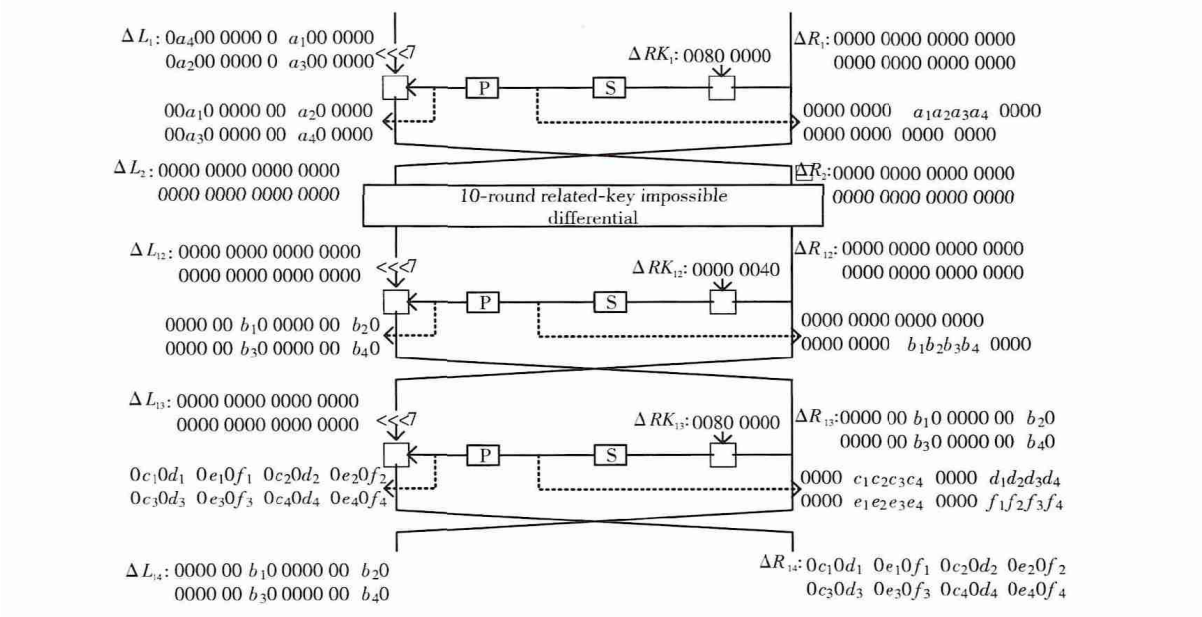

Figure 2 13-round related-key impossible differential paths of ESF

图 2 ESF 算法的 13 轮相关密钥不可能差分路径

$\oplus S_0(L_{14}^0 \oplus \Delta L_{14}^0 \oplus RK_{13}^0 \oplus \Delta RK_{13}^0) = \Delta R_{14,3}^6 \| \Delta R_{14,3}^4 \| \Delta R_{14,3}^2 \| \Delta R_{14,3}^0$ **的数据对。对剩余的数据对继续猜测密钥** RK_{13}^2**,其在主密钥中的对应位置为** $k_{61\sim58}$**,对剩余的数据进行 13 轮部分解密,筛选并保留满足** $S_2(L_{14}^2 \oplus RK_{13}^2) \oplus S_2(L_{14}^2 \oplus \Delta L_{14}^2 \oplus RK_{13}^2 \oplus \Delta RK_{13}^2) = \Delta R_{14,1}^6 \| \Delta R_{14,1}^4 \| \Delta R_{14,1}^2 \| \Delta R_{14,1}^0$ **的数据对。继续猜测** RK_{13}^6**,其在主密钥中的对应位置为** $k_{77\sim74}$**,对剩余的数据对部分解密,保留满足** $S_6(L_{14}^6 \oplus RK_{13}^6) \oplus S_6(L_{14}^6 \oplus \Delta L_{14}^6 \oplus RK_{13}^6 \oplus \Delta RK_{13}^6) = \Delta R_{14,1}^7 \| \Delta R_{14,1}^5 \| \Delta R_{14,1}^3 \| \Delta R_{14,1}^1$ **的数据对。此时还剩余** $2^{n-41}\times2^{-2}\times2^{-4}\times2^{-4}\times2^{-4}=2^{n-55}$ **个数据对。此步的计算复杂度为** $(2^{n-41}\times2^6+2^{n-43}\times2^{10}+2^{n-47}\times2^{14}+2^{n-51}\times2^{18})\times2^{-3}\times(1/13)\approx2^{n-38}$。

