【文章编号】 1004-1540(2007)01-0054-05

# SAFER-64 的弱密钥

侯 宇

(中国计量学院 信息工程学院,浙江 杭州 310018)

【摘 要】 通过对 SARER-64 系统基础模块的深入分析,构建了由 6 个线性逼近式组成的循环逼近式系统.由于循环性,该逼近式系统可以用来对任意轮次的 SARER-64 进行多重线性密码分析,从而确定系统的弱密钥.现以五轮 SARER-64 为例,构建多重线性逼近式并分析系统的弱密钥.

【关键词】 弱密钥;多重线性密码分析;线性逼近式;循环逼近式系统;SAFER-64

【中图分类号】 TP309.7 【文献标识码】 A

## Weak keys of SAFER-64

HOU Yu

(Deparement of Computer Science and Technology, China Jiliang University, Hangzhou 310018, China)

**Abstract**: This paper analyzes the basic modules of SAFER-64 and presents the circulating relations of linear cryptanalysis composed of 6 linear approximations. By the circulating relations, the multiple linear cryptanalysis can be used to determine weak key classes of arbitrate round of SAFER-64. The multiple linear approximations are presented to identify weak key classes of 5 rounds of SAFER-64 in an example.

**Key words**: weak keys; multiple linear cryptanalysis; linear approximations; circulating relations of linear cryptanalysis; SAFER-64

SAFER-64 系统[1]是一个分组长度为 64 比特、密码长度为 64 比特的分组密码系统,它仅使用了字节运算,所需内存小,因此,在智能卡等方面的应用很有优势.

文献[2]的研究表明 5 轮 SAFER-64 对差分密码分析是免疫的,但是截断差分密码分析对 SAFER-64 系统具有较强的攻击威力.文献[3]利用混合差分对与密文对分布之间的不均匀性和差异性,建立密码分析的混合差分法;在此基础上,文献[4]给出了明文对选择策略、限定字节密钥范围算法和错误密钥快速剔除法等密码分析加速技术,很大程度上提高了混合差分法的攻击效果.文献[5]分析了 SAFER-64 基础模块的密码特性,给出 6 轮的线性逼近式及其优势,建立多重线性密码分析法.

本文采用多重线性密码分析研究 SARER-64

【收稿日期】 2007-01-11

【作者简介】 侯 宇(1958 - ),男,浙江温州人,教授.主要研究方向为信息安全理论与技术研究.

系统的弱密钥.通过对基础模块的深入分析,建立了 6 个首尾相连的线性逼近式,组成循环逼近式系统,并分析了逼近式的优势与子密钥之间的关系.由于循环性,该逼近式系统可以用来对任意轮次的 SARER-64 进行多重线性密码分析从而确定系统的弱密钥.今以五轮 SARER-64 为例,构建多重线性逼近式并分析系统的弱密钥.

# 1　SAFER-64 密码系统

令密文 $X$ 和子密钥 $K_i$ 为

$X=(X^1X^2X^3X^4X^5X^6X^7X^8)\in(F_2^8)^8$,

$K_i=(K_i^1K_i^2K_i^3K_i^4K_i^5K_i^6K_i^7K_i^8)\in(F_2^8)^8$.

子密钥"加"

$\sigma_{K_i}:(F_2^8)^8\to(F_2^8)^8,\ X\to\sigma_{K_i}(X)$.

当 $i$ 为奇数时,有

$$\sigma_{K_i}(X)=(X^1\oplus K_i^1,X^2+K_i^2,X^3+K_i^3,X^4\oplus K_i^4,X^5\oplus K_i^5,X^6+K_i^6,X^7+K_i^7,X^8\oplus K_i^8,)$$

当 $i$ 为偶数时,有

$$\sigma_{K_i}(X)=(X^1+K_i^1,X^2\oplus K_i^2,X^3\oplus K_i^3,X^4+lK_i^4,X^5+K_i^5,X^6\oplus K_i^6,X^7\oplus K_i^7,X^8+K_i^8,)$$

$S$ 盒:

$S_1:F_2^8,\ \to F_2^8,Y\to S_1(Y)=Y^{45}\bmod 257$,约定 $S_1(128)=0$;

$S_2:F_2^8,\ \to F_2^8,Y\to S_2(Y)=\log_{45}(Y)$,约定 $S_2(0)=128$.

