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

杜小妮 段娥娥* 王天心
(西北师范大学数学与统计学院 兰州 730070)

摘 要：该文对基于混沌的双模块Feistel结构(CFE)高安全性高速分组算法的安全性进行了分析。分析结果表明，算法不适合用积分攻击、中间相遇攻击、不变量攻击、插值攻击和循环移位攻击分析其安全性；可以抵抗相关密钥攻击；更进一步地构造出了5轮不可能差分特征链，并利用其进行区分攻击；求得算法的活性S盒下界为6，概率约为2^{-21}；算法存在5轮零相关线性特征。

关键词：混沌密码；差分活性S盒；不可能差分攻击；区分攻击；零相关线性攻击
中图分类号：TN918.4 **文献标识码**：A **文章编号**：1009-5896(2021)05-1365-07
DOI: 10.11999/JEIT200057

Security Analysis of Block Cipher CFE

DU Xiaoni DUAN Ee WANG Tianxin
(*College of Mathematics and Statistics, Northwest Normal University, Lanzhou* 730070, *China*)

Abstract: The security of high security and high speed block cipher algorithm of two-module FEistel structure based on Chaos (CFE) is analyzed. The results show that the cipher is not suitable to use integral attack, meat-in-the-middle attack, invariant attack, interpolation attack and circle shift attack to analyze its security. And it can resist the related-key attack. Furthermore, 5 rounds of impossible differential characteristic are constructed and used to distinguish attacks. The lower bound of the active S-box is 6, and the probability is about 2^{-21}. There are 5 rounds of linear characteristic with zero-correlation.

Key words: Chaos cipher; Differential active S-box; Impossible differential attack; Distinguish attack; Zero-correlation linear attack

1 引言

分组密码是密码学的一个重要分支，在保护数据安全方面有着重要的地位，随着1977年DES分组密码算法的公开，开启了分组密码分析的新时代。影响分组密码方案的安全因素有多种，如分组长度以及密钥长度等。分析密码安全性主要包括分析算法的部件性质和分析算法的安全性。算法的部件性质分析主要包括分析算法的结构、S盒、线性层和密钥扩展方案。对于算法的安全性分析主要包括1990年文献[1]针对DES提出的差分攻击，1993年Matsui针对DES提出的线性攻击，计算活性S盒个数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，此外还有不可能差分分析、零相关线性分析、积分攻击、中间相遇攻击、插值攻击、相关密钥攻击、循环移位攻击和不变量攻击等多种攻击方法。

2019年2月中国密码学会启动了分组密码算法设计竞赛活动(http://www.icaisconf.com/)。基于混沌的双模块Feistel结构高安全性高速(high security and high speed block cipher algorithm of two-module FEistel structure based on Chaos, CFE)分组密码算法是参加竞赛的29个分组密码算法之一。该分组密码算法的明文分组支持128位和256位两种模式，加密轮数为5轮。算法使用密钥生成非线性组件S盒，利用明文参与非线性部件的选择，线性变换选用滚动正向加和逆向加策略实现信息扩散。算法设计中先随机选取种子密钥，将其通过混沌迭代系统生成序列，再利用序列构造密码算法的非线性S盒，此设计使得分析者进行密码攻击时，不能将编码环节作为已知因素来构造基于已知S盒的差分和线性分析；非线性S盒受1 bit轮输入因素控制，动态可变，使得分析者不能基于传统的固定编码环节分析方法进行密码攻击。

CFE设计文档给出了5轮差分密码分析活性S盒

收稿日期：2020-01-14；改回日期：2020-11-23；网络出版：2020-12-03
*通信作者： 段娥娥 eeduan@126.com
基金项目：国家自然科学基金(61772022)
Foundation Item: The National Natural Science Foundation of China (61772022)

个数的下界为14，并指出不存在弱密钥。本文针对候选算法CFE的密码部件的性质进行了分析，并研究了算法的安全性，给出了1到5轮最小活性S盒的个数以及概率，构造了5轮不可能差分特征链并利用其进行了区分攻击并讨论了算法5轮零相关线性特征。

本文结构如下，第2节对密码算法进行描述，第3节讨论密码结构和部件的安全性，第4节对密码算法安全性进行分析，第5节总结全文。

2 CFE分组密码算法概述

算法中使用的是一类时空混沌系统，其定义为

$$x_{n+1}(i)=(1-\varepsilon)\,f(x_n(i))+\varepsilon f(x_n(i-1)) \tag{1}$$

式中，$n=0,1,\cdots,N$为离散时间坐标，$x_n(i)$表示第i个格点在时刻n的状态值，$i=0,1,\cdots,L-1$，其中L表示格子的数目，ε为耦合强度，且式(1)的边界条件为$x_n(i+L)=x_n(i)$，子系统f采用Logistic映射，即

$$f(x_n(i))=4x_n(i)(1-x_n(i)) \tag{2}$$

(1) 首先利用时空混沌系统产生序列

(a)将密钥K转为混沌初始值$x_0=(x_0(0),x_0(1),\cdots,x_0(7))$, x_0为双精度浮点数。转化规则为

$$\left.\begin{aligned} x_0(i)&=\frac{K(i)+1}{2^{48}+21}\times\frac{1}{2},\ i=0\\ x_0(i)&=\frac{K(i)+1}{2^{48}+1}\times\frac{1}{2},\ i=1,2,\cdots,7\end{aligned}\right\} \tag{3}$$

