计算机研究与发展
Journal of Computer Research and Development
DOI:10.7544/issn1000-1239.2017.20170455
54(10):2224-2231,2017

轻量级分组密码算法 ESF 的安全性分析

尹 军[1,2,3] 马楚焱[4] 宋 健[1] 曾 光[1] 马传贵[5]
[1](数学工程与先进计算国家重点实验室(中国人民解放军信息工程大学) 郑州 450001)
[2](中国科学院信息工程研究所 北京 100093)
[3](中国科学院大学 北京 100049)
[4](国防科学技术大学 长沙 410073)
[5](陆军航空兵学院 北京 101116)
(yinjun66888@163.com)

Security Analysis of Lightweight Block Cipher ESF

Yin Jun[1,2,3], Ma Chuyan[4], Song Jian[1], Zeng Guang[1], and Ma Chuangui[5]
[1](*State Key Laboratory of Mathematical Engineering and Advanced Computing* (*PLA Information Engineering University*), *Zhengzhou* 450001)
[2](*Institute of Information Engineering*, *Chinese Academy of Sciences*, *Beijing* 100093)
[3](*University of Chinese Academy of Sciences*, *Beijing* 100049)
[4](*National University of Defense Technology*, *Changsha* 410073)
[5](*Army Aviation Institute*, *Beijing* 101116)

Abstract Automatic analysis is one of the important methods to evaluate the security of cryptographic algorithms. It is characterized by high efficiency and easily implement. In ASIACRYPT 2014, Sun et al. presented a MILP-based automatic search differential and linear trails method for bit-oriented block ciphers, which has attracted the attention of many cryptographers. At present, there are still a lack of research about solving the MILP model, such as how to reduce the number of variables and constraint inequalities. According to the differential propagation model of the XOR operation, in EUROCRYPT 2017, Sasaki et al. gave a set of new constraints without dummy variables. The new constraint inequalities can not only preserve the differential propagation for XOR operation, but also reduce the number of variables. At the same time, Sun et al. uses four constraints to describe the property when the input differential variable (the linear mask variable) of an S-box is non-zero and the S-box must be an active, but in this paper, we just use one constraint. Based on these refined constraints and the automatic method for finding high probability trails of block cipher, we establish the refined differential and linear MILP model under the single key assumption for the lightweight block cipher ESF. We have found that the minimum number of active S-boxes in 15-round differential trail of ESF is 19 and the number is 15 in 16-round linear trail. Moreover, we find so far the longest impossible differential and zero-correlation linear approximation distinguishers of ESF.

Key words differential cryptanalysis; linear cryptanalysis; impossible differential; zero-correlation linear approximation; ESF; MILP

收稿日期:2017-06-11;**修回日期**:2017-08-03

基金项目:国家自然科学基金项目(61502532,61379150,61772519,61309016,61502529);数学工程与先进计算国家重点实验室开放基金课题(2016A02);河南省重点科技攻关计划项目(122102210126,092101210502)

This work was supported by the National Natural Science Foundation of China (61502532, 61379150, 61772519, 61309016, 61502529), the Open Foundation of the State Key Laboratory of Mathematical Engineering and Advanced Computing (2016A02), and the Key Scientific and Technological Project of Henan Province (122102210126, 092101210502).

摘　要　自动化分析是当前对密码算法进行安全性评估的重要方法之一,具有高效、易实现的特点.对面向位的分组密码,自从 Sun 等人在 2014 年亚洲密码年会上提出基于 MILP 问题的差分和线性自动化搜索方法,该方法受到了许多密码学者的关注.目前,针对求解多轮密码算法 MILP 模型,如何减少变量和约束不等式的研究工作相对较少,还有很多问题有待解决.根据异或操作的差分传播模式,在 2017 年欧洲密码年会上,Sasaki 等人给出了不带假设变量的新约束不等式,该约束不等式在降低变量和约束数量的前提下保留了异或操作的差分传播性质.同时,对于 S 盒的性质,当输入差分变量(线性掩码)非零时,该 S 盒必定活跃,Sun 等人用了 4 个约束不等式来刻画该性质,经过简单的变换,可以用 1 个约束来表示该性质.基于这些精炼的约束和自动化搜索方法,针对轻量级分组密码算法 ESF,建立单密钥下精炼的差分和线性 MILP 模型,首次给出了 ESF 算法在单密钥情形下的差分和线性分析结果,得到了 15 轮 ESF 算法差分最小活跃 S 盒数量为 19 和 16 轮 ESF 算法线性最小活跃 S 盒数量为 15.此外,还搜索到了轮数最长的不可能差分和零相关线性逼近区分器.

关键词　差分密码分析;线性密码分析;不可能差分;零相关线性逼近;ESF;MILP

中图法分类号　TP309.7

当前,对于轻量级分组密码的设计与分析越来越受到人们关注,密码学者提出了许多轻量级分组密码算法,比较知名的算法有 LBlock[1],PRESENT[2],SKINNY[3],RECTANGLE[4]等.

