嵌套代替-扩散网络的 CLEFIA 结构零相关线性逼近的构造

崔　霆*　　金晨辉
(信息工程大学电子技术学院　郑州　450004)

摘　要：零相关线性分析是一种新的分组密码分析方法。进行零相关线性分析首先需要构造相关系数为 0 的线性逼近。该文研究了嵌套代替-扩散(SP)的 CLEFIA 结构相关系数为 0 的线性逼近构造问题，给出了该结构的一类新的$(4n+1)$轮零相关线性逼近的构造算法。利用该方法可以给出 9 轮 CLEFIA 算法的大量零相关线性逼近。

关键词：分组密码；CLEFIA 结构；零相关线性逼近；扩散结构
中图分类号：TN918.1　　**文献标识码**：A　　**文章编号**：1009-5896(2012)01-0227-04
DOI: 10.3724/SP.J.1146.2011.00475

Construction of Zero-correlation Linear Hull for CLEFIA-like Structure with SPN Round Functions

Cui Ting　　Jin Chen-hui
(*Institution of Electronic Technology*, *Information Engineering University*, *Zhengzhou* 450004, *China*)

Abstract: Zero-correlation linear cryptanalysis is a newly proposed attack of block ciphers. The first step of this cryptanalysis is to construct a zero-correlation linear hull whose correlation value is 0. This paper investigates the construction of zero-correlation linear hull for CLEFIA-like structure with Substitution-Permutation (SP)-type round function. And a new method of finding $(4n+1)$ round zero-correlation linear hull of this structure is proposed. By the proposed method, large amount of zero-correlation linear hulls of 9 round CLEFIA are obtained.

Key words: Block cipher; CLEFIA-like structure; Zero-correlation linear hull; Diffusion structure

1　引言

自Biham等人[1]提出不可能差分分析方法以来，不可能差分分析逐渐发展成了分组密码分析中最有效的方法之一，国内外学者利用该分析方法成功分析了AES[2]，Camellia[3]，ARIA[3]，CLEFIA [4−6]和3D[7]等一大批算法。不可能差分分析方法的主要思想是通过抛弃那些导致不可能差分出现的候选密钥来筛选出正确密钥。实际进行不可能差分分析首先需要构造密码算法的不可能差分。近年来，不可能差分的构造已经成为不可能差分分析研究的一个热点问题，也出现了一些很好的研究成果：文献[8]和文献[9]各自给出了自动搜索密码结构不可能差分的一般性方法；文献[10]给出了一类嵌套代替-扩散(SP)结构和嵌套代替-扩散-代替(SPS)结构的Feistel结构的不可能差分构造方法；文献[11]则给出了一类SP结构的不可能差分构造方法。不可能差分的存在性也在一定程度上反应了密码抵抗不可能差分分析的能力。

由于传统意义的差分分析和线性分析具有很多相似性[12]，从这一意义上说，存在与不可能差分相对应的线性分析方法是可能的。2011年，文献[12]提出了一类新的线性密码分析方法——零相关线性分析。该方法利用相关系数为0的线性逼近来完成对密钥的筛选。该方法利用零相关线性分析方法，以$O(2^{188.4})$的计算复杂度和$O(2^{128})$的数据复杂度攻击了7轮AES-192算法，并以$O(2^{253.3})$的计算复杂度和$O(2^{128})$的数据复杂度攻击了13轮CLEFIA-256算法。与不可能差分分析方法类似，零相关线性分析首先需要构造密码算法相关系数为0的线性逼近，故可以用零相关线性逼近的轮数及个数来度量算法抵抗零相关线性分析的能力。若可以预知某个算法结构的零相关线性逼近，则可以增加密码算法在零相关线性逼近攻击下的可控性，为密码安全性分析奠定基础，且对于分组密码的设计也具有理论和实用价值。

作为一类广义Feistel密码，CLEFIA算法在设计时采用了DSM(Diffusion Switching Mechanism)策略[4]，该策略的参与能够使密码算法很好地抵抗传统的差分分析和线性分析。然而分析表明，存在着对高轮CLEFIA算法有效的不可能差分分析结果和零相关线性分析结果。本文将考察嵌套SP结构的

2011-05-19 收到，2011-09-20 改回
河南省杰出青年科学基金(0312001800)资助课题
*通信作者：崔霆　cuiting_1209@yahoo.com.cn