(b) 将步骤(a)得到的x_0作为初始值，代入式(1)迭代n_0+n次，其中系统参数$\varepsilon=0.2$, $L=8$；

(c) 抛弃前n_0次的状态值，保存后n次的状态值并记为SeqM，其大小为$n\times 8$。

(2) 其次生成密钥流和子密钥

(a) SeqM转为向量**SeqV**，其大小为$8n$；

(b) 将**SeqV**转为8 bit的密钥流序列的规则为

$$\mathrm{KS}=\mathrm{floor}(\mathbf{SeqV}\times 10^{15})\ \bmod\ 256 \tag{4}$$

(c) 取**SeqV**的前n_{ks}个元素作为子密钥，$\mathbf{SK}=\mathbf{SeqV}(0:n_{\mathrm{ks}}-1)$。

(3) 最后生成S盒

(a) 初始化：S1和S2按行赋值$(0,1,\cdots,255)$；

(b) 构造两个16×16的随机矩阵**RM**1和**RM**2：分别取KS连续的256个元素，令$\mathrm{RV1}=\mathrm{KS}(n_{\mathrm{ks}},n_{\mathrm{ks}}+255)$; $\mathrm{RV2}=\mathrm{KS}(n_{\mathrm{ks}}+256,n_{\mathrm{ks}}+511)$，将两者逐行扫描转为$16\times 16$的随机矩阵**RM**1和**RM**2；

(c) 利用**RM**1和**RM**2随机化初始的S1和S2：为了达到这一目标，依次取**RM**1(**RM**2)的每一个位置(k,l)上的元素的最高4位和最低4位表示为另一个位置(i,j)，其中$k=0,1,\cdots,F$; $l=0,1,\cdots,F$，然后对应的将$S1(S2)$位置(k,l)上的数和(i,j)上的数进行交换，按顺序进行256次交换即可。

(4) 加密过程：与明文的两种模式相对应的密文$\boldsymbol{C}$的对应输出为128 bit和256 bit。如图1所示，方案基于Feistel网络进行了5轮加密。轮函数F的设计是本方案的特色，见图2, $F(\boldsymbol{R}0,\mathrm{SK1})$的处理过程如下

(a) 计算$\boldsymbol{R}0$特征码：$\boldsymbol{R}0=[R0(0),R0(1),\cdots,R0(7)]$，将其异或取最低位得到特征码$v$，即

$$\left.\begin{aligned}&\mathrm{tmp}=R0(0)\oplus R0(1)\oplus\cdots\oplus R0(7)\\ &v=\mathrm{tmp}\ \bmod 2\end{aligned}\right\} \tag{5}$$

(b) 正向扩散：将**SK**1表示为字节向量$\mathbf{SK}1=[\mathrm{SK1}(0),\mathrm{SK1}(1),\cdots,\mathrm{SK1}(15)]$。扩散规则如下

$$\left.\begin{aligned}\mathrm{CR0}'(i)&=R0(i)\oplus\mathrm{SK1}(i),\\ &\quad i=0\\ \mathrm{CR0}'(i)&=R0(i)\oplus\mathrm{SK1}(i)\oplus\mathrm{CR0}'(i-1),\\ &\quad i=1,2,\cdots,7\end{aligned}\right\} \tag{6}$$

(c) 逆向扩散：扩散规则如下

$$\left.\begin{aligned}\mathrm{CR0}(i)&=\mathrm{CR0}'(i)\oplus\mathrm{SK1}(i+8),\\ &\quad i=7\\ \mathrm{CR0}(i)&=\mathrm{CR0}'(i)\oplus\mathrm{SK1}(i+8)\oplus\mathrm{CR0}(i+1),\\ &\quad i=6,5,\cdots,0\end{aligned}\right\} \tag{7}$$

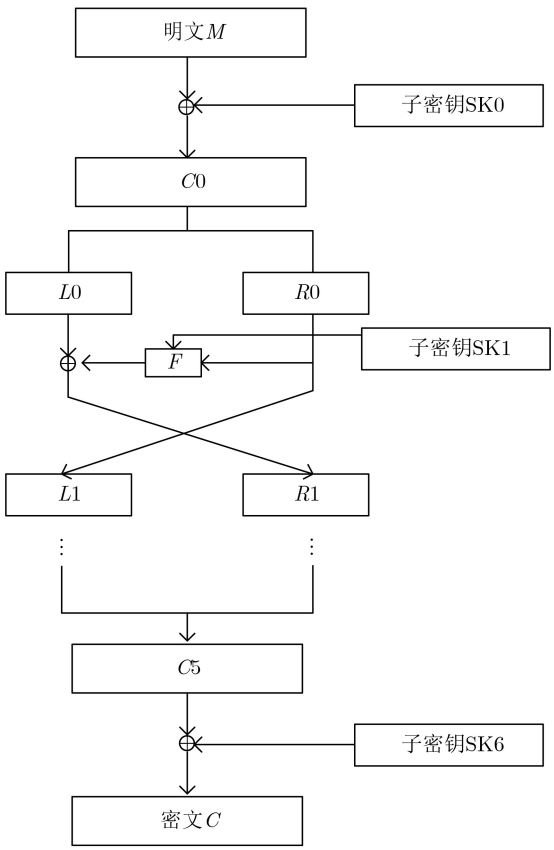

图 1 结构图

(d) S盒选择与替换：若v=0选择S1，否则选择S2；根据得到的S盒，将CR0(i) ($i=0,1,\cdots,7$)进行S盒查表替换，即完成函数F的处理过程。