步骤 5 猜测 R_{12}^1**,总共有** 2^4 **种可能性。对第 12 轮部分解密,保留满足** $F(\Delta R_{12}^1 \oplus \Delta RK_{12}^1) \oplus (\Delta R_{13,2}^6 \| \Delta R_{13,2}^4 \| \Delta R_{13,2}^2 \| \Delta R_{13,2}^0) = 0$ **(**$\Delta R_{13} = \Delta L_{14}$**)的数据对。步骤 4 结束后剩余数据对** 2^{n-55} **个,取** $n=56$**,则满足上面式子的数据对剩余** $2^{n-55}\times2^4=2^5$**。如果经过过滤后仍有数据对剩余,则说明之前猜测的密钥错误,需要重新猜测密钥。步骤 5 的计算复杂度为** $2^{n-55}\times2^4\times2^{18}=2^{23}$。

由以上步骤可知,当选择 $\Delta K=0080\ \ 0000\ \ 0000\ \ 0000\ \ 0000$ **时,对 ESF 算法的 13 轮相关密钥不可能差分攻击可恢复 18 bit 密钥。该 13 轮相关密钥不可能差分攻击所需的数据复杂度为** $2^4\times2^{56}=2^{60}$**,计算复杂度为** $2^{56-39.7}+2^{56-38}+2^{23}\approx2^{23}$ **次 13 轮加密操作。**

3.2 针对 14 轮 ESF 算法的相关密钥不可能差分分析

无论是文献[7,11]还是 3.1 节中的攻击,其分析的复杂度虽然较低,但是恢复的密钥比特不多,在工程中的应用有限。针对这些问题,我们考虑能否适当增大复杂度来恢复更多的密钥比特。当 $\Delta K^{14}=4$ **时,存在 3~12 轮共 10 轮的相关密钥不可能差分路径,该路径加解密过程如表 3 所示。加密和解密过程中的四个“?”中至少有一个非零,显**

Table 3 Related-key differential paths when $\Delta K^{14}=4$

表 3 $\Delta K^{14}=4$ **时的相关密钥不可能差分路径**

Round	ΔL_i	ΔR_i	ΔRK_i	*Round*	ΔL_i	ΔR_i	ΔRK_i
3	0000 0000	0000 0000	0000 0000	13	0000 0000	0000 0000	——
4	0000 0000	0000 0000	0000 0000	12	0000 0000	0000 0000	0000 0000
5	0000 0000	0000 0000	0000 0000	11	0000 0000	0000 0000	0000 0000
6	0000 0000	0000 0000	0000 0000	10	0000 0000	0000 0000	0000 0000
7	0000 0000	0000 0000	0000 0100	9	0000 0000	0000 0000	0000 0000
8	0000 0000	0?0?0?0?	——	8	0?0?0?0?	0000 0000	0020 0000

然矛盾。得到如下 10 轮相关密钥不可能差分路径:

$$(00000000,00000000)\xrightarrow{\Delta K^{14}=4}(00000000,00000000)$$

根据该 10 轮相关密钥不可能差分路径,我们向前扩展 2 轮,向后扩展 2 轮,可以对 14 轮的算法进行攻击。14 轮相关密钥不可能差分攻击的示意图见图 3,其具体过程如下:

步骤 1　选择 2^{24} 个明文生成一个结构,其中 L_1 的第 1、3、4、5、7、9、11、12、13、15、17、19、20、21、23、25、27、28、29、31 bit 和 R_1 的第 1、9、17、25 bit 可以随意取值,剩余位置的取值保证差分为 0,即要保证输入明文差分满足 $\Delta L_{1,3}^{6}\|\Delta L_{1,3}^{4}\|\Delta L_{1,3}^{2}\|\Delta L_{1,3}^{0}=b_1\|b_2\|b_3\|b_4,\Delta L_{1,1}^{5}\|\Delta L_{1,1}^{3}\|\Delta L_{1,1}^{1}\|\Delta L_{1,1}^{7}=c_1\|c_2\|c_3\|c_4,\Delta L_{1,3}^{5}\|\Delta L_{1,3}^{3}\|\Delta L_{1,3}^{1}\|\Delta L_{1,3}^{7}=d_1\|d_2\|d_3\|d_4,\Delta L_{1,0}^{4}\|\Delta L_{1,0}^{2}\|\Delta L_{1,0}^{0}\|\Delta L_{1,0}^{6}=e_1\|e_2\|e_3\|e_4,\Delta L_{1,1}^{4}\|\Delta L_{1,1}^{2}\|\Delta L_{1,1}^{0}\|\Delta L_{1,1}^{6}=f_1\|f_2\|f_3\|f_4,\Delta R_{1,1}^{5}\|\Delta R_{1,1}^{3}\|\Delta R_{1,1}^{1}\|\Delta R_{1,1}^{7}=a_1\|a_2\|a_3\|a_4$,其中 $a_i,b_i,c_i,d_i,e_i,f_i(1\leqslant i\leqslant 4)$ 取所有可能的值,则一个结构包含 $2^{24}\times 2^{24}\times(1/2)=2^{47}$ 个明文对。选取 2^n 个这样的结构,可以形成 2^{n+47} 个明文对。