CLEFIA模型零相关线性逼近链的构造，利用该方法，可以找出9轮CLEFIA算法大量的零相关线性逼近。

2 准备工作

本文若无特别说明，均以“⊕”表示逐位异或运算，以“+”表示实数加法，“·”表示向量点积，$\#S$ 表示集合 S 的元素个数；以 $W(\boldsymbol{\xi})$ 表示向量 $\boldsymbol{\xi}$ 中的非 0 元素个数；$\boldsymbol{M}^{\bar{p}}$ 表示矩阵 $\boldsymbol{M}$ 除去第 p 列之后剩余的列向量。$\mathrm{span}\{\boldsymbol{\alpha}_1,\cdots,\boldsymbol{\alpha}_r\}$ 表示由向量 $\boldsymbol{\alpha}_1,\cdots,\boldsymbol{\alpha}_r$ 张成的子空间。本文中所有的计数均始于 1。

定义 1[4] 设 $f_1,f_2,\cdots,f_n$ 为 $\{0,1\}^m\times\{0,1\}^m\to\{0,1\}^m$ 的变换，k 为轮子密钥，若密码算法采用

$$\begin{aligned}(y_1,y_2,\cdots,y_{2n})=Q_k(x_1,x_2,\cdots,x_{2n})=(x_2\oplus f_1(k,x_1),\\ x_3,x_4\oplus f_2(k,x_3),\cdots,x_{2n-1},x_{2n}\\ \oplus f_n(k,x_{2n-1}),x_1)\end{aligned}$$

为轮函数，则称该模型为 $2n$ 分组 CLEFIA 模型。这里的 $f_1,f_2,\cdots,f_n$ 称为第 1 至第 n 个 f 函数。x_i,y_i 称为轮函数的第 i 个输入、输出块。

备注 1 各参数同定义 1，$2n$ 分组 CLEFIA 模型的逆轮函数 Q_k^{-1} 为

$$\begin{aligned}Q_k^{-1}(y_1,y_2,\cdots,y_{2n})=(y_{2n},y_1\oplus f_1(k,y_{2n}),\\ y_2,y_3\oplus f_2(k,y_2),\cdots,y_{2n-2},\\ y_{2n-1}\oplus f_n(k,y_{2n-2}))\end{aligned}$$

定义 2[4] 设 $f_1,f_2,\cdots,f_n$ 为 $2n$ 分组CLEFIA模型的 n 个 f 函数，若满足 $f_i(x)=P_iS_i(x\oplus k)$，则称该模型为 $2n$ 分组嵌套SP结构的CLEFIA模型，记为 $(2n,r,t)$_CLEFIA。其中，k 是与输入 x 等长的圈子密钥，$S_i(\boldsymbol{y})=(s_{i1}(y_1),s_{i2}(y_2),\cdots,s_{ir}(y_r))$，诸 s_{ij} 均为 $\{0,1\}^t\to\{0,1\}^t$ 的非线性置换；P_i 均为 $\mathrm{GF}(2^t)^r\to\mathrm{GF}(2^t)^r$ 的可逆线性变换，即 $P_i(\boldsymbol{y})=\boldsymbol{M}_i\boldsymbol{y}$，这里 $\boldsymbol{M}_i$ 为 $\mathrm{GF}(2^t)$ 上的 $r\times r$ 矩阵，$\boldsymbol{y}$ 为列向量。

定义 3[12] 设 $F:Z_2^m\to Z_2^n$ 为多输出函数，$\alpha,x\in Z_2^m$，$\beta,F(x)\in Z_2^n$，记 $\rho=\rho_F(\alpha\to\beta)=1/2^m\cdot\sum_{x\in Z_2^m}(-1)^{\beta\cdot F(x)\oplus\alpha\cdot x}$，则称 $\alpha\to\beta$ 为 F 的一个线性逼近，ρ 为该线性逼近的相关系数。特别地，当 $F=f_r\circ f_{r-1}\circ\cdots\circ f_1$ 时，称 $\alpha_1\to\alpha_2\to\cdots\to\alpha_r\to\alpha_{r+1}$ 为 F 的一条组合传递链，其相关系数为 $\prod_{i=1}^{r}\rho_{f_i}(\alpha_i\to\alpha_{i+1})$。

值得指出，对 r 轮迭代型分组密码 F 而言，线性逼近 $\alpha_1\to\alpha_{r+1}$ 的相关系数等于 F 的所有起点为 α_1，终点为 α_{r+1} 的组合传递链的相关系数之和。当起点为 α_1，终点为 α_{r+1} 的每条组合传递链的相关系数均为 0 时，则线性逼近 $\alpha_1\to\alpha_{r+1}$ 的相关系数必为 0。文献[12]指出，可以根据这一事实来寻找零相关线性逼近。