(5) 解密过程：由于本方案的结构严格对称，因此解密过程需将密钥顺序进行调整，并使用逆向Feistel网络完成解密。

3　密码结构和密码部件安全性分析

(1) 密码结构安全性。该密码算法总体结构为Feistel结构，迭代5轮，但轮函数动态可变。

(2) 密码部件性质分析。S盒：S盒是基于混沌系统构造的，且随着种子密钥的不同而不同，并且S盒不公开，这是依赖于密钥的S盒的一个很大的优点，所以事先分析S盒以寻找弱点加以攻击是不可能的。

本部分针对随机选取的一个S盒，其参数为

$$K=[16\,\mathrm{ef\,bf\,bd}\,61\,\mathrm{ef\,bf\,bd}\,36\,\mathrm{ef\,bf\,bd}\,65\,74\,56\,13],\quad \varepsilon=0.2,\ n_0=500 \tag{8}$$

经分析，其满足双射性和严格雪崩准则[2]。但是因为S盒由混沌系统构造，所以其具体密码学性质[3]，如差分均匀度和线性度并不明确。

P置换：P置换为一个线性变换，起到信息扩散作用。算法的线性变换由正向扩散和逆向扩散两部分组成，具体扩散过程见式(6)和式(7)。针对扩散过程可得明文线性变换$\boldsymbol{T}$和密钥线性变换$\boldsymbol{W}$分别为

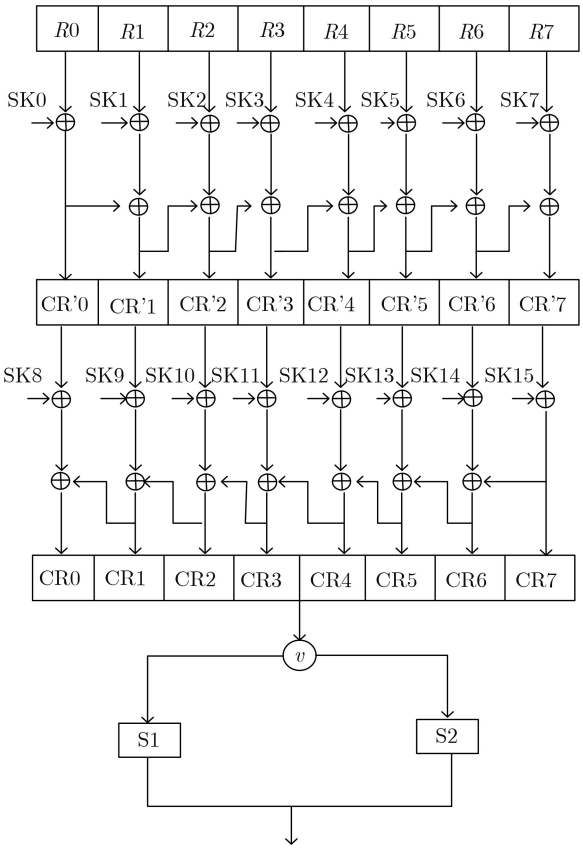

图 2 轮函数

$$\boldsymbol{T}=\begin{pmatrix}0&1&0&1&0&1&0&1\\1&1&0&1&0&1&0&1\\0&0&0&1&0&1&0&1\\1&1&1&1&0&1&0&1\\0&0&0&0&0&1&0&1\\1&1&1&1&1&1&0&1\\0&0&0&0&0&0&0&1\\1&1&1&1&1&1&1&1\end{pmatrix}_{8\times8},\ \boldsymbol{W}=\begin{pmatrix}0&1&0&1&0&1&0&1&1&1&1&1&1&1&1&1\\1&1&0&1&0&1&0&1&0&1&1&1&1&1&1&1\\0&0&0&1&0&1&0&1&0&0&1&1&1&1&1&1\\1&1&1&1&0&1&0&1&0&0&0&1&1&1&1&1\\0&0&0&0&0&1&0&1&0&0&0&0&1&1&1&1\\1&1&1&1&1&1&0&1&0&0&0&0&0&1&1&1\\0&0&0&0&0&0&0&1&0&0&0&0&0&0&1&1\\1&1&1&1&1&1&1&1&0&0&0&0&0&0&0&1\end{pmatrix}_{8\times16} \tag{9}$$

且

$$P(Ri,\mathrm{SK}i{+}1)=\boldsymbol{T}(Ri)\oplus\boldsymbol{W}(\mathrm{SK}i{+}1) \tag{10}$$

对线性变换环节分析得，偶数S盒的各输入字节仅含有输入的奇数位字节信息，与偶数位字节信息无关。

轮函数：轮函数由线性变换P和S盒查表组成，由于每轮只有1 bit控制S盒的选择，整个算法只有5轮，所以共有$2^5=32$种S盒的使用方式。

密钥扩展算法：密钥扩展算法在n_0, n不确定的情况下，存在平移等价密钥，这由混沌序列的性质所决定。

4　密码算法安全性分析

这里只对128 bit的CFE算法详细叙述其分析过程并给出结果，而256 bit的算法有类似的分析过程与结果。

4.1　差分攻击

评估一个分组密码算法抗差分攻击能力的常用方法是估计其差分活性S盒个数的下界[4]。差分活性S盒个数越多，对应的差分特征概率越小。因此，差分活性S盒个数的下界体现了差分特征概率的上界，若差分特征概率的上界小于某个标准，则该算法具有抵抗差分攻击的能力。