混淆层:

$S:(F_2^8)^8\to(F_2^8)^8,X\to S(X)$,

$S(X)=(S_1(X^2),S_2(X^2),S_2(X^3),S_1(X^4),S_1(X^5),S_2(X^6),S_2(X^7),S_1(X^8))$.

扩散层是三层伪哈达码变换

$P:(F_2^8)^8\to(F_2^8)^8,X\to P(X)=P_1P_2P_1P_2P_1(X)$.

其中

$P_1:(F_2^8)^8\to(F_2^8)^8,X\to P_1(X)$,

$P_1(X)=(PHT(X^1X^2),PHT(X^3X^4),PHT(X^5X^6),PHT(X^7X^8))$.

$PHT:(F_2^8)^2\to(F_2^8)^2,YZ\to PHT(YZ)=(2Y+Z\bmod 256,Y+Z\bmod 256)$.

$P_2:(F_2^8)^8\to(F_2^8)^8,\ X\to P_2(X)=(X^1Xi3X^5X^7X^2X^4X^6X^8)$.

子密钥的生成算法见文[1][2].$n$ 轮 SAFER-64 加密算法为

$E(X)=\sigma_{K_{2n+1}}\sigma_{K_{2n+1}}P\sigma_{K_2n}S\sigma_{K_{2n-1}}\cdots P\sigma_{K_4}S\sigma_{K_3}P\sigma_{K_2}S\sigma_{K_1}(X)$.

# 2　基础模块的密码特性

## 2.1　模 256 的加运算

对于模 256 的加运算 $Z=X+Y\bmod 256$,有如下的线性逼近及其逼近优势:

$$\begin{aligned}&\mathrm{bias}(Z[0]=X[0]\oplus Y[0])=2^{-1},\\&\mathrm{bias}(Z[1]=X[1]\oplus Y[1]<\oplus X[0]><\oplus Y[0]>)=2^{-2}.\end{aligned}\tag{1}$$

这里用 bias($L$)表示线性逼近式 $L$ 的逼近优势;而<>是任选项.为了书写简洁,在不引起歧义的前提下,将略去以下逼近式中的异或运算符"⊕".

当模 256 的加运算中的一个变量为常数时,比如 $Y$ 等于常数 $K$,则有

$$\begin{aligned}&\mathrm{bias}(Z[0]=X[0]K[0])=2^{-1},\\&\mathrm{bias}(Z[1]=(X[0]\cdot K[0])X[1]K[1])=2^{-1}.\end{aligned}\tag{2}$$

## 2.2　$S_1$ 和 $S_2$ 的密码特性

对于 $Y=S_1(X)$ 和 $Z=S_2(X)$,有如下的线性逼近及其逼近优势:

$$\mathrm{bias}(Y[1]=X[1])=2^{-5},\mathrm{bias}(Y[1]=X[2])=2^{-4},$$

$$\mathrm{bias}(Y[2]=X[1])=\frac{12}{256}\approx 2^{-4.4},$$

$$\mathrm{bias}(Z[1]=X[1])=2^{-5},\mathrm{bias}(Z[1]=X[2])=2^{-4.4},$$

$$\mathrm{bias}(Z[2]=X[1])=2^{-4},$$

$$\mathrm{bias}(Z[0]\wedge Z[1]=X[1])=2^{-5},\mathrm{bisa}(Z[0]\wedge Z[1]=X[2])=2^{-6},\mathrm{bias}(Z[0]\wedge Z[2]=X[1])=2^{-4}.\tag{3}$$