对分组密码 2 种经典的密码分析方法是差分密码分析[5]和线性密码分析[6].差分密码分析是 1990 年由 Biham 和 Shamir 提出的,他们利用这种方法攻击了 DES 密码算法,其主要思想是通过分析一个特选的明文对差分对相应密文对差分的影响来恢复密钥信息.差分攻击最重要的步骤是寻找高概率差分特征.线性密码分析是 Matsui[6]在 1993 年的欧洲密码年会(欧密会)上提出来的,它属于已知明文攻击范畴,通过分析明密文之间的线性关系,构建明密文之间线性偏差不为 0 的线性逼近表达式,利用该线性逼近表达式来恢复密钥.此外,在上述 2 种密码分析方法的基础上,提出了许多扩展的密码分析方法,例如不可能差分密码分析[7]、零相关线性逼近[8]等,不可能差分密码分析的基本思想就是利用概率为零(或者非常小)的差分特征,排除那些导致差分概率为零(或者非常小)的差分特征对应的密钥.零相关线性逼近是由 Bogdanov 和 Rijmen 首次提出,通过寻找密码算法中相关度为零的线性逼近表达式,区分密码算法与随机置换,进行密钥恢复.

在上面 2 类密码分析方法中,寻找最优的差分特征和线性逼近是进行有效攻击的关键,其复杂度要低于暴力搜索.自动化分析是非常流行和高效的寻找最优差分和线性特征的方法,其主要思想是通过编程软件,自动化搜索差分和线性特征.目前,这类工作已经取得了很多成果,在 1994 年欧洲密码年会上,Matsui 提出了分支定界搜索算法,搜索 DES 的差分特征[9];在 2013 年 Mouha 和 Preneel 构造了一个工具,基于可满足性模问题(satisfiability modulo theories, SMT),搜索流密码 Salsa20 的最优差分特征[10];此外,计算活跃 S 盒数量的下界是另外一种评估分组密码抵抗差分和线性分析的方法.在 2011 年 Mouha 等人将计算活跃 S 盒数量的问题转化成混合整数线性规划(mixed-integer linear programming, MILP)问题,应用于面向字的分组密码[11];在 2014 年亚洲密码年会上,Sun 等人扩展了 Mouha 等人的方法,对面向位的分组密码,在单密钥和相关密钥模型建立 MILP 模型,分别计算最小活跃 S 盒数量的下界,搜索到了许多密码算法差分和线性特征[12];2016 年 Cui 等人在差分和线性 MILP 方法基础上,实现了不可能差分和零相关线性逼近的自动化搜索[13].同时,在 2017 年欧洲密码年会上,Sasaki 等人扩展 MILP 方法,提出了新的自动化搜索不可能差分的工具[14].

ESF[15]是刘宣等人基于吴文玲研究员的 LBlock 算法改进的轻量级分组密码算法,同时在置换层还采用了 PRESENT 算法的 P 置换形式,分组长度 64 b,密钥长度 80 b.针对 ESF 的密码分析,刘宣等人给出了 ESF 算法 8 轮不可能差分区分器来攻击 11 轮 ESF 算法[16],攻击的数据和时间复杂度分别是 2^{59} 和 $2^{75.5}$.随后,陈玉磊等人利用文献[16]中刘宣等人给出的 8 轮不可能差分区分器,根据轮密钥之间的关系,通过改变原有轮数扩展和密钥猜测的顺序,改进了 11 轮 ESF 的不可能差分攻击结果,攻击的数据和时间复杂度[17]分别是 2^{53} 和 2^{32}.

本文的主要贡献有 4 个方面：

1) 根据 Sasaki 等人在 2017 年亚洲密码年会上给出的改进 XOR 操作约束[①]，以及我们改变的 S 盒相关的约束，建立了更加精炼的 MILP 模型，大大减少了建立 MILP 模型的约束和变量数量；

2) 基于精炼的 MILP 模型，建立单密钥下 ESF 算法的差分和线性 MILP 模型，首次给出了 ESF 算法在单密钥情形下的差分和线性分析结果；

3) 基于精炼的 MILP 模型，建立 ESF 算法的不可能差分和零相关线性逼近 MILP 模型，给出了 ESF 算法的不可能差分和零相关线性分析结果.

4) 在输入输出差分只有一个活跃半字节的情形下，通过 Gurobi 软件求解该模型，搜索到了 15 轮 ESF 算法差分最小活跃 S 盒数量为 19；在输入输出掩码只有一个活跃比特位的情形下，搜索得到 16 轮 ESF 算法线性最小活跃 S 盒数量为 15. 此外，我们还搜索到最长 9 轮的不可能差分和 8 轮的零相关线性区分器. 具体的攻击结果如表 1 所示：

Table 1 The Attack Results for ESF

表 1 ESF 算法攻击结果

Attack Type	Rounds	Reference
Differential Attack	15	This Paper
Linear Attack	16	This Paper
Impossible Differential Attack	8	Ref[16]
Impossible Differential Attack	8	Ref[17]
Impossible Differential Attack	9	This Paper
Zero correlation Linear Approximation	8	This Paper

1 准备知识

本节首先给出常用的符号和术语说明，然后简要描述轻量级分组密码算法 ESF.