性质1　CFE分组算法的差分活性S盒个数下界见表1。

表 1　差分活性S盒个数下界

轮数	1	2	3	4	5
128/256 bit	0	2	3	5	6

证明 以128 bit为例取5轮差分特征$(0000\alpha000,00000000)\to(00000\beta0\beta,0000\alpha0\gamma0)$，记$\Delta\mathrm{CR}i$, ΔYi, $i=1,2,\cdots,5$为S盒的输入输出差分，且每轮取特征码相同的概率为2^{-1}。

第1轮：活性S盒为0个，其中$\Delta\mathrm{CR}1=0$, $\Delta Y1=0$, $\Delta R1=\Delta L0\oplus\Delta Y1=\Delta L0$, $\Delta L1=\Delta R0$。

第2轮：活性S盒为2个，其中$\Delta\mathrm{CR}2=(0,0,0,0,0,\alpha,0,\alpha)$, $\Delta Y2=(0,0,0,0,0,\Delta Y2(5),0,\Delta Y2(7))$, $\Delta R2=\Delta L1\oplus\Delta Y2=\Delta Y2$, $\Delta L2=\Delta R1$。

第3轮：活性S盒为1个，其中$\Delta Y2(5)=\Delta Y2(7)$的概率为$2^{-8}$, $\Delta\mathrm{CR}3=(0,0,0,0,0,0,\Delta Y2(7),0)$, $\Delta Y3=(0,0,0,0,0,0,\Delta Y3(6),0)$, $\Delta R3=\Delta L2\oplus\Delta Y3=(0,0,0,0,\alpha,0,\Delta Y3(6),0)$, $\Delta L3=\Delta R2$。

第4轮：活性S盒为2个，其中α取定，$\Delta Y3(6)$有254种取法，则$\alpha\neq\Delta Y3(6)$的概率为$254/255=2^{-0.0050}$，且$\Delta\mathrm{CR}4=(0,0,0,0,0,\alpha\oplus\Delta Y3(6),0,\Delta Y3(6))$, $\Delta Y4=(0,0,0,0,0,\Delta Y4(5),0,\Delta Y4(7))$, $\Delta L4=\Delta R3$, $\Delta R4=\Delta L3\oplus\Delta Y4=(0,0,0,0,0,\Delta Y2(5)\oplus\Delta Y4(5),0,\Delta Y2(7)\oplus\Delta Y4(7))$。

第5轮：活性S盒为1个。由于使用的S盒是双射，且两个S盒输入的字节有1bit不同，则输出不同。因为数字化的混沌序列输出的是均匀分布的伪随机数，其值为$1,2,\cdots,255$，那么$\Delta Y2(5)=\Delta Y2(7)\neq0$完全相同的概率为$1/255=2^{-7.9943}$。故$\Delta Y2(5)\oplus\Delta Y4(5)=\Delta Y2(7)\oplus\Delta Y4(7)$的概率为$2^{-7.9943}$，则有$\Delta\mathrm{CR}5=(0,0,0,0,0,0,\Delta Y2(7)\oplus\Delta Y4(7),0)$。

综上，获得差分活性S盒个数为6的概率约为$2^{-21}\doteq(2^{-1})^5\times2^{-8}\times2^{-0.0050}\times2^{-7.9943}$。 证毕

需要说明的是，方案的提交者给出的活性S盒的下界个数为14，应该有误。

4.2 不可能差分攻击

在不可能差分分析[5,6]中，攻击者利用不可能出现的输入输出差分模式排除错误密钥，从而缩小密钥的搜索空间。为此，本文构造5轮不可能差分特征如下。

性质2 若$\alpha=(0,0,0,\alpha_1,0,0,0,0)$, $\alpha_1=\varepsilon_10$, ε_1为α_1的非零高7 bit，$\gamma=(0,0,0,0,0,0,0,\gamma_1)$, $\gamma_1=\varepsilon_20$, ε_2为γ_1的非零高7 bit，则$(\alpha,0)\xrightarrow{5}(0,\gamma)$是5轮不可能差分(见图3)。

证明 在加密方向，取明文的输入差分为$(\alpha,0)$，于是第1轮的输出密文差分为$(0,\alpha)$；

第2轮进入非线性层的输入差分为$(0,0,0,0,0,\alpha_1,0,\alpha_1)$，第2轮的输出密文差分为$(\alpha,\beta)$，其中$\beta=(0,0,0,0,0,S^5(\alpha_1),0,S^7(\alpha_1))$，且有$S^i(\alpha_1)\neq0$, $i=5,7$；