为方便起见，下文用 $(\Gamma\boldsymbol{y})_f$ 表示输出组合为 $\Gamma\boldsymbol{y}$ 时 f 的输入组合。则有

(1)设 $f(x)=\boldsymbol{A}\times\boldsymbol{x}$ 为 $\mathrm{GF}(2^n)^m\to\mathrm{GF}(2^n)^m$ 的线性变换，$\boldsymbol{A}$ 为 $\mathrm{GF}(2^n)$ 上的 m 阶方阵，$\Gamma\boldsymbol{y}$ 为列向量，则有 $(\Gamma\boldsymbol{y})_f=\boldsymbol{A}^{\mathrm{T}}\times\Gamma\boldsymbol{y}$[13]；

(2)当 f 是双射时，$(\Gamma\boldsymbol{y})_f=0$ 当且仅当 $\Gamma\boldsymbol{y}=0$。

定义 4[10] 设 $x\in\mathrm{GF}(2^n)$，定义特征函数 $\chi_n:\mathrm{GF}(2^n)\to\mathrm{GF}(2)$ 为

$$\chi_n(x)=\begin{cases}0, & x=0\\ 1, & x\neq 0\end{cases}$$

通常，若 $\boldsymbol{X}=(x_1,\cdots,x_m)\in\mathrm{GF}(2^n)^m$，用 $\chi_n(\boldsymbol{X})$ 表示 $(\chi_n(x_1),\cdots,\chi_n(x_m))$，用 $\chi_n(\boldsymbol{X},s)$ 表示 $\chi_n(\boldsymbol{X})$ 的第 s 个分量，即 $\chi_n(x_s)$。

定义 5[14] 设 $\boldsymbol{A}$ 是 $\mathrm{GF}(2^n)$ 上的 $r\times t$ 矩阵，$\boldsymbol{\alpha}$ 是 $\mathrm{GF}(2^n)$ 上的 t 维列向量，则定义矩阵 $\boldsymbol{A}$ 的（线性）分支数为 $B(\boldsymbol{A})=\min\{W(\boldsymbol{\alpha})+W(\boldsymbol{A}^{\mathrm{T}}\boldsymbol{\alpha}):\boldsymbol{\alpha}\in[\mathrm{GF}(2^n)]^t\setminus\{0\}\}$。

当 $\boldsymbol{A}$ 的分支数达到最大值 $r+1$ 时，称其为MDS(极大最小距离可分)矩阵[14]。

3 $(2n,r,t)$_CLEFIA 结构零相关线性逼近的构造

首先本文将给出 CLEFIA 结构的组合传递链规律。

定理 1 $2n$分组CLEFIA模型加密变换的一轮线性逼近必具有形式

$$\begin{aligned}(\Gamma x_1,\Gamma x_2,\cdots,\Gamma x_{2n})\to(\Gamma x_2,\Gamma x_3\oplus\beta_2,\cdots,\Gamma x_{2n-1}\\ \oplus\beta_{2n},\Gamma x_{2n},\Gamma x_1\oplus\beta_1)\end{aligned}$$

且此时 f_j 的线性逼近为 $\beta_j\to\Gamma x_{2j}$。

证明 由线性逼近的定义可以直接验证。 证毕

据定理 1，有

定理 2 $2n$分组CLEFIA模型脱密变换的一轮线性逼近必具有形式

$$\begin{aligned}(\Gamma y_1,\cdots,\Gamma y_{2n})\to(\Gamma y_{2n}\oplus\gamma_1,\Gamma y_1,\cdots,\\ \Gamma y_{2n-2}\oplus\gamma_n,\Gamma y_{2n-1})\end{aligned}$$

且此时 f_j 的线性逼近为 $\gamma_i\to\Gamma x_{2i}$。

以下约定$2n$分组CLEFIA结构的第 i 轮、第 s 块的输入组合系数为 $\Gamma_{\mathrm{in}}x_s^i$，第 i 轮、第 s 块的输出组合系数为 $\Gamma_{\mathrm{out}}x_s^i$。由上述定理可知：