步骤 2　对选择的明文对在 $\Delta K=$0000　0400　0000　0000　0000 的情况下进行 14 轮加密得到密文对,过滤密文对,保留使得输出差分满足如下式子的数据对:$\Delta L_{14,2}^{6}\|\Delta L_{14,2}^{4}\|\Delta L_{14,2}^{2}\|\Delta L_{14,2}^{0}=p_1\|p_2\|p_3\|p_4,\Delta R_{14,1}^{7}\|\Delta R_{14,1}^{5}\|\Delta R_{14,1}^{3}\|\Delta R_{14,1}^{1}=q_1\|q_2\|q_3\|q_4,\Delta R_{14,3}^{7}\|\Delta R_{14,3}^{5}\|\Delta R_{14,3}^{3}\|\Delta R_{14,3}^{1}=r_1\|r_2\|r_3\|r_4,\Delta R_{14,1}^{6}\|\Delta R_{14,1}^{4}\|\Delta R_{14,1}^{2}\|\Delta R_{14,1}^{0}=s_1\|s_2\|s_3\|s_4,\Delta R_{14,3}^{6}\|\Delta R_{14,3}^{4}\|\Delta R_{14,3}^{2}\|\Delta R_{14,3}^{0}=t_1\|t_2\|t_3\|t_4$,其中 $p_i,q_i,r_i,s_i,t_i(1\leqslant i\leqslant 4)$ 取所有可能的值。此时还有 $2^{n+47}\times 2^{-44}=2^{n+3}$ 个数据对剩余。

步骤 3　首先猜测密钥 RK_1^2,其在主密钥中的相应位置为 $k_{59\sim 56}$,部分加密第 1 轮,保留满足等式 $S_2(R_1^2\oplus RK_1^2)\oplus S_2(R_1^2\oplus\Delta R_1^2\oplus RK_1^2\oplus\Delta RK_1^2)=\Delta L_{1,0}^{4}\|\Delta L_{1,0}^{2}\|\Delta L_{1,0}^{0}\|\Delta L_{1,0}^{6}$ 的数据对。然后猜测密钥 RK_1^1,该轮密钥在主密钥中的位置为 $k_{55\sim 52}$,对剩余的数据对部分加密第 1 轮,保留满足等式 $S_1(R_1^1\oplus RK_1^1)\oplus S_1(R_1^1\oplus\Delta R_1^1\oplus RK_1^1\oplus\Delta RK_1^1)=\Delta L_{1,1}^{4}\|\Delta L_{1,1}^{2}\|\Delta L_{1,1}^{0}\|\Delta L_{1,1}^{6}$ 的数据对。对剩余的数据对继续猜测密钥 RK_1^3,其在主密钥中的相应位置为 $k_{63\sim 60}$,保留满足等式 $S_3(R_1^3\oplus RK_1^3)\oplus S_3(R_1^3\oplus\Delta R_1^3\oplus RK_1^3\oplus\Delta RK_1^3)=\Delta L_{1,3}^{5}\|\Delta L_{1,3}^{3}\|\Delta L_{1,3}^{1}\|\Delta L_{1,3}^{7}$ 的数据对。继续猜测密钥 RK_1^5,其在主密钥中的对应位置为 $k_{71\sim 68}$,保留满足等式 $S_5(R_1^5\oplus RK_1^5)\oplus S_5(R_1^5\oplus\Delta R_1^5\oplus RK_1^5\oplus$