1.1 常用的符号和术语

L_i：第 i 轮 ESF 算法输出的左 32 b；

R_i：第 i 轮 ESF 算法输出的右 32 b；

F：轮函数；

K_i：第 i 轮 32 b 子密钥；

ΔX：表示 X_1 和 X_2 的差分，$X_1 \oplus X_2 = \Delta X$；

$\lll 7$：循环左移 7 b.

1.2 ESF 算法

ESF 算法是基于 Lblock 算法改进的轻量级分组密码算法，分组长度 64 b，密钥长度 80 b，迭代轮数为 32 轮. ESF 算法采用广义的 Feistel 结构，轮函数为 SPN 结构. 一轮的 ESF 加密流程如图 1 所示[②]. 其中轮函数 F 为 SPN 结构，由非线性变换 S 函数和置换函数 P 组成，轮函数 F 如图 2 所示. 轮函数 F 为 $F(R_i, K_i) = P(S(K_i \oplus R_i))$，其中的 S 函数是一个非线性变换，由 8 个并行的 4×4 的 S 盒构成，8 个 S 盒的具体分布如表 2 所示.

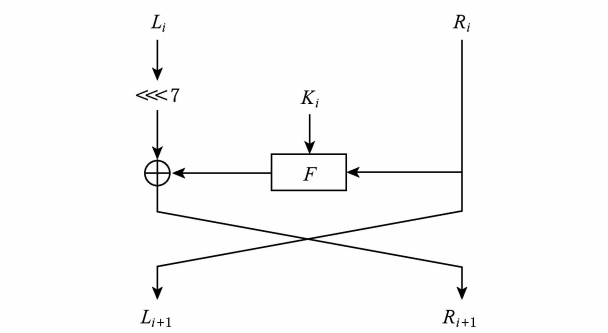


Fig. 1 1-round ESF encryption

图 1 1 轮 ESF 加密过程

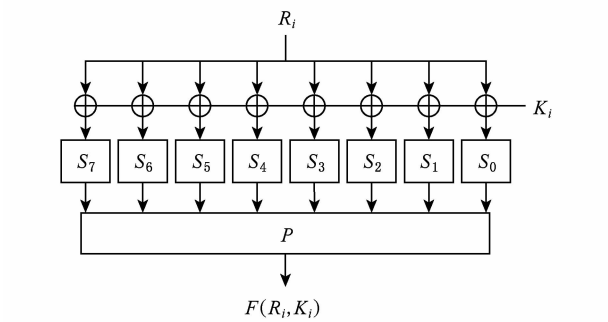


Fig. 2 The round function of ESF

图 2 ESF 轮函数

Table 2 The S-Boxes of ESF

表 2 ESF 的 S 盒

S-Boxes	The S-Boxes Input Value(In hexadecimal representation)															
	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

① 该约束出现在 Sasaki 等人在 2017 年欧洲密码年会上作的报告 slide 中，具体请参考 https://eurocrypt2017.di.ens.fr/slides/A09-new-impossible-differential.pdf.

② 图 1 和图 2 由 TikZ for Cryptographers 产生，具体详情请参考 http://www.iacr.org/authors/tikz/.

具体变换如下:

$$a=a_7 \| a_6 \| \cdots \| a_0 \rightarrow b=b_7 \| b_6 \| \cdots \| b_0,$$

$$b_7=S_7(a_7),$$
$$b_6=S_6(a_6),$$
$$b_5=S_5(a_5),$$
$$b_4=S_4(a_4),$$
$$b_3=S_3(a_3),$$
$$b_2=S_2(a_2),$$
$$b_1=S_1(a_1),$$
$$b_0=S_0(a_0).$$

P 置换函数将 32 b 的($b_{31} \| b_{30} \| \cdots \| b_1 \| b_0$)映射成($c_{31} \| c_{30} \| \cdots \| c_1 \| c_0$),具体如下:

$b=(b_{31} \| b_{30} \| \cdots \| b_1 \| b_0) \rightarrow c=(c_{31} \| c_{30} \| \cdots \| c_1 \| c_0)$,当 $i=0,1,\cdots,7$ 时,

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

在本文中,我们只考虑单密钥情形下的密码分析.因此对于密钥扩展算法,具体细节可参考文献[15].

2　基于 MILP 问题的自动化分析技术

在本节中,我们主要介绍 MILP,后面详细介绍基于 MILP 模型自动化搜索差分特征、线性特征、不可能差分和零相关线性逼近,具体应用于 ESF 算法上产生约束不等式的过程.同时给出我们优化的 MILP 模型.