而对于加密运算 $Y=\sigma_{K_{2r}}S\sigma_{K_{2r-1}}(X)$,特别地有以下线性逼近及其优势:

$$\mathrm{bias}(Y^i[2]=X^i[1])=\begin{cases}2^{-4.4}, & K_{2r}^i[0]=0\\2^{-5}, & K_{2r}^i[0]=1,K_{2r}^i[1]=0\\0, & K_{2r}^i[0]=K_{2r}^i[1]=1\end{cases}\quad i=1,4,5,8\tag{4}$$

$$\mathrm{bias}(Y^j[1]=X^j[2])=\begin{cases}2^{-4.4}, & K_{2r-1}^i[0]=[0]\\2^{-5}, & K_{2r-1}^i[0]=K_{2r-1}^i[1]=1\\0, & K_{2r-1}^i[0]=1,K_{2r-1}^i[1]=0\end{cases}\quad j=2,3,6,7\tag{5}$$

### 2.3 P 变换的密码特性

根据模 256 加运算的密码特性以及字节移位变换的特点，$Z=P(Y)$ 有如下的线性逼近及其逼近优势：

$$\begin{aligned}
&\mathrm{bias}(Z^6[1]Z^7[1]=Y^2[1]Y^4[1]Y^5[1]Y^7[1])=2^{-3},\\
&\mathrm{bias}(Z^2[2]Z^4[1]Z^5[2]Z^7[1]=Y^4[2]Y^6[2])=2^{-3.4},\\
&\mathrm{bias}(Z^4[1]Z^6[1]=Y^2[1]Y^3[1]Y^6[1]Y^7[1])=2^{-3},\\
&\mathrm{bias}(Z^2[2]Z^3[2]Z^6[1]Z^7[1]=Y^4[2]Y^7[2])=2^{-3.4},\\
&\mathrm{bias}(Z^4[1]Z^7[1]=Y^3[1]Y^4[1]Y^5[1]Y^6[1])=2^{-3},\\
&\mathrm{bias}(Z^3[2]Z^4[1]Z^5[2]Z^6[1]=Y^6[2]Y^7[2])=2^{-3.4}
\end{aligned}\tag{6}$$

## 3 线性密码分析

综合上述基础模块密码分析，可以构造 SAFER-64 一轮加密 $Z=P\sigma_{K_2}S\sigma_{K_1}(X)$ 的线性逼近式：

$$\begin{aligned}
&Z^6[1]Z^7[1]=X^2[2]X^4[1]X^5[2]X^7[1],\\
&Z^2[2]Z^4[1]Z^5[2]Z^7[1]=X^4[1]X^6[1],\\
&Z^4[1]Z^6[1]=X^2[2]X^3[2]X^6[1]X^7[1],\\
&Z^2[2]Z^3[2]Z^6[1]Z^7[1]=X^4[1]X^7[1],\\
&Z^4[1]Z^7[1]=X^3[2]X^4[1]X^5[2]X^6[1],\\
&Z^3[2]Z^4[1]Z^5[2]Z^6[1]=X^6[1]X^7[1].
\end{aligned}\tag{7}$$

上面 6 式首尾相连构成一循环逼近式，因此可以用来对任何轮次的加密进行线性密码分析，而且很方便地构造多重线性密码分析.

式(7)中各逼近式的逼近优势与子密钥的取值紧密相关，下面予以详细分析.

### 3.1 含有 $X^j[1](j=6,7)$ 逼近式的优势与 $K_1^j$ 相关而与 $K_{2r-1}^j(r>1)$ 无关

当式(7)中各式用作第一轮加密的逼近式时，根据模 256 加运算的密码特性(2)，含有 $X^j[1]$ 逼近式的优势不为零的条件是 $K_1^j[0]=0$. 但是，当它们用作后续轮($r>1$)加密的逼近式时，含有 $X^j[1]$ 逼近式的优势便与子密钥 $K_{2r-1}^j$ 无关了. 我们以式(7)中的第 6 式为例加以证明. 设 $Y=\sigma_{K_{2r-2}}S\sigma_{K_{2r-3}}(X)$，$Z=P(Y)$，$W=\sigma_{K_{2r-1}}(Z)$，$r>1$. 由密码特性，得到

$$\mathrm{bias}(W^6[1]\wedge W^7[1]=Z^6[0]\cdot K_{2r-1}^6[0]\wedge Y^7[0]\cdot K_{2r-1}^7[0]\wedge Y^7[1])=2^{-1}.$$