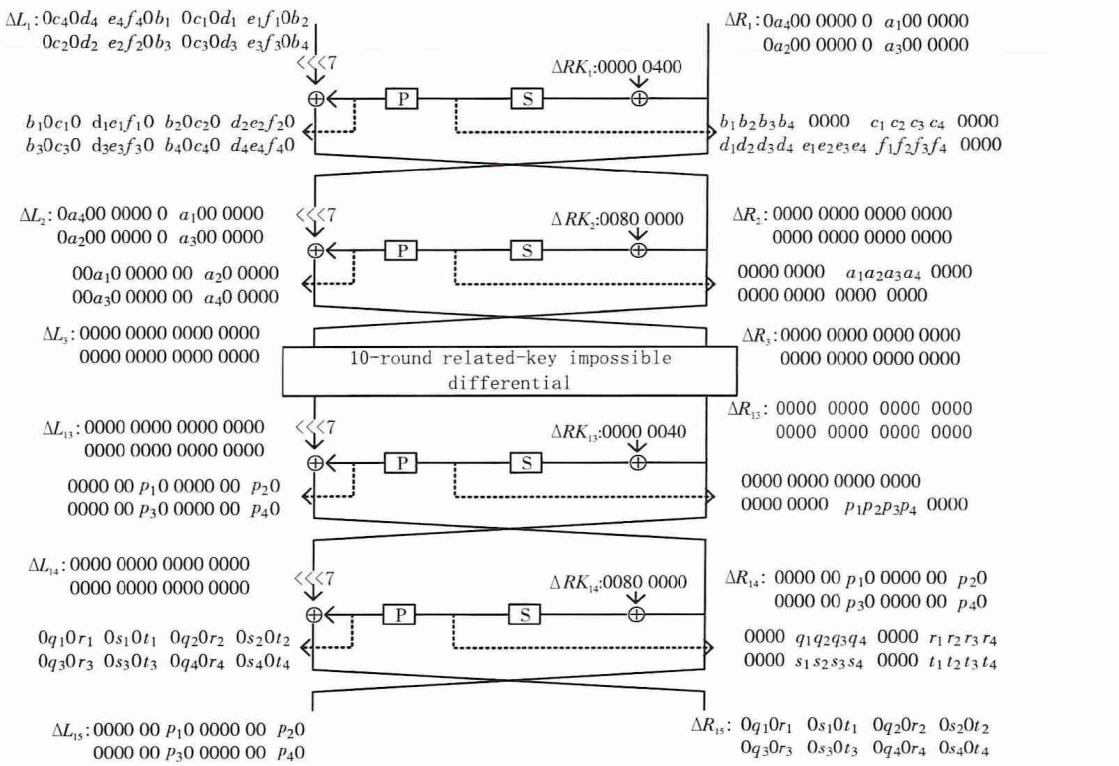

Figure 3　14-round related-key impossible differential paths of ESF

图 3　ESF 算法的 14 轮相关密钥不可能差分路径

$\Delta RK_1^5)=\Delta L_{1,1}^5 \parallel \Delta L_{1,1}^3 \parallel \Delta L_{1,1}^1 \parallel \Delta L_{1,1}^7$的数据对。对剩余的数据对继续猜测密钥$RK_1^7$,其在主密钥中的对应位置为$k_{79\sim76}$,保留满足式子$S_7(R_1^7 \oplus RK_1^7) \oplus S_7(R_1^7 \oplus \Delta R_1^7 \oplus RK_1^7 \oplus \Delta RK_1^7)=\Delta L_{1,3}^6 \parallel \Delta L_{1,3}^4 \parallel \Delta L_{1,3}^2 \parallel \Delta L_{1,3}^0$的数据对。此时还有$2^{n+3} \times 2^{-20}=2^{n-17}$个数据对剩余。此步的计算复杂度为$(2^{n+3} \times 2^4+2^{n-1} \times 2^8+2^{n-5} \times 2^{12}+2^{n-9} \times 2^{16}+2^{n-13} \times 2^{20}) \times 2^{-3} \times (1/14) \approx 2^{n+2.51}$。

