嵌套SP网络的New-Structure系列结构的零相关线性逼近与不可能差分性质研究

付立仕,崔 霆,金晨辉
(解放军信息工程大学,河南郑州 450001)

摘 要: 分组密码的安全性分析是密码学的重要研究内容,其中不可能差分分析和零相关线性分析是密码算法安全性分析的重要方法.本文利用中间相错方法,通过对扩散层进行限制,给出了嵌套SP网络的New-Structure系列结构的零相关线性逼近.给出了New-Structure I和New-Structure IV结构中概率非零的差分传递链和相关优势非零的线性逼近传递链在结构上的一致性.此外也给出了嵌套SP网络New-Structure I、III的16/22轮不可能差分特征.最后给出在分组规模和密钥规模均为128比特时,对New-Structure I,III,IV进行21/28/22轮的不可能差分攻击和19/28/22轮的多维零相关线性逼近攻击所需要的时间复杂度和数据复杂度.本文的结果对基于New-Structure结构设计的密码算法的安全性分析提供了理论依据.

关键词: 信息安全;不可能差分分析;零相关线性分析;New-Structure系列
中图分类号: TN918.1 **文献标识码:** A **文章编号:** 0372-2112 (2017)06-1367-08
电子学报URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2017.06.013

Zero Correlation Linear Approximations and Impossible Differentials of New-Structure Series with SP Networks

FU Li-shi, CUI Ting, JIN Chen-hui
(*PLA Information Engineering University, Zhengzhou, Henan* 450001, *China*)

Abstract: The security analysis of block cipher is an important respect in cryptology. Impossible differential analysis and zero-correlation linear cryptanalysis are important methods to evaluate the security of cryptographic algorithms. Based on miss-in-the-middle method and the restrictions on the diffusion layer, this paper gives the zero correlation linear approximations for New-Structure series with SP networks. This paper also presents the consistency between the structures of the differential characteristic with nonzero probability and linear approximation with nonzero correlation coefficient in New-Structure I and New-Structure IV. Moreover, this paper gives the 16/22-round impossible differentials for New-Structure I and III with SP networks respectively. Finally, when the block size and key size are both 128-bit, this paper gives the time complexities and data complexities of the 21/28/22-round impossible differential attack (resp. 19/28/22-round multidimensional zero-correlation linear approximation attack) on New-Structure I, III, IV. The results provide theoretical foundations for one cryptographic algorithm based on New-Structure series.

Key words: information security; impossible differential cryptanalysis; zero-correlation linear cryptanalysis; New-Structure series

1 引言

不可能差分分析方法和零相关线性逼近分析方法是目前针对分组密码的两种较为强力的攻击方法,这两种方法分别利用密码算法中差分转移概率为零的差分特征和优势为零的线性逼近来构造区分器,进而区分出正确密钥和错误密钥.不可能差分分析是由L. Kundsen[1]和E. Biham[2]独立地提出,它已被用至对AES[3]、MISTY1[4]、FOX[5,6]、SIMON[7]、LBlock[7]等算法的分析上,且取得了很好的攻击成果.零相关线性分析

收稿日期:2015-10-22;修回日期:2016-01-27;责任编辑:覃怀银
基金项目:国家自然科学基金(No.61272488, No.61402523)

可以看作是不可能差分分析在线性分析领域对应的分析方法[8~11]，并在 E2[12]、Camellia[13]、CLEFIA[13]、HIGHT[14]等算法的安全性分析上取得了好的应用. 在对具体的密码算法进行不可能差分分析和零相关线性分析时,寻找更长轮数的不可能差分特征和零相关线性逼近就成了问题的关键[15,16].

文献[17]以活动 S 盒个数的最大化为目标设计了 New-Structure Ⅰ~Ⅳ 结构. 该系列结构可以用更少的轮数提供更好的差分和线性的安全性. 文献[18]给出了嵌套 SP 网络的 New-Structure Ⅰ~Ⅳ 轮数依次为 15/∞/19/16 的不可能差分特征,但并未给出它们的零相关线性逼近,本文从线性逼近的角度刻画了嵌套 SP 网络的 New-Structure Ⅰ~Ⅳ 的安全性. 本文指出 New-Structure Ⅰ 的概率非零的 n 轮差分传递链/相关优势非零的 n 轮线性逼近传递链和 New-Structure Ⅳ 中相关优势非零的 n 轮线性逼近传递链/概率非零的 n 轮差分传递链的结构之间存在一致性,因此可通过研究 New-Structure Ⅰ 的不可能差分/零相关线性逼近来给出 New-Structure Ⅳ 的零相关线性逼近/不可能差分特征. 通过对 P 盒进行限制,本文给出了嵌套 SP 网络的 New-Structure Ⅰ~Ⅳ 的 16/∞/22/16 轮零相关线性逼近. 此外,我们分别给出了嵌套 SP 网络的 New-Structure Ⅰ 和 New-Structure Ⅲ 的 16/22 轮不可能差分特征,本文的结果优于文献[18]给出的不可能差分特征的轮数. 最后,本文给出了嵌套 SP 网络的 New-Structure Ⅰ~Ⅳ 结构的不可能差分特征和零相关线性逼近分别在不可能差分攻击和多维零相关线性逼近攻击中的具体应用,以及具体攻击所需的时间复杂度和数据复杂度.

表 1 嵌套 SP 网络的 New-Structure Ⅰ、Ⅱ、Ⅲ、Ⅳ 的不可能差分/零相关线性逼近的区分器轮数对比

结构	New Ⅰ	New Ⅱ	New Ⅲ	New Ⅳ
不可能差分特征的轮数[18]	15	∞	19	16
本文给出的零相关线性逼近的轮数	16	∞	22	16
本文给出的不可能差分特征的轮数	16	∞	22	16

2 预备知识

$\#\{x\}$:x 的个数;$\boldsymbol{P}^{\mathrm{T}}$:矩阵 $\boldsymbol{P}$ 的转置;$\boldsymbol{P}^{-1}$:矩阵 $\boldsymbol{P}$ 的逆;$\boldsymbol{P}_{(j)}$:矩阵 $\boldsymbol{P}$ 的第 j 列;$\boldsymbol{E}_{(i)}$:单位矩阵 $\boldsymbol{E}$ 的第 i 列;$\boldsymbol{P}_{(i,j)}$:矩阵 $\boldsymbol{P}$ 的第 i 行第 j 列交叉位置的元素;$\boldsymbol{e}_{|j|}$:第 j 分量非零,其它分量均为零的向量;$\boldsymbol{e}_{|j_1,j_2,\cdots,j_s|}$:第 $j_1,j_2,\cdots,j_s$ 分量非零,其它分量均为零的向量;$\Lambda_F(\boldsymbol{\alpha})$:函数 F 的输入掩码为 $\boldsymbol{\alpha}$ 时所对应的相关优势非零的输出掩码,本文利用 $\Lambda_F^{(1)}(\boldsymbol{\alpha}),\Lambda_F^{(2)}(\boldsymbol{\alpha}),\cdots$ 对相同输入掩码对应的输出掩码予以区分;$(\Delta\boldsymbol{X}_1^i,\Delta\boldsymbol{X}_2^i,\Delta\boldsymbol{X}_3^i,\Delta\boldsymbol{X}_4^i)$:第 $i+1$ 轮的输入差分;$(\boldsymbol{\gamma}_1^i,\boldsymbol{\gamma}_2^i,\boldsymbol{\gamma}_3^i,\boldsymbol{\gamma}_4^i)$:第 $i+1$ 轮的输入掩码;$\Delta_F(\Delta\boldsymbol{x})$:函数 F 的输入差分为 $\Delta\boldsymbol{x}$ 时所对应的转移概率非零的输出差分,本文利用 $\Delta_F^{(1)}(\Delta\boldsymbol{x}),\Delta_F^{(2)}(\Delta\boldsymbol{x}),\cdots$ 对相同输入差分特征的输出差分予以区分;· 代表两个比特串的内积.

定义 1[19] 函数 $\chi:F_{2^n}^l\to F_2^l$ 为 $\chi(x_1,\cdots,x_l)=(\theta(x_1),\cdots,\theta(x_l))$,$\theta:F_{2^n}\to F_2$ 为

$$\theta(x)=\begin{cases}0, & \text{当 } x=0;\\ 1, & \text{当 } x\neq 0.\end{cases}$$

则称 $\chi(x_1,\cdots,x_l)$ 为 $(x_1,\cdots,x_l)$ 的模式,其中 $F_{2^n}^l$(F_2^l)是域 F_{2^n}(二元域)中元素构成的 l 维向量空间. 为了方便,记 $\chi_i(x_1,\cdots,x_l)=\theta(x_i)$,其中 $1\leqslant i\leqslant l$.