推论 1 $2n$分组CLEFIA模型的各 f 函数依次设为 $f_1,f_2,\cdots,f_n$，则对 $\forall 1\le s\le n$：

(1)若首轮输入组合系数仅 $\Gamma_{\mathrm{in}}\boldsymbol{x}_{2s-1}^1$ 非0，则必有 $\Gamma_{\mathrm{in}}\boldsymbol{x}_{2s-2}^{2n+1}=\mathop{\oplus}_{i=1}^{n}(\Gamma_{\mathrm{in}}\boldsymbol{x}_{(2s-1)}^1)_{f_i}$；

(2)若末轮输出组合系数仅 $\Gamma_{\mathrm{out}}\boldsymbol{x}_{2s-1}^{2n+1}$ 非0，则必

有$\Gamma_{\text{out}}\boldsymbol{x}_{2s-2}^{1}=\overset{n}{\underset{i=1}{\oplus}}(\Gamma_{\text{out}}\boldsymbol{x}_{(2s-1)}^{\text{out}})_{f_i}$。

命题 1[12]　设$(\Gamma x,\Gamma y)\to\Gamma z$为函数$f(x,y)=x\oplus y$的线性逼近，且相关系数非零，则必有$\Gamma x=\Gamma y=\Gamma z$。

定理 3　$(2n,r,t)$_CLEFIA结构的各f函数P变换矩阵表示依次设为$\boldsymbol{M}_1,\boldsymbol{M}_2,\cdots,\boldsymbol{M}_n$，若存在GF$(2^t)$上的$r$维非零列向量$\boldsymbol{\alpha},\boldsymbol{\beta}$及$1\le k,p\le n$，使：(1)对$\forall 1\le i\le n,i\ne k$，均有$\chi(\boldsymbol{M}_i^{\mathrm{T}}\boldsymbol{\alpha},p)=0$成立；(2)$\chi(\boldsymbol{M}_k^{\mathrm{T}}\boldsymbol{\alpha},p)=1$；(3)对$\forall 1\le j\le n$，均有$\chi(\boldsymbol{M}_j^{\mathrm{T}}\boldsymbol{\beta},p)=0$。则$(2n,r,t)$_CLEFIA至少存在$2n$个$4n+1$轮非平凡零相关线性逼近。

证明　对$\forall 1\le s\le n$，首轮输入组合系数除$\Gamma_{\text{in}}\boldsymbol{x}_{2s-1}^{1}=\boldsymbol{\alpha}$之外，其余系数均取0，则由推论1知，有$\Gamma_{\text{in}}\boldsymbol{x}_{2s-2}^{2n+1}=\overset{n}{\underset{i=1}{\oplus}}\left[\boldsymbol{M}_i^{\mathrm{T}}\boldsymbol{\alpha}\right]_{S_i}$；相应地，$4n+1$轮输出组合系数仅$\Gamma_{\text{out}}\boldsymbol{x}_{2s-1}^{4n+1}=\boldsymbol{\beta}$，其余系数均取0，则有$\Gamma_{\text{out}}\boldsymbol{x}_{2s-2}^{2n+1}=\overset{n}{\underset{i=1}{\oplus}}\left[\boldsymbol{M}_i^{\mathrm{T}}\boldsymbol{\beta}\right]_{S_i}$。又

$$\chi(\Gamma_{\text{in}}\boldsymbol{x}_{2s-2}^{2n+1},p)=\chi\left(\overset{n}{\underset{i=1}{\oplus}}\left[\boldsymbol{M}_i^{\mathrm{T}}\boldsymbol{\alpha}\right]_{S_i},p\right)=\chi\left(\left[\boldsymbol{M}_k^{\mathrm{T}}\boldsymbol{\alpha}\right]_{S_k},p\right)=1$$

且

$$\chi\left(\Gamma_{\text{out}}\boldsymbol{x}_{2s-2}^{2n+1},p\right)=\chi\left(\overset{n}{\underset{i=1}{\oplus}}\left[\boldsymbol{M}_i^{\mathrm{T}}\times\boldsymbol{\beta}\right]_{S_i},p\right)=0$$

这就说明$\Gamma_{\text{in}}\boldsymbol{x}_{2s-2}^{2n+1}\ne\Gamma_{\text{out}}\boldsymbol{x}_{2s-2}^{2n+1}$，该式与引理1的结论$\Gamma_{\text{in}}\boldsymbol{x}_{2s-2}^{2n+1}=\Gamma_{\text{out}}\boldsymbol{x}_{2s-2}^{2n+1}$矛盾。因此$(0,\cdots,0,\Gamma_{\text{in}}\boldsymbol{x}_{2s-1}^{1}=\boldsymbol{\alpha},0,\cdots,0)\not\to(0,\cdots,0,\Gamma_{\text{out}}\boldsymbol{x}_{2s-1}^{4n+1}=\boldsymbol{\beta},0,\cdots,0)$必为$(2n,r,t)$_CLEFIA结构的$4n+1$轮非平凡零相关线性逼近。