第3轮输入的右半部分为β；

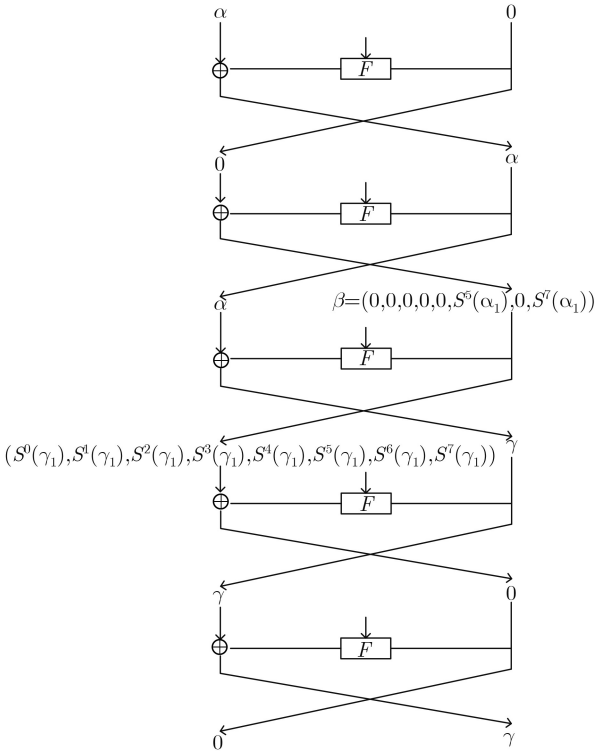

图 3 5轮不可能差分特征图

在解密方向，选择密文差分$(0,\gamma)$，则第5轮的输入差分为$(\gamma,0)$；

第4轮进入轮函数非线性层的输入差分为$\delta=(\gamma_1,\gamma_1,\gamma_1,\gamma_1,\gamma_1,\gamma_1,\gamma_1,\gamma_1)$，输出差分应为

$$(S^0(\gamma_1),S^1(\gamma_1),\cdots,S^6(\gamma_1),S^7(\gamma_1)) \tag{11}$$

事实上，对明文差为$(\alpha,0)$，密文差为$(0,\gamma)$，应有

$$\begin{aligned}&(0,0,0,0,0,S^5(\alpha_1),0,S^7(\alpha_1))=\beta\\&=(S^0(\gamma_1),S^1(\gamma_1),\cdots,S^6(\gamma_1),S^7(\gamma_1))\end{aligned} \tag{12}$$

然而，由于$\gamma_1=\varepsilon_20\neq0$，两个不同的明文所取的S盒相同，必有$S^i(\gamma_1)\neq0, i=0,1,2,3,4,6$，故矛盾。证毕

注意：不可能差分路径不唯一，如取α为$(0,\alpha_1,0,\alpha_1,0,\alpha_1,0,\alpha_1)$, α_1的含义如上时亦为另一条不可能差分路径，此处不再一一列举。

根据以上分析，可以进一步作区分攻击：设m_0和m_1对应的密文分别为c_0和c_1。明文(m_0^1,m_1^1)与(m_0,m_1)存在关系

$$m_0\oplus m_0^1=(0,0,0,\alpha_1,0,0,0,0)\neq m_0\oplus m_1^1 \tag{13}$$

其中，$\alpha_1=\varepsilon_10$, ε_1为α_1的非零高7 bit。现有密文c，仅知道它对应的明文是m_0^1和m_1^1其中之一。此时，若$c_0\oplus c=(0,0,0,0,0,0,0,\gamma_1)$, $\gamma_1=\varepsilon_20$, ε_2为γ_1的非零高7 bit，则可判定c不是m_0^1对应的密文，而是m_1^1对应的密文，攻击成功。

4.3 零相关线性分析

零相关线性分析[7,8]利用相关度为零的线性逼

近来区分分组密码算法与随机置换。基于相关度为零的线性逼近表达式进行密钥恢复。

性质 3　若输入掩码模式为$(\alpha,0)\to(0,\beta)$，其中

$$\alpha=(0,0,0,0,0,0,\alpha',0),\quad \beta=(0,0,0,0,0,0,0,\beta') \tag{14}$$

且α', β'的高7 bit非零，则CFE算法存在5轮零相关线性特征。具体区分器如图4所示。

证明　如图4所示，给定输入掩码模式为$(\alpha,0)$且α'的高7 bit非零时，第3轮右边输出的前7 Byte肯定非零；而在给定输出掩码模式为$(0,\beta)$且β'的高7 bit非零时，第3轮右边输出的前7 Byte为零，矛盾，因此CFE算法存在5轮零相关线性特征。证毕

4.4 积分攻击

积分攻击[9,10]的主要目的是找到特定的集合$\boldsymbol{V}=\{0,1\}^n$，对于相应的密文$c(x)(x\in\boldsymbol{V})$，计算相应的积分值$\int_V c\mathrm{d}v=\sum_{x\in\boldsymbol{V}}c(x)$。如果对某些特殊形式的明文对应的密文$C_i$能确定$\sum C_i$的值，那么可以将这个算法与随机置换区分。

图5中空格代表平衡值，α代表活跃值，β代表稳定值，γ代表不确定值。根据算法可得

$$L3=L5\oplus\boldsymbol{T}^{-1}(S^{-1}(R3)\oplus\boldsymbol{W}(\mathrm{SK4})) \tag{15}$$

即要得到$L3(x)$还需知道$R3$和SK4，由3轮积分区分器可知

$$\sum_x L3^{(i)}(x)=\sum_x(L5^{(i)}\oplus\boldsymbol{T}^{-1}(S(R3^{(i)})\oplus\boldsymbol{W}(\mathrm{SK4}))^{(i)})=0,\ i=0,1,\cdots,6 \tag{16}$$

因此，利用上述3轮积分区分器对5轮算法实施攻击时，需猜测$L3$和SK4两个值。若式(16)成立，则$L3$和SK4为正确猜测值。

但是S盒由混沌系统生成，属于不确定元素，所以对CFE分组密码算法做积分攻击较困难。

4.5 中间相遇攻击

构造中间相遇区分器[11,12]的基本思想是给定一组满足一定条件的明文集(δ-集)作为输入，考察明文集经密码函数(随机置换)加密后，按明文集次序截取对应输出密文集固定位置的取值构成一个有序序列，根据该序列可取值范围随密码函数和随机置换的不同，将密码函数与随机置换区分。