定义 2[1] 给定函数 $F:F_{2^n}\to F_{2^n}$ 的一个差分特征 $\alpha\to\beta$,其中 $\alpha\in F_{2^n},\beta\in F_{2^n}$. 差分特征 $\alpha\to\beta$ 的概率即为 $p_F(\alpha\to\beta)=2^{-n}\times\#\{x\in F_{2^n}:F(x)\oplus F(x\oplus\alpha)=\beta\}$. 如果 $p_F(\alpha\to\beta)=0$,称 $\alpha\to\beta$ 是 F 的不可能差分特征.

定义 3[8] 给定函数 $F:F_{2^n}\to F_{2^n}$ 的一个线性逼近 $\alpha\to\beta$,其中 $\alpha\in F_{2^n},\beta\in F_{2^n}$. $C_F(\alpha\to\beta)=2\times 2^{-n}\times\#\{x\in F_{2^n}:\alpha\cdot x\oplus\beta\cdot F(x)=0\}-1$ 为 $\alpha\to\beta$ 的相关系数,$C_F(\alpha,\beta)$ 的绝对值称为该线性逼近的相关优势. 如果 $C_F(\alpha\to\beta)=0$,称 $\alpha\to\beta$ 是 F 的零相关线性逼近.

文献[15]给出了三类基本运算中线性逼近的相关系数非零的充分条件.

引理 1[15] 在异或运算⊕中,当且仅当掩码满足 $a_1=a_2=a_3$ 时,线性逼近的相关系数非零.

引理 2[15] 在分支运算中,当且仅当掩码满足 $a_1\oplus a_2\oplus a_3=0$ 时,线性逼近的相关系数非零.

引理 3[15] 设可逆 $\boldsymbol{P}$ 置换的矩阵表示为 $\boldsymbol{P}$,则当且仅当 $\boldsymbol{P}^{\mathrm{T}}\boldsymbol{a}_2=\boldsymbol{a}_1$ 时,置换的线性逼近 $\boldsymbol{a}_1\to\boldsymbol{a}_2$ 的相关系数非零.

目前常用中间相错的方法来寻找不可能差分特征和零相关线性逼近[1],也可以利用具体密码模型中不可能差分特征与零相关线性逼近之间的等价关系[16]来寻找不可能差分特征和零相关线性逼近.

3 嵌套 SP 网络的 New-Structure Series 的不可能差分特征与零相关线性逼近

New-Structure Ⅰ~Ⅳ 的具体结构如图 1 所示,本文设这 4 类结构的分组规模为 $4n$-bit,每个分支处理 n-bit 数据. 由于本文研究的是嵌套 SP 网络的 New-Structure Ⅰ~Ⅳ 的不可能差分特征和零相关线性逼近,我们设定 New-Structure Ⅰ~Ⅳ 中的 F 函数先进行 S 盒变换,再进行 P 盒变换,且轮密钥在 S 盒运算之前参与 F 函数.

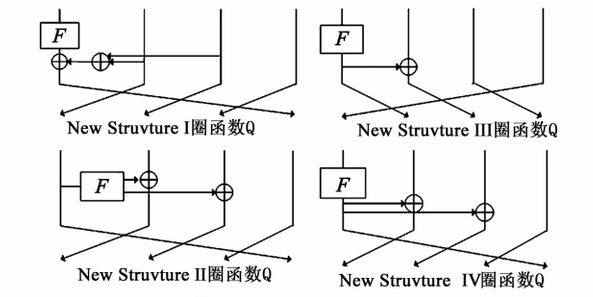


图1　New Structure系列结构

3.1　嵌套 SP 网络的 New-Structure I/IV 的 16 轮零相关线性逼近和嵌套 SP 网络的 New-Structure I 的 16 轮不可能差分特征

引理 4　设 $a,b,c,d,a',b',c',d' \in F_{2^n}$,则有

(Ⅰ)设$(a,b,c,d)\to(a',b',c',d')$为 New-Structure I 圈函数 Q 的概率非零的差分特征,则有

$(a',b',c')=(b,c,d)$和 $d'=b\oplus c\oplus\beta$,其 F 函数的差分特征为 $a\to\beta$,且

$$p_Q((a,b,c,d)\to(a',b',c',d'))=p_F(a\to\beta)=p_F(a\to b\oplus c\oplus d').$$

(Ⅱ)设$(a,b,c,d)\to(a',b',c',d')$为 New-Structure I 圈函数 Q 的相关优势非零的线性逼近,则有

$b'\oplus c=a'\oplus b=d',c'=d$,其 F 函数的线性逼近为 $a\to b'\oplus c$,且

$$\rho_Q((a,b,c,d)\to(a',b',c',d'))=\rho_F(a\to b'\oplus c).$$

证明　(1)不妨记圈函数的输入为(x,y,z,u),其中$(x,y,z,u)\in F_{2^n}^4$. 由于$(a,b,c,d)\to(a',b',c',d')$为 New-Structure I 圈函数 Q 的概率非零的差分特征,则有

$$\begin{aligned}&p_Q((a,b,c,d)\to(a',b',c',d'))\\&=\frac{1}{2^{4n}}\#\{(x,y,z,u)\in F_{2^n}^4:(y\oplus b,z\oplus c,u\oplus d,y\oplus b\oplus(z\oplus c)\oplus F(x\oplus a))\oplus(y,z,u,y\oplus z\oplus F(x))\\&=(a',b',c',d')\}\\&=\frac{1}{2^{4n}}\#\{(x,y,z,u)\in F_{2^n}^4:(b,c,d,b\oplus c\oplus F(x\oplus a)\oplus F(x))=(a',b',c',d')\}.\end{aligned}$$

故由 $p_Q((a,b,c,d)\to(a',b',c',d'))\neq 0$ 知$(b,c,d)=(a',b',c')\}$,且

$$\begin{aligned}&p_Q((a,b,c,d)\to(a',b',c',d'))\\&=\frac{1}{2^n}\#\{x\in F_{2^n}:b\oplus c\oplus F(x\oplus a)\oplus F(x)=d'\}\\&=p_F(a\to b\oplus c\oplus d').\end{aligned}$$

(2) 设$(a,b,c,d)\to(a',b',c',d')$为 New-Structure I 圈函数 Q 的相关优势非零的线性逼近,则

$$\begin{aligned}&(a,b,c,d)\cdot(x,y,z,u)\oplus(a',b',c',d')\cdot(y,z,u,y\oplus z\oplus F(x))\\&=(b\oplus a'\oplus d')\cdot y\oplus(c\oplus b'\oplus d')\cdot z\oplus(d\oplus c')\cdot u\oplus a\cdot x\oplus d'\cdot F(x).\end{aligned}$$

因此,

$$\begin{aligned}&\rho_Q((a,b,c,d)\to(a',b',c',d'))\\&=2^{-4n}\times\sum_{(x,y,z,u)\in F_{2^n}^4}(-1)^{(a,b,c,d)\cdot(x,y,z,u)\oplus(a',b',c',d')\cdot(y,z,u,y\oplus z\oplus F(x))}\\&=2^{-4n}\times\sum_{(x,y,z,u)\in F_{2^n}^4}(-1)^{(b\oplus a'\oplus d')\cdot y\oplus(c\oplus b'\oplus d')\cdot z\oplus(d\oplus c')\cdot u\oplus a\cdot x\oplus d'\cdot F(x)}\\&=2^{-4n}\times\sum_{(x,y,z,u)\in F_{2^n}^4}(-1)^{(b\oplus a'\oplus d')\cdot y\oplus(c\oplus b'\oplus d')\cdot z\oplus(d\oplus c')\cdot u\oplus a\cdot x\oplus d'\cdot F(x)}\\&=2^{-n}\times\sum_{y\in F_{2^n}}(-1)^{(b\oplus a'\oplus d')\cdot y}\times 2^{-n}\times\sum_{z\in F_{2^n}}(-1)^{(c\oplus b'\oplus d')\cdot z}\\&\quad\times 2^{-n}\times\sum_{u\in F_{2^n}}(-1)^{(d\oplus c')\cdot u}\times 2^{-n}\times\sum_{x\in F_{2^n}}(-1)^{a\cdot x\oplus d'\cdot F(x)}.\end{aligned}$$

由于对于形式为 $\sum_{y\in F_{2^n}}(-1)^{A\cdot y}$ 的函数,若 y 遍历 F_{2^n},则当 $A=0$ 时,$\sum_{y\in F_{2^n}}(-1)^{A\cdot y}=2^n$,而当 $A\neq 0$ 时,$\sum_{y\in F_{2^n}}(-1)^{A\cdot y}=0$. 由于 $\rho_Q((a,b,c,d)\to(a',b',c',d'))\neq 0$,因此可得 $b'\oplus c=a'\oplus b=d',c'=d$. 进一步可得,

$$\begin{aligned}&\rho_Q((a,b,c,d)\to(a',b',c',d'))\\&=2^{-4n}\times\sum_{(x,y,z,u)\in F_{2^n}^4}(-1)^{(a,b,c,d)\cdot(x,y,z,u)\oplus(a',b',c',d')\cdot(y,z,u,y\oplus z\oplus F(x))}\\&=2^{-n}\times 2^n\times 2^{-n}\times 2^n\times 2^{-n}\times 2^n\times 2^{-n}\times\sum_{x\in F_{2^n}}(-1)^{a\cdot x\oplus d'\cdot F(x)}\\&=2^{-n}\times\sum_{x\in F_{2^n}}(-1)^{a\cdot x\oplus d'\cdot F(x)}\\&=2^{-n}\times\sum_{x\in F_{2^n}}(-1)^{a\cdot x\oplus(b'\oplus c)\cdot F(x)}=\rho_F(a\to b'\oplus c).\end{aligned}$$

即 $\rho_Q((a,b,c,d)\to(a',b',c',d'))=\rho_F(a\to b'\oplus c)$,故(Ⅱ)成立.