同理可证，当首轮输入组合系数除$\Gamma_{\text{in}}\boldsymbol{x}_{2s-1}^{1}=\boldsymbol{\beta}$之外，其余系数均取0，$4n+1$轮输出组合系数仅$\Gamma_{\text{out}}\boldsymbol{x}_{2s-1}^{4n+1}=\boldsymbol{\alpha}$，其余系数均取0，此时$(0,\cdots,0,\Gamma_{\text{in}}\boldsymbol{x}_{2s-1}^{1}=\boldsymbol{\beta},0,\cdots,0)\not\to(0,\cdots,0,\Gamma_{\text{out}}\boldsymbol{x}_{2s-1}^{4n+1}=\boldsymbol{\alpha},0,\cdots,0)$也为$(2n,r,t)$_CLEFIA结构的$4n+1$轮零相关线性逼近。由$s$的任意性知$(2n,r,t)$_CLEFIA至少存在$2n$个$4n+1$轮零相关线性逼近。　　证毕

定理3给出了零相关线性逼近存在的一个充分条件，只需找出满足条件(1)~条件(3)的$\boldsymbol{\alpha},\boldsymbol{\beta}$值即可找到相应的零相关线性逼近。然而定理3的条件难以直接用来寻找$\boldsymbol{\alpha},\boldsymbol{\beta}$，下面的两个定理给出了搜索$\boldsymbol{\alpha},\boldsymbol{\beta}$可行的方法。

定理 4　设$\boldsymbol{A}_1,\boldsymbol{A}_2,\cdots,\boldsymbol{A}_m$为GF$(2^n)$上的$r\times r$可逆矩阵，若记$V=\overset{m}{\underset{i=1}{\cap}}\text{span}\{(\boldsymbol{A}_i^{-1})^{\overline{p}}\}$，$\Omega=\{\boldsymbol{\alpha}:\chi(\boldsymbol{A}_i\boldsymbol{\alpha},p)=0\text{对}1\le i\le m\text{均成立}\}$，则有$V=\Omega$。这里的$\text{span}\{(\boldsymbol{A}_i^{-1})^{\overline{p}}\}$表示由矩阵$\boldsymbol{A}_i^{-1}$除去第$p$列后剩余的列向量张成的线性子空间。

证明　因$\boldsymbol{A}_i$的列向量线性无关，故对任意非零向量$\boldsymbol{\alpha}\in V$，也即对$1\le i\le m$，均唯一地存在$r-1$维非零列向量$\boldsymbol{\beta}^i=(\boldsymbol{\beta}_1^i,\cdots,\boldsymbol{\beta}_{p-1}^i,\boldsymbol{\beta}_p^i,\cdots,\boldsymbol{\beta}_r^i)^{\mathrm{T}}$使得$\boldsymbol{\alpha}=(\boldsymbol{A}_i^{-1})^{\overline{p}}\times\boldsymbol{\beta}^i$成立。构造$r$维列向量$\boldsymbol{\gamma}_i=(\boldsymbol{\beta}_1^i,\cdots,\boldsymbol{\beta}_{p-1}^i,0,\boldsymbol{\beta}_p^i,\cdots,\boldsymbol{\beta}_r^i)^{\mathrm{T}}$，则有$\boldsymbol{\alpha}=(\boldsymbol{A}_i^{-1})^{\overline{p}}\times\boldsymbol{\beta}^i=\boldsymbol{A}_i^{-1}\times\boldsymbol{\gamma}_i$成立。也即$\boldsymbol{\gamma}_i=\boldsymbol{A}_i\times\boldsymbol{\alpha}$。同时由$\boldsymbol{\gamma}_i$的定义知$\chi(\boldsymbol{A}_i\boldsymbol{\alpha},p)=0$。也即$V\subseteq\Omega$。