2.1　混合整数线性规划(MILP)

MILP 问题是运筹学中的一类优化问题,旨在线性约束条件下求解目标函数的最小值或最大值.目前,求解这类问题目前有很多成熟的商业软件,例如 Gurobi[18],Cplex[19],MAGMA[20]等.下面具体给出 MILP 的定义.

定义 1. MILP.假设 $\boldsymbol{A} \in \mathbb{R}^{m \times n}$,$\boldsymbol{b} \in \mathbb{R}^m$ 和 $\boldsymbol{c}_1$,$\boldsymbol{c}_2,\cdots,\boldsymbol{c}_n \in \mathbb{R}^n$,寻找一个向量 $\boldsymbol{x}=(x_1,x_2,\cdots,x_n)$,在相应的线性约束条件 $\boldsymbol{A}\boldsymbol{x} \leqslant \boldsymbol{b}$ 下求解线性函数 $\boldsymbol{c}_1 x_1+\boldsymbol{c}_2 x_2+\cdots+\boldsymbol{c}_n x_n$ 的最小值或者最大值.

2.2　建立改进的自动化搜索差分特征 MILP 模型

根据 Sun 等人对面向位的分组密码建立差分特征自动化搜索方法,通过对密码算法的每轮差分变量使用二元域上的 0 和 1 变量来描述,同时这些变量受限于密码算法特殊的操作和结构.根据文献[12,21],下面介绍建立 ESF 算法差分特征搜索 MILP 模型的过程.

在 ESF 算法中,一共包含 4 个操作:循环移位、P 置换、XOR(异或)操作、S 盒,其中循环移位和 P 置换,可以根据相应的比特位置给出等式约束.重点考虑 2 个操作:

1) XOR 操作.$\oplus$:$F_2^{32} \times F_2^{32} \rightarrow F_2^{32}$.

2) S 盒.S:$F_2^4 \rightarrow F_2^4$.

首先对于 S 盒,引入新的 0-1 变量 A_t 表示 S 盒是否活跃,定义为

$$A_t=\begin{cases}1, & \text{S 盒有非零差分},\\ 0, & \text{其他}.\end{cases}$$

很自然地,选择 $f=\sum_t A_t$ 作为建立 ESF 算法差分 MILP 问题的目标函数.下面具体给出对 ESF 算法操作的差分变量约束.

2.2.1　ESF 算法 XOR 操作差分约束

假设 XOR 操作的输入差分分别为 $\Delta\boldsymbol{a}$ 和 $\Delta\boldsymbol{b}$,输出差分为 $\Delta\boldsymbol{c}$.其中 $\Delta\boldsymbol{a}=(\Delta a_0,\Delta a_1,\cdots,\Delta a_{31})$,$\Delta\boldsymbol{b}=(\Delta b_0,\Delta b_1,\cdots,\Delta b_{31})$,$\Delta\boldsymbol{c}=(\Delta c_0,\Delta c_1,\cdots,\Delta c_{31})$.同时对 $0 \leqslant i \leqslant 31$,满足有 $\Delta a_i \oplus \Delta b_i=\Delta c_i$.下面给出对异或操作差分约束:

$$\begin{cases}\Delta a_i+\Delta b_i+\Delta c_i \geqslant 2d_i,\\ d_i \geqslant \Delta a_i; d_i \geqslant \Delta b_i; d_i \geqslant \Delta c_i,\\ \Delta a_i+\Delta b_i+\Delta c_i \leqslant 2,\end{cases} \tag{1}$$

其中,d_i 是假设的 0,1 变量,$0 \leqslant i \leqslant 31$.

在 2017 年欧洲密码年会上,Sasaki 等人针对 XOR 操作,改进了 Sun 等人给出的约束式(1).给出了不带假设的 0-1 变量约束式(2),对于 ESF 算法,每轮可以减少 32 个变量和 32 个约束.这样可以显著减少求解 MILP 模型的时间,提高效率,增加攻击轮数.

$$\begin{cases}\Delta a_i+\Delta b_i \geqslant \Delta c_i,\\ \Delta b_i+\Delta c_i \geqslant \Delta a_i,\\ \Delta a_i+\Delta c_i \geqslant \Delta b_i,\\ \Delta a_i+\Delta b_i+\Delta c_i \leqslant 2.\end{cases} \tag{2}$$

2.2.2　ESF 算法 S 盒操作差分约束

假设($\Delta x_0,\Delta x_1,\Delta x_2,\Delta x_3$)和($\Delta y_0,\Delta y_1,\Delta y_2,\Delta y_3$)分别表示 ESF 算法 4×4 的 S 盒的输入和输出差分,A_t 表示这个 S 盒是否活跃.