而由 $P$ 变换密码特性，有

$$\mathrm{bias}(Z^6[1]Z^7[1]=Y^2[1]Y^4[1]Y^5[1]Y^7[1])=2^{-3},$$

$$\mathrm{bias}(Z^6[0]Z^6[1]Z^7[1]=Y^2[1]Y^4[1]Y^5[1]Y^7[0]Y^7[1])=2^{-3},$$

$$\mathrm{bias}(Z^6[1]Z^7[0]Z^7[1]=Y^2[1]Y^4[1]Y^5[1]Y^7[0]Y^7[1])=2^{-3},$$

$$\mathrm{bias}(Z^6[0]Z^7[0]Z^6[1]Z^7[1]=Y^2[1]Y^4[1]Y^5[1]Y^7[1])=2^{-3}.$$

由模 256 加和 $S$ 盒的密码特性可知

$$\mathrm{bias}(Y^2[1]Y^4[1]Y^5[1]Y^7[1]=X^2[2]X^4[1]X^5[2]X^7[1]=\mathrm{bias}(Y^2[1]Y^4[1]Y^5[1]Y^7[0]Y^7[1]=X^2[2]X^4[1]X^5[2]X^7[1])=2^{-14.3}.$$

综合以上各式可知，无论子密钥 $K_{2r-1}^6$、$K_{2r-1}^7$ 取何值，逼近式

$$W^6[1]W^7[1]=X^2[2]X^4[1]X^5[2]X^7[1]$$

的优势不变. 即当 $r>1$ 时，逼近式(7-6)的优势跟子密钥 $K_{2r-1}^6$、$K_{2r-1}^7$ 取值无关.

### 3.2 第 1、5 式的优势与 $K_{2r}^i(i=4,5)$ 无关；当 $K_{2r-1}^j[0]=1$ 且 $K_{2r-1}^j[1]=0(j=2,3)$ 时优势为零，$K_{2r-1}^j$ 取其他值时优势为 $2^{-18}\sim2^{-17.4}$

以第 1 式为例，设 $\overline{Y}=S\sigma_{K_{2r-1}}(X)$，$Y=\sigma_{K_{2r}}(\overline{Y})$，$Z=P(Y)$. 因为有

$$\mathrm{bias}(Z^6[1]Z^7[1]=Y^2[1]Y^4[1]Y^5[1]Y^7[1]<Y^4[0]Y^5[0]>\!<Y^4[0]Y^7[0]>\!<Y^5[0]Y^7[0]>)=2^{-3}.$$

因此，当 $K_{2r}^4$、$K_{2r}^5$ 均为偶数时我们选用逼近式 $Z^6[1]Z^7[1]=Y^2[1]Y^4[1]Y^5[1]Y^7[1]$，从而有

$$\mathrm{bias}(Y^2[1]Y^4[1]Y^5[1]Y^7[1]=\overline{Y}^2[1]\overline{Y}^4[1]\overline{Y}^5[1]\overline{Y}^7[1])=2^{-1}.$$

当 $K_{2r}^4$、$K_{2r}^5$ 均为奇数时我们选用逼近式 $Z^6[1]Z^7[1]=Y^2[1]Y^4[1]Y^5[1]Y^7[1]Y^4[0]Y^5[0]$，从而有

$$\mathrm{bias}(\overline{Y}^2[1]\overline{Y}^4[1]\overline{Y}^5[1]\overline{Y}^7[1]\overline{Y}^4[0]\overline{Y}^5[0]=\overline{Y}^2[1]\overline{Y}^4[1]\overline{Y}^5[1]\overline{Y}^7[1]=2^{-1}.$$

而当 $K_{2r}^4$、$K_{2r}^5$ 中有一个为奇数时，比如 $K_{2r}^4$ 为偶数，$K_{2r}^5$ 为奇数，我们选用逼近式 $Z^6[1]Z^7[1]=Y^2[1]Y^4[1]Y^5[1]Y^7[1]Y^5[0]Y^7[0]$，从而有

$$\mathrm{bias}(Y^2[1]Y^4[1]Y^5[1]Y^7[1]Y^5[0]Y^7[0]=\overline{Y}^2[1]\overline{Y}^4[1]\overline{Y}^5[1]\overline{Y}^7[1]\overline{Y}^7[0]=2^{-1}.$$

因此，无论 $K_{2r}^4$、$K_{2r}^5$ 为何值，该逼近式的优势不变.