引理 5　设 $a,b,c,d,a',b',c',d'\in F_{2^n}$,则有

(Ⅰ)设$(a,b,c,d)\to(a',b',c',d')$为 New-Structure IV 圈函数 Q 的概率非零的差分特征,则有

$b'\oplus c=a'\oplus b=d',c'=d$,其 F 函数的差分特征为 $a\to b'\oplus c$,且

$$p_Q((a,b,c,d)\to(a',b',c',d'))=p_F(a\to b'\oplus c).$$

(Ⅱ)设$(a,b,c,d)\to(a',b',c',d')$为 New-Structure IV 圈函数 Q 的优势非零的线性逼近,则有

$(a',b',c')=(b,c,d)$和 $d'=b\oplus c\oplus\beta$,其 F 函数的线性逼近为 $a\to\beta$,且

$$\rho_Q((a,b,c,d)\to(a',b',c',d'))=\rho_F(a\to\beta).$$

证明　引理 5 的证明与引理 4 类似,在此不再展开详细证明.

由引理 4 及引理 5 可直接得到 New-Structure I/New-Structure IV 中概率非零的 n 轮差分传递链和相关优势非零的 n 轮线性逼近传递链的结构,如定理 1 及定理 2 所示.

定理 1　设 $a_{i,j}\in F_{2^n}$,其中 $i\in\{0,\cdots,n\}$,$j\in\{1,2,$

3,4\},则有

(Ⅰ)设$(a_{0,1},a_{0,2},a_{0,3},a_{0,4})\rightarrow(a_{1,1},a_{1,2},a_{1,3},a_{1,4})\rightarrow\cdots\rightarrow(a_{n,1},a_{n,2},a_{n,3},a_{n,4})$为 New-Structure Ⅰ中概率非零的 n 轮差分传递链,则有$(a_{i+1,1},a_{i+1,2},a_{i+1,3})=(a_{i,2},a_{i,3},a_{i,4})$和 $a_{i+1,4}=a_{i,2}\oplus a_{i,3}\oplus\beta_i$,第 $i(i\in\{0,\cdots,n-1\})$ 轮 F 函数的差分特征为 $a_i\rightarrow\beta_i$,且

$$p((a_{0,1},a_{0,2},a_{0,3},a_{0,4})\rightarrow\cdots\rightarrow(a_{n,1},a_{n,2},a_{n,3},a_{n,4}))=\prod_{i\in\{0,\cdots,n-1\}}p_F(a_{i,1}\rightarrow a_{i+1,4}\oplus a_{i,2}\oplus a_{i,3}).$$

(Ⅱ)设$(a_{0,1},a_{0,2},a_{0,3},a_{0,4})\rightarrow(a_{1,1},a_{1,2},a_{1,3},a_{1,4})\rightarrow\cdots\rightarrow(a_{n,1},a_{n,2},a_{n,3},a_{n,4})$为 New-Structure Ⅰ中相关优势非零的 n 轮线性逼近传递链,则有 $a_{i+1,2}\oplus a_{i,3}=a_{i+1,1}\oplus a_{i,2}=a_{i+1,4}$,$a_{i+1,3}=a_{i,4}$,第 $i(i\in\{0,\cdots,n-1\})$ 轮 F 函数的线性逼近为 $a_{i,1}\rightarrow a_{i+1,2}\oplus a_{i,3}$,且

$$\rho((a_{0,1},a_{0,2},a_{0,3},a_{0,4})\rightarrow\cdots\rightarrow(a_{n,1},a_{n,2},a_{n,3},a_{n,4}))=\prod_{i\in\{0,\cdots,n-1\}}\rho_F(a_{i,1}\rightarrow a_{i+1,2}\oplus a_{i,3}).$$

定理 2 设 $a_{i,j}\in F_{2^n}$,其中 $i\in\{0,\cdots,n\}$,$j\in\{1,2,3,4\}$,则有

(Ⅰ)设$(a_{0,1},a_{0,2},a_{0,3},a_{0,4})\rightarrow(a_{1,1},a_{1,2},a_{1,3},a_{1,4})\rightarrow\cdots\rightarrow(a_{n,1},a_{n,2},a_{n,3},a_{n,4})$为 New-Structure Ⅳ 中概率非零的 n 轮差分传递链,则有 $a_{i+1,2}\oplus a_{i,3}=a_{i+1,1}\oplus a_{i,2}=a_{i+1,4}$,$a_{i+1,3}=a_{i,4}$,第 $i(i\in\{0,\cdots,n-1\})$ 轮 F 函数的差分特征为 $a_{i,1}\rightarrow a_{i+1,2}\oplus a_{i,3}$,且

$$p((a_{0,1},a_{0,2},a_{0,3},a_{0,4})\rightarrow\cdots\rightarrow(a_{n,1},a_{n,2},a_{n,3},a_{n,4}))=\prod_{i\in\{0,\cdots,n-1\}}p_F(a_{i,1}\rightarrow a_{i+1,2}\oplus a_{i,3}).$$

(Ⅱ)设$(a_{0,1},a_{0,2},a_{0,3},a_{0,4})\rightarrow(a_{1,1},a_{1,2},a_{1,3},a_{1,4})\rightarrow\cdots\rightarrow(a_{n,1},a_{n,2},a_{n,3},a_{n,4})$为 New-Structure Ⅳ 中相关优势非零的 n 轮线性逼近传递链,则有$(a_{i+1,1},a_{i+1,2},a_{i+1,3})=(a_{i,2},a_{i,3},a_{i,4})$和 $a_{i+1,4}=a_{i,2}\oplus a_{i,3}\oplus\beta_i$,第 $i(i\in\{0,\cdots,n-1\})$ 轮 F 函数的线性逼近为 $a_i\rightarrow\beta_i$,且

$$\rho((a_{0,1},a_{0,2},a_{0,3},a_{0,4})\rightarrow\cdots\rightarrow(a_{n,1},a_{n,2},a_{n,3},a_{n,4}))=\prod_{i\in\{0,\cdots,n-1\}}\rho_F(a_{i,1}\rightarrow a_{i+1,4}\oplus a_{i,2}\oplus a_{i,3}).$$

由定理 1 及定理 2 可知,New-Structure Ⅰ中概率非零的 n 轮差分传递链(相关优势非零的 n 轮线性逼近传递链)与 New-Structure Ⅳ 中相关优势非零的 n 轮线性逼近传递链(概率非零的 n 轮差分传递链)具有相同的结构形式.

引理 6[18] 在 New-Structure Ⅳ 中,若一条概率非零的差分传递链满足$(\Delta\boldsymbol{X}_1^0,\Delta\boldsymbol{X}_2^0,\Delta\boldsymbol{X}_3^0,\Delta\boldsymbol{X}_4^0)=(\boldsymbol{0},\boldsymbol{0},\boldsymbol{0},\Delta\boldsymbol{x})$,则 $\Delta_P(\Delta\boldsymbol{x})=\Delta\boldsymbol{X}_1^7\oplus\Delta\boldsymbol{X}_3^7\oplus\Delta\boldsymbol{X}_4^7$;若一条概率非零的差分传递链满足$(\Delta\boldsymbol{X}_1^t,\Delta\boldsymbol{X}_2^t,\Delta\boldsymbol{X}_3^t,\Delta\boldsymbol{X}_4^t)=(\Delta\boldsymbol{y},\boldsymbol{0},\boldsymbol{0},\boldsymbol{0})$,则 $\Delta\boldsymbol{y}\oplus\Delta_{F^{-1}}^{(1)}(\Delta\boldsymbol{y})\oplus\Delta_{F^{-1}}^{(2)}(\Delta\boldsymbol{y})=\Delta\boldsymbol{X}_1^{t-9}\oplus\Delta\boldsymbol{X}_3^{t-9}\oplus\Delta\boldsymbol{X}_4^{t-9}$.