为方便讨论，做出如下规定：记第i轮第j路的输入为$X_{i,j}$，输出为$Y_{i,j}$，输入差分为$\Delta X_{i,j}$，输出差分为$\Delta Y_{i,j}$，其中$1\le i\le 5,1\le j\le 2$。记第i轮的F函数F_i的输入为F_i^{I}，输出为F_i^{O}，输入差分为ΔF_i^{I}，输出差分为ΔF_i^{O}。令

$$F^{\Delta}:(\{0,1\}^{128},\{0,1\}^{64})\to\{0,1\}^{64} \tag{17}$$

再定义

$$F^{\Delta}(m,\delta)=\mathrm{Trunc}_{64}(F(m)\oplus F(m\oplus(\delta,0))) \tag{18}$$

其中，Trunc_{64}代表高64 bit的截断差分。

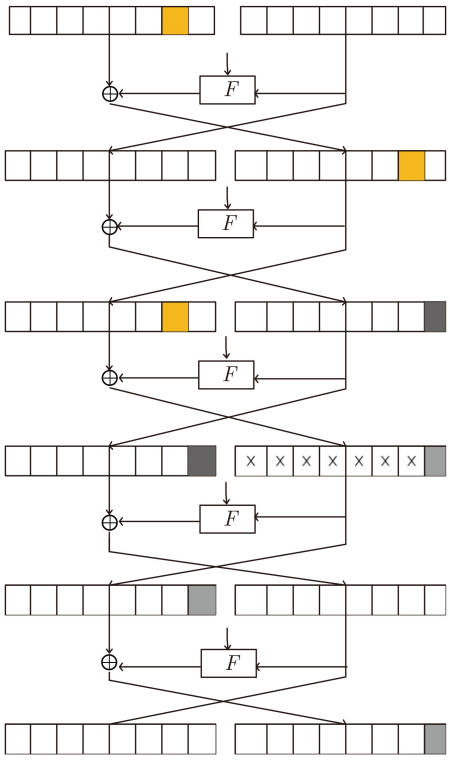

图 4 5轮零相关线性区分器

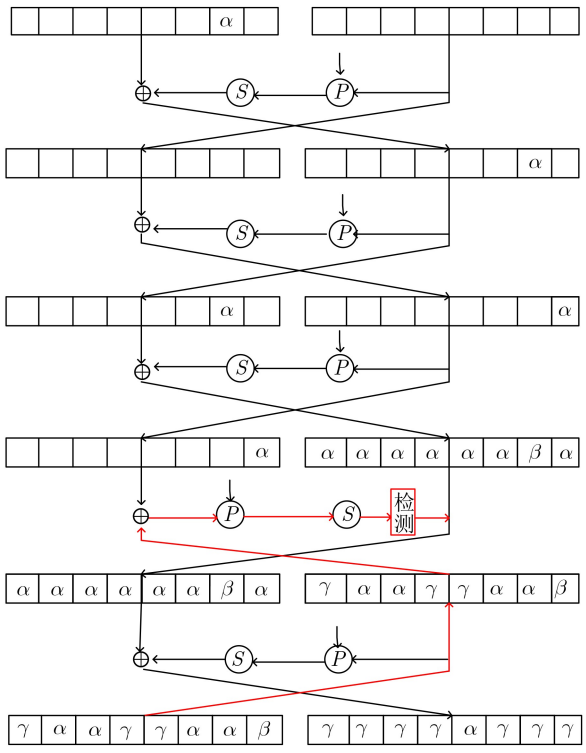

图 5 积分攻击

如图6，构造5轮中间相遇区分器。设$A,C\in\{0,1\}^{64}\backslash\{0\}$，对输入差分为$(A,0)$且输出差分为$(C,?)$的明文对$(m,m')$，$A$的取值有$2^8-1$种可能，$C$的取值有$2^{64}-1$种可能。若$A_1=\Delta F_2^{\mathrm{O}},B$的值确定，那么可给出式(19)的3个差分方程。由于A_1最多只能取2^8-1个不同的值，B最多只能取$2^{64}-1$个不同的值，所以最多可取$2^{64}-1$个不同的差分方程簇

$$\left.\begin{aligned}&\Delta F_2(A)=A_1\\&\Delta F_3(A_1)=A\oplus B\\&\Delta F_4(B)=A_1\oplus C\end{aligned}\right\}\tag{19}$$

进而可求出$(F_2^{\mathrm{I}},F_3^{\mathrm{I}},F_4^{\mathrm{I}})$的所有可能值。一个$(F_2^{\mathrm{I}},F_3^{\mathrm{I}},F_4^{\mathrm{I}})$的一组取值对应于一个序列$(F^{\Delta}(m,1),F^{\Delta}(m,2),\cdots,F^{\Delta}(m,b))$，$(2<b<2^8-1)$，所以最多有$2^{64}-1$个与明文$(m,m')$无关的可能的序列，且其值仅由$A,C$的值决定。

由上述推导可知第1轮的子密钥为$\mathrm{SK1}=\boldsymbol{W}^{-1}(S(F_1^{\mathrm{O}})\oplus\boldsymbol{T}(F_1^{\mathrm{I}}))$，但是S盒不确定，故恢复密钥比较困难。