首先,为了保证 $\Delta x_0,\Delta x_1,\Delta x_2,\Delta x_3$ 有任意一个是 1 时,$A_t=1$,用不等式约束:

$$\begin{cases}\Delta x_0-A_t \leqslant 0,\\ \Delta x_1-A_t \leqslant 0,\\ \Delta x_2-A_t \leqslant 0,\\ \Delta x_3-A_t \leqslant 0.\end{cases}$$

我们通过分析上面的 4 个不等式,对其进行改进,使用 1 个不等式来表示这个约束条件:

$$\Delta x_0+\Delta x_1+\Delta x_2+\Delta x_3-4A_t \leqslant 0. \tag{3}$$

这样给出的约束不等式能够保证S盒差分传播的正确性,同时,在建立ESF算法的MILP模型中,每轮可以减少24个约束.

其次,当$A_t=1$时,$\Delta x_0,\Delta x_1,\Delta x_2,\Delta x_3$必定有一个非零,用不等式约束为

$$\Delta x_0+\Delta x_1+\Delta x_2+\Delta x_3-A_t\geqslant 0. \tag{4}$$

最后,对于双射的S盒,因为非零的输入差分必然导致非零的输出差分,反之亦然,用不等式约束为

$$\begin{cases}4\sum_{j=0}^{3}\Delta y_j-\sum_{i=0}^{3}\Delta x_i\geqslant 0,\\ 4\sum_{i=0}^{3}\Delta x_i-\sum_{j=0}^{3}\Delta y_j\geqslant 0.\end{cases} \tag{5}$$

除了式(3)~(5)对S盒差分的约束,Sun等人还提出了2套系统的方法,通过产生线性不等式来描述S盒的差分性质,使得刻画的S盒差分性质更加精确.这2种方法分别是逻辑状态模型和S盒所有可能差分模式的凸闭包H表示.对于第2种方法,在n维空间计算所有离散点的凸闭包H表示,通过SAGE中Sage.geometry.polyhedron类Inequality_generator()函数即可以得到凸闭包的H表示[22].但是,该函数产生的不等式非常多,对于ESF的每个S盒,都有大于300个不等式,因此要尽量减少不等式的数量,因此Sun等人设计了一个贪心算法来最大数量移除一部分不等式.表3给出了ESF算法8个S盒使用不同方法产生的不等式数量结果.

Table 3 The Number of Differential Inequalities Obtained by Different Methods

表3 使用不同方法产生的差分不等式数量

S-Boxes	The Number of the H-Representation of the Convex Hulls	The Number of Inequalities Obtained by Greedy Algorithm
ESF S_0	327	24
ESF S_1	327	23
ESF S_2	325	25
ESF S_3	368	31
ESF S_4	321	26
ESF S_5	321	29
ESF S_6	327	23
ESF S_7	368	32

2.3 建立自动化搜索线性特征MILP模型

为了自动化搜索ESF算法的线性特征,需要考虑ESF算法基本操作的线性掩码传播模式.因为位的旋转是一个简单的置换,可以根据相应的位给出等式约束,下面重点给出异或、分支和S盒操作的线性掩码传播约束.

首先对于S盒,引入新的0-1变量A_t表示线性活跃S盒,定义为

$$A_t=\begin{cases}1,\ \text{S盒有非零输出掩码},\\ 0,\ \text{其他}.\end{cases}$$

很自然地,选择$f=\sum_t A_t$作为建立ESF算法搜索线性特征MILP模型的目标函数.

根据文献[12,21],下面具体给出对ESF算法操作的线性掩码变量约束.

2.3.1 ESF算法XOR操作线性掩码约束

假设ESF算法XOR操作中,$\boldsymbol{a}=(a_0,a_1,\cdots,a_{31})$和$\boldsymbol{b}=(b_0,b_1,\cdots,b_{31})$是异或操作的输入掩码,$\boldsymbol{c}=(c_0,c_1,\cdots,c_{31})$是其输出掩码,约束如下:

$$\boldsymbol{a}=\boldsymbol{b}=\boldsymbol{c}.$$

2.3.2 ESF算法分支操作线性掩码约束

在ESF算法分支操作中,$\boldsymbol{a}=(a_0,a_1,\cdots,a_{31})$是输入掩码,$\boldsymbol{b}=(b_0,b_1,\cdots,b_{31})$和$\boldsymbol{c}=(c_0,c_1,\cdots,c_{31})$是输出掩码,约束如下:对$0\leqslant i\leqslant 31$,$a_i\oplus b_i\oplus c_i=0$,根据式(2),约束为

$$\begin{cases}a_i+b_i\geqslant c_i,\\ a_i+c_i\geqslant b_i,\\ b_i+c_i\geqslant a_i,\\ a_i+b_i+c_i\leqslant 2.\end{cases}$$

2.3.3 ESF算法S盒线性掩码约束

假设(x_0,x_1,x_2,x_3)和(y_0,y_1,y_2,y_3)分别表示ESF算法4×4的S盒的输入和输出掩码,A_t表示这个S盒是否活跃.