此外，由上述密码特性和堆积原理[2]可知，这两

个逼近式当 $K^j_{2r-1}[0]=1$ 且 $K^j_{2r-1}[1]=0(j=2,3)$时优势为零,$K^j_{2r-1}$取其他值时优势为$2^{-18}\sim2^{-17.4}$.

### 3.3 第 2、4 式的优势与 $K^4_{2r}$、$K^6_{2r-1}$、$K^7_{2r-1}$的关系

定义以下 8 个密钥子集:$S_0=\{0,1,\cdots,31,128,129,\cdots,159\}$, $S_1=\{32,33,\cdots,63,160,161,\cdots,191\}$, $S_2=\{64,65,\cdots,95,192,193,\cdots,223\}$, $S_3=\{96,97,\cdots,127,224,225,\cdots,255\}$和 $T_0=\{0,4,\cdots,252\}$, $T_1=\{1,5,\cdots,253\}$, $T_2=\{2,6,\cdots,254\}$, $T_3=\{3,7,\cdots,255\}$, 则式(7)中的第 2、4 式的优势分别如表 1、表 2 所示.

**表 1　逼近式 $Z^2[2]Z^4[1]Z^5[2]Z^7[1]=X^4[1]X^6[1]$的优势**

| $K^4_{2r}\backslash K^6_{2r-1}$ | $K^6_{2r-1}\in S_0$ | $K^6_{2r-1}\in S_1$ | $K^6_{2r-1}\in S_2$ | $K^6_{2r-1}\in S_3$ |
|---|---|---|---|---|
| $K^4_{2r}\in T_0$ | 0 | $2^{-10}$ | $2^{-9.4}$ | $2^{-9.4}$ |
| $K^4_{2r}\in T_1$ | $2^{-10}$ | $2^{-9.4}$ | $2^{-9.4}$ | $2^{-10}$ |
| $K^4_{2r}\in T_2$ | $2^{-9.4}$ | $2^{-9.4}$ | $2^{-10}$ | 0 |
| $K^4_{2r}\in T_3$ | $2^{-9.4}$ | 0 | 0 | $2^{-9.4}$ |

**表 2　逼近式 $Z^2[2]Z^3[1]Z^5[2]Z^7[1]=X^4[1]X^7[1]$的优势**

| $K^4_{2r}\backslash K^7_{2r-1}$ | $K^7_{2r-1}\in S_0$ | $K^7_{2r-1}\in S_1$ | $K^7_{2r-1}\in S_2$ | $K^7_{2r-1}\in S_3$ |
|---|---|---|---|---|
| $K^4_{2r}\in T_0$ | $2^{-9.4}$ | $2^{-9.4}$ | $2^{-10}$ | 0 |
| $K^4_{2r}\in T_1$ | $2^{-10}$ | $2^{-9.4}$ | $2^{-9.4}$ | $2^{-10}$ |
| $K^4_{2r}\in T_2$ | 0 | $2^{-10}$ | $2^{-9.4}$ | $2^{-9.4}$ |
| $K^4_{2r}\in T_3$ | $2^{-9.4}$ | 0 | 0 | $2^{-9.4}$ |

### 3.4 第 3 式的优势当 $K^j_{2r-1}[0]=1$ 且 $K^j_{2r-1}[1]=0$ $(j=2,3)$时为零,$K^j_{2r-1}$取其他值时优势为 $2^{-19}\sim2^{-17.8}$. 第 6 式的优势见表 3 所示.