4.6 其他攻击

插值攻击：插值攻击[13]实质上是一种代数方法，其基本思想是将密文看作明文的多项式函数，然后通过研究多项式性质来分析一个加密算法所具有的密码学性质。插值攻击一般对那些轮函数次数比较低且具有比较紧凑的表达式的密码算法有效。因为CFE算法轮函数的S盒性质不确定，故明文和密文之间的多项式函数的次数不确定，所以用插值攻击分析比较困难。

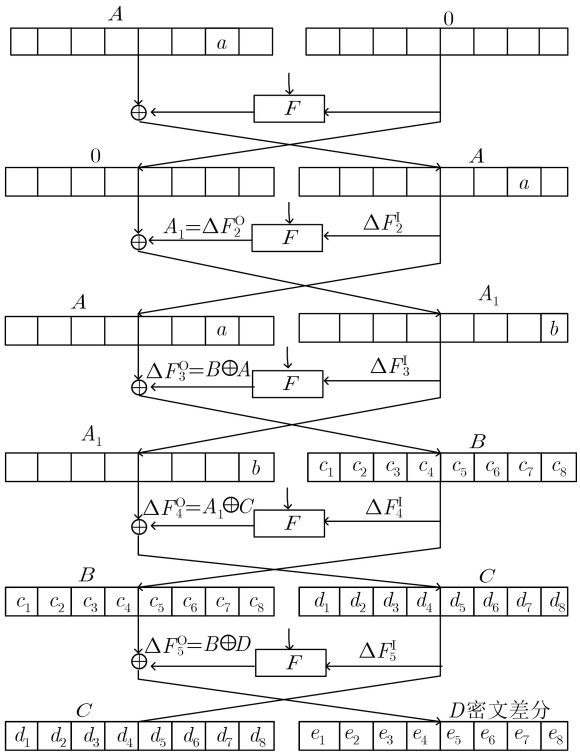

图 6 5轮中间相遇区分器

相关密钥攻击：在相关密钥[14]模型下，攻击者能够通过某种方式获得明文及其在某些未知密钥下所对应的密文。攻击者虽不知道这些密钥的具体值，但知道甚至可以选取这些密钥之间的关系。由于在CFE密钥扩展算法中，每轮的轮子密钥由混沌序列生成，排列方式与取值都不同且无法确定，所以两个轮子密钥之间没有关系，故无法确定或选取这些密钥之间的关系，该算法可以抗击相关密钥攻击。

循环移位攻击：循环移位攻击对于要考察的密码函数$\boldsymbol{F}$，首先寻找满足$F(\overleftarrow{X})=\overleftarrow{F(X)}$的旋转对$(X,\overleftarrow{X})$然后利用旋转对的性质进行区分攻击、密钥恢复攻击和原象攻击，其中运算符“$\leftarrow$”是某种移位变换。而在CFE算法中，S盒的选取由明文决定，且由混沌系统所生成，其性质不确定，所以很难找到满足$F(\overleftarrow{X})=\overleftarrow{F(X)}$的旋转对，故对CFE算法做循环移位攻击较困难。

不变量分析：非线性不变函数[15]：给定分组密码$E_k:\{0,1\}^n\to\{0,1\}^n$，如果存在一个可以有效计算的非线性布尔函数$g:\{0,1\}^n\to\{0,1\}$使得$g(P)\oplus g(E_k(P))$对任意明文$P$和一些密钥$k$成立，则称函数$g$是$E_k$的非线性不变函数。由于CFE算法的S盒性质未知，非线性不变函数g很难求得，所以对CFE算法做不变量分析较困难。

5 类似结构的混沌密码分析对比

在2016年，文献[16]对Fridrich的混沌图像加密方案进行了密码分析。对于密码算法设计，CFE算法基于时空混沌系统式(1)构造密钥和非线性部件S盒，然后使用了5轮Feistel结构。与之相似，Fridrich的方案是基于混沌方程$g(x)=(\beta+1)(1+1/\beta)^{\beta}x(1-x)^{\beta}$，$\beta\in[1,4]$设计的，然后迭代几轮位置置换和值替换(使用了非线性函数g)。不同的是，Fridrich方案的非线性部件使用的是模加，而CFE算法则使用了S盒。在密码分析方面，文献[16]讨论了Fridrich方案的一些数学性质，并给出了Solak选择密文攻击方法的实际缺陷和应用，而本文主要讨论了CFE算法的密码部件的性质，然后进行了一系列传统的密码分析。

6 结束语

本文对CFE分组算法的安全性进行了分析，结果显示，因为算法具有动态S盒特性，而积分攻击、插值攻击、循环移位攻击、中间相遇攻击和不变量攻击对S盒的密码学特性有较强的依赖性，所以该算法不适合用这些攻击方法，并且由密钥扩展方案

可得该算法可以抵抗相关密钥攻击；其次本文构造出了5轮不可能差分特征链，并利用其进行区分攻击；更进一步地，求得算法的活性S盒下界为6，概率约为2^{-21}；最后指出了算法存在5轮零相关线性特征。接下来我们的工作将着重对该算法的S盒进行研究。

参 考 文 献

[1] BIHAM E and SHAMIR A. Differential cryptanalysis of DES-like cryptosystems[J]. *Journal of Cryptology*, 1991, 4(1): 3–72. doi: 10.1007/BF00630563.