1)为了保证输出掩码y_0,y_1,y_2,y_3有任意一个是1时,$A_t=1$,用不等式约束:

$$y_0+y_1+y_2+y_3-4A_t\leqslant 0. \tag{6}$$

2)当$A_t=1$时,y_0,y_1,y_2,y_3必定有一个非零,用不等式约束:

$$y_0+y_1+y_2+y_3-A_t\geqslant 0. \tag{7}$$

3)对于双射的S盒,因为非零的输入线性掩码必然导致非零的输出线性掩码,反之亦然,用不等式约束:

$$\begin{cases}4\sum_{j=0}^{3}y_j-\sum_{i=0}^{3}x_i\geqslant 0,\\ 4\sum_{i=0}^{3}x_i-\sum_{j=0}^{3}y_j\geqslant 0.\end{cases} \tag{8}$$

除了式(6)~(8)对S盒线性掩码的约束,计算S盒所有非零线性偏差线性掩码传播模式的凸闭包H表示,然后利用Sun等人给出的贪心算法来来选择最大数量移除不可能线性掩码模式不等式.通过不同方法产生的不等式数量结果如表4所示:

Table 4　The Number of Inequalities Obtained by Different Methods

表 4　使用不同方法产生的不等式数量

S-Boxes	The Number of the H-Representation of the Convex Hulls	The Number of Inequalities Obtained by Greedy Algorithm
ESF S_0	137	26
ESF S_1	137	29
ESF S_2	138	25
ESF S_3	125	32
ESF S_4	125	28
ESF S_5	125	27
ESF S_6	137	28
ESF S_7	125	34

对于异或操作约束、S 盒操作约束、逻辑状态模型、凸闭包 H 表示、贪心算法,详细内容请参阅文献[12,21].

2.4　建立自动化搜索不可能差分 MILP 模型

为了搜索 ESF 算法的不可能差分,根据 Cui 等人和 Sasaki 等人给出的自动化搜索不可能差分工具,只需要简单修改一下基于 MILP 模型的差分特征搜索工具,就可以得到自动化搜索不可能差分的 MILP 模型.

假设 Δ_I 和 Δ_O 分别表示输入和输出的差分,为了测试(Δ_I,Δ_O)是不可能的差分对,在建立的差分 MILP 模型中增加固定的输入和输出差分的某些比特作为约束,在该模型中不必考虑目标函数,如果 MILP 求解器输出错误信息(例如 Gurobi 输出 infeasible),那么就可以知道这是一条不可能差分路径.

2.5　建立自动化搜索零相关线性逼近 MILP 模型

基于 MILP 模型搜索零相关线性逼近,跟搜索不可能差分类似,只需要修改相应的线性特征 MILP 模型,就可以得到自动化搜索零相关线性逼近的 MILP 模型.

对于建立不可能差分和零相关线性逼近自动化分析 MILP 模型,详细内容请参阅文献[13-14].

3　轻量级分组密码 ESF 的安全性分析

根据第 2 节所叙,结合 ESF 算法的加密过程,用 Python 编程分别产生自动化搜索差分特征、线性特征、不可能差分和零相关线性逼近"lp"文件格式的 MILP 模型,并且调用 Gurobi7.0.2 来求解相应的 MILP 模型.求解 MILP 模型的实验环境在一台服务器上进行,该服务器配置如表 5 所示:

Table 5　Experimental Environment for Solving MILP Model

表 5　MILP 模型试验求解环境

Item	Configuration
CPU	Intel Xeon E7-4820 v2
RAM	512 GB
OS	Windows Server 2008 R2 Enterprise
Software	Gurobi7.0.2

3.1　ESF 算法差分分析结果

通过建立 r 轮 ESF 算法的差分 MILP 模型,可以知道产生的差分 MILP 模型有 $373r+1$ 个不等式、$72r+64$ 个变量,ESF 算法前 15 轮在单密钥情形下差分活跃 S 盒数量的下界,如表 6 所示:

Table 6　The Results for Single-key Differential Analysis on ESF

表 6　ESF 算法单密钥差分分析结果

Rounds	# Active S-Boxes	Rounds	# Active S-Boxes
1	0	9	11
2	1	10	12
3	2	11	14
4	3	12	15
5	4	13	16
6	6	14	18
7	8	15	19
8	9	16	

从表 6 我们知道对于 15 轮的 ESF 算法最小差分活跃 S 盒数量是 19.对于超过 15 轮的模型,由于求解花费的时间关系(超过 15 d),我们只考虑前 15 轮的模型.因为 ESF 算法 S 盒的最优差分概率是 2^{-2},估计全轮$(32=15+15+2)$的 ESF 最大差分概率是$(2^{-2})^{19+19+1}=2^{-78}$,小于暴力搜索成功的概率 2^{-64}.因而,我们证明 ESF 对单密钥差分攻击是安全的.