结合引理 6,并基于 New-Structure Ⅰ中相关优势非零的 n 轮线性传递链和 New-Structure Ⅳ 中概率非零的 n 轮差分传递链在结构上的一致性,本文可直接给出 New-Structure Ⅰ结构的线性逼近传递链的性质,如推论 1 所示.

推论 1 在 New-Structure Ⅰ中,若相关优势非零的线性逼近传递链满足$(\boldsymbol{\gamma}_1^0,\boldsymbol{\gamma}_2^0,\boldsymbol{\gamma}_3^0,\boldsymbol{\gamma}_4^0)=(\boldsymbol{0},\boldsymbol{0},\boldsymbol{0},\boldsymbol{\alpha})$,则 $\Lambda_F(\boldsymbol{\alpha})=\boldsymbol{\gamma}_1^7\oplus\boldsymbol{\gamma}_3^7\oplus\boldsymbol{\gamma}_4^7$;若相关优势非零的线性逼近传递链满足$(\boldsymbol{\gamma}_1^t,\boldsymbol{\gamma}_2^t,\boldsymbol{\gamma}_3^t,\boldsymbol{\gamma}_4^t)=(\boldsymbol{\beta},\boldsymbol{0},\boldsymbol{0},\boldsymbol{0})$,则 $\boldsymbol{\beta}\oplus\Lambda_{F^{-1}}^{(1)}(\boldsymbol{\beta})\oplus\Lambda_{F^{-1}}^{(2)}(\boldsymbol{\beta})=\boldsymbol{\gamma}_1^{t-9}\oplus\boldsymbol{\gamma}_3^{t-9}\oplus\boldsymbol{\gamma}_4^{t-9}$.

基于推论 1,接下来我们将 New-Structure Ⅰ和 New-Structure Ⅳ 中的非线性函数具体为 SP 网络结构,并通过中间相错方法给出嵌套 SP 网络的 New-Structure Ⅰ的 16 轮零相关线性逼近,如定理 3 所示.

定理 3 设 $GF(2^n)$ 上的矩阵 $\boldsymbol{P}_{d\times d}$为嵌套 SP 网络的 New-Structure Ⅰ的扩散层,若存在 $i\neq j_2$,使得 $\boldsymbol{P}_{(j_1,i)}^{-1}\neq\boldsymbol{0}$ 且 $\boldsymbol{P}_{(j_2,i)}=\boldsymbol{0}$,则$(\boldsymbol{0},\boldsymbol{0},\boldsymbol{0},\boldsymbol{e}_{|j_1|})\nrightarrow(\boldsymbol{e}_{|j_2|},\boldsymbol{0},\boldsymbol{0},\boldsymbol{0})$为嵌套 SP 网络的 New-Structure Ⅰ的 16 轮零相关线性逼近.

证明 我们仅需要从加、脱密方向在组合 $\boldsymbol{\gamma}_1^7\oplus\boldsymbol{\gamma}_3^7\oplus\boldsymbol{\gamma}_4^7$ 处找出矛盾,结合推论 1 知需要证明 $\boldsymbol{e}_{|j_2|}\oplus\Lambda_{F^{-1}}^{(1)}(\boldsymbol{e}_{|j_2|})\oplus\Lambda_{F^{-1}}^{(2)}(\boldsymbol{e}_{|j_2|})\neq\Lambda_F(\boldsymbol{e}_{|j_1|})$,即证明

$$\boldsymbol{e}_{|j_2|}\oplus\Lambda_{S^{-1}}^{(1)}(\boldsymbol{P}^{\mathrm{T}}\times\boldsymbol{e}_{|j_2|})\oplus\Lambda_{S^{-1}}^{(2)}(\boldsymbol{P}^{\mathrm{T}}\times\boldsymbol{e}_{|j_2|})\oplus((\boldsymbol{P}^{\mathrm{T}})^{-1}\times\Lambda_S(\boldsymbol{e}_{|j_1|}))\neq0.$$

由 $i\neq j_2$ 知 $\chi_i(\boldsymbol{e}_{|j_2|})=0$,不妨令 $\boldsymbol{e}_{|j_2|}$ 中非零的分量为 ξ,$\Lambda_S(\boldsymbol{e}_{j_1})$中非零分量为 v,则

$$\chi_i[\Lambda_{S^{-1}}^{(1)}(\boldsymbol{P}^{\mathrm{T}}\times\boldsymbol{e}_{|j_2|})]=\chi_i[\Lambda_{S^{-1}}^{(2)}(\boldsymbol{P}^{\mathrm{T}}\times\boldsymbol{e}_{|j_2|})]=\chi_i[\xi\cdot\boldsymbol{P}_{(j_2)}^{\mathrm{T}}]=\theta(\boldsymbol{P}_{(i,j_2)}^{\mathrm{T}})=\theta(\boldsymbol{P}_{(j_2,i)})=0.$$

$$\text{又}\chi_i[(\boldsymbol{P}^{\mathrm{T}})^{-1}\times\Lambda_S(\boldsymbol{e}_{|j_1|})]=\theta[v\cdot(\boldsymbol{P}^{\mathrm{T}})_{(i,j_1)}^{-1}]=\theta[(\boldsymbol{P}^{\mathrm{T}})_{(i,j_1)}^{-1}]=\theta(\boldsymbol{P}_{(j_1,i)}^{-1})\neq0,\text{故}$$

$$\boldsymbol{e}_{|j_2|}\oplus\Lambda_{S^{-1}}^{(1)}(\boldsymbol{P}^{\mathrm{T}}\times\boldsymbol{e}_{|j_2|})\oplus\Lambda_{S^{-1}}^{(2)}(\boldsymbol{P}^{\mathrm{T}}\times\boldsymbol{e}_{|j_2|})\oplus((\boldsymbol{P}^{\mathrm{T}})^{-1}\times\Lambda_S(\boldsymbol{e}_{|j_1|}))\neq0.$$

接下来,本文给出嵌套 SP 网络的 New-Structure Ⅰ的 16 轮不可能差分特征,如定理 4 所示. 我们首先给出 New-Structure Ⅰ的差分传递链的性质.

性质 1 在 New-Structure Ⅰ中,若概率非零的差分传递链满足$(\Delta\boldsymbol{X}_1^0,\Delta\boldsymbol{X}_2^0,\Delta\boldsymbol{X}_3^0,\Delta\boldsymbol{X}_4^0)=(\boldsymbol{0},\boldsymbol{0},\boldsymbol{0},\Delta\boldsymbol{x})$,则 $\Delta_F^{(1)}(\Delta\boldsymbol{x})\oplus\Delta_F^{(2)}(\Delta\boldsymbol{x})\oplus\Delta\boldsymbol{x}=\Delta\boldsymbol{X}_1^{12}$;若概率非零的差分传递链满足$(\Delta\boldsymbol{X}_1^t,\Delta\boldsymbol{X}_2^t,\Delta\boldsymbol{X}_3^t,\Delta\boldsymbol{X}_4^t)=(\boldsymbol{0},\Delta\boldsymbol{y},\boldsymbol{0},\Delta\boldsymbol{y})$,则 $\Delta_{F^{-1}}(\Delta_{F^{-1}}(\Delta\boldsymbol{y}))=\Delta\boldsymbol{X}_1^{t-4}$.

定理 4 设 $GF(2^n)$ 上的矩阵 $\boldsymbol{P}_{d\times d}$为嵌套 SP 网络的 New-Structure Ⅰ结构的扩散层,且存在 $i\neq j_1$,使得 $\boldsymbol{P}_{(i,j_1)}=\boldsymbol{0}$ 且 $\boldsymbol{P}_{(i,j_2)}^{-1}\neq\boldsymbol{0}$,则$(\boldsymbol{0},\boldsymbol{0},\boldsymbol{0},\boldsymbol{e}_{|j_1|})\nrightarrow(\boldsymbol{0},\boldsymbol{P}\times\boldsymbol{e}_{|j_2|},\boldsymbol{0},\boldsymbol{P}\times\boldsymbol{e}_{|j_2|})$为嵌套 SP 网络的 New-Structure Ⅰ结构的 16 轮不可能差分特征.

证明 我们仅需要从加、脱密方向在 $\Delta\boldsymbol{X}_1^{12}$ 处找出矛盾,结合性质 1,即证明

$$\Delta_{P\circ S}^{(1)}(\boldsymbol{e}_{|j_1|})\oplus\Delta_{P\circ S}^{(2)}(\boldsymbol{e}_{|j_1|})\oplus\boldsymbol{e}_{|j_1|}\neq\Lambda_{(P\circ S)^{-1}\circ(P\circ S)^{-1}}(\boldsymbol{P}\times$$

$\boldsymbol{e}_{|j_2|}$).