对任意$\boldsymbol{\alpha}\in\Omega$，对$1\le i\le m$，令$\boldsymbol{\theta}^i=(\boldsymbol{\theta}_1^i,\boldsymbol{\theta}_2^i,\cdots,\boldsymbol{\theta}_r^i)^{\mathrm{T}}=\boldsymbol{A}_i\boldsymbol{\alpha}$，由$\Omega$的定义知$\boldsymbol{\theta}_p^i=0$。令$r-1$维向量$\boldsymbol{\vartheta}^i=(\theta_1^i,\cdots,\theta_{p-1}^i,\theta_{p+1}^i,\cdots,\theta_r^i)^{\mathrm{T}}$，故有$\boldsymbol{\alpha}=\boldsymbol{A}_i^{-1}\times\boldsymbol{\theta}_i=(\boldsymbol{A}_i^{-1})^{\overline{p}}\times\boldsymbol{\vartheta}^i$成立。也即$\boldsymbol{\alpha}\in\text{span}\{(\boldsymbol{A}_i^{-1})^{\overline{p}}\}$，因此$\Omega\subseteq V$。　　证毕

记$\Omega_1=\{\boldsymbol{\alpha}:\chi(\boldsymbol{M}_k^{\mathrm{T}}\boldsymbol{\alpha},p)=1\text{且}\chi(\boldsymbol{M}_i^{\mathrm{T}}\boldsymbol{\alpha},p)=0\text{对}1\le i\le n,i\ne k\text{成立}\}$，$\Omega_2=\{\boldsymbol{\alpha}:\chi(\boldsymbol{M}_i^{\mathrm{T}}\boldsymbol{\alpha},p)=0\text{对}1\le i\le n\text{成立}\}$，$\Omega_3=\{\boldsymbol{\alpha}:\chi(\boldsymbol{M}_i^{\mathrm{T}}\boldsymbol{\alpha},p)=0\text{对}1\le i\ne k\le n\text{成立}\}$，$V_1=\overset{}{\underset{i\ne k}{\cap}}\text{span}\{[(\boldsymbol{M}_i^{\mathrm{T}})^{-1}]^{\overline{p}}\}\setminus\overset{n}{\underset{i=1}{\cap}}\text{span}\{[(\boldsymbol{M}_i^{\mathrm{T}})^{-1}]^{\overline{p}}\}$，$V_2=\overset{n}{\underset{i=1}{\cap}}\text{span}\{[(\boldsymbol{M}_i^{\mathrm{T}})^{-1}]^{\overline{p}}\}$，$V_3=\overset{}{\underset{i\ne k}{\cap}}\text{span}\{[(\boldsymbol{M}_i^{\mathrm{T}})^{-1}]^{\overline{p}}\}$。

由定理4知$\Omega_2=V_2$，同时注意到$\Omega_1\cup\Omega_2=\Omega_3=V_3$，因此$\Omega_1=\Omega_3\setminus\Omega_2=V_3\setminus V_2=V_1$。故定理3可重新表达为下面的定理：

定理 5　$(2n,r,t)$_CLEFIA结构的各f函数P变换矩阵表示依次设为$\boldsymbol{M}_1,\boldsymbol{M}_2,\cdots,\boldsymbol{M}_n$，若存在GF$(2^t)$上的$r$维列向量$\boldsymbol{\alpha},\boldsymbol{\beta}$及$1\le k,p\le n$，使$\boldsymbol{\alpha}\in\overset{}{\underset{i\ne k}{\cap}}\text{span}\{[(\boldsymbol{M}_i^{\mathrm{T}})^{-1}]^{\overline{p}}\}\setminus\overset{n}{\underset{i=1}{\cap}}\text{span}\{[(\boldsymbol{M}_i^{\mathrm{T}})^{-1}]^{\overline{p}}\}$和$\boldsymbol{\beta}\in\overset{n}{\underset{j=1}{\cap}}\text{span}\{[(\boldsymbol{M}_j^{\mathrm{T}})^{-1}]^{\overline{p}}\}\setminus\{0\}$，则对$\forall 1\le s\le n$，$(0,\cdots,0,\Gamma_{\text{in}}\boldsymbol{x}_{2s-1}^{1}=\boldsymbol{\alpha},0,\cdots,0)\not\to(0,\cdots,0,\Gamma_{\text{out}}\boldsymbol{x}_{2s-1}^{4n+1}=\boldsymbol{\beta},0,\cdots,0)$和$(0,\cdots,0,\Gamma_{\text{in}}\boldsymbol{x}_{2s-1}^{1}=\boldsymbol{\beta},0,\cdots,0)\not\to(0,\cdots,0,\Gamma_{\text{out}}\boldsymbol{x}_{2s-1}^{4n+1}=\boldsymbol{\alpha},0,\cdots,0)$均为$(2n,r,t)$_CLEFIA的$4n+1$轮零相关线性逼近。