**表 3　逼近式 $Z^3[2]Z^4[1]Z^5[2]Z^6[1]=X^6[1]X^7[1]$的优势**

| $K^6_{2r-1}\backslash K^7_{2r-1}$ | $K^7_{2r-1}\in S_0$ | $K^7_{2r-1}\in S_1$ | $K^7_{2r-1}\in S_2$ | $K^7_{2r-1}\in S_3$ |
|---|---|---|---|---|
| $K^6_{2r-1}\in S_0$ | $2^{-12}$ | $2^{-9.4}$ | $2^{-9.7}$ | $2^{-8.7}$ |
| $K^6_{2r-1}\in S_1$ | $2^{-9.4}$ | $2^{-9.2}$ | $2^{-8.7}$ | $2^{-9.7}$ |
| $K^6_{2r-1}\in S_2$ | $2^{-9.7}$ | $2^{-8.7}$ | $2^{-9.2}$ | $2^{-9.4}$ |
| $K^6_{2r-1}\in S_3$ | $2^{-8.7}$ | $2^{-9.7}$ | $2^{-9.4}$ | $2^{-12}$ |

## 4　多重线性密码分析

对于 SAFER-64 任意轮数的加密,让式(7)中的第 1 至第 6 式轮流用作首轮加密逼近式,便可以构造 6 个不同的线性逼近式,对系统进行多重线性密码分析. 以 5 轮加密为例,设加密的输入输出为 $C=\sigma_{K_{11}}P\sigma_{K_{10}}S\sigma_{K_9}\cdots P\sigma_{K_2}S\sigma_{K_1}(X)$,有以下 6 个线性逼近式:

$$\begin{aligned}
&C^4[1]C^6[1]=X^2[2]X^4[1]X^5[2]X^7[1],\\
&C^2[2]C^3[2]C^6[1]C^7[1]=X^4[1]X^6[1],\\
&C^4[1]C^7[1]=X^2[2]X^3[2]X^6[1]X^7[1],\\
&C^3[2]C^4[1]C^5[2]C^6[1]=X^4[1]X^7[1],\\
&C^6[1]C^7[1]=X^3[2]X^4[1]X^5[2]X^6[1],\\
&C^2[2]C^4[1]C^5[2]C^7[1]=X^6[1]X^7[1].
\end{aligned}\tag{8}$$

当上式中的一个或若干个逼近式的优势非零时,根据本文关于密钥特性的分析,可以确定相关子密钥的限值范围,从而确定种子密钥的限值范围. 这些子密钥便是系统的弱密钥. 比如,式(8)中的第 3 式优势非零时,其各轮子密钥必须满足以下表达式:

$$(K^2_1,K^3_1,K^6_1,K^7_1\in R)\wedge(K^4_4\in T_0\wedge K^6_3\in S_1\cup S_2\cup S_3)\vee(K^4_4\in T_1)\vee(K^4_4\in T_2\wedge K^6_3\in S_0\cup S_1\cup S_2)\vee(K^4_4\in T_3\wedge K^6_3\in S_0\cup S_3)\wedge(K^2_5\in T_0\cup T_2\cup T_3)\wedge(K^3_9\in T_0\cup T_2\cup T_3)$$

这里集合 $R=\{0,2,\cdots,254\}$;符号“∧”、“∨”分别表示逻辑“与”和逻辑“或”.

根据 SAFER-64 子密钥生成算法,便可从上式求解出相关字节种子密钥的限值范围:

$K^2\in\{0,2\cdots,14,32,34\cdots,78,96,98\cdots,142,160,162,\cdots,206,224,226,\cdots254\}$

$K^3\in\{2,6,\cdots,250,254\mid 2+8i,6+8i,i=0,1,\cdots31\}$,

$((K^4\in T_0\cup T_1)\wedge K^6\in R)\vee(K^4\in T_2\wedge K^6\in\{128,130,\cdots,254\})\vee(K^4\in T_3\wedge K^6\in\{0,2\cdots,126\})$,

$K^7\in R$.