从加密方向考察有 $\Delta \boldsymbol{X}_1^{12}=\Delta_{P\circ S}^{(1)}(\boldsymbol{e}_{|j_1|})\oplus\Delta_{P\circ S}^{(2)}(\boldsymbol{e}_{|j_1|})\oplus\boldsymbol{e}_{|j_1|}=\boldsymbol{P}\times[\Delta_S^{(1)}(\boldsymbol{e}_{|j_1|})\oplus\Delta_S^{(2)}(\boldsymbol{e}_{|j_1|})]\oplus\boldsymbol{e}_{|j_1|}$. 令 $\boldsymbol{\varpi}=\Delta_S^{(1)}(\boldsymbol{e}_{|j_1|})\oplus\Delta_S^{(2)}(\boldsymbol{e}_{|j_1|})$,并假设 $\boldsymbol{\varpi}$ 的第 k 分量为 ϖ_k. 由 $i\neq j_1$ 知 $\boldsymbol{e}_{|j_1|}$ 的第 i 分量为 0,故 $\chi_i(\Delta \boldsymbol{X}_1^{12})=\chi_i((\boldsymbol{P}\times\boldsymbol{\varpi})\oplus\boldsymbol{e}_{|j_1|})=\chi_i(\boldsymbol{\varpi}_{j_1}\cdot\boldsymbol{P}_{(j_1)}\oplus\boldsymbol{e}_{|j_1|})$. 由 $\boldsymbol{P}_{(i,j_1)}=\boldsymbol{0}$ 知 $\chi_i(\boldsymbol{\varpi}_{j_1}\cdot\boldsymbol{P}_{(j_1)})=\theta(\boldsymbol{\varpi}_{j_1}\cdot\boldsymbol{P}_{(i,j_1)})=0$,又 $\chi_i(\boldsymbol{e}_{|j_1|})=0$,故 $\chi_i(\Delta \boldsymbol{X}_1^{12})=0$.

另一方面,从脱密方向考察 $\Delta \boldsymbol{X}_1^{12}$,有

$$\begin{aligned}\Delta \boldsymbol{X}_1^{12}&=\Delta_{(P\circ S)^{-1}\circ(P\circ S)^{-1}}(\boldsymbol{P}\times\boldsymbol{e}_{|j_2|})=\Delta_{(P\circ S)^{-1}\circ S^{-1}}\boldsymbol{P}^{-1}(\boldsymbol{P}\times\boldsymbol{e}_{|j_2|})\\&=\Delta_{(P\circ S)^{-1}\circ S^{-1}}(\boldsymbol{e}_{|j_2|})\\&=\Delta_{S^{-1}\circ P^{-1}}(\Lambda_{S^{-1}}(\boldsymbol{e}_{|j_2|}))=\Delta_{S^{-1}\circ P^{-1}}(\boldsymbol{e}'_{|j_2|})\\&=\Delta_{S^{-1}}(\boldsymbol{P}^{-1}\times\boldsymbol{e}_{|j_2|}).\end{aligned}$$

故 $\chi_i(\Delta_{S^{-1}}(\boldsymbol{P}^{-1}\times\boldsymbol{e}'_{|j_2|}))=\chi_i(\boldsymbol{P}^{-1}\times\boldsymbol{e}'_{|j_2|})=\theta(\boldsymbol{P}^{-1}_{(i,j_2)})\neq0$,这与从加密方向得出 $\chi_i(\Delta \boldsymbol{X}_1^{12})=\boldsymbol{0}$ 的结论相矛盾.

基于 New-Structure I 中概率非零的 n 轮差分传递链和 New-Structure IV 中相关优势非零的 n 轮线性传递链在结构上的一致性,我们可由性质 1 直接得到 New-Structure IV 线性逼近传递链的性质,如性质 2 所示. 基于性质 2,定理 5 给出了嵌套 SP 网络的 New-Structure IV 的 16 轮零相关线性逼近.

性质 2　在 New-Structure IV 中,若相关优势非零的线性逼近传递链满足 $(\boldsymbol{\gamma}_1^0,\boldsymbol{\gamma}_2^0,\boldsymbol{\gamma}_3^0,\boldsymbol{\gamma}_4^0)=(\boldsymbol{0},\boldsymbol{0},\boldsymbol{0},\boldsymbol{\alpha})$,则 $\Lambda_F^{(1)}(\boldsymbol{\alpha})\oplus\Lambda_F^{(2)}(\boldsymbol{\alpha})\oplus\boldsymbol{\alpha}=\boldsymbol{\gamma}_1^{12}$. 若相关优势非零的线性逼近传递链满足 $(\boldsymbol{\gamma}_1^t,\boldsymbol{\gamma}_2^t,\boldsymbol{\gamma}_3^t,\boldsymbol{\gamma}_4^t)=(\boldsymbol{0},\boldsymbol{\beta},\boldsymbol{0},\boldsymbol{\beta})$,则 $\Lambda_{F^{-1}}(\Lambda_{F^{-1}}(\beta))=\boldsymbol{\gamma}_1^{t-4}$.

定理 5　设 GF(2^n)上的矩阵 $\boldsymbol{P}_{d\times d}$为嵌套 SP 网络的 New-Structure IV 结构的扩散层,且存在 $i\neq j_1$ 使得 $\boldsymbol{P}^{-1}_{(j_1,i)}=\boldsymbol{0}$ 且 $\boldsymbol{P}_{(j_2,i)}\neq\boldsymbol{0}$,则 $(\boldsymbol{0},\boldsymbol{0},\boldsymbol{0},\boldsymbol{e}_{|j_1|})\nrightarrow(\boldsymbol{0},(\boldsymbol{P}^{\mathrm{T}})^{-1}\times\boldsymbol{e}_{|j_2|},\boldsymbol{0},(\boldsymbol{P}^{\mathrm{T}})^{-1}\times\boldsymbol{e}_{|j_2|})$ 为嵌套 SP 网络的 New-Structure IV 结构的 16 轮零相关线性逼近.

证明　我们仅需要从加脱密方向在 γ_1^{12} 处得出矛盾,即证明 $\Lambda_{P\circ S}^{(1)}(\boldsymbol{e}_{|j_1|})\oplus\Lambda_{P\circ S}^{(2)}(\boldsymbol{e}_{|j_1|})\oplus\boldsymbol{e}_{|j_1|}\neq\Lambda_{(P\circ S)^{-1}\circ(P\circ S)^{-1}}((\boldsymbol{P}^{\mathrm{T}})^{-1}\times\boldsymbol{e}_{|j_2|})$,该证明过程与定理 4 类似.

3.2　嵌套 SP 网络的 New-Structure II 的任意轮的零相关线性逼近

文献[18]中给出了 New-Structure II 任意轮的不可能差分特征,在本文中我们考察对于 New-Structure II 是否有任意轮的零相关线性逼近存在.

定理 6　设 $(\alpha,\alpha,\alpha,\alpha)$ 为 New-Structure II 结构 1 圈的输入掩码,则其输出掩码必为 $(\alpha,\alpha,\alpha,\alpha)$.

证明　不妨令 New-Structure II 的四个输入变量为 (x_1,x_2,x_3,x_4),则根据其圈函数表达式可得输出为 $(x_2\oplus F(x_1),x_3\oplus F(x_1),x_4,x_1)$. 对于线性逼近 $(\alpha,\alpha,\alpha,\alpha)\rightarrow(\alpha,\alpha,\alpha,\alpha)$,其线性概率为

$$\begin{aligned}&\Pr_{x_1,x_2,x_3,x_4}\{(\alpha,\alpha,\alpha,\alpha)\cdot(x_1,x_2,x_3,x_4)\oplus(\alpha,\alpha,\alpha,\alpha)\\&\cdot(x_2\oplus F(x_1),x_3\oplus F(x_1),x_4,x_1)=0\}\\&=\Pr_{x_1,x_2,x_3,x_4}\{(\alpha\oplus\alpha)\cdot(x_1\oplus x_2\oplus x_3\oplus x_4)=0\}=1.\end{aligned}$$

故当 New-Structure II 结构的输入掩码为 $(\alpha,\alpha,\alpha,\alpha)$时,其输出掩码也为 $(\alpha,\alpha,\alpha,\alpha)$.

基于定理 6,我们直接给出 New-Structure II 的任意 n 轮零相关线性逼近,如下推论 2 所示.