步骤4 猜测密钥RK_1^7、RK_1^6、RK_1^5、RK_1^4、RK_2^5,它们在主密钥中的相应位置分别为$k_{79\sim76}$、$k_{75\sim72}$、$k_{71\sim68}$、$k_{67\sim64}$、$k_{58\sim55}$,其中$k_{79\sim76}$、$k_{71\sim68}$、$k_{58\sim55}$在步骤3中已经猜测过,只需猜测剩余的密钥比特。保留满足以下等式的数据对:$S_5(R_2^5 \oplus RK_2^5) \oplus S_5(R_2^5 \oplus \Delta R_2^5 \oplus RK_2^5 \oplus \Delta RK_2^5)=\Delta L_{2,1}^5 \parallel \Delta L_{2,1}^3 \parallel \Delta L_{2,1}^1 \parallel \Delta L_{2,1}^7$。此时还有$2^{n-17} \times 2^{-4}=2^{n-21}$个数据对剩余。此步的计算复杂度为$2^{n-17} \times 2^{28} \times 2^{-2} \times (1/14) \approx 2^{n+5.19}$。

步骤5 猜测密钥RK_{14}^4,它在主密钥中的相应位置为$k_{56\sim53}$,这4 *bit*密钥在步骤3中已经猜测过,所以只需要保留满足以下等式的数据对:$S_4(R_{14}^4 \oplus RK_{14}^4) \oplus S_4(R_{14}^4 \oplus RK_{14}^4 \oplus RK_{14}^4 \oplus \Delta RK_{14}^4)=\Delta R_{15,3}^7 \parallel \Delta R_{15,3}^5 \parallel \Delta R_{15,3}^3 \parallel \Delta R_{15,3}^1$,$R_{14}=L_{15}$。继续猜测密钥$RK_{14}^0$,其在主密钥中的对应位置为$k_{40\sim37}$,保留满足等式$S_0(R_{14}^0 \oplus RK_{14}^0) \oplus S_0(R_{14}^0 \oplus \Delta R_{14}^0 \oplus RK_{14}^0 \oplus \Delta RK_{14}^0)=\Delta R_{15,3}^6 \parallel \Delta R_{15,3}^4 \parallel \Delta R_{15,3}^2 \parallel \Delta R_{15,3}^0$的数据对。对剩余数据对猜测密钥$RK_{14}^2$,其在主密钥中的对应位置为$k_{48\sim45}$,保留满足等式$S_2(R_{14}^2 \oplus RK_{14}^2) \oplus S_2(R_{14}^2 \oplus \Delta R_{14}^2 \oplus RK_{14}^2 \oplus \Delta RK_{14}^2)=\Delta R_{15,1}^6 \parallel \Delta R_{15,1}^4 \parallel \Delta R_{15,1}^2 \parallel \Delta R_{15,1}^0$的数据对。对剩余的数据对猜测密钥$RK_{14}^6$,其对应主密钥的$k_{64\sim61}$,$k_{63\sim61}$在步骤3中已经猜测过,只需猜测剩余的1 bit,保留满足式子$S_6(R_{14}^6 \oplus RK_{13}^6) \oplus S_6(R_{14}^6 \oplus \Delta R_{14}^6 \oplus RK_{14}^6 \oplus \Delta RK_{14}^6)=\Delta R_{15,1}^7 \parallel \Delta R_{15,1}^5 \parallel \Delta R_{15,1}^3 \parallel \Delta R_{15,1}^1$的数据对。此时还有$2^{n-21} \times 2^{-16}=2^{n-37}$个数据对剩余。此步的计算复杂度为$(2^{n-21} \times 2^{28}+2^{n-25} \times 2^{32}+2^{n-29} \times 2^{36}+2^{n-33} \times 2^{37}) \times 2^{-3} \times (1/14) \approx 2^{n+1.84}$。

步骤6 猜测R_{13}^1,共有2^4种可能性,保留满足等式$F(\Delta R_{13}^1 \oplus \Delta RK_{13}^1) \oplus (\Delta R_{14,2}^6 \parallel \Delta R_{14,2}^4 \parallel \Delta R_{14,2}^2 \parallel \Delta R_{14,2}^0)=0$的数据对。取$n=38$,则步骤5中剩余的数据对为$2^{n-37}=2$个,故上式成立时还剩余$2^{n-37} \times 2^4=2^5$个数据对。如果经过过滤后仍有数据对剩余则说明之前猜测的密钥错误,则需要重新猜测密钥。由以上过程可知本步骤的计算复杂度为$2^{38-37} \times 2^4 \times 2^{37}=2^{42}$。