注意到

$$\left\{\overset{}{\underset{i\ne k}{\cap}}\text{span}\{[(\boldsymbol{M}_i^{\mathrm{T}})^{-1}]^{\overline{p}}\}\setminus\overset{n}{\underset{i=1}{\cap}}\text{span}\{[(\boldsymbol{M}_i^{\mathrm{T}})^{-1}]^{\overline{p}}\}\right\}\cap\left\{\overset{n}{\underset{j=1}{\cap}}\text{span}\{[(\boldsymbol{M}_j^{\mathrm{T}})^{-1}]^{\overline{p}}\}\setminus\{0\}\right\}=\phi$$

故定理5中的$\boldsymbol{\alpha}$与$\boldsymbol{\beta}$的取值一定不会相等。因此有

推论 2　条件同定理5，可以构造$(2n,r,t)$_CLEFIA模型

$$2n\times\#\left(\overset{}{\underset{i\ne k}{\cap}}\text{span}\{[(\boldsymbol{M}_i^{\mathrm{T}})^{-1}]^{\overline{p}}\}\setminus\overset{n}{\underset{i=1}{\cap}}\text{span}\{[(\boldsymbol{M}_i^{\mathrm{T}})^{-1}]^{\overline{p}}\}\right)\times\#\left(\overset{n}{\underset{j=1}{\cap}}\text{span}\{[(\boldsymbol{M}_j^{\mathrm{T}})^{-1}]^{\overline{p}}\}\setminus\{0\}\right)$$

条$4n+1$轮零相关线性逼近。

4　CLEFIA算法的零相关线性逼近

CLEFIA算法采用了$(4,4,8)$_CLEFIA模型，并利用DSM策略[4]设计了各圈的扩散结构，即两个f

函数中，扩散层采用的矩阵 $\boldsymbol{M}_1, \boldsymbol{M}_2$ 为MDS矩阵，且 $\left[(\boldsymbol{M}_1^{\mathrm{T}})^{-1} \| (\boldsymbol{M}_2^{\mathrm{T}})^{-1}\right]$ 也是MDS矩阵。

引理 1[14] $\mathrm{GF}(2^n)$ 上的矩阵是MDS矩阵当且仅当该矩阵行列式的任一子式非奇异。

引理 2 设 $\boldsymbol{A}_1, \boldsymbol{A}_2$ 为 $\mathrm{GF}(2^n)$ 上的 $r \times r$ 矩阵，且 $B\left([\boldsymbol{A}_1 | \boldsymbol{A}_2]\right) = r+1$，则 $\#\bigcap_{i=1}^{2} \mathrm{span}\{\boldsymbol{A}_i^{\overline{p}}\} = 2^{n(r-2)}$。

证明 对 $\forall 1 \le p \le r$，设 $[\boldsymbol{A}_i]^{\overline{p}} = [\varepsilon_{i,1}, \cdots, \varepsilon_{i,r-1}]$，则由线性代数知识容易验证 $\#\bigcap_{i=1}^{2} \mathrm{span}\{\boldsymbol{A}_i^{\overline{p}}\} = \#\left\{(x_1, \cdots, x_{r-1}, y_1, \cdots, y_{r-1}) \in \mathrm{GF}(2^n)^{2r-2} : \left(\bigoplus_{j=1}^{r-1} x_j \varepsilon_{1,j}\right) \oplus \left(\bigoplus_{j=1}^{r-1} y_j \varepsilon_{2,j}\right) = 0\right\}$。

由引理1知，$[\boldsymbol{A}_1 | \boldsymbol{A}_2]$ 的任意 r 列线性无关，因此从 $[\boldsymbol{A}_1^{\overline{p}} \mid \boldsymbol{A}_2^{\overline{p}}]$ 中抽出的任意不大于 r 个列向量均线性无关。故方程组 $\left(\bigoplus_{j=1}^{r-1} x_j \varepsilon_{1,j}\right) \oplus \left(\bigoplus_{j=1}^{r-1} y_j \varepsilon_{2,j}\right) = 0$ 等价于 $\left(\bigoplus_{j=1}^{r-1} x_j \varepsilon_{1,j}\right) \oplus y_1 \varepsilon_{2,1} = \left(\bigoplus_{j=2}^{r-1} y_j \varepsilon_{2,j}\right)$，后者解空间维数恰为 $r-2$。 证毕