[2] 杨伟伟, 刘光杰, 戴跃伟. 基于交叉耦合映像格子时空混沌的S盒设计[J]. 应用科学学报, 2015, 33(4): 438–448. doi: 10.3969/j.issn.0255-8297.2015.04.010.
YANG Weiwei, LIU Guangjie, and DAI Yuewei. Design of S-boxes based on spatiotemporal chaotic systems of cross coupled map lattices[J]. *Journal of Applied Sciences—Electronics and Information Engineering*, 2015, 33(4): 438–448. doi: 10.3969/j.issn.0255-8297.2015.04.010.

[3] 贾平, 徐洪, 戚文峰. 轻量S盒密码性质研究[J]. 密码学报, 2015, 2(6): 497–504. doi: 10.13868/j.cnki.jcr.000096.
JIA Ping, XU Hong, and QI Wenfeng. Research on cryptographic properties of lightweight S-boxes[J]. *Journal of Cryptologic Research*, 2015, 2(6): 497–504. doi: 10.13868/j.cnki.jcr.000096.

[4] 杨萍. 基于MILP方法的轻量级分组密码的安全性分析[D]. [硕士论文], 山东师范大学, 2018.
YANG Ping. Security analysis of lightweight block cipher based on MILP method[D]. [Master dissertation], Shandong Normal University, 2018.

[5] 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.

[6] 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.

[7] 张仕伟, 陈少真. SIMON不可能差分及零相关路径自动化搜索算法[J]. 软件学报, 2018, 29(11): 3544–3553. doi: 10.13328/j.cnki.jos.005296.
ZHANG Shiwei and CHEN Shaozhen. Automatic search algorithm for impossible differential trials and zero-correlation linear trials in SIMON[J]. *Journal of Software*, 2018, 29(11): 3544–3553. doi: 10.13328/j.cnki.jos.005296.

[8] 马楚焱, 刘国强, 李超. 对PICO和RECTANGLE的零相关线性分析[J]. 密码学报, 2017, 4(5): 413–422. doi: 10.13868/j.cnki.jcr.000193.
MA Chuyan, LIU Guoqiang, and LI Chao. Zero-correlation linear cryptanalysis on PICO and RECTANGLE[J]. *Journal of Cryptologic Research*, 2017, 4(5): 413–422. doi: 10.13868/j.cnki.jcr.000193.

[9] DUO Lei, LI Chao, and FENG Keqin. Square like attack on camellia[C]. The International Conference on Information and Communications Security, Zhengzhou, China, 2007: 269–283. doi: 10.1007/978-3-540-77048-0_21.

[10] 任炯炯, 李航, 陈少真. 减轮Simeck算法的积分攻击[J]. 电子与信息学报, 2019, 41(9): 2156–2163. doi: 10.11999/JEIT180849.
REN Jiongjiong, LI Hang, and CHEN Shaozhen. Integral attack on reduced-round simeck algorithm[J]. *Journal of Electronics & Information Technology*, 2019, 41(9): 2156–2163. doi: 10.11999/JEIT180849.

[11] 邓元豪, 金晨辉, 赵杰卿. Type-3型广义Feistel结构的中间相遇攻击[J]. 密码学报, 2019, 6(1): 27–36. doi: 10.13868/j.cnki.jcr.000280.
DENG Yuanhao, JIN Chenhui, and ZHAO Jieqing. Meet-in-the-middle attack on Type-3 Feistel structure[J]. *Journal of Cryptologic Research*, 2019, 6(1): 27–36. doi: 10.13868/j.cnki.jcr.000280.

[12] 汪艳凤, 吴文玲. 分组密码TWINE的中间相遇攻击[J]. 软件学报, 2015, 26(10): 2684–2695. doi: 10.13328/j.cnki.jos.004805.
WANG Yanfeng and WU Wenling. Meet-in-the-Middle attack on TWINE block cipher[J]. *Journal of Software*, 2015, 26(10): 2684–2695. doi: 10.13328/j.cnki.jos.004805.

[13] JAKOBSEN T and KNUDSEN L R. The interpolation attack on block ciphers[C]. The International Workshop on Fast Software Encryption, Haifa, Israel, 1997: 28–40. doi: 10.1007/BFb0052332.

[14] 金晨辉, 杨阳, 祁传达. 对混沌序列密码的相关密钥攻击[J]. 电子与信息学报, 2006, 28(3): 410–414.
JIN Chenhui, YANG Yang, and QI Chuanda. A related-key attack on chaotic stream ciphers[J]. *Journal of Electronics & Information Technology*, 2006, 28(3): 410–414.

[15] TODO Y, LEANDER G, and SASAKI Y. Nonlinear invariant attack: Practical attack on full SCREAM, iSCREAM, and Midori64[J]. *Journal of Cryptology*, 2019, 32(4): 1383–1422. doi: 10.1007/s00145-018-9285-0.

[16] XIE E Y, LI Chengqing YU Simin, *et al*. On the cryptanalysis of Fridrich's chaotic image encryption scheme[J]. *Signal Processing*, 2017, 132: 150–154. doi: 10.1016/j.sigpro.2016.10.002.

杜小妮：女，1972年生，教授，博士生导师，研究方向为密码学与信息安全.

段娥娥：女，1996年生，硕士生，研究方向为密码学与信息安全.

王天心：女，1997年生，硕士生，研究方向为密码学与信息安全.

责任编辑：马秀强