由以上分析可知,当选择$\Delta K=$0000 0400 0000 0000 0000时,对ESF算法的14轮相关密钥不可能差分攻击可恢复37 bit密钥,需要$2^{38+24}=2^{62}$次选择明文对,计算复杂度为$2^{40.51}+2^{43.19}+2^{39.84}+2^{42} \approx 2^{43.95}$次14轮加密操作。

3.3 结果对比

综上所述,本文分别给出了13轮ESF和14轮ESF的相关密钥不可能差分攻击。前者的数据复杂度为2^{60},计算复杂度为2^{23}次13轮加密操作,可恢复18 bit密钥;后者的数据复杂度为2^{62},计算复杂度为$2^{43.95}$次14轮加密,可恢复37 bit密钥。文献[7,11]都只给出了11轮ESF的不可能差分攻击路径,相比较而言,我们结合相关密钥所得的分析结果在攻击的轮数、恢复的密钥比特数等方面均具有较大优势,具体比较情况如表4所示。

Table 4 Cryptanalysis result comparison of ESF

表4 ESF算法的攻击结果比较

攻击类型	轮数	复杂度		来源
		数据	计算	
Impossible DC	11	2^{64}	$2^{75.5}$	文献[7]
Impossible DC	11	2^{53}	2^{32}	文献[10]
Rel-Key Impossible DC	13	2^{60}	2^{32}	本文
Rel-Key Impossible DC	14	2^{62}	$2^{43.95}$	本文

4 结束语

本文将相关密钥与不可能差分相结合,利用ESF密钥扩展算法的弱点,通过选取不经过S盒的非零密钥差分使得活跃S盒的个数最少、差分链的长度增加,首先构造出10轮相关密钥不可能差分路径,并在此基础上分别攻击了13、14轮的ESF算法,攻击的计算复杂度远低于穷举攻击的复杂度。未来工作可以考虑设计算法利用计算机完成更多轮数相关密钥不可能差分路径的搜索或者结合新的分析方法,进而实现更高轮数ESF算法的攻击,恢复更多的密钥比特。

参考文献:

[1] Daemen J, Borg S, Rjimen V. The design of Rijndael: AES—The advance encryption standard[M]. Berlin: Springer-Verlag, 2002.

[2] National Bureau of Standards. Federal information process-

ing standard 46:Data encryption standard[S]. New York:National Bureau of Standards,1997.

[3] Bogdanov A,Knudsen L R,Leander G,et al. PRESENT:An ultra-lightweight block cipher [C]// Proc of Cryptographic Hardware and Embedded Systems,2007:450-466.

[4] Hong D,Sung J,Hong S,et al. HIGHT:A new block cipher suitable for low-resource device [C]// Proc of Cryptographic Hardware and Embedded Systems,2006:46-59.

[5] Izadi M, Sadeghiyan B, Sadeghian S,et al.,MIBS:A new lightweight block cipher[C]// Proc of Cryptology and Network Security,2009:334-348.

[6] Ojha S,Kumar N,Jain K,et al. TWIS—A lightweight block cipher[C]// Proc of Information Systems Security, 2009:280-291.

[7] Liu Xuan, Liu Feng, Meng Shuai. Impossible differential cryptanalysis of lightweight block ciper ESF[J]. Computer Engineering & Science,2013,35(9):85-95. (in Chinese)

[8] Wu Wen-ling,Zhang Lei,LBlock:A lightweight block cipher [C]// Proc of Applied Cryptography and Network Security, 2011:327-344.

[9] Knudsen L R. Cryptanalysis of LOKI 91[C]// Proc of AUSCRYPT'92,1993:196-208.

[10] Biham E. New types of cryptanalytic attacks using related keys[C]// Proc of EUROCRYPT'93. LNCS 765:398-409.

[11] Chen Yu-lei,Wei Hong-ru. Impossible differential cryptanalysis of ESF[J]. Computer Science,2016,43(8):89-91. (in Chinese)

附中文参考文献:

[7] 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.

[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.

作者简介:

谢敏(1976-),**女,湖南常德人,博士,副教授,研究方向为编码与密码。E-mail**:mxie@xidian.edu.cn

XIE Min,born in 1976,PhD,associate professor, her research interests include coding, and cryptography.

杨盼(1992-),**男,河南南阳人,硕士,研究方向为轻量级分组密码分析。E-mail**:yangpan20_11@163.com

YANG Pan,born in 1992,MS,his research interests include cryptanalysis of lightweight block ciphers.