推论 2　对于任意 n 轮线性逼近 $(\alpha,\alpha,\alpha,\alpha)\rightarrow(\beta_1,\beta_2,\beta_3,\beta_4)$,若 $\beta_1,\beta_2,\beta_3,\beta_4$ 中至少有一个与 α 不等,则 $(\alpha,\alpha,\alpha,\alpha)\rightarrow(\beta_1,\beta_2,\beta_3,\beta_4)$ 为 New-Structure II 的 n 轮零相关线性逼近.

由推论 2 可知,New-Structure II 存在任意轮的零相关线性逼近,且该线性逼近对 F 函数没有限制,因此对嵌套 SP 网络的 New-Structure II 也必然存在任意轮的零相关线性逼近.

3.3　嵌套 SP 网络的 New-Structure III 结构的 22 轮零相关线性逼近/22 轮不可能差分特征

引理 7　设 $a,b,c,d,a',b',c',d'\in F_{2^n}$,$(a,b,c,d)\rightarrow(a',b',c',d')$为 New-Structure III 圈函数 Q 的相关优势非零的线性逼近,则有 $a'=d,b'=b\oplus\gamma,c'=b,d'=c$,其 F 函数的线性逼近为 $a\rightarrow\gamma$,且

$$\rho_Q((a,b,c,d)\rightarrow(a',b',c',d'))=\rho_F(a\rightarrow\gamma).$$

证明　引理 7 的证明过程与引理 4 之(II)的证明过程类似,在此不再展开证明.

根据引理 7,我们可得 New-Structure III 的线性逼近传递链有如下性质.

性质 3　在 New-Structure III 中,若相关优势非零的线性逼近传递链满足 $(\boldsymbol{\gamma}_1^0,\boldsymbol{\gamma}_2^0,\boldsymbol{\gamma}_3^0,\boldsymbol{\gamma}_4^0)=(\boldsymbol{0},\boldsymbol{0},\boldsymbol{\alpha},\boldsymbol{0})$,则 $\boldsymbol{\varepsilon}\oplus\Lambda_F^{(1)}(\boldsymbol{\varepsilon})\oplus\Lambda_F^{(2)}(\boldsymbol{\varepsilon})\oplus\Lambda_F^{(3)}(\boldsymbol{\varepsilon})\oplus\Lambda_F^{(4)}(\boldsymbol{\varepsilon})=\boldsymbol{\gamma}_2^{10}$,其中 $\boldsymbol{\varepsilon}=\Lambda_F(\boldsymbol{\alpha})$;若相关优势非零的线性逼近传递链满足 $(\boldsymbol{\gamma}_1^t,\boldsymbol{\gamma}_2^t,\boldsymbol{\gamma}_3^t,\boldsymbol{\gamma}_4^t)=(\boldsymbol{\beta},\boldsymbol{\beta},\boldsymbol{\beta},\boldsymbol{\beta})$,则有 $\boldsymbol{\gamma}_2^{t-12}=\boldsymbol{0}$.

根据性质 3,我们通过限定嵌套 SP 网络的 New-Structure III 中扩散层的结构,给出了嵌套 SP 网络的 New-Structure III 中 22 轮的零相关线性逼近,如定理 7 所示.

定理 7　设 GF(2^n)上的可逆矩阵 $\boldsymbol{P}_{d\times d}$为嵌套 SP 网络的 New-Structure III 的扩散层,若 $(\boldsymbol{P}^{\mathrm{T}})^{-1}_{(i_1)},(\boldsymbol{P}^{\mathrm{T}})^{-1}_{(i_2)},\cdots,(\boldsymbol{P}^{\mathrm{T}})^{-1}_{(i_t)},\boldsymbol{E}_{(i_1)},\boldsymbol{E}_{(i_2)},\cdots,\boldsymbol{E}_{(i_t)}$线性无关,其中 $i_1,i_2,\cdots,i_t$ 为 $(\boldsymbol{P}^{\mathrm{T}})^{-1}_{(j)}$ 中非零分量的位置. 则对任意的 $\boldsymbol{\beta}\in\mathrm{GF}(2^n)^d\backslash\{\boldsymbol{0}\}$,$(\boldsymbol{0},\boldsymbol{0},\boldsymbol{e}_{|j|},\boldsymbol{0})\nrightarrow(\boldsymbol{\beta},\boldsymbol{\beta},\boldsymbol{\beta},\boldsymbol{\beta})$均为嵌套 SP 网络的 New-Structure III 结构的 22 轮零相关线性逼近.

证明　根据性质 3,我们仅需要从加、脱密方向在 $\boldsymbol{\gamma}_2^{10}$ 处寻找矛盾,即证明 $\boldsymbol{\varepsilon}\oplus\Lambda_F^{(1)}(\boldsymbol{\varepsilon})\oplus\Lambda_F^{(2)}(\boldsymbol{\varepsilon})\oplus\Lambda_F^{(3)}(\boldsymbol{\varepsilon})\oplus\Lambda_F^{(4)}(\boldsymbol{\varepsilon})\neq\boldsymbol{0}$,其中 $\boldsymbol{\varepsilon}=\Lambda_F(\boldsymbol{e}_{|j|})$.

由于 $\boldsymbol{\varepsilon}=\Lambda_F(\boldsymbol{e}_{|j|})=\Lambda_{P\circ S}(\boldsymbol{e}_{|j|})=(\boldsymbol{P}^{\mathrm{T}})^{-1}\times\Lambda_s(\boldsymbol{e}_{|j|})$，记 $\Lambda_s(\boldsymbol{e}_{|j|})=\boldsymbol{e}'_{|j|}$，并设 $e'_{|j|}$ 非零分量为 ξ，故 $\boldsymbol{\varepsilon}=((\boldsymbol{P}^{\mathrm{T}})^{-1}_{(1,j)}\cdot\xi,(\boldsymbol{P}^{\mathrm{T}})^{-1}_{(2,j)}\cdot\xi,\cdots,(\boldsymbol{P}^{\mathrm{T}})^{-1}_{(n,j)}\cdot\xi)^{\mathrm{T}}$.

又 $(\boldsymbol{P}^{\mathrm{T}})^{-1}$ 中第 j 列中非零的分量位置为 $i_1,i_2,\cdots,i_t$，则 $\boldsymbol{\varepsilon}=\boldsymbol{e}_{|i_1,i_2,\cdots,i_t|}$，故可得 $\Lambda_F(\boldsymbol{\varepsilon})=\Lambda_{P\circ S}(\boldsymbol{e}_{|i_1,i_2,\cdots,i_t|})=(\boldsymbol{P}^{\mathrm{T}})^{-1}\times\Lambda_S(\boldsymbol{e}_{|i_1,i_2,\cdots,i_t|})$. 下面考察 $\boldsymbol{\varepsilon}\oplus\Lambda_F^{(1)}(\boldsymbol{\varepsilon})\oplus\Lambda_F^{(2)}(\boldsymbol{\varepsilon})\oplus\Lambda_F^{(3)}(\boldsymbol{\varepsilon})\oplus\Lambda_F^{(4)}(\boldsymbol{\varepsilon})$.

设 $\boldsymbol{\varpi}_k$ 为 $\bigoplus_{m=1}^{4}\Lambda_S^{(m)}(\boldsymbol{e}_{|i_1,\cdots,i_t|})$ 的第 k 分量，则对 $k\notin\{i_1,\cdots,i_t\}$，总有 $\boldsymbol{\varpi}_k=0$ 成立. 不妨记 $\boldsymbol{e}_{|i_1,\cdots,i_t|}$ 中非零分量依次为 $e_{i_1},e_{i_2},\cdots e_{i_t}$，因此有

$$(\boldsymbol{P}^{\mathrm{T}})^{-1}\times\bigoplus_{m=1}^{4}\Lambda_S^{(m)}(\boldsymbol{e}_{|i_1,\cdots,i_t|})\oplus\boldsymbol{e}_{|i_1,\cdots,i_t|}=\bigoplus_{l=1}^{t}(\boldsymbol{\varpi}_{i_l}\times(\boldsymbol{P}^{\mathrm{T}})^{-1}_{(i_l)})\oplus\bigoplus_{l=1}^{t}(e_{i_l}\times\boldsymbol{E}_{(i_l)}).$$

因 $(\boldsymbol{P}^{\mathrm{T}})^{-1}_{(i_1)},(\boldsymbol{P}^{\mathrm{T}})^{-1}_{(i_2)},\cdots,(\boldsymbol{P}^{\mathrm{T}})^{-1}_{(i_t)},\boldsymbol{E}_{(i_1)},\boldsymbol{E}_{(i_2)},\cdots,\boldsymbol{E}_{(i_t)}$ 线性无关，故有 $\bigoplus_{l=1}^{t}(\boldsymbol{\varpi}_{i_l}\times(\boldsymbol{P}^{\mathrm{T}})^{-1}_{(i_l)})\oplus\bigoplus_{l=1}^{t}(\boldsymbol{e}_{i_l}\times\boldsymbol{E}_{(i_l)})\neq\boldsymbol{0}$.