结论 CLEFIA算法至少存在 $2^{42} - 2^{34} - 2^{26} + 2^{18}$ 条9轮零相关线性逼近。

证明 由引理2知，对一组给定的 (p,k)，有 $\#\bigcap_{j=1}^{2} \mathrm{span}\{[(\boldsymbol{M}_j^{\mathrm{T}})^{-1}]^{\overline{p}}\} \setminus \{0\} = 2^{8\times 2} - 1$，而对 $i \ne k$，子空间 $\mathrm{span}\{[(\boldsymbol{M}_i^{\mathrm{T}})^{-1}]^{\overline{p}}\}$ 的维数为3，据推论2知结论成立。 证毕

5 结束语

零相关线性分析作为一种新型的密码分析技术，设计者和攻击者都需要认真地评估其对密码算法安全性的影响。由于开展零相关线性攻击首先需要构造密码算法的零相关线性逼近。因此通过给出某个密码算法的零相关线性逼近的构造方法是很有意义的。本文研究了嵌套SP结构的CLEFIA模型的零相关线性逼近的构造问题，给出了该模型的 $4n+1$ 轮零相关线性逼近的构造方法。本文为分组密码设计和分析提供了参照。

参 考 文 献

[1] Biham E, Biryukov A, and Shamir A. Cryptanalysis of skipjack reduced to 31 rounds using impossible differentials[C]. EUROCRYPT'99, Springer-Verlag, 1999, LNCS 1592: 12–23.

[2] Zhang Wen-tao, Wu Wen-ling, and Feng Deng-guo. New results on impossible differential cryptanalysis of reduced AES[C]. ICISC 2007, Springer-Verlag, 2007, LNCS 4817: 239–250.

[3] Wu Wen-ling, Zhang Wen-tao, and Feng Deng-guo. Impossible differential cryptanalysis of reduce round ARIA and Camellia[J]. *Journal of Computer Science and Technology*, 2007, 22(3): 449–456.

[4] Shirai T, Shibutani K, and Akishita T, *et al*.. The 128-bit blockcipher CLEFIA[C]. FSE 2007, LNCS 3017: 181–195.

[5] Wang Wei and Wang Xiao-yun. Impossible differential cryptanalysis of CLEFIA-128/192/256[J]. *Journal of Software*, 2009, 20(9): 2587–2596.

[6] Zhang Wen-ying and Han Jing. Impossible differential cryptanalysis of reduced round CLEFIA[C]. Inscrypt 2008, Springer-Verlag, 2009, LNCS 5487: 181–191.

[7] 唐学海, 李超, 王美一, 等. 3D 密码的不可能差分攻击[J]. 电子与信息学报, 2010, 32(10): 2516–2520.
Tang Xue-hai, Li Chao, Wang Mei-yi, *et al*.. Impossible differential attack on 3D cipher[J]. *Journal of Electronics & Information Technology*, 2010, 32(10): 2516–2520.

[8] Kim Jongsung, Hong Seokhie, and Lim Jongin. Impossible differential cryptanalysis using matrix method[J]. *Discrete Mathematics*, 2010, 310(5): 988–1002.

[9] Luo Yi-yuan, Wu Zhong-ming, and Lai Xue-jia. A unified method for finding impossible differentials of block cipher structures[R].Cryptology ePrint Archive, Report 2009/627.

[10] Wei Yue-chuan, Li Ping, Sun Bing, *et al*.. Impossible differential cryptanalysis on Feistel ciphers with SP and SPS round functions[C]. Applied Cryptography and Network Security, Springer-Verlag, 2010, LNCS 6123: 105–122.

[11] Li Rui-lin, Sun Bing, and Li Chao. Impossible differential cryptanalysis of SPN ciphers[R]. Cryptology ePrint Archive, Report 2010/307.

[12] Bogdanov A and Rijmen V. Zero-correlation linear cryptanalysis of block cipher[R]. Cryptology ePrint Archive, Report 2011/123.

[13] Kang Ju-sung, Hong Seokhie, Lee Sangjin, *et al*.. Practical and provable security against differential and linear cryptanalysis for substitution-permutation networks[J]. *ETRI Journal*, 2001, 23(4): 158–167.

[14] Youssef A, Mister S, and Tavares S. On the design of linear transformations for substitution permutation encryption networks[C]. Workshop on Selected Areas in Cryptography-SAC'97, Ottawa, Workshop record, 1997: 40–48.

崔 霆： 男，1985 年生，博士生，研究方向为密码学.

金晨辉： 男，1965 年生，教授，研究方向为密码学和信息安全.