3.2　ESF 算法线性分析结果

建立 r 轮 ESF 算法的线性 MILP 模型,对于 r 轮 ESF 算法,线性 MILP 模型有 $421r+1$ 个不等式、$104r+64$ 个变量.ESF 算法前 16 轮在单密钥情形下线性活跃 S 盒数量的下界,如表 7 所示.

从表 7 可知,对于 16 轮的 ESF 算法最小线性活跃 S 盒数量是 15.对于超过 16 轮的模型,跟 ESF 算法差分分析一样,由于求解模型花费的时间关系(超过 12 d),我们只考虑前 16 轮的模型.因为 ESF 算法 S 盒的最大线性偏差为 $\varepsilon=\pm 2^{-2}$,估计全轮$(32=16+16)$的 ESF 最小活跃 S 盒数量为 30(实际的大于 30),由堆积引理[6],最大线性偏差的平方为

$\varepsilon^2=2^{-58}$,那么对全轮的线性攻击需要已知的明文量约为 2^{58},小于暴力搜索需要的明文量 2^{64}. 但是,实际所需要的明文量肯定比 2^{58} 大,是否存在全轮活跃 S 盒数小于 32 的线性路径仍然不能确定. 因而,对于证明全轮 ESF 是否抵抗线性攻击仍然是一个开放问题.

Table 7 The Results for Linear Analysis on ESF

表 7 ESF 算法线性分析结果

Rounds	# Active S-Boxes	Rounds	# Active S-Boxes
1	0	9	7
2	1	10	8
3	2	11	9
4	2	12	10
5	3	13	11
6	4	14	13
7	5	15	14
8	6	16	15

3.3 ESF 算法不可能差分分析结果

根据 2.4 节自动化搜索不可能差分方法,建立 r 轮 ESF 算法的不可能差分 MILP 模型. 即在相应的差分 MILP 模型的基础上增加 2 个约束,分别将输入和输出差分的 1 个半字节位置固定为常数,其他位置为 0,并计算模型是否有解,总共需要遍历 $(16\times16)^2=2^{16}$ 种情形. 共搜索到 2 108 条 9 轮 ESF 的不可能差分,没有搜索到 10 轮的不可能差分. 其中 7 条如下所示(输入输出数值用 16 进制表示):

(0100000000000000)↛(1000000000000000),
(0100000000000000)↛(4000000000000000),
(0100000000000000)↛(5000000000000000),
(0100000000000000)↛(8000000000000000),
(0100000000000000)↛(9000000000000000),
(0100000000000000)↛(C000000000000000),
(0100000000000000)↛(D000000000000000).

3.4 ESF 算法零相关线性逼近分析结果

根据 2.5 节自动化搜索零相关线性逼近的方法,建立 r 轮 ESF 算法的零相关线性逼近 MILP 模型,对于每轮的 MILP 模型,分别在相应的线性 MILP 模型基础上增加了 2 个约束,分别是固定输入和输出掩码的 1 个比特位置为 1,其他位全为 0,总共需要遍历 $64^2=4096$ 种情形. 共搜索到 925 条 8 轮的零相关线性逼近,在此条件下,没有搜索到 9 轮的零相关线性逼近. 其中的 7 条如下所示(输入输出数值用 16 进制表示):

(0000000080000000)↛(4000000000000000),
(0000000000800000)↛(0000040000000000),
(0000000000000100)↛(8000000000000000),
(0000000000000020)↛(0000100000000000),
(0000000000000001)↛(0000400000000000),
(0000000000000001)↛(0000040000000000),
(0000000000000001)↛(0000000100000000).

4 结束语

在本文中,基于 Sun 等人给出的差分和线性自动化搜索方法,根据 Sasaki 等人改进的 XOR 操作约束和我们改进的 S 盒相应的约束,进一步精炼 MILP 模型,减少了 ESF 算法产生 MILP 模型的变量和约束数量,使得 MILP 问题的求解更加高效. 我们将优化的 MILP 模型应用到轻量级分组密码算法 ESF,在单密钥情形下成功获取了减轮 ESF 算法的差分和线性最小活跃 S 盒数量,并搜索到最长的不可能差分和零相关线性区分器. 同时,证明了全轮 ESF 足够抵抗差分攻击,然而对于证明全轮 ESF 是否抵抗线性攻击仍然是一个开放问题.