即 $\boldsymbol{\varepsilon}\oplus\Lambda_F^{(1)}(\boldsymbol{\varepsilon})\oplus\Lambda_F^{(2)}(\boldsymbol{\varepsilon})\oplus\Lambda_F^{(3)}(\boldsymbol{\varepsilon})\oplus\Lambda_F^{(4)}(\boldsymbol{\varepsilon})\neq\boldsymbol{0}$，定理得证.

推论 3 设 GF(2^n) 上的可逆矩阵 $\boldsymbol{P}_{d\times d}$ 为嵌套 SP 网络的 New-Structure III 的扩散层，若 i,j 满足 $(\boldsymbol{P}^{\mathrm{T}})^{-1}_{(j)}=\boldsymbol{e}_{|i|}$，且 $(\boldsymbol{P}^{\mathrm{T}})^{-1}_{(i)}\neq k\boldsymbol{e}_{|i|}$，其中 k 为常数，则对任意的 $\boldsymbol{\beta}\in\mathrm{GF}(2^n)^d\setminus\{\boldsymbol{0}\}$，$(\boldsymbol{0},\boldsymbol{0},\boldsymbol{e}_{|j|},\boldsymbol{0})\nrightarrow(\boldsymbol{\beta},\boldsymbol{\beta},\boldsymbol{\beta},\boldsymbol{\beta})$ 均为 New-Structure III 结构的 22 轮零相关线性逼近.

这是由于 $(\boldsymbol{P}^{\mathrm{T}})^{-1}_{(i)}\neq k\boldsymbol{e}_{|i|}$，有 $(\boldsymbol{P}^{\mathrm{T}})^{-1}_{(i)}$ 与 $\boldsymbol{E}_{(i)}$ 线性无关，则推论 3 中的条件满足定理 7 给出的限制条件.

引理 8[18] 设 GF(2^n) 上的矩阵 $\boldsymbol{P}_{d\times d}$ 为 MDS 矩阵，则矩阵 $[\boldsymbol{P}|\boldsymbol{E}]$ 的任意 $r(r\leqslant d)$ 列均线性无关.

推论 4 设 GF(2^n) 上的可逆矩阵 $\boldsymbol{P}_{d\times d}$ 为嵌套 SP 网络的 New-Structure III 的扩散层，$\boldsymbol{P}_{d\times d}$ 为 MDS 矩阵，$(\boldsymbol{P}^{\mathrm{T}})^{-1}_{(j)}$ 中非零分量的个数小于 $\frac{d+1}{2}$，则对任意的 $\beta\in\mathrm{GF}(2^n)^d\setminus\{\boldsymbol{0}\}$，$(\boldsymbol{0},\boldsymbol{0},\boldsymbol{e}_{|j|},\boldsymbol{0})\nrightarrow(\boldsymbol{\beta},\boldsymbol{\beta},\boldsymbol{\beta},\boldsymbol{\beta})$ 均为嵌套 SP 网络的 New-Structure III 结构的 22 轮零相关线性逼近.

由引理 8 知若 $\boldsymbol{P}_{d\times d}$ 为 MDS 矩阵，则当 $t<\frac{d+1}{2}$ 时，$\boldsymbol{P}_{(i_1)},\boldsymbol{P}_{(i_2)},\cdots,\boldsymbol{P}_{(i_t)},\boldsymbol{E}_{(i_1)},\boldsymbol{E}_{(i_2)},\cdots,\boldsymbol{E}_{(i_t)}$ 必线性无关，故推论 4 中的条件满足定理 7 给出的限制条件. 推论 3 和推论 4 说明存在使得嵌套 SP 网络的 New-Structure III 有 22 轮零相关线性逼近的 P 盒.

引理 9 设 $a,b,c,d,a',b',c',d'\in F_{2^s}$，$(a,b,c,d)\rightarrow(a',b',c',d')$ 为 New-Structure III 圈函数 Q 的概率非零的差分特征，则有 $a'=d,b'=\beta,c'=b\oplus\beta,d'=c$，其 F 函数的差分特征为 $a\rightarrow b'$，且

$$p_Q((a,b,c,d)\rightarrow(a',b',c',d'))=p_F(a\rightarrow b').$$

证明 引理 9 的证明过程与引理 4 之 (I) 的证明过程类似，故在此不再展开证明.

根据引理 9 我们可得 New-Structure III 结构差分传递链的性质，如下所示.

性质 4 在 New-Structure III 中，若概率非零的差分传递链满足 $(\Delta\boldsymbol{X}_1^0,\Delta\boldsymbol{X}_2^0,\Delta\boldsymbol{X}_3^0,\Delta\boldsymbol{X}_4^0)=(\boldsymbol{0},\Delta\boldsymbol{x},\boldsymbol{0},\boldsymbol{0})$，则 $\Delta\boldsymbol{X}_2^9=\boldsymbol{0}$；若概率非零的差分传递链满足 $(\Delta\boldsymbol{X}_1^t,\Delta\boldsymbol{X}_2^t,\Delta\boldsymbol{X}_3^t,\Delta\boldsymbol{X}_4^t)=(\Delta z,\boldsymbol{0},\boldsymbol{0},\Delta z)$，则 $\Delta\boldsymbol{X}_2^{t-13}=\Delta_{F^{-1}}(\Delta z)\oplus(\bigoplus_{i=1}^{4}\Delta_{F^{-1}}^{(i)}(\Delta_{F^{-1}}(\Delta z)))$.

定理 8 给出了嵌套 SP 网络的 New-Structure III 的 22 轮不可能差分特征，该结果优于文献[17]给出的 19 轮不可能差分特征.

定理 8 设 GF(2^n) 上的可逆矩阵 $\boldsymbol{P}_{d\times d}$ 为嵌套 SP 网络的 New-Structure III 的扩散层，若 $\boldsymbol{P}^{-1}_{(j_1,j_1)}=\boldsymbol{0}$，则对任意的 $\Delta\boldsymbol{x}\in\mathrm{GF}(2^n)^d\setminus\{\boldsymbol{0}\}$，$(\boldsymbol{0},\Delta\boldsymbol{x},\boldsymbol{0},\boldsymbol{0})\nrightarrow(\boldsymbol{P}\times\boldsymbol{e}_{|j_1|},\boldsymbol{0},\boldsymbol{0},\boldsymbol{P}\times\boldsymbol{e}_{|j_1|})$ 均为嵌套 SP 网络的 New-Structure III 结构的 22 轮不可能差分特征.

证明 根据性质 4，我们只需证明 $\Delta_{F^{-1}}(\boldsymbol{P}\times\boldsymbol{e}_{|j_1|})\oplus(\bigoplus_{i=1}^{4}\Delta_{F^{-1}}^{(i)}(\Delta_{F^{-1}}(\boldsymbol{P}\times\boldsymbol{e}_{|j_1|})))\neq\boldsymbol{0}$. 由于 $\Delta_{F^{-1}}(\boldsymbol{P}\times\boldsymbol{e}_{|j_1|})=\Delta_{S^{-1}\circ\boldsymbol{P}^{-1}}(\boldsymbol{P}\times\boldsymbol{e}_{|j_1|})=\Delta_{S^{-1}}(\boldsymbol{P}^{-1}\times\boldsymbol{P}\times\boldsymbol{e}_{|j_1|})=\Delta_{S^{-1}}(\boldsymbol{e}_{|j_1|})=\boldsymbol{e}'_{|j_1|}$，不妨设 $\boldsymbol{e}'_{j_1}$ 中非零分量为 ξ，则有 $\Delta_{F^{-1}}(\boldsymbol{e}'_{|j_1|})=\Delta_{S^{-1}\circ\boldsymbol{P}^{-1}}(\boldsymbol{e}'_{|j_1|})=\Delta_{S^{-1}}(\xi\cdot\boldsymbol{P}^{-1}_{(j_1)})$.

由 $\boldsymbol{P}^{-1}_{(j_1,j_1)}=0$ 知 $\chi_{j_1}(\Delta_{F^{-1}}^{(i)}(\boldsymbol{e}'_{|j_1|}))=0,i\in\{1,2,3,4\}$. 结合 $\chi_{j_1}(\boldsymbol{e}'_{|j_1|})=1$ 知 $\chi_{j_1}(\boldsymbol{e}'_{|j_1|}\oplus(\bigoplus_{i=1}^{4}\Delta_{F^{-1}}^{(i)}(\boldsymbol{e}'_{|j_1|})))=1$，即 $\boldsymbol{e}'_{|j_1|}\oplus(\bigoplus_{i=1}^{4}\Delta_{F^{-1}}^{(i)}(\boldsymbol{e}'_{|j_1|}))\neq\boldsymbol{0}$，故 $\Delta_{F^{-1}}(\boldsymbol{P}\times\boldsymbol{e}'_{|j_1|})\oplus(\bigoplus_{i=1}^{4}\Delta_{F^{-1}}^{(i)}(\Delta_{F^{-1}}(\boldsymbol{P}\times\boldsymbol{e}'_{|j_1|})))\neq\boldsymbol{0}$，得出矛盾，定理得证.