又比如,当式(8)中的第 1、3、5 逼近式的优势同时非零时,便得到系统种子密钥的限值范围如下:

$K^2\in\{2,6,10,14,34,38,42,46,50,54,58,62,66,70,74,78,98,102,106,110,114,118,122,126,\cdots_{+128}\}$,

$K^3\in\{18,22,26,30,34,38,42,46,50,54,58,62,82,86,90,94,98,102,106,110,114,118,122,126,\cdots_{+128}\}$

$(K^4\in D\wedge K^6\in A_{+128}\wedge K^7\in A\cup A_{+128}\vee(K^4\in D_{+1}\wedge K^6\in A\cup A_{+128}\wedge K^7\in A_{+128})\vee$

$(K^4\in D_{+8}\wedge K^6\in B_{+128}\wedge K^7\in B_{+8}\cup B_{+136}\vee(K^4\in D_{+9}\wedge K^6\in C\cup C_{+128}\wedge K^7\in A_{+136})\vee$

$(K^4\in D_{+16}\wedge K^6\in C_{+128}\wedge K^7\in C\cup C_{+128}\vee(K^4\in D_{+17}\wedge K^6\in C\cup C_{+128}\wedge K^7\in C_{+128})\vee$

$(K^4\in D_{+24}\wedge K^6\in B_{+136}\wedge K^7\in C\cup C_{+128})\vee(K^4\in D_{+25}\wedge K^6\in B_{+8}\cup B_{+136}\wedge K^7\in B_{+28})\vee$

$(K^4\in D_{+128}\wedge K^6\in A\wedge K^7\in A)\vee(K^4\in D_{+129}\wedge K^6\in A\cup A_{+128}\wedge K^7\in A\cup A_{+128})\vee$

$(K^4\in D_{+136}\wedge K^6\in B\wedge K^7\in B_{+8})\vee(K^4\in D_{+137}\wedge K^6\in C\cup C_{+128}\wedge K^7\in B_{+8}\cup B_{+136})\vee$

$(K^4\in D_{+144}\wedge K^6\in C\wedge K^7\in C)\vee(K^4\in D_{+145}\wedge K^6\in C\cup C_{+128}\wedge K^7\in C\cup C_{+128})\vee$

$(K^4\in D_{+152}\wedge K^6\in B_{+8}\wedge K^7\in B)\vee(K^4\in D_{+153}\wedge K^6\in B_{+8}\cup B\wedge K^7\in B_{+8}\cup B)$

其中集合

$A=\{0,2\cdots,126\}$,

$B=\{0,2\cdots,22,32,34,\cdots,54,64,66,\cdots,86,96,98,\cdots,118\}$,

$C=\{0,2,4,6,24,26,\cdots,38,56,58,\cdots,70,88,90,\cdots,102,120,122,124,126\}$,

$D=\{0,2,4,6,32,34,36,64,66,68,70,96,98,100,102\}$.

而集合$\{e_0,e_1\cdots,e_m,\cdots_{+128}\}$、$\{e_0,e_1,e_2\cdots\}_{+n}$定义如下：

$$\{e_0,e_1\cdots,e_m,\cdots_{+n}\}=\{e_0,e_1,\cdots,e_m,e_0+n,e_1+n,\cdots,e_m+n\},$$

$$\{e_0,e_1,e_2\cdots\}_{+n}=\{e_0+n,e_1+n,e_2+n,\cdots\}.$$

## 【参 考 文 献】


[1] MASSEY J L. SAFER K-64: A Byte-Oriented Block-Ciphering Algorithm[M]//. Fast Software Encryption, Cambridge Security Workshop Proceedings. Berlin: Springer-Verlag, 1994:1-17.

[2] 冯登国. 密码分析学[M]. 北京:清华大学出版社,2000:22-35.

[3] 闫 勇,苏开宇,侯 宇. SAFER-64 密码分析的混合差分法[J]. 中国计量学院学报,2003,14(2):109-113.

[4] 侯 宇,苏开宇,闫 勇. SAFER-64 密码分析的加速技术[J]. 中国计量学院学报,2005,16(1):27-30.

[5] 侯 宇,苏开宇,闫 勇. SAFER-64 的多重线性密码分析[J]. 中国计量学院学报,2006,17(1):56-59.