参 考 文 献

[1] Wu Wenling, Zhang Lei. LBlock: A lightweight block cipher [G] //LNCS 6715: Proc of the 9th Int Conf on Applied Cryptography and Network Security (ACNS 2011). Berlin: Springer, 2011: 327-344

[2] Bogdanov A, Knudsen L R, Leander G, et al. PRESENT: An ultra-lightweight block cipher [G] //LNCS 4727: Proc of the 9th Int Workshop on Cryptographic Hardware and Embedded Systems (CHES 2007). Berlin: Springer, 2007: 450-466

[3] Beierle C, Jean J, Kölbl S, et al. The SKINNY family of block ciphers and its low-latency variant MANTIS [G] // LNCS 9815: Advances in Cryptology (CRYPTO 2016). Berlin: Springer, 2016: 123-153

[4] Zhang Wentao, Bao Zhenzhen, Lin Dongdai, et al. RECTANGLE: A bit-slice lightweight block cipher suitable for multiple platforms [J]. Science China Information Sciences, 2015, 58(12): 1-15

[5] Biham E, Shamir A. Differential cryptanalysis of DES-like cryptosystems [G] //LNCS 537: Advances in Cryptology (CRYPT0 1990). Berlin: Springer, 1990: 2-21

[6] Matsui M. Linear cryptanalysis method for DES cipher [G] //LNCS 765: Advances in Cryptology (EUROCRYPT 1993). Berlin: Springer, 1993: 386-397

[7] Biham E, Biryukov A, Shamir A. Cryptanalysis of skipjack reduced to 31 rounds using impossible differentials [G] // LNCS 1592: Advances in Cryptology (EUROCRYPT 1999). Berlin: Springer, 1999: 12-23

[8] Bogdanov A, Rijmen V. Linear hulls with correlation zero and linear cryptanalysis of block ciphers [J]. Designs Codes & Cryptography, 2014, 70(3): 369-383

[9] Matsui M. On correlation between the order of S-boxes and the strength of DES [G] //LNCS 950: Advances in Cryptology (EUROCRYPT 1994). Berlin: Springer, 1994: 366-375

[10] Mouha N, Preneel B. Towards finding optimal differential characteristics for ARX: Application to Salsa20 [EB/OL]. [2017-06-11]. http://eprint.iacr.org/2013/328.

[11] Mouha N, Wang Qingju, Gu Dawu, et al. Differential and linear cryptanalysis using mixed-integer linear programming [G] //LNCS 7537: Proc of the 7th Int Conf on Information Security and Cryptology (Inscrypt 2011). Berlin: Springer, 2011: 57-76

[12] Sun Siwei, Hu Lei, Wang Peng, et al. Automatic security evaluation and (related-key) differential characteristic search: Application to SIMON, PRESENT, LBlock, DES (L) and other bit-oriented block ciphers [G] //LNCS 8873: Advances in Cryptology (ASIACRYPT 2014). Berlin: Springer, 2014: 158-178

[13] Cui Tingting, Jia Keting, Fu Kai, et al. New automatic search tool for impossible differentials and zero-correlation linear approximations [EB/OL]. [2017-06-08]. https://eprint.iacr.org/2016/689

[14] Sasaki Y, Todo Y. New impossible differential search tool from design and cryptanalysis aspects [G] //LNCS 10212: Advances in Cryptology (EUROCRYPT 2017). Berlin: Springer, 2017: 185-215

[15] Liu Xuan, Zhang Wenying, Liu Xiangzhong, et al. Eight-sided fortress: A lightweight block cipher [J]. Journal of China Universities of Posts and Telecommunications, 2014, 21(1): 104-108

[16] Liu Xuan, Liu Feng, Meng Shuai. Impossible differential cryptanalysis of lightweight block cipher ESF [J]. Computer Engineering & Science, 2013, 35(9): 89-93 (in Chinese)
(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)

[17] Chen Yulei, Wei Hongru. Impossible differential cryptanalysis of ESF [J]. Computer Science, 2016, 43(8): 89-91 (in Chinese)
(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)

[18] Gurobi. Gurobi optimizer reference manual [EB/OL]. [2017-06-03]. http://www.gurobi.com

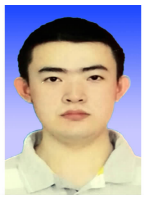
[19] IBM. User-Manual CPLEX 12 [EB/OL]. [2017-06-03]. https://www-01.ibm.com/software/commerce/optimization/cplex-optimizer/index.html

[20] Computational Algebra Group. School of Mathematics and Statistics, University of Sydney: Magma Computational Algebra System [EB/OL]. [2017-06-03]. http://magma.maths.usyd.edu.au

[21] Sun Siwei, Hu Lei, Song Lin, et al. Automatic security evaluation of block ciphers with S-bP structures against related-key differential attacks [G] //LNCS 8567: Proc of the 9th Int Conf on Information Security and Cryptology (Inscrypt 2013). Berlin: Springer, 2013: 39-51

[22] Stein W. Sage Tutorial v8.0 [EB/OL]. [2017-05-23]. http://doc.sagemath.org/html/en/tutorial/tour.html

Yin Jun, born in 1993. Master candidate. His main research interests include automatic analysis of cryptographic algorithms.



Ma Chuyan, born in 1994. Master candidate. His main research interests include automatic analysis of block ciphers.

Song Jian, born in 1993. Master candidate. His main research interests include security analysis of cryptographic protocols.

Zeng Guang, born in 1980. PhD, associate professor. His main research interests include security analysis of Hash function.

Ma Chuangui, born in 1962. Professor and PhD supervisor. His main research interests include network and information security.