3.4 嵌套 SP 网络的 New-Structure I ~ IV 结构的不可能差分特征和零相关线性逼近的应用

第 3.1 节至第 3.3 节研究了 New-Structure I ~ IV 的不可能差分特征和零相关线性逼近的最长轮数，本节将研究这些不可能差分特征和零相关线性逼近在具体攻击中的应用. 在以下分析中，我们假设采用嵌套 SP 网络的 New-Structure I ~ IV 结构的分组密码算法的明文输入规模和密钥规模均为 128 比特，S 盒为 8 进 8 出的非线性变换，P 盒为 4 × 4 的扩散层，即每轮有 32 比特密钥参与 F 函数运算，且 F 函数及其逆函数的每个输出比特都与输入的 32 比特相关.

依据现有攻击技术，基于第 3.1 节至第 3.3 节给出的 New-Structure I ~ IV 的不可能差分特征和零相关线性逼近，我们给出基于这些区分器能攻击到的最长轮数，攻击结果如表 2 所示. 此外，若一个算法采用 New-Structure II 结构，则该算法存在任意轮的不可能差分特征和零相关线性逼近，且任意轮的不可能差分特征和零相关线性逼近仅能被用来做区分攻击，而不能被用来做密钥恢复攻击.

表 2　本文嵌套 SP 网络的 New-Structure I、III、IV 不可能差分攻击/多维零相关攻击的最长轮数

算法采用的结构	区分器轮数/不可能差分攻击轮数/数据量/时间复杂度	区分器轮数/多维零相关攻击轮数/数据量/时间复杂度
New-Structure I	$16/21/2^{116}/2^{117.2}$	$16/19/2^{122.78}/2^{123.75}$
New-Structure III	$22/28/2^{116.5}/2^{115.05}$	$22/28/2^{118.78}/2^{115.7}$
New-Structure IV	$16/22/2^{116.5}/2^{115.4}$	$16/22/2^{122.8}/2^{108.08}$

4　结论

本文从不可能差分分析和零相关线性分析的角度对嵌套 SP 网络的 New-Structure 系列算法进行了分析,给出了它们目前最长的不可能差分特征和零相关线性逼近.本文在给出嵌套 SP 网络的 New-Structure I 和 New-Structure IV 的不可能差分特征和零相关线性逼近时,基于 New-Structure I 中概率非零的 n 轮差分传递链(相关优势非零的 n 轮线性逼近传递链)和 New-Structure IV 中相关优势非零的 n 轮线性逼近传递链(概率非零的 n 轮差分传递链)的结构之间的一致性,简化了证明过程.此外,本文给出了这些不可能差分特征和零相关线性逼近在不可能差分攻击和多维零相关线性攻击中的具体应用.本文的结果为基于嵌套 SP 网络的 New-Structure 系列结构设计的密码算法的不可能差分分析和零相关线性分析提供了理论依据.

致谢　非常感谢匿名评审专家的建议.

参考文献

[1] Knudsen L. DEAL-a 128-bit Block Cipher[R]. Bergen, Norway: Department of Informatics, University of Bergen,1998.

[2] Biham E, Biryukov A, Shamir A. Cryptanalysis of Skipjack reduced to 31 rounds using impossible differentials [A]. Jacques S. Advances in Cryptology— EUROCRYPT'1999 [C]. Prague, Czech Republic: Springer, 1999. 2 – 23.

[3] Biham E, Dunkelman O, Keller N. Related-Key impossible differential attacks on 8-round AES-192[A]. David P. Topics in Cryptology-CT-RSA'2006 [C]. San Jose, USA: Springer,2006. 21 – 33.

[4] Dunkelman O, Keller N. An improved impossible differential attack on MISTY1[A]. Josef P. Advances in Cryptology-—ASIACRYPT' 2008 [C]. Melbourne, Australia: Springer,2008. 441 – 454.

[5] 魏悦川,孙兵,李超. FOX 密码的不可能差分分析[J]. 通信学报,2010,31(9):24 – 29.
Wei Yue-chuan, Sun Bing, Li Chao. Impossible differential attacks on FOX[J]. Journal on Communications,2010,31(9):24 – 29. (in Chinese)

[6] Li X R, Fu F W, Guang X. Multiple impossible differential cryptanalysis on reduced FOX[J]. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences,2015, E98 – A(3):906 – 911.

[7] Boura C, Plasencia M N, Suder V. Scrutinizing and improving impossible differential attacks: applications to CLEFIA, Camellia, LBlock and Simon[A]. Palash S. Advances in Cryptology— ASIACRYPT'2014[C]. Taiwan, China: Springer,2014. 179 – 199.

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

[9] Bogdanov A, Wang M. Zero correlation linear cryptanalysis with reduced data complexity[A]. Bruce S. Advances in Cryptology— FSE'2012 [C]. Washington, DC, USA: Springer,2012. 29 – 48.

[10] Bogdanov A, Leander G, Nyberg K. Integral and multidimensional linear distinguishers with correlation zero [A]. Wang X Y. Advances in Cryptology—ASIACRYPT'2012 [C]. Beijing, China: Springer, 2012. 244 – 261.

[11] Bogdanov A, Boura C, Rijmen V. Key difference invariant bias in block ciphers[A]. Kazue S. Advances in Cryptology—ASIACRYPT'2013[C]. Bangalore, India: Springer, 2013. 357 – 376.

[12] Wen L, Wang M, Bogdanov A. Multidimensional zero-correlation linear cryptanalysis of E2[A]. Pointcheval. Advances in Cryptology—AFRICACRYPT '2014[C]. Marrakesh, Morocco: Springer,2014. 147 – 164.

[13] Bogdanov A, Geng H, Wang M. Zero-correlation linear cryptanalysis with FFT and improved attacks on ISO standards Camellia and CLEFIA[A]. Tanja L. Selected Areas in Cryptography—SAC'2013[C]. Burnaby, Canada: Springer,2013. 306 – 323.

[14] Wen L, Wang M Q, Bogdanov A. Multidimensional zero-correlation attacks on lightweight block cipher HIGHT: improved cryptanalysis of an ISO standard [J]. Information Processing Letters, 2014, 114(6): 322 – 330.

[15] Blondeau C, Nyberg K. New links between differential and linear cryptanalysis[A]. Thomas J. Advances in Cryptology—EUROCRYPT'2013 [C]. Athens: Springer, 2013.

388 – 404.

[16] Blondeau C, Bogdanov A, Wang M. On the (in) equivalence of impossible differential and zero-correlation distinguishers for Feistel-and Skipjack-type ciphers[A]. Yoko K, Applied Cryptography and Network Security—ACNS′2014[C]. Lausanne, Switzerland: Springer, 2014. 271 – 288.

[17] Wu S B, Wang M S. Security Evaluation Against Differential Cryptanalysis for Block Cipher Structures[EB/OL]. http://eprint. iacr. org/2011/551, 2011.

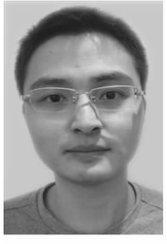
[18] Cui T, Jin C H. Impossible differential evaluations for New-Structure series[J]. Chinese Journal of Electronics, 2014, 23(2): 357 – 360.

[19] Wei Y C, Li P, Sun B, Li C. Impossible differential cryptanalysis on Feistel ciphers with SP and SPS round functions[A]. Jafri M A, Applied Cryptography and Network Security—ACNS′10[C]. Beijing, China: Springer, 2010. 105 – 122.

[20] 张庆贵. 不可能差分攻击中的明文对筛选方法[J]. 计算机工程, 2010, 36(2): 127 – 129.
Zhang Qing-gui. Plaintext pair sieve methods in impossible differential attack[J]. Computer Engineering, 2010, 36(2): 127 – 129. (in Chinese)

作者简介

付立仕 女, 1989 年生于河南南阳. 现为解放军信息工程大学密码工程学院博士研究生. 主要研究方向为分组密码的设计与分析. E-mail: 15036018167@163.com



崔 霆 男, 1985 年生于安徽铜陵. 现为解放军信息工程大学讲师. 主要研究方向为分组密码.
E-mail: cuiting_1209@126.com

金晨辉 男, 1965 年生于河南周口. 现为解放军信息工程大学教授、博士生导师. 主要研究方向为密码学.
E-mail: jinchenhui@126.com